Alexander Roßnagel, Mark Bedner, Michael Knopp

Rechtliche Anforderungen an die Aufbewahrung von Vorratsdaten

Die Aufbewahrung von Vorratsdaten ist in § 113a Abs. 10 TKG nur sehr kursorisch geregelt. Die dort genannten Anforderungen genügen nach Überzeugung der Autoren nicht der Schutzpflicht des Staates für die informationelle Selbstbestimmung der Betroffenen. Um die Verhältnismäßigkeit der Umsetzungsregelungen zur Vorratsspeicherung zu gewährleisten, seien die in § 113a Abs. 10 TKG genannten abstrakten Anforderungen an die Aufbewahrung der Daten entweder verfassungskonform so zu interpretieren, dass sie dem gebotenen Schutz entsprechen, oder vom Gesetzgeber in einer Überarbeitung des Wortlauts in diesem Sinn zu konkretisieren. Der Beitrag untersucht die verfassungsrechtlich gebotenen Schutzmaßnahmen im Einzelnen.

Prof. Dr. Alexander Roßnagel

Vizepräsident der Universität Kassel, Univ.-Prof. für Öffentliches Recht, Leiter der „Projektgruppe verfassungsverträgliche Technikgestaltung (provet)" und Wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR), Saarbrücken
E-Mail: a.rossnagel@uni-kassel.de

Mark Bedner, LL.M.

Ass. iur., Mitarbeiter in der „Projektgruppe verfassungsrechtliche Technikgestaltung (provet)" und Stipendiat des CASED (Center for Advanced Security Research Darmstadt).
E-Mail: markbedner@uni-kassel.de

Michael Knopp

Ass. iur., Wissenschaftlicher Mitarbeiter der „Projektgruppe verfassungsrechtliche Technikgestaltung (provet)". Projektbearbeitungen zuletzt „Bürgerportale" und „Prozessketten zwischen Wirtschaft und Verwaltung" (BMI).
E-Mail: michaelknopp@uni-kassel.de

1 Prüfrahmen

Die konkrete rechtsstaatlich gebotene Ausgestaltung der Vorratsdatenspeicherung regelt die Richtlinie zur Vorratsdatenspeicherung nicht,[1] sondern überlässt es dem Mitgliedstaat, die jeweils verfassungsrechtlich gebotenen Maßnahmen vorzuschreiben. Jenseits der Frage der Aufbewahrung bleibt außerdem den Mitgliedstaaten die Aufgabe, den allgemeinen Rechtsrahmen der Vorratsdatenspeicherung zu gestalten, also Regelungen zu Fehlerfolgen, zum Abrufverfahren, zur Ausgestaltung der rechtlichen Stellung der Betroffenen und der Verpflichteten sowie zur Gewährleistung der erforderlichen Kontrolle zu treffen.

Nach seiner „Solange"-Rechtsprechung[2] wird das Bundesverfassungsgericht seine Gerichtsbarkeit über die Anwendbarkeit von abgeleitetem Gemeinschaftsrecht nicht mehr ausüben, solange die Europäischen Gemeinschaften und insbesondere die Rechtsprechung des Europäischen Gerichtshofs einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften generell gewährleisten. Dieser muss dem vom Grundgesetz als unabdingbar gebotenen Grundrechtsschutz im Wesentlichen entsprechen.

Da es keine Anhaltspunkte gibt, die daran grundsätzlich zweifeln lassen, prüft das Bundesverfassungsgericht nicht die Verfassungsmäßigkeit der Vorratsdatenspeicherung[3], soweit sie von der Richtlinie festgelegt ist, sondern überlässt dies dem Europäischen Gerichtshof.[4] Angesichts des Konfliktpotentials einer grundsätzlichen Infragestellung des Grundrechtsschutzes durch den Europäischen Gerichtshof ist eine Fortsetzung der „Solange"-Rechtsprechung auch in diesem Fall wahrscheinlich, zumal eine Entscheidung des Europäischen Gerichtshofs über die materielle Rechtmäßigkeit der Richtlinie nach einer Vorlage des Verwaltungsgerichts Wiesbaden noch aussteht.[5]

In seine Kontrollkompetenz fällt jedoch die Überprüfung, ob der Gesetzgeber den mitgliedstaatlichen Spielraum den Vorgaben des Grundgesetzes gemäß ausgestaltet hat. Das Gericht hat daher auch zu prüfen, ob die gespeicherten Vorratsdaten ihrem Risiko für die informationelle Selbstbestimmung entsprechend geschützt werden.

