

Prof. Dr. Alexander Roßnagel / Ass. jur. Mark Bedner, LL.M. / Ass. jur. Michael Knopp

Beantwortung der Fragen 11 – 13 des Fragenkatalogs

Die folgende Beantwortung gliedert sich in zwei Teile. Im ersten Teil wird das in der rechtswissenschaftlichen Literatur zu findende Verständnis der entscheidenden Regelungen in § 113a TKG referiert. Da diese unzureichend sind, um angesichts des Risikos der Vorratsdatenspeicherung die notwendige Verhältnismäßigkeit der Gesamtreglung herzustellen, werden im zweiten Teil Ergänzungen und Gestaltungsoptionen erörtert, die als notwendig erachtet werden, um den erforderlichen Schutz der informationelle Selbstbestimmung und des Fernmeldegeheimnisses sicherzustellen. Nur mit diesen Sicherungen können die nicht europarechtlich determinierten Regelungen des § 113a TKG als verhältnismäßig angesehen werden.

1. Auslegungen des § 113 TKG

1.1 Die „im Bereich der Telekommunikation erforderlichen Sorgfalt“ zur Sicherstellung der Datenqualität (Abs. 10 Satz 1 Alt. 1)

§ 113a Abs. 10 TKG enthält gemeinsam mit § 113a Abs. 11 TKG die maßgebliche Regelung für die Modalitäten der Speicherung dar. Die „im Bereich der Telekommunikation erforderliche Sorgfalt“ ist in der Gesetzesbegründung und in der Literatur nur unzureichend konkretisiert. So steht in der Gesetzesbegründung lediglich, dass „der Verpflichtete die zu speichernden Verkehrsdaten mit der Sorgfalt zu behandeln hat, die beim Umgang mit vom Fernmeldegeheimnis geschützten Daten erforderlich ist“.¹ Folgt man der Literatur, bedeutet dies eine Bekräftigung des einfachgesetzlichen Schutzes des Fernmeldegeheimnisses aus § 88 TKG. Außerdem wird auf die – bezüglich des erforderlichen Sicherheitsniveaus ebenfalls sehr offen gehaltenen – Vorschriften des § 109 TKG und des § 9 BDSG mit Anlage verwiesen.²

Beide Regelungen erklären Maßnahmen nur dann für erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Die besonders hohe Schutzbedürftigkeit der Vorratsdaten und das hohe Schadenspotential beim Abhandenkommen der Daten werden damit weder in der Gesetzesbegründung noch im Gesetz selbst deutlich gemacht. Es ist daher zu fordern, dass der Gesetzgeber die Vorschrift insoweit konkretisiert, dass diesen beiden Gesichtspunkten Rechnung getragen wird. Bezüglich der hierzu erforderlichen Maßnahmen und Gestaltungsanforderungen an die Organisation und insbesondere die Technik, sei auf die Erwägungen weiter unten verwiesen.

Der Begriff der „Qualität der Daten“ kann weitgehend mit dem informatorischen Schutzziel der „Integrität von Daten“ gleichgesetzt werden. Integrität in diesem Sinn bedeutet die Vollständigkeit und Korrektheit der Daten (Datenintegrität) und die korrekte Funktionsweise eines

¹ BT-Drs. 16/5846, 72.

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

Systems (Systemintegrität).³ Die Gesetzesbegründung spricht davon, dass „die Daten korrekt (und unverändert) gespeichert werden“.⁴

Es muss also gewährleistet sein, dass die in § 113a TKG aufgezählten Verkehrsdaten korrekt gespeichert werden. Korrekt sind Daten, wenn sie den bezeichneten Sachverhalt unverfälscht wiedergeben.⁵ Die in § 113a TKG angegebenen Daten müssen inhaltlich stimmig, technisch einwandfrei und reproduzierbar gespeichert werden.

