Zeitschrift für Wirtschafts- und Steuerstrafrecht

wistra

24. Jahrgang · Heft 1 · 14. Januar 2005

Professor Dr. Thomas Hoeren, Universität Münster

Auskunftspflichten der Internetprovider an Strafverfolgungs- und Sicherheitsbehörden – eine Einführung

Die zunehmenden Auskunftsbegehren der Strafverfolgungs- und Sicherheitsbehörden stellen Access Provider oft vor ein Problem. Die Regelungsmaterie ist kompliziert, verteilen sich doch die Regelungen zu den Auskunftspflichten gleich auf mehrere Gesetze und detailreiche Vorschriften. Und jeder Fehler rächt sich für den Provider: Informiert er zu viel, schreien seine Kunden; informiert er zu wenig, schreien die Behörden. In dieser komplexen Lage will der folgende Beitrag einen ersten Pfad durch den Normendschungel vor dem Hintergrund des neuen Telekommunikationsgesetzes schlagen.

* * *

Im Rahmen der Aufklärung und der Verhinderung von Straftaten wenden sich Sicherheits- und Strafverfolgungsbehörden häufig auch an Tk-Anbieter, um die Telekommunikation von Nutzern zu überwachen oder um Auskünfte zu erlangen, über die ein Provider aufgrund von Kundenverträgen oder Log-Dateien verfügt. Auskunftsanordnungen und Tk-Überwachung stehen dabei in einem Spannungsfeld zwischen der Verteidigung der Sicherheit des Staates, einer effektiven Strafverfolgung und der Wahrung der Rechte Dritter einerseits und den Grundrechten des von der Auskunft oder Überwachung Betroffenen andererseits, insbesondere dessen informationellem Selbstbestimmungsrecht. Auskunfts- und Überwachungsmaßnahmen bedeuten immer gewichtige Grundrechtseingriffe und sind nur im Rahmen einer gesetzlichen Grundlage zulässig.

Provider haben zwar, auch als potentielle Opfer von Straftaten und zum Schutz ihrer Dienstleistungen und Kunden ein besonderes Interesse an effizienter Missbrauchsbekämpfung. Andererseits stellt sich für Provider auch im Hinblick auf eine mögliche Haftung die Frage, in welchen Fällen und in welchem Umfang sie Daten überhaupt herausgeben dürfen oder müssen. Der nachfolgende Überblick skizziert zunächst die wichtigsten Befugnisse der Strafverfolgungs- und Sicherheitsbehörden bei Maßnahmen gegen einzelne Nutzer und gibt anschließend Empfehlungen zum Verhalten der Provider bei entsprechenden Ersuchen. Hinweise erfolgen auch auf die Neuerungen durch die Umgestaltung des TKG[1]; ferner werden die Änderungen in einem Überblick zusammengefasst.

Die einschlägige Befugnisnorm für Strafverfolgungs- und Sicherheitsbehörden richtet sich zunächst danach, ob es um die Aufklärung bereits begangener Straftaten (repressiv) oder die Abwehr künftiger Gefahren (präventiv) geht.
Weiter ist zu unterscheiden, ob die angeordneten Maßnahmen
- Inhalte der Kommunikation,
- Verbindungsdaten oder
- Bestandsdaten betreffen.

Sowohl Inhalte wie auch Verbindungsdaten der Telekommunikation stehen unter dem besonderen Schutz des Fernmeldegeheimnisses; deshalb sind Eingriffe nur unter engen Voraussetzungen erlaubt.

I. Überwachung von Kommunikationsinhalten

Jegliche Inhalte der Telekommunikation, wie etwa Inhalte von E-Mails, Telefax und auch jeder Online-Datenaustausch unterliegen dem Fernmeldegeheimnis. Dieses schützt die unbeobachtete Kommunikation natürlicher und juristischer Personen und verpflichtet Betreiber und Mitarbeiter von geschäftsmäßigen wie gewerblichen Tk-Anbietern zur Verschwiegenheit. Eine Überwachung und Aufzeichnung der Kommunikation bedeutet einen äußerst schwerwiegenden Eingriff in die Grundrechte des Betroffenen, zumal sie ihn regelmäßig in einer Situation vermeintlicher Vertraulichkeit trifft[2]. Sie ist daher nur in engen Grenzen zulässig, wenn ein Gesetz die Einschränkung des Fernmeldegeheimnisses zu diesem Zweck ausdrücklich gestattet. Die Überwachungs- und Auskunftsverpflichtungen richten sich an geschäftsmäßige Tk-Anbieter und betreffen damit auch innerbetriebliche, private Telekommunikation von Mitarbeitern oder Studenten auch an Hochschulen, wenn die Tk-Nutzung – insbesondere des E-Mail-Dienstes – auch für private Zwecke erlaubt oder geduldet ist[3].

1 TKG vom 22. Juni 2004, BGBL. I 2004, S. 1190.
2 BVerfG, wistra 2003, 217, 222 = JurPC Web-Dok. 101/2003, Abs. 74.
3 *Rieß* in Roßnagel, Handbuch Datenschutzrecht, 2003, Teil 6.4, Rn. 77.

1. TKÜ durch Strafverfolgungsbehörden – §§ 100a, b StPO

Die wichtigste gesetzliche Grundlage, die Staatsanwaltschaft und Polizei eine Telekommunikations-Überwachung zur Aufklärung begangener Straftaten gestattet, stellt § 100a i.V.m. § 100b StPO dar. Ziel ist die Erlangung und Sicherung von Beweisen für die Strafverfolgung sowie die Ermittlung des Aufenthaltsorts des Beschuldigten. Diese Eingriffsmaßnahme hat im Ermittlungsverfahren in den vergangenen Jahren stetig zugenommen und ist von 3667 im Jahr 1995 auf 15741 im Jahr 2000 angestiegen[4], wobei der Löwenanteil auf Betäubungsmitteldelikte entfiel[5]. Im Online-Bereich geht es dabei vorrangig um die Aufzeichnung und Überwachung von E-Mail-Kommunikation, Internettelefonie und Mailboxsystemen.

Die Telekommunikations-Überwachung und -aufzeichnung bedeutet einen gravierenden Eingriff für den Betroffenen und ist an folgende Voraussetzungen gebunden:

(1) Es müssen bestimmte Tatsachen vorliegen, die den Verdacht der Beteiligung an einer der schweren Straftaten begründen, die im Straftatenkatalog des § 100a StPO abschließend aufgezählt sind. Genannt sind u.a. Delikte wie Friedensverrat, Hochverrat, Geld- oder Wertpapierfälschung, Menschenhandel, Bandendiebstahl, Tötungsdelikte, Raubdelikte, Erpressung, schwere Brandstiftung und ähnliche gemeingefährliche Straftaten, Verstöße gegen das Waffengesetz oder das Kriegswaffenkontrollgesetz und Rauschgiftdelikte. Nicht enthalten sind computerspezifische Delikte wie Ausspähen von Daten, Computerbetrug oder Computersabotage.

(2) Zulässig ist die Überwachung ferner nur, wenn sie unentbehrlich und verhältnismäßig[6] ist, weil andernfalls die Erforschung des Sachverhalts oder die Ermittlung des Beschuldigten aussichtslos oder wesentlich erschwert wäre. Dies trifft zu, wenn andere Aufklärungsmittel nicht vorhanden sind[7].