2 Anforderungen nach § 113 TKG

Nach § 113a Abs. 10 Satz 1 TKG hat der zur Aufbewahrung Verpflichtete „betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten". Die „im Bereich der Telekommunikation erforderliche Sorgfalt"

1 Art. 7 der Richtlinie zur Vorratsspeicherung enthält lediglich allgemeine Vorgaben zu Datenschutz und Datensicherheit.

2 *BVerfGE* 73, 339.

3 Siehe *Dix/Petri* in diesem Heft.

4 S. hierzu auch *Leutheuser-Schnarrenberger,* ZRP 2007, 9.

5 *VG Wiesbaden*, K&R 2009, 354 mit Anm. Schnabel.

ist in der Gesetzesbegründung und in der Literatur nur unzureichend konkretisiert. So wird in der Gesetzesbegründung lediglich ausgeführt, dass „der Verpflichtete die zu speichernden Verkehrsdaten mit der Sorgfalt zu behandeln hat, die beim Umgang mit vom Fernmeldegeheimnis geschützten Daten erforderlich ist“.[6] Folgt man der Literatur, so bedeutet dies eine Bekräftigung des einfachgesetzlichen Schutzes des Fernmeldegeheimnisses aus § 88 TKG. Außerdem wird auf die – bezüglich des erforderlichen Sicherheitsniveaus ebenfalls sehr allgemein gehaltenen – Vorschriften des § 109 TKG und § 9 BDSG mit Anlage verwiesen.[7]

Zur Begrenzung des Datenzugangs fordert § 113a Abs. 10 Satz 2 TKG technische und organisatorische Maßnahmen der verpflichteten TK-Anbieter, die gewährleisten sollen, dass ausschließlich berechtigtes Personal Zugriff auf die Daten erlangt. Die Vorschrift ist mit der Regelung in § 9 BDSG vergleichbar. Dort wird ebenfalls von „technischen und organisatorischen Maßnahmen“ gesprochen, darüber hinausgehend aber auf die Anlage verwiesen, die vergleichsweise konkrete Maßnahmen zur praktischen Umsetzung enthält.

Aus § 5 BDSG und § 88 Abs. 2 und 3 TKG folgen weitere Vorgaben zur Wahrung des Daten- und Telekommunikationsgeheimnisses, darunter die Pflicht, die Mitarbeiter auf das Datengeheimnis zu verpflichten. Angesichts der anderweitigen und teilweise viel konkreteren Regelungen des gleichen Sachverhalts wird sogar vorgebracht, die Regelungen in § 113a Abs. 10 TKG seien nicht notwendig gewesen.[8]

Schließlich fordert § 113 Abs. 11 TKG, die Daten innerhalb eines Monats nach Ablauf der sechsmonatigen Aufbewahrungsfrist zu löschen. Mit dieser kurzen Regelung bleiben auch bezüglich der Löschung wesentliche Fragen ungeregelt.

3 Risikoadäquater Schutz

Die Vorratsdatenspeicherung verursacht aufgrund des Datenumfangs, der Bestimmung zur Überwachung, der abrufgerechten Sammlung und dem Erfordernis einer schnellen Abrufbarkeit besondere Risiken für die Grundrechtsträger.[9] Aus den Daten lassen sich Profile des Kommunikations- und Bewegungsverhaltens erstellen, Personenbeziehungen nachvollziehen und aus den Kontakten mit Menschen und Institutionen Rückschlüsse auf die Person des Betroffenen ziehen.[10] Diese Erkenntnisse sind für viele Personengruppen von Interesse und können in den falschen Händen mit großer Schadenswirkung für den Betroffenen missbraucht werden. Das erklärte Ziel der schnellen und gezielten

6 BT-Drs. 16/5846, 72.

7 Sehr kurz *Scheurle/Mayen*, TKG, 2. Aufl. 2008, § 113a Rn. 31; lediglich unter Verweis auf die EU-Richtlinie *Heun*, Handbuch Telekommunikationsrecht, 2. Aufl. 2007, Teil 1 B, Rn. 181; unter Anlehnung an die Gesetzesbegründung *Graulich* in Arndt/Fetzer/Scherer, TKG, 2008, § 113a Rn. 37.

8 *Graulich* (Fn. 7), Rn. 37.