„Qualität der Daten“ heißt aber auch Vollständigkeit der Daten. Vollständig bedeutet, dass alle Teile der Information verfügbar sind.⁶ „Informationen“ sind die nach § 113a TKG zu speichernden verschiedenartigen Verkehrsdaten. Daraus folgt, dass nur genau die im Gesetz genannten Daten erhoben werden sollen. Die Vollständigkeit ist dann nicht gegeben, wenn zu wenige oder aber auch zu viele Daten erhoben werden. Es muss demzufolge innerhalb der aufzeichnenden Soft- und Hardware technisch unmöglich sein, über den Gesetzeszweck hinaus gehende Daten, insbesondere Inhaltsdaten, mitzuspeichern. Die ordnungsgemäße Speicherung durch die Soft- und Hardware ist somit Teil der Funktionsweise des IT-Systems und folglich ein Aspekt der Systemintegrität.

1.2 Die „im Bereich der Telekommunikation erforderlichen Sorgfalt“ zum Schutz der gespeicherten Daten (Abs. 10 Satz 1 Alt. 2)

Der „Schutz der gespeicherten Daten“ wird in der Gesetzesbegründung mit der Unveränderbarkeit der Daten umschrieben.⁷ Veränderungen an den Daten sollen weitgehend ausgeschlossen werden. Daraus folgt das Erfordernis eines Zugriffsschutzes für die Daten. Da es eine absolute Sicherheit nicht geben kann, ist zu gewährleisten, dass Manipulationen nicht unbemerkt bleiben dürfen. Das bedeutet, dass Techniken erforderlich sind, mit deren Hilfe unautorisierte Manipulationen a posteriori erkennbar sind.⁸ Da der Zugriffsschutz keine nachträgliche Prüfung der Datenintegrität ermöglicht, ist entweder eine hier kaum praktikierbare systembezogene Sicherung durch nicht wiederbeschreibbare Medien oder der Einsatz elektronischer Signaturen zur Erfüllung der in der Gesetzesbegründung geäußerten Erwartung erforderlich. Auf diese Weise kann verhindert werden, dass unautorisiert manipulierte Daten weiterverarbeitet werden und der mögliche Schaden begrenzt wird.

1.3 Begrenzung des Datenzugangs auf besonders ermächtigte Personen (Abs. 10 Satz 2)

Zur Begrenzung des Datenzugangs fordert Satz 2 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 und darüber hinausgehend auf die Anlage verwiesen, die vergleichsweise konkrete Maßnahmen zur praktischen Umsetzung enthält.

³ *Holznel*, Recht der IT-Sicherheit, 2003, 13.

⁴ BT-Drs. 16/5846, 72.

⁵ *Holznel* (Fn. 3), 13.

⁶ *Holznel* (Fn. 3), 13.

⁷ BT-Drs. 16/5846, 72.

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

Eine weitere Konkretisierung der organisatorischen Maßnahmen findet sich in § 5 BDSG und § 88 Abs. 2 und 3 TKG. An der Datenverarbeitung beteiligte Mitarbeiter der TK-Unternehmen sind gemäß § 5 BDSG auf das Datengeheimnis zu verpflichten. Eine speziellere Geheimhaltungsverpflichtung für den Bereich der TK-Unternehmen ist in § 88 Abs. 2 TKG zu finden. Angesichts der anderweitigen und teilweise viel konkreteren Regelungen des gleichen Sachverhalts wird vorgebracht, die Regelungen in § 113a Abs. 10 TKG seien nicht notwendig gewesen.⁹ Bezogen auf die besondere Schutzbedürftigkeit der nach § 113a TKG gespeicherten Daten erscheint es jedoch sinnvoll, die mit diesen Daten befassten Mitarbeiter nicht nur allgemein auf Geheimhaltung zu verpflichten, sondern den betrauten Personenkreis gesondert auszuwählen und zu begrenzen.

2. Erforderliche technisch-organisatorische Maßnahmen

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 erforderlichen 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 –, wird dies den gesteigerten Risiken durch die Vorratsdatenspeicherung nicht gerecht. Die Vorratsdatenspeicherung verursacht aufgrund des Datenumfangs, der Bestimmung zur Überwachung im Fall des Abrufs und der Bestimmung zu einer schnellen Abrufbarkeit besondere Risiken für die Grundrechtsträger. Daher reichen die Maßnahmen, die bislang für den Bereich der Telekommunikation ausreichend waren, hierfür nicht aus. Vielmehr sind zur Sicherung der Verhältnismäßigkeit des Grundrechtseingriffs Ergänzungen speziell zur Sicherung der Vorratsdaten zu fordern, die über den in § 113a Abs. 10 TKG bestimmten Schutz, 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.