(3) Enthalten muss die Anordnung Namen und Anschrift und die Rufnummer oder eine andere Kennung (§ 100b Abs. 2 Satz 2 StPO) des Anschlusses einer bestimmten Person. Dies ist in erster Linie der Beschuldigte. Wenn gesicherte Tatsachen und nicht nur Vermutungen[8] dafür vorliegen, dass andere Personen Nachrichten vom und zum Verdächtigen weiterleiten oder dass der Beschuldigte den Anschluss anderer Personen benutzt, darf sich die Überwachung auch gegen diese Kontaktpersonen richten. Umstritten ist, ob eine Tk-Überwachung auch zulässig ist, wenn die Identität des Tatverdächtigen noch nicht feststeht[9]. Dagegen spricht aber die hohe Bedeutung des grundgesetzlich verankerten Fernmeldegeheimnisses, die eine restriktive Auslegung der Eingriffsnorm gebietet sowie der Wortlaut des § 100a StPO; danach kann zwar der Aufenthaltsort unbekannt sein, jedoch müssen Name und Anschrift genannt sein[10]. Auch die Rechtsprechung zur Vorgängernorm des § 12 FAG verlangte jedenfalls strenge Anforderungen an eine hinreichende Individualisierung des Betroffenen[11]. Ferner – über Namen und Anschrift des Beschuldigten, Rufnummer oder andere Kennung des Tk-Anschlusses hinaus – müssen Angaben zu Art, Umfang und Dauer der Maßnahme enthalten sein, die verfolgte Straftat bezeichnet sein und Tatsachen und Beweislage, welche die Überwachung rechtfertigen, knapp dargelegt sein[12] (Erforschung des Sachverhalts oder Aufenthaltsermittlung).

(4) Die Tk-Überwachung muss schriftlich durch einen Richter angeordnet sein und ist – auch bei jeder Verlängerung – auf höchstens drei Monate zu befristen. Bei Gefahr im Verzug kann die Anordnung auch durch den Staatsanwalt – niemals aber durch deren Hilfsbeamte[13] – getroffen werden; wenn sie nicht binnen drei Tagen durch den Richter bestätigt wird, tritt die staatsanwaltliche Anordnung außer Kraft.

Dem Tk-Anbieter obliegt es nicht, die inhaltlichen Voraussetzungen der Anordnung, wohl aber die formellen Anforderungen – z.B. schriftliche Anordnung durch den Richter – zu überprüfen. Bei Vorlage der Anordnung muss er die Überwachung dem Richter, Staatsanwalt oder den im Polizeidienst tätigen Hilfsbeamten ermöglichen. Für die tatsächliche Durchführung der Abhörmaßnahme sind die Tk-Anbieter nach § 17a ZSEG zu entschädigen; dabei handelt es sich um keine Übernahme der tatsächlichen Kosten[14]. Die Betroffenen sind von den Strafverfolgungsbehörden über die Überwachungsmaßnahme nachträglich zu benachrichtigen.

Auf der Grundlage von §§ 100a, b StPO kann auch Auskunft über Verbindungsdaten verlangt werden. Dieser gegenüber der Inhaltsüberwachung geringere Eingriff muss sich aber im Rahmen der Anordnung halten[15].

2. TKÜ durch Nachrichtendienste – G 10

Auch die Nachrichtendienste des Bundes – Bundesverfassungsschutz, der militärische Abschirmdienst (MAD) und der Bundesnachrichtendienst (BND) – sowie der Länder – die Landesämter für Verfassungsschutz – sind befugt, die Telekommunikation in Einzelfällen zu überwachen und aufzeichnen, § 1 G 10. Verpflichtet zur Ermöglichung der Überwachung sind geschäftsmäßige Tk-Anbieter, § 2 G 10; angefordert werden können auch Auskünfte über den Fernmeldeverkehr.

Die Maßnahmen setzen den Verdacht voraus, dass jemand eine der katalogartig aufgelisteten Straftaten des § 3 G 10 plant, begeht oder begangen hat. Aufgezählt sind insbesondere Friedens- und Hochverrat, Landesverrat, die Gefährdung der äußeren Sicherheit wie der demokratischen Grundordnung oder der Sicherheit des Bundes oder eines Landes. Im Einzelnen sind die Eingriffsbefugnisse geregelt im MADG (insbes. § 10 Abs. 3) für den militärischen Abschirmdienst, im BND-Gesetz für den Bundesnachrichtendienst (insbes. § 8 Abs. 3 a) und im BVerfSchG für das Bundesamt für Verfassungsschutz (insbes. §§ 8 Abs. 8, 9, und 9 Abs. 4) sowie den Landesverfassungsschutzgesetzen (LVerfSchG).

Neben der Individualüberwachung gegen Verdächtige oder deren Kontaktpersonen (Nachrichtenmittler; Personen, deren Anschluss benutzt wird) ermöglicht das G 10 dem BND auch die verdachtslose strategische Überwachung zur Aufklärung abstrakter Gefahrenlagen und zur Erstellung von Lagebildern, um bestimmten Gefahren wie etwa terroristischen Anschlägen rechtzeitig begegnen zu können. Ohne Bezug auf bestimmte Personen wird dabei zunächst die Telekommunikation aus oder zu bestimmten Regionen überwacht, um daraus geheimdienstlich relevante Vorgänge herauszufiltern. Anders als bei der Strafver-

4 *Bäumler* in Roßnagel, Teil 8.3, Rn. 54.
5 Max-Planck-Institut für ausländisches und internationales Strafrecht – Freiburg, http://www.iuscrim.mpg.de/forsch/krim/albrecht.html; *Bizer*, Praxis der Tk-Überwachung, DuD 2002, 216 ff.
6 *Ehmer* in Büchner/Ehmer/Geppert, Beck'scher TkG-Kommentar, 2. Aufl., § 88 TKG, Rn. 3; *Nack* in KK-StPO, § 100a, Rn. 24.
7 *Hoeren/Sieber/Büttgen*, Handbuch Multimediarecht, Teil 16.3, Rn. 102; *Meyer-Goßner*, StPO, § 100a, Rn. 7.
8 BVerfG, wistra 2003, 217, 222 f. = JurPC Web-Dok. 101/2003, Abs. 78.
9 So *Meyer-Goßner*, § 100a, Rn. 9; Löwe/Rosenberg, § 100a, Rn. 20; a.A: *Ehmer* in Büchner/Ehmer/Geppert, § 88 TKG, Rn. 8.
10 *Ehmer* in Büchner/Ehmer/Geppert, § 88 TKG, Rn. 8.
11 *Ehmer* in Büchner/Ehmer/Geppert, § 88 TKG, Rn. 8 mit Rspr.Nw.
12 BGH, wistra 2003, 67, 68 = JurPC Web-Dok. 296/2003.
13 HmbDSB, 18. TB, Kap. 3, S. 29; *Nack* in KK-StPO, § 100b, Rn. 1.
14 *Meyer-Goßner*, § 100b, Rn. 9; *Pernice*, Die Telekommunikations-Überwachungsverordnung (TKÜV), DuD 2002, 207, 210.
15 Schönke/Schröder-*Lenckner*, StGB, § 206, Rn. 13; *Eckhardt*, Neue Regelungen der Tk-Überwachung, DuD 2002, 197, 198; *Ehmer* in Büchner/Ehmer/Geppert, § 88 TKG, Rn. 5; *Nack* in KK-StPO, § 100a, Rn. 20.

folgung muss der BND insoweit keine Rufnummern oder Kennungen angegeben. Die TKÜV wurde im Hinblick auf Umsetzung dieser Maßnahmen zum 23.08.2002 ergänzt[16].