9 S. hierzu auch den Beitrag von *Pfitzmann* und *Köpsell* in diesem Heft.

10 Die Auswertungsmöglichkeiten werden ausführlich in der Stellungnahme des Chaos Computer Clubs für das BVerfG erläutert, s. unter http://www.ccc.de/vds/ VDSfinal18.pdf, S. 5 ff.; s. auch *Hensel*, in diesem Heft.

Abrufbarkeit verursacht zusätzlich hohe Risiken für missbräuchliche Nutzungen.

Die bestehenden Regelungen zum Schutz der Grundrechte der von dem Eingriff der Vorratsdatenspeicherung Betroffenen sind nach der gängigen Auslegung vollkommen unzureichend, die Risiken durch den Eingriff in einer verhältnismäßigen Weise zu begrenzen. Der Verweis auf die „im Bereich der Telekommunikation erforderliche Sorgfalt" ist inhaltsleer. Sollte damit der ohnehin von TK-Anbietern für TK-Daten realisierte Schutz gemeint sein – darauf deuten die amtliche Begründung und die Kommentarliteratur hin –, wird dies den gesteigerten Risiken durch die Vorratsdatenspeicherung nicht gerecht. Für die besondere Gefährdung der Grundrechtsträger reichen die Maßnahmen, die bislang für den Bereich der Telekommunikation ausreichend waren, nicht aus.

4 Erforderliche Schutzmaßnahmen

Zur Sicherung der Verhältnismäßigkeit des Grundrechtseingriffs durch die Vorratsdatenspeicherung sind Ergänzungen speziell zur Sicherung der Vorratsdaten erforderlich, die über das bisherige Verständnis des in § 113a Abs. 10 TKG bestimmten Schutzes, vor allem die Zugangsbeschränkung auf besonders ermächtigte Mitarbeiter, hinausgehen. Diese sind entweder als verfassungskonforme Anforderungen der „im Bereich der Telekommunikation erforderlichen Sorgfalt" anzusehen oder für eine verfassungsgemäße Neufassung des §§ 113a TKG zu fordern

4.1 Datenspeicherung

Bei der Speicherung der Daten ist es erforderlich, durch Fehlererkennungs- und Fehlerkorrekturverfahren die Wahrscheinlichkeit der Speicherung von Falschinformationen zu vermindern. Plausibilitäts- und Verifikationsverfahren müssen sowohl während der Speicherung als auch danach regelmäßig und automatisiert prüfen, ob die gespeicherten Daten plausibel sind. So ist beispielsweise zu prüfen, ob Uhrzeiten stimmen können, ob Kennungen überhaupt vergeben worden sein können (fortlaufende Kundennummern) oder die gespeicherte IP-Adresse zur zugewiesenen IP-Range gehört.

Zur Begrenzung der Eingriffe durch den Datenabruf ist zu fordern, dass die Daten so sortiert und abgerufen werden können, dass der Abruf stets auf das Erforderliche und Angeordnete begrenzt werden kann. So ist beispielsweise zur Verfolgung eines bestimmten Kontaktmusters das Erheben der im Bereich des Mobilfunks gespeicherten Standortdaten nicht erforderlich. Ebenso kann sich die Ermittlung auf bestimmte Zeitpunkte oder auf Zeiträume beschränken, die kürzer als die vorgehaltenen sechs Monate sind. Auch müssen bei der Überprüfung der Telefondienstenutzung nicht unbedingt auch die weiteren über die Telefonverbindung genutzten Dienste von Interesse sein. In diesen Fällen muss die Trennung der nicht benötigten Daten oder die Aussonderung der benötigten Daten durch den Anbieter möglich sein.

Zur Gewährleistung der Qualität der Daten gehört damit auch das Vorhalten entsprechender Filterungsmechanismen. Die Filterung hat durch den Anbieter zu erfolgen, so dass die berechtigten Stellen Daten, die von ihrer konkreten Berechtigung nicht umfasst sind, gar nicht erst erhalten. Den anordnenden Gerichten gibt dies die Möglichkeit, die Erforderlichkeit genauer zu prüfen und den Umfang von Zugriffsermächtigungen genauer zu begrenzen.[11]

Der Verpflichtete muss außerdem sicherstellen, dass er nur Hard- und Software einsetzt, die gewährleistet, dass nur die vom Gesetz geforderten und zugelassenen Daten gespeichert werden. Insbesondere ist auszuschließen, dass Inhaltsdaten gespeichert werden. Damit der Verpflichtete diese Anforderung erfüllen kann, müssen die Hersteller ihre Erfassungs- und Speichersysteme hinsichtlich dieser Anforderungen zertifizieren lassen.