2.1 Datenspeicherung (Qualität)

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 Zeiträume beschränken, die kürzer als die vorgehaltenen sechs Monate sind. Auch müssen bei der Überprüfung der Telefondienstnutzung 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

⁹ *Graulich* (Fn. 1), Rn. 37.

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.

2.2 Datenaufbewahrung

Die Aufbewahrung der Daten ist sowohl für den zur Speicherung Verpflichteten als auch die zum Abruf berechtigten Stellen. Grundsätzlich sind zur Erkennung von durchgeführten Datenveränderungen kryptographisch sichere Hashfunktionen einzusetzen.¹⁰ 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 auf mögliche Manipulation überprüft werden. Angesichts der sich ständig durch Löschung und neu hinzukommende Daten verändernden Daten wird dies jedoch technisch keine triviale Aufgabe darstellen. Um den unbefugten Zugriff zu verhindern, ist zudem die verschlüsselte Aufbewahrung verbindlich zu fordern. Dem Anhang zu § 9 BDSG entsprechend ist zudem die zur Aufbewahrung der Daten genutzte Hardware gegen Zutritt und Zugang zu sichern.

Zur Datenaufbewahrung gehören auch eine Datensicherung mittels Backups und eine entsprechende Sicherungsstrategie. Hinsichtlich dieser Backupdaten gelten alle ergangenen und folgenden Erwägungen sowie die zusätzlichen Anforderungen, dass die Backupdaten regelmäßig verifiziert werden. So muss automatisiert und durch tatsächliche Stichproben geprüft werden, ob die Daten tatsächlich und vollständig gesichert wurden.

2.2.1 Funktionale Trennung

Wichtig für die Risikoverringerung ist die Trennung der Daten, um für jeden Betroffenen keine zentrale Sammlung entstehen zu lassen. Optimal wäre eine sogar physische Trennung der Datenspeicher sowie der Abrufmöglichkeiten. Als erstes sind weiterhin nach §§ 111, 112 TKG vorzuhaltende Bestandsdaten und Verkehrsdaten zu trennen. Vor allem aber ist die Speicherung der nach § 113a TKG zu speichernden 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.

2.2.2 Trennung der Daten nach Dienst- oder Kommunikationsarten

Da viele Diensteanbieter heute nicht mehr nur eine der in § 113a Abs. 1 – 6 TKG erfassten Dienstarten anbieten, könnten bei diesen Datensammlungen entstehen, in denen Daten zu verschiedenen Kommunikationsarten einer Person zusammenkommen. 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 ge-

¹⁰ Eckert (Fn. 8), 8.

trennt oder gesondert zu verschlüsseln. Sollten die Sicherungsmaßnahmen unbefugt überwunden werden, 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, so dass auch hier die Missbrauchsgefahr im Umfang begrenzt werden kann.

2.2.3 Trennung nach anschluss- und dienstbezogenen Daten

In der Literatur wird außerdem vorgeschlagen, die Daten verteilt – 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.¹¹

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. Ebenso ist nicht ersichtlich, ob die Nummer Quelle oder Ziel des Anrufs war und welcher Dienst genutzt wurde. Über Referenznummern und unter Beteiligung beider Stellen kann dann der komplette Datensatz rekonstruiert werden. Die Vorgehensweise stellt eine Anwendung des Vier-Augen-Prinzips auf institutioneller Ebene dar.¹²

2.2.4 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.¹³ Die Kennzeichnung stellt jedoch kein technisches Hindernis einer Weitergabe dar, indem sie untrennbar verbunden wäre und auch nach der unbefugten Weitergabe die Herkunft erkennbar machen würde. Eine solche untrennbare Kennzeichnung wäre zwar wünschenswert,¹⁴ ist aber technisch derzeit nicht machbar.¹⁵

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 Kennzeich-

¹¹ Ziebarth, DuD 2009, 29.

¹² Ziebarth, DuD 2009, 29.