Die schriftliche Anordnung, die Grund, Art, Umfang und Dauer der Maßnahme beinhalten muss, erfolgt durch den zuständigen Bundesminister bzw. die oberste Landes-Verfassungsschutzbehörde. Die zur Überwachung berechtigten Behörden sind verpflichtet, entstandenen Aufwand der Tk-Anbieter bei Auskunftsersuchen oder der Ermöglichung der Tk-Überwachung zu entschädigen, §§ 20 G 10, 17a Abs. 1 Nr. 3 ZSEG. Außerdem ist der Betroffene von der anordnenden Stelle über die heimliche Fernmeldeüberwachung zu informieren, sobald eine Gefährdung des Maßnahmenzwecks ausgeschlossen werden kann.

3. TKÜ durch Zollkriminalamt – § 39 AWG

Zur Verhütung von Straftaten nach dem Außenwirtschaftsgesetz (AWG) oder dem Kriegswaffenkontrollgesetz (KWKG) ist das Zollkriminalamt berechtigt, den Fernmeldeverkehr zu überwachen und aufzuzeichnen, § 39 ff. AWG. Es handelt sich dabei um präventive Maßnahmen gegen Verdächtige und deren Kontaktpersonen. Die schriftliche Anordnung gegenüber geschäftsmäßigen Tk-Anbietern erfolgt durch das zuständige Landgericht, bei Gefahr in Verzug durch den Bundesfinanzminister. Auch insoweit ist eine nachträgliche Mitteilung an den Betroffenen durch das Zollkriminalamt vorgesehen. Entstandener Aufwand muss entsprechend § 17a ZSEG entschädigt werden. Die Regelung ist bis 31. 12. 2004 befristet.

II. Auskunft über Verbindungsdaten

Gegenstand von Auskunftsverlangen sind häufig auch Verbindungsdaten. Diese beschreiben die näheren Umstände der Telekommunikation, also wer wann mit wem kommuniziert hat und unterliegen wie die Inhalte dem besonderen Schutz des Fernmeldegeheimnisses. Hierzu rechnen insbesondere Datum und Uhrzeit einer Nutzung, dynamische IP-Adresse, in Anspruch genommener Dienst und nachgefragte URL. Verbindungsdaten werden bei jedem Nutzungsvorgang von Online-Diensten automatisch generiert und liegen bei Anbietern gespeichert vor, soweit diese sie für Abrechungszwecke aufbewahren dürfen. Waren Daten vorher zu löschen, etwa weil bei kostenlosen Zugängen keine Speicherung zu Abrechnungszwecken erforderlich ist und erfolgen darf, so sind diese Daten auch für Strafverfolgungsbehörden nicht verfügbar. Der zur Verfügung stehende Datenpool ist auch eingeschränkt, soweit Dienste von Nutzern anonym genutzt werden.

1. Auskunft an Strafverfolgungsbehörden – §§ 100g, h StPO

Eine wichtige Ermittlungsmaßnahme der Strafverfolgung stellt das Auskunftsersuchen an Erbringer geschäftsmäßiger Tk-Dienste nach § 100g StPO dar. Die §§ 100g, h StPO ersetzen den bis 31. 12. 2001 geltenden § 12 FAG und gelten ihrerseits vorläufig bis zum 31. 12. 2004. Ein auf §§ 100g, h StPO gestütztes Auskunftsersuchen kann nicht nur

- Verbindungsdaten abgewickelter Telekommunikation,
- sondern auch zukünftige Daten betreffen.

Den Strafverfolgungsbehörden dient der Auskunftsanspruch einerseits zur Beschaffung von Beweismitteln und der Bestimmung des Beschuldigten zur Tatzeit, andererseits auch zur Überprüfung, ob und gegen wen eine Tk-Überwachung nach § 100a StPO erfolgversprechend erscheint. Auch soweit im Vorfeld einer Durchsuchung der Zielrechner ermittelt werden soll, in dem die gesuchten Beweismittel gespeichert sind, werden Auskünfte über § 100g StPO eingeholt[17]. In der Praxis geht es häufig darum, eine zu einem bestimmten Zeitpunkt zugeteilte IP-Adresse einem bestimmten Nutzer zuzuordnen.

a) Voraussetzungen der Auskunftsanordnung

Die Auskunftsanordnung nach §§ 100g, h setzt voraus, dass:

- bestimmte Tatsachen den Verdacht einer Straftat begründen
- und die Auskunft erforderlich ist
- für die Aufklärung einer Straftat von erheblicher Bedeutung
- oder[18] die Aufklärung einer Straftat, die mittels einer Endeinrichtung der Telekommunikation begangen wurde (Schwere der Tat unerheblich).

Als Straftaten von erheblicher Bedeutung gelten vor allem die Katalogtaten des § 100a StPO. In Frage kommen aber auch andere Straftaten, die im konkreten Fall erhebliche Bedeutung haben, etwa wegen der Begehungsart, des Ausmaßes des Schadens oder des Grades der Bedrohung der Allgemeinheit[19]. Bei einem einfachen Diebstahl dreier Handys ist aber, wie das LG Münster[20] feststellt, nicht von einer erheblichen Bedeutung der Straftat auszugehen. Ein Auskunftsanspruch scheidet ferner aus bei Bagatelldelikten, die nur auf Strafantrag verfolgt werden und bei Ordnungswidrigkeiten[21].

Dagegen kommt es bei Straftaten, die mittels Endeinrichtung – Telefon, Faxgerät, PC – begangen werden, nicht auf die Schwere der Delikte an, da andernfalls derartige Delikte regelmäßig nicht aufklärbar sind[22]. Auch bei minder schweren Straftaten wie etwa beim Versand strafrechtlich relevanter Mails mittels PC kann Auskunft angeordnet werden. Das LG Ulm hat dies im Fall einer Beleidigung bejaht, nachdem ein Unbekannter in einer Annonce unter www.sexanzeigen.de als Kontakt die Telefonnummer einer jungen Frau angeben hatte[23].

b) Inhalt und Umfang des Auskunftsanspruchs

Der Auskunftsanspruch betrifft Verbindungsdaten. In Frage kommen in erster Linie Verbindungsdaten des Beschuldigten. Abgefragt werden können aber auch Verbindungsdaten von – auch unverdächtigen – Kontaktpersonen. Insoweit müssen sichere Anhaltspunkte[24] bestehen, dass diese Personen als Nachrichtenmittler Informationen von oder zum Verdächtigen weiterleiten oder dass der Verdächtige den Anschluss dieser Personen benutzt. Bei der Aufklärung von „Hacker-Angriffen", in denen sich der Täter unerlaubt über Computer-Netzwerke einwählt, dürfen auch die Verbindungsdaten der Betreiber der missbrauchten und zwischengeschalteten Netzwerke beauskunftet werden[25]. Ausgenommen sind lediglich Verbindungsdaten von Personen, denen ein Zeugnisverweigerungsrecht zusteht.