4.2 Datenaufbewahrung

Die Aufbewahrung der Daten ist sowohl für den zur Speicherung Verpflichteten als auch für die zum Abruf berechtigten Stellen zu betrachten. Grundsätzlich sind zur Erkennung von durchgeführten Datenveränderungen kryptographisch sichere Hashfunktionen einzusetzen.[12] So können in regelmäßigen Zeitabständen über vordefinierte Teile der Datensätze, beispielsweise einzelne Dateien der Datenbank, Hashwerte gebildet und diese ebenso regelmäßig nach einer gewissen Zeit oder bei Abrufen auf mögliche Manipulation überprüft werden. Angesichts der sich ständig durch Löschung und neu hinzukommende Daten verändernden Datenbestände wird dies jedoch technisch keine triviale Aufgabe sein.

Zur Datenaufbewahrung gehören auch eine Datensicherung mittels Backups und eine entsprechende Sicherungsstrategie. Diese Backupdaten sind genauso zu sichern wie die ursprünglichen Vorratsdaten.

Funktionale Trennung

Wichtig für die Risikoverringerung ist die Trennung der Daten, um für den jeweils Betroffenen keine zentrale Sammlung entstehen zu lassen. Optimal wäre eine sogar physische Trennung der Datenspeicher sowie der Abrufmöglichkeiten. Als erstes sind nach §§ 111 f. TKG vorzuhaltende Bestandsdaten und gespeicherte Verkehrsdaten zu trennen. Vor allem aber ist die Speicherung der in § 113a TKG genannten Daten getrennt von allen anderen Daten vorzunehmen. Auch Verkehrsdaten, die nach § 96 Abs. 1 TKG erhoben werden, sind von Anfang an getrennt zu speichern, selbst wenn sie sich inhaltlich mit den nach § 113a TKG gespeicherten Daten überschneiden und somit eine doppelte Speicherung erforderlich wird. Nur so kann der Kreis der Zugriffsberechtigten hinsichtlich der nach § 113a TKG gespeicherten Daten eng begrenzt gehalten werden. Sollte eine Kompromittierung der Datenspeicher stattfinden, wird der Schaden durch die Trennung der Daten begrenzt. Durch diese Trennung können außerdem unterschiedliche Löschkonzepte mit unterschiedlichen Löschfristen realisiert werden.

Trennung nach Dienst- oder Kommunikationsarten

Da viele Diensteanbieter heute nicht mehr nur eine der in § 113a Abs. 1-6 TKG erfassten Dienstearten anbieten, könnten bei diesen Datensammlungen entstehen, in denen Daten zu verschiedenen Kommunikationsarten einer Person enthalten wären. Um die Risiken für die einzelnen Betroffenen zu senken und eine Profilbildung durch Unberechtigte zu erschweren, sind die Daten auch bei solchen Anbietern nach Dienst- oder Kommunikationsarten getrennt zu halten oder gesondert zu verschlüsseln. Sollten die Sicherungsmaßnahmen unbefugt überwunden werden,

11 S. 5.1.

12 *Eckert*, IT-Sicherheit, 4. Aufl. 2006, 8.

würde diese Trennung verhindern, dass das gesamte Telekommunikationsverhalten der Betroffenen über den gespeicherten Zeitraum eingesehen werden kann. Die Trennung ermöglicht auch ein weiteres Aufteilen der Zugriffsermächtigungen. Auch diesbezüglich kann so die Missbrauchsgefahr weiter begrenzt werden.

Trennung nach anschluss- und dienstbezogenen Daten

In der Literatur wird außerdem vorgeschlagen, die Daten verteilt und unter Obhut verschiedener öffentlicher Einrichtungen zu speichern. Der Vorschlag sieht vor, zwei Datenbanken zu nutzen, nämlich eine für dienstbezogene und eine zweite für anschlussbezogene Verkehrsdaten. Manche der Daten geben ausschließlich Auskunft über den Kommunikationsdienst und die näheren Umstände seiner Inanspruchnahme (dienstbezogene Daten). Andere lassen darüber hinaus Rückschlüsse auf den Anschluss zu (anschlussbezogene Daten). Als Beispiel wird ein herkömmliches Telefonat mit den nach § 113a TKG anfallenden Daten genannt. Die beteiligten Rufnummern (§ 113a Abs. 2 Nr. 1 TKG) sind anschlussbezogene Daten, während der aufgezeichnete Beginn und das Ende des Telefonats (§ 113a Abs. 2 Nr. 1 TKG) dienstbezogene Daten darstellen. Hinsichtlich der anfallenden anschlussbezogenen Daten soll auch eine Trennung nach einzelnen Anschlüssen erfolgen.[13]