¹³ BeckOK (Hegmann), 3. Ed. 2009, § 101 Rn. 7f.

¹⁴ Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts. Gutachten für das Bundesministerium des Innern, 2001, 127f.

¹⁵ Böhme/Pfitzmann, DuD 2008, 346.

nung mehr als nur die Quelle erfassen und die ersuchende Stelle, die verantwortliche Person, einen Verweis auf die richterliche Anordnung und den Zeitpunkt der Übermittlung enthalten.

2.2.5 Beschränkung der Datennutzung auf bestimmte geschützte Umgebungen

Auch wenn die Kennzeichnung der Daten nicht als sichere Maßnahme zur Missbrauchsverhinderung genutzt werden kann, scheidet ein technischer Schutz der Daten nicht aus. Während § 113a Abs. 10 TKG die Anbieter zur erforderlichen Sorgfalt verpflichtet, fehlt eine ähnliche Vorschrift für die ersuchenden Stellen. Zwar kommen hier nur die Daten einzelner Personen in Betracht, es geht nicht um den Schutz der Verkehrsdaten sämtlicher Anbieterkunden. Andererseits wird der übrige Akteninhalt regelmäßig die personale Zuordnung zulassen.

Auch in den die abrufenden Stellen betreffenden Regelungen sind Sicherungsmaßnahmen vorzusehen. Sie könnten vorgeben, dass die Daten nur in einer geschützten Umgebung oder nur mit einer nicht frei zugänglichen Software eingesehen werden können. Zudem darf die Einsichtnahme nur nach einer sicheren Authentifizierung des Einsicht Nehmenden möglich sein.

2.2.6 Verschlüsselung

Eine weitere Schutzmaßnahme, die erstreckt auf alle Stationen der nach § 113a TKG erfassten Daten gesetzlich angeordnet werden muss, ist die lückenlose Verschlüsselung der Daten. Weder beim Anbieter und Aufzeichnungsverpflichteten noch bei der Übermittlung oder anschließend bei der ersuchenden Stelle dürfen die Daten unverschlüsselt zugänglich sein.

Die Verkehrsdaten sind mittels sicherer Algorithmen zu verschlüsseln. Die verwendete Software 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 oder sogar durch den Gesetzgeber in einer Anlage zu § 113a TKG festgelegt werden.

2.3 Löschung

Die Löschung der Daten ist derzeit in § 113a Abs. 11 TKG geregelt und schreibt die Löschung innerhalb eines Monats nach Ablauf der sechsmonatigen Aufbewahrungsfrist vor. Damit bleiben jedoch auch bezüglich der Löschung wesentliche Fragen unregelt, außerdem ermöglicht die Regelung eine unnötige Verlängerung der Speicherdauer.

Die Löschung der Daten muss so erfolgen, dass sie nicht mehr wiederhergestellt werden können. Dazu reicht es nicht aus, lediglich die Verweise zu den Dateien im Dateisystem zu löschen. Die Daten sind vielmehr mindestens einmal, besser mehrfach, mit Zufallsdaten zu überschreiben, so dass sie nicht wieder hergestellt werden können.

Die erfolgreiche Löschung sollte regelmäßig stichprobenartig überprüft werden. Hierzu könnte auch eine Verpflichtung zur Hinzuziehung eines internen oder externen Datenschutzbeauftragten gedacht werden. Die Überwachung der Löschung sollte jedenfalls klar geregelt werden. In technischer Hinsicht gilt das Gleiche 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.

2.4 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. Denkbar wäre zum Beispiel, dass amerikanische Formate für die Ausgabe verwendet werden (Unterscheidung nach AM und PM oder Datumsangaben im Format MM/DD/YYYY) und diese nicht unmittelbar erkennbar sind, so dass es dadurch zur Weitergabe falscher Daten an die Ermittlungsbehörden kommt¹⁶ und damit die Strafverfolgung Unschuldiger eingeleitet wird.