Welche Verbindungsdaten abgefragt werden dürfen, zählt § 100g Abs. 3 StPO abschließend auf: im Fall einer Verbindung

16 Erste Verordnung zur Änderung der Telekommunikationsüberwachungsverordnung (TKÜV), BGBl I, S. 3317.
17 *Bizer*, Verpflichtung zur Herausgabe von Tk-Verbindungsdaten an den Staatsanwalt, DuD 2002, 237.
18 § 100g enthält zwei voneinander unabhängige Tatbestandsalternativen, hierzu: BT-Drs. 14/7008, S. 6; LG Wuppertal, B. v. 13. 2. 2002, 30 Qs 5/02; a.A.: LG Köln, B. v. 5. 2. 2002, 107 QS 36/02, auch die zweite Alternative setzt eine Straftat von erheblicher Bedeutung voraus.
19 BVerfG, wistra 2003, 217, 222 f. = JurPC Web-Dok. 101/2003, Abs. 76, 81.
20 LG Münster, B. v. 07.01.2002, Az. 8 Qs 2/02, JurPC Web-Dok. 50/2003.
21 BT-Drs. 14/7008, S. 7; *Bär*, Auskunftsanspruch über Telekommunikationsdaten, MMR 2002, 358, 361; *Meyer-Goßner*, § 100g, Rn. 6; *Nack* in KK-StPO, § 100g, Rn. 4.
22 BTR-Drs. 702/01, S. 7.
23 LG Ulm, B. v. 21.03.2002, 2 Qs 2016/02, JurPC Web-Dok. 44/2003.
24 BVerfG, wistra 2003, 217, 222 f. = JurPC Web-Dok. 101/2003, Abs. 78.
25 BT-Drs. 14/7008, S. 7.

- die Berechtigungskennungen, Kartennummern, Standortkennung sowie Rufnummer oder Kennung des anrufenden und angerufenen Anschlusses oder der Endeinrichtung,
- Beginn und Ende der Verbindung nach Datum und Uhrzeit,
- und die in Anspruch genommene Tk-Dienstleistung,
- Endpunkte festgeschalteter Verbindungen und ihr Beginn und Ende nach Datum und Uhrzeit und
- sonstige zum Aufbau, zur Aufrechterhaltung und Abrechnung notwendigen Verbindungsdaten.

Diese Daten gehören zu den Daten, die nach der TDSV (§ 6) grundsätzlich erhoben, gespeichert und verarbeitet werden dürfen, also ohnehin legal zur Verfügung stehen[26].

Unter „Kennung" wird dabei auch die IP-Adresse von Computern verstanden. Streitig ist jedoch, ob die „Kennung" auch die hinter der IP-Nummer oder E-Mail-Adresse stehende Person umfasst oder diese Daten als Bestandsdaten nach § 113 TKG abgefragt werden können. Nach ganz überwiegender Ansicht werden feste IP-Adressen, die stets einer bestimmten Person zugeordnet werden können, als Bestandsdaten der Telekommunikation angesehen. Dynamische IP-Adressen hingegen, die vom Tk-Anbieter wechselnd vergeben werden, gelten als Verbindungsdaten[27]. Ebenso wurde aus der Vorgängerregelung des § 12 FAG die Pflicht abgeleitet, eine Auskunft über die Identität auch bei wechselnden Nutzern zu erteilen[28]. Demzufolge sind bei Auskunftsersuchen zu Einwahl-Log-Dateien, um eine dynamische IP-Adresse zu einem bestimmten Zeitpunkt einem bestimmten Benutzer zuzuordnen, die §§ 100g, h StPO einschlägig; um die Zuordnung von Bestandsdaten kann nach § 113 TKG (früher § 89 Abs. 6 TKG) ersucht werden.

c) Insbesondere: Zukünftige Verbindungen

Das Auskunftsersuchen kann sich nicht nur auf abgewickelte Vorgänge, sondern auch auf zukünftige Verbindungen bis zu jeweils drei Monaten erstrecken, § 100g Abs. 1 S. 3 StPO. Dies wirft in der Praxis von Tk-Anbietern vor allem folgende Fragen auf:

(1) In welchem Umfang darf die Speicherung zukünftiger Kommunikationsdaten angeordnet werden?

Tatsächlich darf das Ersuchen nur die Daten einbeziehen, die ohnehin zulässigerweise nach dem Telekommunikationsrecht erhoben und verarbeitet werden dürfen. Darüber hinaus gehende, andere Verbindungsdaten können die Strafverfolgungsbehörden nur unter den strikten Voraussetzungen der Tk-Überwachung nach § 100a StPO erlangen[29].

(2) Kann die Speicherung künftiger Verbindungsdaten angeordnet werden, wenn der Tk-Anbieter regelmäßig keine Daten speichert (und speichern darf) – weil die Daten für Abrechnungszwecke nicht erforderlich sind?

Diese Fragestellung betrifft insbesondere Anbieter kostenloser Dienste. In der Tat legitimiert § 100g StPO nur die Anordnung der Herausgabe ohnehin zulässigerweise vorhandener Verbindungsdaten. Weder berechtigt die Norm noch verpflichtet sie den Provider zur Aufzeichnung von Verbindungsdaten, die er nicht schon für Betriebs- oder Abrechnungszwecke rechtmäßigerweise speichert[30]. Das heißt: Ein Tk-Anbieter kann nur verpflichtet werden, solche künftigen Daten herauszugeben, die er sowieso speichert; § 100g gibt keine Rechtsgrundlage, eine darüber hinausgehende Speicherung anzuordnen[31].

Akut wurde gerade diese Fragestellung in Zusammenhang mit dem Anonymisierungsdienst AN.ON, der Nutzern kostenlos zur Verfügung steht und daher auch keine Verbindungsdaten speichert. Auf Antrag des BKA verpflichtete das AG Frankfurt, gestützt auf §§ 100g, h StPO, den Anonymisierungsdienst zur Protokollierung von Verbindungsdaten, um den Besucher einer kinderpornographischen Website zu identifizieren. Mit Beschluss vom 15. 9. 2003 hob das LG Frankfurt[32] die Anordnung auf. Das Landgericht unterstrich, dass die Vorschriften der §§ 100g, h StPO nur die Fälle regeln, in denen Daten grundsätzlich aufgezeichnet und gespeichert werden (dürfen). Anderweitige Protokollierungen von Daten können nur bei Vorliegen der Voraussetzungen einer Telekommunikationsüberwachung, §§ 100a, b StPO angeordnet werden. Daher war auch die nachfolgende Durchsuchungs- und Beschlagnahmeanordnung des Protokolldatensatzes rechtswidrig, weil mit diesen Maßnahmen nicht die Voraussetzungen der §§ 100g, h StPO umgangen werden dürfen[33].

d) Formelle Voraussetzungen

In formeller Hinsicht ist eine schriftliche richterliche Anordnung erforderlich, die nur in Eilfällen „bei Gefahr im Verzug" durch die Staatsanwaltschaft – nicht die Polizei[34] – ersetzt werden kann und dann binnen drei Tagen vom Richter bestätigt werden muss. Enthalten muss die Anordnung Art, Umfang und Dauer der Maßnahme. Das bedeutet für den Regelfall, dass auch Namen und Anschrift des Betroffenen und dessen Rufnummer bzw. Kennung bezeichnet sein müssen. Ausnahmsweise genügt eine „räumlich und zeitlich bestimmte Bezeichnung der Telekommunikation" bei Straftaten von erheblicher Bedeutung, falls deren Aufklärung andernfalls aussichtslos oder wesentlich erschwert wäre. Damit sollen eben die Fälle erfasst werden, in denen Name und Anschrift des Betroffenen gerade erst ermittelt werden sollen[35]. Wie bestimmt diese Anordnung sein muss, hängt von der Schwere der Tat und der Anzahl der möglicherweise betroffenen Unbeteiligten ab.