Ein Angreifer, der eine Datenbank mit dienstbezogenen Daten kontrolliert, kann herausfinden, dass und wann telefoniert wurde, aber nicht wer an dem Gespräch beteiligt war. Wer die anschlussbezogene Datei kontrolliert, kann wegen der Trennung nur die Beteiligung einer Rufnummer erkennen, jedoch nicht, wer Gesprächspartner war und wann das Telefonat geführt wurde. Nur über Referenznummern und unter Beteiligung beider Stellen kann der komplette Datensatz rekonstruiert werden. Die Vorgehensweise stellt eine Anwendung des Mehr-Augen-Prinzips auf institutioneller Ebene dar.[14]

Kennzeichnung der Daten

Bereits nach § 101 Abs. 3 StPO wird die Kennzeichnung der nach § 100g Abs. 1 StPO erhobenen Daten gefordert. Dies umfasst jedoch lediglich die Kennzeichnung der Daten als Ergebnisse einer verdeckten Ermittlungsmaßnahme. Die Herkunft der Daten wird so erkennbar gemacht.[15] Die Kennzeichnung stellt jedoch kein technisches Hindernis einer Weitergabe dar, indem sie untrennbar mit den Daten verbunden wäre und auch nach der unbefugten Weitergabe ihre Herkunft erkennbar machen würde. Eine solche untrennbare Kennzeichnung wäre zwar wünschenswert,[16] ist aber technisch derzeit nicht machbar.[17]

Dennoch ist in Erwägung zu ziehen, zumindest zur Warnung eine Kennzeichnung der Verkehrsdaten bereits durch den Anbieter vor der Übermittlung vornehmen zu lassen. Auch wenn diese entfernt werden kann, werden die Daten auf diese Weise bereits von Anfang an so gekennzeichnet, dass ihr Ursprung für alle Beteiligten deutlich wird. Auch sollte die Kennzeichnung über die Quellenangabe hinaus die ersuchende Stelle, die verantwortliche Person, einen Verweis auf die richterliche Anordnung und den Zeitpunkt der Übermittlung enthalten.

Verschlüsselung

Als weitere Schutzmaßnahme, die für alle Stationen der nach § 113a TKG erfassten Daten erforderlich ist, sind die Daten lückenlos zu verschlüsseln. Weder beim Anbieter und Aufzeichnungsverpflichteten noch bei der Übermittlung oder anschließend bei der ersuchenden Stelle dürfen die Daten unverschlüsselt zugänglich sein.[18]

Die Verkehrsdaten sind mittels sicherer Algorithmen zu verschlüsseln. Die verwendete Soft- und Hardware sollte durch das BSI oder Datenschutzbeauftragte zertifiziert werden und einer regelmäßigen Überprüfung auf Sicherheit durch diese unterliegen. Wird vor einer solchen Überprüfung eine Sicherheitslücke in den Algorithmen oder der Technik festgestellt, sind Maßnahmen verpflichtend vorzusehen, um die Sicherheit der Daten wieder herzustellen. Einzelheiten zu den Algorithmen, der verwendeten Hard- und Software und den zu treffenden Maßnahmen sollten durch die Bundesnetzagentur in (technischen) Richtlinien, durch den Bundesinnenminister in einer Verordnung oder sogar durch den Gesetzgeber in einer Anlage zu § 113a TKG festgelegt werden.

4.3 Löschung

Die Regelung zur Löschung in § 113a Abs. 11 TKG lässt wesentliche Fragen offen und ermöglicht eine unnötige Verlängerung der Speicherungsdauer.

Zu fordern ist eine Konkretisierung des Wortlauts der Vorschrift dahingehend, dass die Löschung der Daten so erfolgen muss, dass sie nicht mehr wiederhergestellt werden können. Dazu reicht es nicht aus, lediglich die Verweise zu den Dateien im Dateiverzeichnis zu löschen. Sie sind vielmehr mindestens einmal, besser mehrfach, mit Zufallsdaten zu überschreiben.[19]

Die erfolgreiche Löschung sollte regelmäßig stichprobenartig überprüft werden. Hierzu könnten auch interne oder externe Datenschutzbeauftragte eingesetzt werden. Die Überwachung der Löschung sollte klar geregelt werden. Das Gleiche gilt für die Löschung der Daten bei der ersuchenden Stelle. Auch § 101 Abs. 8 Satz 1 StPO enthält keine weiteren Vorgaben für die Löschung.