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

2.5 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 zum einen die verpflichteten Stellen, die damit von einer weiteren Pflicht betroffen werden. Die verpflichteten Stellen haben jeglichen Datenzugriff, dessen Zweck, die verantwortliche Person, zugrunde liegende Anordnungen, den Zeitpunkt, den genauen Datenumfang und den Empfänger festhalten. Die Aufbewahrungsfrist dieser Dokumentation ist gesondert festzulegen und darf nicht enden, bevor nicht die Benachrichtigung des Betroffenen sichergestellt und eine entsprechende 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 die 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.

Der Zugang mittels Chipkarte sollte zur zusätzlichen Sicherung überdies 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 zugewiesenen, 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 soll jede Kombination zweier Mitarbeiter eine Freigabe der Daten ermöglichen. In den Protokollen ist festzuhalten, welche beiden Mitarbeiter jeweils beteiligt waren.

¹⁶ So kam es im Rahmen der „Filesharingüberwachung“ 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>.

Auf diese Weise kann der technische Schutz durch die Verschlüsselung auch organisatorisch durch das Vier-Augen-Prinzip unterstützt werden.

2.6 Notwendige Rahmenregelungen

Die Umsetzung technischer Sicherungen, die das Verständnis der erforderlichen Sorgfalt verfassungskonform ausgestalten, reicht jedoch nicht aus, um die Vorratsdatenspeicherung verfassungsgemäß zu gestalten.

Die 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 Zugangsauthentifikation, die technische Sicherung durch Verschlüsselung der Daten und die Zugriffsdokumentation.

Abgesehen von der Kennzeichnungspflicht und Löschungspflicht in § 101 StPO ist gänzlich unregelt, 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.¹⁷ Die Kennzeichnung bietet damit keinen Schutz vor einer unbefugten Weitergabe. 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 folgende rechtliche Sicherungsmaßnahmen erforderlich.

2.6.1 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. Rückweisend auf die Anforderung der Sortierbarkeit und Trennbarkeit der Daten 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 zur Einrichtung von Schwerpunktstaatsanwaltschaften mit besonders befähigten Staatsanwälten, beispielsweise gerade im Telekommunikations- und IT-Bereich, sollten besonders ausgebildete Richter für diese Bereiche vorgesehen werden.

2.6.2 Benachrichtigungspflichten und nachträgliche gerichtliche Kontrolle

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 gericht-

¹⁷ *Böhme/Pfitzmann*, DuD 2008, 342.

tet war und gegenüber denen der Eingriff unerheblich war, 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, gänzlich 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.

Die Rechtsschutzgarantie für den Betroffenen stellt die effektivste Kontrolle des Umgangs mit den nach § 113a TKG gespeicherten Daten dar. Voraussetzung für den Betroffenen zur Wahrnehmung seines Rechtsschutzes ist jedoch das Wissen um die Ermittlungsmaßnahme. Den Betroffenen ist zwar bekannt, dass ihre Daten gespeichert werden, jedoch nicht, ob tatsächlich ein Abruf erfolgt. Einschränkungen dieser Benachrichtigung sind also 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 Diensteanbieter der überwachten Anschlüsse versenden und diese die Kunden in der nächsten Rechnung oder mittels „E-Mail-Newsletter“ auf die Datenübermittlung an die Behörden samt Aktenzeichen hinweisen.

In Anlehnung an die „Doktrin der Früchte vom verbotenen Baum“ sollten rechtswidrige Ermittlungs- und Überwachungsmaßnahmen ein ausnahmsloses Beweisverwertungsverbot nach sich ziehen. Nur mit Konsequenzen belegte Eingriffe führen zur Einhegung und beugen der leichtfertigen Nutzung der Daten durch die Behörden vor.

2.6.3 Entschädigungsregelung

Als rechtswidrig festgestellte Datenübermittlungen sollten eine finanzielle Entschädigung der Betroffenen zur Folge haben. Bei der Festsetzung der Höhe der Entschädigung sollte die Intensität (beispielsweise wenn mehrere TK-Dienste gleichzeitig überwacht werden) und die Dauer der Ermittlungsmaßnahme berücksichtigt werden. Nicht nur direkt Betroffene, gegen die sich das Ermittlungsverfahren richtete, sondern auch und gerade von vornerein unverdächtige Dritte sollten entschädigt werden.

2.6.4 Haftungsregelungen

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