Auskünfte nach § 100g StPO müssen unverzüglich erteilt werden. Dies fordert das Gesetz nunmehr ausdrücklich, damit ein Ermittlungserfolg nicht durch verspätete Auskünfte gefährdet oder gar vereitelt wird. Ein Verstoß kann mit Zwangsmitteln – Ordnungsgeld und Ordnungshaft – geahndet werden und kann sogar eine Strafbarkeit wegen Strafvereitelung nach sich ziehen[36]. Zu beachten ist, dass nur Verbindungsdaten und keine Inhalte nach §§ 100g, h StPO herausgegeben werden dürfen, neben dem eigentlichen Mailinhalt also auch nicht der „Betreff" und Dateianlagen[37].

Schließlich eröffnet § 100g Abs. 2 auch die Möglichkeit einer Zielwahlsuche. Damit werden Anschlüsse ermittelt, von denen aus eine Telekommunikationsverbindung zum Beschuldigten oder dessen Nachrichtenmittlern aufgebaut wurden. Gestattet ist die Zielwahlsuche jedoch nur, wenn es ansonsten aussichtslos oder wesentlich erschwert wäre, Klarheit über den Sachverhalt oder den Aufenthaltsort des Beschuldigten zu bekommen. Denn diese Maßnahme bedeutet eine besonders schwerwiegenden Eingriff, da die Verbindungsdaten all jener (auch unverdächtiger) Personen einbezogen werden – und ähnlich einer Ras-

26 Hierzu *Bär*, MMR 2002, 358, 359; *Gercke*, Die Speicherung von Nutzungsdaten, DuD 2002, 481.
27 So *Bäumler* in Roßnagel, Teil 8.3, Rn. 60; *Schaar*, Datenschutz bei Web-Service, RDV 2003, 59, 62; *Petri*, Im Schatten des Leviathan – Zum Verhältnis von Sicherheit und Freiheit anhand von Beispielen aus der Tk-Überwachung, RDV 2003, 16, 20; *Bär*, MMR 2002, 358, 359 u. Hinweis auf AG Frankfurt/Main MMR 1999, 428; LG Ulm, B. v. 21. 2. 2002, 2 Qs 2016/02 (jeweils bejahend für die Herausgabe von Verbindungsdaten nach § 12 FAG); *Nack* in KK-StPO, § 100a, Rn. 13, 16.
28 *Petri*, RDV 2003, 16, 20; BGH-Ermittlungsrichter, B. v. 26. 10. 2001, DuD 2001, 759; *Schaar*, RDV 2003, 59, 60.
29 *Meyer-Goßner*, § 100g, Rn. 4, 10.
30 *Bäumler* in Roßnagel, Teil 8.3, Rn. 60; *Eckhardt*, DuD 2002, 197, 201.
31 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD SH), 24. Tätigkeitsbericht 2002, S. 27.
32 LG Frankfurt, Az. 5/6 Qs 47/03.
33 Pressemitteilung des ULDSH v. 4. 11. 2003 zur Entscheidung des LG Frankfurt, Az. 5/8 Qs 26/03, http://www.datenschutzzentrum.de/material/themen/presse/anonip4.htm.
34 *Meyer-Goßner*, § 100h, Rn. 6.
35 *Meyer-Goßner*, § 100h, Rn. 4.
36 *Nack* in KK-StPO, § 100g, Rn. 4.
37 Hamburgerischer Datenschutzbeauftragte, 18. Tätigkeitsbericht 2000/2001, S. 62.

terfahndung abgeglichen werden –, zu denen im fraglichen Zeitraum Tk-Verbindungen hergestellt wurden[38].

Auskunftsersuchen müssen von den Ermittlungsbehörden dem Betroffen nachträglich mitgeteilt werden. Provider sind für entstandene Kosten nach § 17a ZSEG zu entschädigen[39].

2. Auskunft an Nachrichtendienste – § 2 G 10

Seit der Antiterrorgesetzgebung bestehen auch gegenüber Anbietern geschäftsmäßiger Tk-Dienste weitgehende Auskunftsrechte für Nachrichtendienste, also Verfassungsschutzbehörden, BND und MAD, allerdings unter den verfahrensrechtlichen Voraussetzungen des Gesetzes zu Artikel 10 GG. Die Auskunftsbefugnisse erstrecken sich auf Telekommunikations-Verbindungsdaten sowie auf Nutzungsdaten von Telediensten auch künftiger Kommunikation oder Nutzung; insofern gehen sie über § 100g StPO hinaus.

Auskunftsverpflichtungen bestehen bei tatsächlichen Anhaltspunkten für schwerwiegende sicherheitsgefährdende oder geheimdienstliche Tätigkeiten. Sie sind auch legitimiert zum Schutz vor Bestrebungen, durch Gewaltanwendung auswärtige Belange der Bundesrepublik zu gefährden sowie bei Bestrebungen, die den Gedanken der Völkerverständigung verletzen. Die Einzelheiten ergeben sich für den militärischen Abschirmdienst aus § 10 Abs. 3 MADG, für den Bundesnachrichtendienst aus § 8 Abs. 3a BNDG, für den Verfassungsschutz der Länder aus den jeweiligen Landesgesetzen und für den Verfassungsschutz des Bundes aus dem Bundesverfassungsschutzgesetz (BVerfSchG), das in § 8 Abs. 5–12 eine Reihe weiterer, umfassender Auskunftsverpflichtungen enthält. Auf Antrag des Präsidenten des Bundesamtes, über den ein besonders beauftragtes Ministerium zu entscheiden hat, können Finanzdienstleistungsinstitute, Postdienstleistungsunternehmen, Luftfahrt- und Telekommunikationsunternehmen zu umfassenden Auskünften verpflichtet werden. Dabei beziehen sich die Auskunftsverpflichtungen immer auf einen Einzelfall und legitimieren nicht die Übermittlung ganzer Datenbestände[40].

III. Auskunft über Bestandsdaten

Bestandsdaten dürfen für die Vertragsabwicklung erhoben und gespeichert werden und unterliegen nicht dem Fernmeldegeheimnis. Typischerweise beinhalten sie Name, Vorname und Anschrift des Nutzers, Geburtsdatum, Bankverbindung oder eine statische IP-Adresse. Besonders wichtig in der Praxis sind die Auskunftsbefugnisse für Sicherheitsbehörden nach § 113 TKG und das automatisierte Abrufverfahren nach § 112 TKG; aufgrund ihrer Aktualität haben diese für Sicherheitsbehörden den „Charakter eines zweiten Melderegisters"[41]. Das manuelle Auskunftsverfahren gilt für geschäftsmäßige Tk-Anbieter; während das automatisierte Abrufverfahren für Anbieter von öffentlichen Tk-Diensten gilt.