Von der Löschung sind Protokolle über erfolgte Zugriffe und die Dokumentation der Datenaufbewahrung auszunehmen, da auch nach der Löschung zur Wahrung der Rechtsschutz- und Aufsichtsmöglichkeiten die Zugriffe, Datenabrufe und weitere relevante Vorgänge nachvollziehbar bleiben müssen.

4.4 Datenabruf

Der Abruf der korrekt gespeicherten Daten darf keinen anderen Sinngehalt durch die Verarbeitung zwecks Ausgabe (Bildschirm, Ausdruck) zulassen. Dies könnte etwa durch die verkürzte und hierdurch falsche Wiedergabe von Nummern oder Uhrzeiten geschehen.[20]

Neben der Qualitätssicherung des Abrufs ist auch die Sicherheit des Abrufs durch entsprechende verbindliche Vorgaben zu gewährleisten. Hierzu gehören ein hohes Authentifizierungsniveau und die Transportverschlüsselung der Datensätze.

13 *Ziebarth*, DuD 2009, 29.

14 *Ziebarth*, DuD 2009, 29.

15 BeckOK (*Hegmann*), 2009, § 101 Rn. 7 f.

16 *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts. Gutachten für das Bundesministerium des Innern, 2001, 127 f.

17 *Böhme/Pfitzmann*, DuD 2008, 346.

18 S. hierzu auch *Pfitzmann/Köpsell*, in diesem Heft.

19 Zum sicheren Löschen siehe auch *Fox*, DuD 2/2009, S. 110 ff.

20 So kam es im Rahmen der „Filesharing-überwachung" vereinzelt zu Zahlendrehern bei der IP-Adresse, so dass letztlich Ermittlungsverfahren und Abmahnung völlig Unschuldige trafen; http://www.heise.de/newsticker/Falscher-Anschluss-unter-dieser-IP-Nummer--/meldung/97304.

4.5 Beschränkung des Personenkreises

Die Zahl der an der Datenverarbeitung beteiligten Mitarbeiter der verpflichteten Unternehmen ist auf ein Minimum zu beschränken. Neben dieser quantitativen Begrenzung des betrauten Personenkreises, sollte auch eine gesonderte Auswahl der zur Datenverarbeitung Berechtigten anhand von Zuverlässigkeitskriterien erfolgen. Ausgewählte und betraute Mitarbeiter sind sorgfältig einzuweisen, regelmäßig zu schulen und auf das Datengeheimnis gemäß § 5 BDSG zu verpflichten.

Der Datenzugriff sollte nur mittels Chipkarte oder Passwort erfolgen und so ausgestaltet werden, dass nur bei gleichzeitiger Autorisierung durch mindestens zwei Berechtigte samt jeweiliger Chipkarte eine Entschlüsselung der Daten erfolgen kann. Werden Passwörter verwendet, so darf die Freigabe der Daten nur durch Eingabe mindestens zweier, jeweils einem Mitarbeiter zugewiesener Passwörter möglich sein. Ein dritter oder sogar vierter Mitarbeiter sollte ebenfalls über ein eigenes Passwort oder eine Chipkarte verfügen, so dass eine Art Stellvertreterregelung greift, falls berechtigte Mitarbeiter abwesend sind. Aus dem „Pool" der drei bis vier Mitarbeiter sollte jede Kombination zweier Mitarbeiter eine Freigabe der Daten ermöglichen. Auf diese Weise wird das Mehr-Augen-Prinzip technisch verbindlich.

4.6 Dokumentation

Vor allem zur Durchführung einer effektiven Aufsicht und Kontrolle sowie zur Wahrung der Rechtsschutzmöglichkeiten der Betroffenen ist eine unveränderbare, beweissichere und lückenlose Dokumentation des Umgangs mit den nach § 113a TKG gespeicherten Daten erforderlich. Dies betrifft zuerst die verpflichteten Stellen. Diese haben jeglichen Datenzugriff, dessen Zweck, die verantwortliche Person, zugrunde liegende Anordnungen, den Zeitpunkt, den genauen Datenumfang und den Empfänger festzuhalten. Die Aufbewahrungsfrist dieser Dokumentation ist gesondert festzulegen und darf nicht enden, bevor nicht die Benachrichtigung des Betroffenen sichergestellt und eine ausreichende darauf folgende Zeitspanne abgelaufen ist.