1. Auskunft nach § 113 TKG

Nach § 113 TKG besteht für geschäftsmäßige Tk-Anbieter die Pflicht, den Strafverfolgungs- und Sicherheitsbehörden im Einzelfall Bestandsdaten zu übermitteln, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Gefahrenabwehr oder zur Erfüllung ihrer Aufgaben erforderlich ist. Für dieses „vereinfachte Auskunftsverfahren" ist ein richterlicher Beschluss nicht notwendig. Ausreichend ist ein Ersuchen von Polizeibehörden, Staatsanwaltschaften, Bußgeldbehörden[42], Verfassungsschutzbehörden des Bundes und der Länder, BND, MAD oder Zollkriminalamt.

Die Vorschrift erlaubt jedoch keineswegs, sämtliche vorhandenen Bestandsdaten anzufordern. Auskunft kann vielmehr nur über die Daten mit besonderem Telekommunikationsbezug verlangt werden wie Name und Anschrift des Nutzers. Nicht zulässig sind Abfragen etwa von Bankverbindungen des Nutzers, Beruf, eventuelle Mahnungen oder die Zugehörigkeit zu einer bestimmten gesellschaftlichen Gruppe, der ein Sondertarif eingeräumt ist[43]. Auskünfte über solche Daten dürfen nur aufgrund einer – anderweitigen – Rechtsgrundlage herausverlangt werden, die dieses Auskunftsbegehren stützt. Auch bei Bagatelldelikten ist eine Auskunft nicht gerechtfertigt[44]. Der Aufwand der TK-Dienste wird nach dem ZSEG erstattet. Der Betroffene darf nicht über die Auskünfte an Sicherheitsbehörden informiert werden.

Geschäftsmäßige Tk-Anbieter haben auf Ersuchen der zuständigen Stellen unverzüglich Auskunft zu erteilen
- über die gespeicherten Bestandsdaten (§ 95 TKG), die sie zur Vertragsabwicklung speichern dürfen (entspricht der bisherigen Regelung in § 89 Abs. 6 TKG)
- und die Daten, die sie im Rahmen der neu eingeführten Speicherpflicht des § 111 TKG speichern müssen. Diese Pflicht dient der Identifizierung der Nutzer und umfasst Namen und Anschrift des Rufnummerninhabers, Geburtsdatum, Vertragsbeginn und ggf. Vertragsende.

Die zuständigen Stellen dürfen diese Auskünfte verlangen, soweit dies erforderlich ist
- für die Verfolgung von Straftaten oder Ordnungswidrigkeiten,
- zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung
- oder für die Erfüllung der gesetzlichen Aufgaben der Bundes- und Landes-verfassungsschutzbehörden, des BND oder des MAD.

Neu ist, dass Tk-Anbieter auch Zugriffsdaten, die Inhalte oder Umstände der Telekommunikation schützen, auf Ersuchen mitteilen müssen; d.h. insbesondere Passwörter, PIN und PUK. Auskunftsberechtigt sind insoweit:
- Strafverfolger im Rahmen ihrer Ermittlungen, § 161 Abs. 1 Satz 1, § 163 Abs. 1 StPO,
- Polizei zur Gefahrenabwehr entsprechend den Bundes- und Landesgesetzen,
- Verfassungsschutz gemäß den Verfassungsschutzgesetzen des Bundes (§ 8 Abs. 1) bzw. der Länder,
- der BND gemäß § 2 Abs. 1 BNDG sowie
- der MAD nach Maßgabe von § 4 Abs. 1 MADG.

Verbleibt es bei dieser Regelung, müssen Zugangskennungen ohne richterlichen Beschluss und auf bloßes Verlangen der berechtigten Stellen herausgegeben werden. Zu beachten ist dabei, dass für alle „dahinter stehenden" Verbindungsdaten eine gesonderte Anordnung erforderlich ist, die die Voraussetzungen der einschlägigen Befugnisnorm erfüllt (z.B. §§ 100g, h StPO). An andere öffentliche oder nicht öffentliche Stellen dürfen diese Daten nicht übermittelt werden.

Für entstehende Kosten ist eine Entschädigung entsprechend § 17a ZSEG vorgesehen; Betroffene selbst dürfen über die Auskunft nicht informiert werden.

2. Auskunft aus Kundendateien

Das alte TKG sah in § 90 Abs. 1 eine Pflicht für Anbieter geschäftsmäßiger Tk-Dienste vor, Kundendateien elektronisch verfügbar zu halten. Zu speichern waren insbesondere Namen und Anschriften, Rufnummern und Rufnummernkontingente.

38 BVerfG, wistra 2003, 217, 222 f. = JurPC Web-Dok. 101/2003, Abs. 72 ff.; *Meyer-Goßner*, § 100g, Rn. 11.
39 *Meyer-Goßner*, § 100h, Rn. 6.
40 *Rublack*, Terrorismusbekämpfungsgesetz: Neue Befugnisse für die Sicherheitsbehörden, DuD 2002, 203.
41 *Bizer*, Auskunftspflichten über Bestandsdaten, DuD 2002, 429.
42 *Schaar*, RDV 2003, 59, 60.
43 *Bizer*, DuD 2002, 429; BfD, Materialien, Ziff. 4.6.1.
44 *Bizer*, DuD 2002, 429.

Die Sicherheitsbehörden hatten auf das Kundenverzeichnis über die Regulierungsbehörde für Post und Telekommunikation (RegTP) einen unentgeltlichen Online-Zugriff zur Erfüllung ihrer Aufgaben[45]. Adressat des § 90 TKG waren zwar alle geschäftsmäßigen Tk-Anbieter, jedoch war die Norm auf Access- und Host-Provider nur eingeschränkt anwendbar, da diese keine Rufnummern vergeben; IP-Adressen zählen nicht zu den zu registrierenden Rufnummern[46].

Nach der Neuregelung des TKG beschränkt sich das automatisierte Abrufverfahren auf Anbieter öffentlicher Tk-Dienste, § 112 TKG. Diese unterliegen ebenfalls der Speicherpflicht hinsichtlich der Identifizierungsdaten, § 111 TKG. Die Daten sind in die zu führenden Kundendateien aufzunehmen und für das automatisierte Abrufverfahren bereit zu halten. Der Kreis der Abfrageberechtigten wurde erheblich ausgeweitet und bezieht nun auch Notrufabfragestellen, die Bundesanstalt für Finanzdienstleistungsaufsicht und Behörden ein, die für die Bekämpfung von Schwarzarbeit zuständig sind.

IV. Zugriff innerhalb allgemeiner strafprozessualer Befugnisse

Beim Anfangsverdacht einer Straftat, d.h. wenn nach den kriminalistischen Erfahrungen eine verfolgbare Straftat möglich erscheint, muss ein Ermittlungsverfahren eingeleitet werden. Die Staatsanwaltschaft hat zur Aufklärung des Sachverhalts belastende wie entlastende Umstände zu erforschen. Im Rahmen ihrer allgemeinen strafprozessualen Befugnisse, vor allem Zeugenbefragung, Durchsuchung und Beschlagnahme, kann sie auch auf Bestandsdaten der Telekommunikation zugreifen. Verbindungsdaten und Inhalte der Telekommunikation bleiben hiervon ausgenommen, da sie vom Fernmeldegeheimnis geschützt sind und nur über die speziellen Eingriffsnormen des §§ 100a, b StPO – für Inhalte – und §§ 100g, h StPO herausgegeben werden und herausverlangt werden dürfen[47].

1. Auskunft im Ermittlungsverfahren, §§ 161, 160 StPO

§§ 160 ff. StPO schaffen die rechtliche Grundlage für umfassende Ermittlungstätigkeiten von Polizei und Staatsanwalt im Ermittlungsverfahren. Insbesondere gibt § 161 Abs. 1 StPO einen Auskunftsanspruch gegen Behörden und damit gegen Stellen, die öffentliche Aufgaben wahrnehmen. Hierzu gehören auch Hochschulrechenzentren und öffentlich geförderte Forschungseinrichtungen. Die Auskunft ist auch hier auf Bestandsdaten beschränkt.

Nach dem neu überarbeiteten TKG soll sich die Auskunftsberechtigung (§ 111 TKG) nicht nur auf Bestandsdaten erstrecken, sondern auch auf die Daten, die im Rahmen der neuen Identifizierungspflicht (§ 109 TKG) gespeichert werden müssen. Darüber hinaus können im Rahmen von Ermittlungsverfahren auch Zugangskennungen wie Passwörter, PIN und PUK abgefragt werden.

2. Durchsuchung

Die Durchsuchung (§§ 102 ff. StPO) dient dem gezielten Auffinden von Beweismitteln, um diese anschließend durch eine Beschlagnahme (§§ 94 ff. StPO) amtlich sicherzustellen. In Betracht kommen auch Daten und Datenträger. In der Praxis von Providern erscheinen Durchsuchung und Beschlagnahme meist als einheitlicher Vorgang. Tatsächlich handelt es sich dabei um zwei häufig aufeinander folgende Akte, die auf unterschiedlichem Rechtsgrund beruhen und gegen die auch gesondert Rechtsmittel eingelegt werden kann[48]. Eine Beschlagnahmeanordnung ist beispielsweise nicht vonnöten, wenn ein Gegenstand freiwillig herausgegeben wird[49]. Zulässig ist eine Durchsuchung nicht nur von Wohnung, Räumen, Person und Sachen des Verdächtigen (§ 102 StPO), sondern auch von unbeteiligten Dritten (§ 103 StPO), sofern Tatsachen dafür vorliegen, dass die Durchsuchung dort zum Auffinden der gesuchten Beweismittel führt.

In formeller Hinsicht muss eine schriftliche richterliche Anordnung vorliegen. Lediglich in Eilfällen, wenn die vorherige Einholung eines richterlichen Durchsuchungsbeschlusses den Zweck der Durchsuchung gefährden würde, können Staatsanwaltschaft und Polizei zunächst ohne Einschaltung eines Richters tätig werden[50]. Eine richterliche Durchsuchungsanordnung bleibt sechs Monate in Kraft; binnen dieser Zeit muss die Durchsuchung vorgenommen werden[51].

In der Anordnung sind Zweck und Ziel der Maßnahme und die betroffenen Räumlichkeiten genau zu bezeichnen. Das bedeutet, dass sich der Zugriff auf Datenspeicher innerhalb der genannten Räume beschränken muss und ein Online-Zugriff auf Daten außerhalb der im Durchsuchungsbefehl genannten Räumlichkeit nicht zulässig ist[52]. Allerdings kann die Anordnung jederzeit – bei Gefahr in Verzug auch vor Ort durch Polizei oder Staatsanwaltschaft – erweitert werden, wenn sich beispielsweise EDV-Anlagen in anderen als den angegebenen Räumen befinden.

Bei einer Durchsuchung nach Daten in einem Netzwerk muss unterschieden werden: Eine Durchsuchung auf Daten in einem lokalen Netzwerk, beispielsweise innerhalb der Online-Verbindungen eines Betriebes, ist problemlos möglich. Anders verhält es sich, wenn nach Daten durchsucht wird, ohne dass dabei der Standort des Servers bekannt ist. Denn das Gesetz verlangt eine genaue Bezeichnung der „Räume"; die Anordnung einer Durchsuchung nach Datenbeständen innerhalb Deutschlands wäre unverhältnismäßig[53]. Deshalb wäre eine derartige Anordnung unzulässig; gegebenenfalls muss der Zielrechner aufgrund einer Anordnung nach §§ 100g, h StPO vorab ermittelt werden.

Bei allen strafprozessualen Maßnahem ist der Verhältnismäßigkeitsgrundsatz zu beachten, der unangemessen gravierende Eingriffe verbietet bzw. die Wahl des am wenigsten einschneidenden Mittels gebietet[54]. Als unverhältnismäßig und damit rechtswidrig hat beispielsweise das LG Stuttgart[55] die Wohnungsdurchsuchung bei einem Host – Provider angesehen, in der sich der Internet-Server mit verdächtigen Website-Inhalten von Kunden befand. Denn an Stelle einer Durchsuchung hätten die Polizeibehörden den Provider zunächst über die verdächtigen Inhalte in Kenntnis setzen und ihn zur Sperrung auffordern müssen. Nur im Falle der Nichtbefolgung hätte die weitergehende Maßnahme einer Durchsuchung stattfinden dürfen.

---

45 VG Darmstadt, NJW 2001, 2273, 2374.
46 *Ehmer* in Büchner/Ehmer/Geppert, § 90 TKG, Rn. 4; *Hoeren/Sieber/Sieber*, Teil 19, Rn. 722; Rote Karte für Internetschnüffler, hrsg. vom ULD SH, abrufbar unter www.datenschutzzentrum.de/material/themen/rotekarte/info.htm, Ziff. 1.6.
47 *Meyer-Goßner*, § 161, Rn. 18 und Rn. 13 zu § 99; *Dembowski* in Roßnagel, Teil 8.1, Rn. 35; so auch die Begründung zum TKG vom 17. 10. 2003, Teil 7, Abschnitt 1, § 86, BT-Drs. 15/2316.
48 BGH, wistra 1995, 348 = NJW 1995, 3397.
49 *Meyer-Goßner*, § 94, Rn. 12.
50 BverfG, wistra 2001, 137, 140 = NJW 2001, 1121, 1123.
51 BverfG, wistra 1997, 223 = NJW 1997, 2165.
52 *Hoeren/Sieber/Sieber*, Teil 19, Rn. 688 mwN.
53 Über die Bezeichnung des Ausmaßes der Durchsuchungsanordnung vgl. etwa BVerfGE 20, 162, 227; 42, 212, 221; 44, 353, 371; BVerfG, wistra 1992, 60 = NStZ 1992, S. 91.
54 *Hoeren/Sieber/Sieber*, Teil 19, Rn. 685.
55 LG Stuttgart, B. v. 7.5.2001, zitiert in *Sakowski*, E-Mail (II), http://www.sakowski.de/onl-r/onl-r53.html.