Die Dokumentation darf jedoch hier nicht enden, da den ersuchenden Behörden unter bestimmten Voraussetzungen die Weitergabe an weitere Stellen erlaubt ist. Außerdem sollten auch innerhalb der ersuchenden Stellen die Einsichtnahmen nachvollziehbar sein, um eine nachträgliche Kontrolle zu ermöglichen. Eine technische Möglichkeit zur Realisierung der beweissicheren Zugriffsdokumentation ist der Einsatz von Chipkarten mit hohem Sicherheitsstandard, die außerdem eine eigene, manipulationssichere Datums- und Zeitfunktion enthalten sollten.

5 Notwendige Rahmenregelungen

Die Umsetzung technischer Sicherungen, die die erforderliche Sorgfalt verfassungskonform konkretisieren, reicht jedoch nicht aus, um die Vorratsdatenspeicherung verfassungsgemäß zu gestalten.

Die derzeit vorgesehene Vorgabe von Sicherheitsmaßnahmen in Technischen Richtlinien, die ohne Beteiligung des Gesetzgebers geändert und gelockert werden können, kann den verfassungsrechtlichen Schutzauftrag nicht ausreichend erfüllen. Bereits auf Gesetzesebene müssen die Mindestanforderungen an die technisch-organisatorische Sicherheit verbindlich gemacht werden. Dies betrifft vor allem die Trennung der Daten, die erforderliche Zugangsauthentifizierung, die technische Sicherung durch Verschlüsselung der Daten und die Zugriffsdokumentation.

Abgesehen von der Kennzeichnungs- und Löschungspflicht in § 101 StPO ist ungeregelt, wie die einmal an die Behörden übermittelten Daten gehandhabt werden sollen und geschützt werden müssen. Die Kennzeichnung der Daten kann zwar in den Akten und auch an den Daten vorgenommen werden. Es besteht jedoch bislang keine Möglichkeit, die Daten so zu kennzeichnen, dass die Kennzeichnung nicht oder nur mit unverhältnismäßigem Aufwand von den Daten getrennt werden könnte.[21] Die Kennzeichnung bietet damit keinen Schutz vor einer unbefugten Weitergabe.[22] Um die diesbezügliche Schutzpflicht zu erfüllen, sind auch für die abrufenden Stellen besondere Vorgaben zur sicheren Aufbewahrung und zum Zugriffsschutz verbindlich festzulegen.

Neben den oben geschilderten technischen und organisatorischen Maßnahmen sind zudem die folgenden rechtlichen Sicherungsmaßnahmen erforderlich.

5.1 Richtervorbehalt

Der Richtervorbehalt für die Herausgabe der nach § 113a TKG gespeicherten Daten ist in § 100g Abs. 2 StPO durch Verweis auf §§ 100a Abs. 3, 100b Abs. 1-4 StPO bereits geregelt. Ob er angesichts einer Vielzahl von Fällen, entsprechendem Zeitdruck und Personalmangel eine ausreichende Sicherung gewährleistet, ist eine empirische Frage, der hier nicht nachgegangen werden kann.[23] Wird die Anforderung der Sortierbarkeit und Trennbarkeit der Daten erfüllt,[24] besteht für die Gerichte jedoch nicht nur die Möglichkeit, die Voraussetzungen der Auskunftsnorm grundsätzlich zu prüfen, sondern auch diese Voraussetzungen und die Erforderlichkeit für die einzelnen angeforderten Datenarten zu prüfen, so dass der Gestaltungsspielraum wächst.

In Anlehnung an die Einrichtung von Schwerpunktstaatsanwaltschaften mit besonders befähigten Staatsanwälten, beispielsweise gerade im TK- und IT-Bereich sollten besonders ausgebildete Richter für diese Bereiche vorgesehen werden.

5.2 Benachrichtigungspflicht

Die Benachrichtigungspflichten treffen derzeit die ersuchenden Stellen. Für die Staatsanwaltschaft ist § 101 Abs. 4 Nr. 6 StPO maßgeblich. Die Regelung in § 101 Abs. 4 Satz 2 StPO, nach der die Benachrichtigung Betroffener, gegen die die Ermittlungsmaßnahme nicht gerichtet war, bei vermeintlicher Unerheblichkeit unterbleiben kann, ist zu weit. Ob ein Interesse an der Benachrichtigung besteht und ob der Eingriff unerheblich ist, kann und sollte nicht die Ermittlungsbehörde entscheiden. Ebenso ist die Möglichkeit, wenn auch nur mit gerichtlicher Entscheidung, ganz auf die Benachrichtigung zu verzichten, wenn die Voraussetzungen der Benachrichtigung auch in Zukunft mit an Sicherheit grenzender Wahrscheinlichkeit nicht eintreten werden (§ 101 Abs. 6 Satz 2 StPO), eine ungerechtfertigte Beschneidung der Rechtsschutzmöglichkeiten des Betroffenen.

21 *Böhme/Pfitzmann*, DuD 2008, 342.

22 S. oben 4.2.

23 Kritisch hierzu *Albrecht/Grafe/Kilching*, Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO, 2008, S. 410.

24 S. oben 4.2.

Die Rechtsschutzgarantie für den Betroffenen stellt die effektivste Kontrolle des Umgangs mit den nach § 113a TKG gespeicherten Daten dar. Voraussetzung ist jedoch das Wissen der Betroffenen um die Ermittlungsmaßnahme. Diesen ist zwar bekannt, dass ihre Daten gespeichert werden, jedoch nicht, ob tatsächlich ein Abruf erfolgt. Einschränkungen dieser Benachrichtigung sind daher äußerst restriktiv zu handhaben und dürfen nicht gänzlich unterbleiben.

Der erforderliche Aufwand einer Benachrichtigung ist ebenfalls kein Argument, diese zu unterlassen. Denkbar ist, dass die Staatsanwaltschaften automatisiert nach Abschluss des Ermittlungsverfahrens eine Mitteilung samt Aktenzeichen an die Dienstanbieter der überwachten Anschlüsse versenden und diese die Kunden in der nächsten Rechnung oder gesondert auf die Datenübermittlung an die Behörden samt Aktenzeichen hinweisen.

In Anlehnung an die „Doktrin der Früchte des vergifteten Baumes" sollten rechtswidrige Ermittlungs- und Überwachungsmaßnahmen ein ausnahmsloses Beweisverwertungsverbot nach sich ziehen. Nur mit Konsequenzen belegte Eingriffe führen zur Einhegung von Missbrauchsrisiken und beugen der leichtfertigen Nutzung der Daten durch die Behörden vor.

5.3 Entschädigungsregelung

Als rechtswidrig festgestellte Datenübermittlungen sollten außerdem eine finanzielle Entschädigung der Betroffenen zur Folge haben. Bei der Festsetzung der Höhe der Entschädigung sollte die Intensität (gesteigert etwa durch die gleichzeitige Überwachung mehrerer TK-Dienste) und die Dauer der Ermittlungsmaßnahme berücksichtigt werden. Nicht nur direkt Betroffene, gegen die sich das Ermittlungsverfahren richtete, sondern auch und gerade von vornherein unverdächtige Dritte sollten entschädigt werden.

Missbrauchsfälle oder Fehler im Herrschaftsbereich der Diensteanbieter sollten ebenfalls zur Entschädigung der Betroffenen führen. Der Betrag pro Datensatz sollte eine solche Höhe erreichen, dass der Anbieter schon aus finanziellen Gründen darauf achtet, dass die Sicherheitsmaßnahmen greifen und nur verlässliches und geschultes Personal eingesetzt wird.

6 Fazit

Die derzeit vorgesehene Absicherung der auf Vorrat gespeicherten Verkehrsdaten ist gemessen am notwendigen Schutz der Betroffenen völlig unzureichend. Sie entspricht den üblichen Sicherungsmaßnahmen für normale, einzelne Verarbeitungen von personenbezogenen Daten in der Telekommunikation. Die Speicherung eines Großteils des Fernkommunikationsverhaltens sämtlicher Teilnehmer führt jedoch zu besonders hohen Risiken für die Betroffenen und stellt einen tiefen Eingriff dar. Die durch Missbrauch oder Fehler bekannt gewordenen Informationen können nicht mehr zurückgenommen werden, der Schaden des Betroffenen ist irreversibel.

Sollen die Regelungen zur Umsetzung der Richtlinie zur Vorratsspeicherung die verfassungsrechtlich gebotene Verhältnismäßigkeit wahren, sind sie um entsprechende Sicherungsgarantien auf Gesetzesebene zu ergänzen. Fehlen diese, können die Umsetzungsregelungen nicht als verfassungsgemäß anerkannt werden.