3. Beschlagnahme

Als Beschlagnahme wird der Akt der amtlichen Sicherstellung von Gegenständen bezeichnet, die potentiell als Beweismittel für ein Strafverfahren relevant sind. Hat eine Person Gewahrsam an einem solchen Gegenstand und gibt ihn nicht freiwillig heraus, so muss er im Wege der Beschlagnahme zwangsweise sichergestellt werden.

Dazu ist eine schriftliche Anordnung durch einen Richter erforderlich, in Eilfällen ist eine Beschlagnahmeanordnung aber auch durch Staatsanwaltschaft oder Polizei zunächst in mündlicher, telefonischer oder fernschriftlicher Form möglich[56]. Beschlagnahmt werden können auch Daten, indem der entsprechende Datenträger sichergestellt wird oder die Daten direkt an den Computer der Staatsanwaltschaft übermittelt werden[57]. Dies gilt auch für Bestandsdaten. Bei Daten, die dem Fernmeldegeheimnis unterliegen – Inhalte und Verbindungsdaten –, richtet sich die Herausgabe nach den spezielleren Regelungen der §§ 100a, b und 100g, h StPO. Liegen deren enge Voraussetzungen nicht vor, so darf auch keine Durchsuchungs- und Beschlagnahmeanordnung ergehen, um die Daten zu erlangen. Dies bestätigte auch das LG Frankfurt[58] in seinem Beschluss zum Fall des Anonymisierungsdienst AN.ON, bei dem ein Protokolldatensatz beschlagnahmt worden war, der dem Tk-Geheimnis unterlag (Verbindungsdaten), obwohl die Voraussetzungen der §§ 100g, h StPO nicht gegeben waren[59].

Geht es um die Beschlagnahme von E-Mails, so werden drei Phasen unterschieden[60]: Das Versenden der Mail vom Absender bis zum Ankommen an der Mailbox des Empfängers (Phase 1), die Zwischenspeicherung in der Mailbox, also auf dem Server des Empfänger-Providers (Phase 2) und das Abrufen der Mail bis zum Empfänger (Phase 3).

(1) Solange sich eine Mail auf dem Transportweg befindet, greift nach einhelliger Auffassung in Rechtsprechung[61] und Literatur[62] der Schutz des Tk-Geheimnisses. Das heißt, eine Beschlagnahme darf ausschließlich unter den Voraussetzungen der §§ 100a, b StPO angeordnet werden. Dies betrifft jedenfalls die Übermittlung als solche und damit den Weg vom Absender über seinen Provider bis zur Speicherung in der Mailbox (Phase 1) und beim Abruf den Weg von der Mailbox bis zum Empfänger (Phase 3).

(2) Umstritten ist aber, ob der besondere Schutz des Tk-Geheimnisses auch für Mails in der Mailbox des Betreibers gilt[63]. Dies ist bedeutsam für die Folgefrage, auf welcher Rechtsgrundlage und damit unter welchen Voraussetzungen die Beschlagnahme von E-Mails während der Zwischenspeicherung beim Empfänger-Provider angeordnet werden darf.

Das LG Hanau[64] und das LG Mannheim[65] rechnen auch die Zwischenspeicherung in der Mailbox des Empfänger-Providers zum Übermittlungsvorgang und betrachten die Versendung von Mails als einheitlichen Kommunikationsvorgang. Nach dieser Ansicht[66] stellt jede Beschlagnahme von Mails – auch bei Zwischenspeicherung in der Mailbox – eine Tk-Überwachung dar, die nur entsprechend §§ 100a, b StPO zulässig ist (d.h. bei richterlicher Anordnung wegen einer Katalogtat i.S. des § 100a StPO). Der Übermittlungsvorgang sei erst mit dem Herunterladen der Mails beim Nutzer beendet[67]. Eine Beschlagnahme scheide aus, weil die Beschlagnahmevorschriften nicht ausdrücklich auf das Tk-Geheimnis Bezug nehmen, wie es § 85 Abs. 3 S. 3 TKG bei einer Einschränkung des Fernmeldegeheimnisses fordert[68].

Abweichend hiervon hält das LG Ravensburg[69] das Tk-Geheimnis nicht für anwendbar. In der Mailbox befindliche Mails seien mit einer postlagernden Briefzustellung vergleichbar und daher entsprechend einer Postbeschlagnahme (§ 99 StPO) zu behandeln. Danach dürfen Postsendungen im Gewahrsam geschäftsmäßiger Post- und Telekommunikationsanbieter beschlagnahmt werden, soweit eine richterliche (in Eilfällen staatsanwaltschaftliche) Anordnung vorliegt, wobei es auf ein schweres Delikt wie im Straftatenkatalog des § 100a StPO nicht ankommt. Ähnlich wird teilweise eine Beschlagnahme gemäß § 94 StPO für zulässig gehalten[70].

V. Auskünfte an Polizei zur Verhinderung zukünftiger Straftaten

Ein Auskunftsverlangen über Nutzerdaten kann der Verhinderung künftiger Straftaten und der Abwehr drohender Gefahren dienen. Die Befugnisse der zur Gefahrenabwehr zuständigen Behörden, insbesondere der Polizei[71], ergeben sich in erster Linie aus den Polizei- bzw. Gefahrenabwehrgesetzen der jeweiligen Bundesländer[72]. Spezielle präventive Befugnisse bestehen auch für das Bundeskriminalamt (im BKAG[73]), Verfassungsschutz (im BVerfSchG), den militärischen Abschirmdienst (im MADG), und das Zollkriminalamt (im AWG) und im BGSG[74]. Der Polizei stehen dabei eine Fülle von Datenerhebungsbefugnissen für Zwecke der Vorbeugung zur Verfügung, die neben Auskunftsverlangen beispielsweise auch die Rasterfahndung – allerdings keine Tk-Überwachung – umfassen[75]. Aufgrund des vorbeugenden Charakters der Maßnahmen ist nicht nur der Kreis der Betroffenen – u.a. Verdächtige, mögliche Straftäter, Kontaktpersonen, potentielle Opfer – sehr weit, sondern auch Art und Profil der betroffenen Daten; eine Erhebung muss jedoch immer verhältnismäßig sein[76]. Eine Auskunft über Verbindungsdaten erfordert eine spezielle Ermächtigungsgrundlage, die sich ausdrücklich auf Tk-Vorgänge bezieht, da Verbindungsdaten dem Fernmeldegeheimnis unterliegen. Eine allgemeine ordnungsbehördliche Generalklausel oder der Verweis auf die Amtshilfe genügt dem nicht.

VI. Eigene Übermittlungen an Strafverfolgungsbehörden

Von der Auskunftspflicht abzugrenzen ist die Frage, ob Rechenzentrumsmitarbeiter bei einem konkreten Verdacht einer Straftat von sich aus Daten an Strafverfolgungsbehörden übermitteln

56 *Meyer-Goßner*, § 98, Rn. 8.
57 *Meyer-Goßner*, § 94, Rn. 16 a mwN.
58 Pressemitteilung des Datenschutzzentrums 4. 11. 2003 zur Entscheidung des LG Frankfurt, Az. 5/8 Qs 26/03, http://www.datenschutzzentrum.de/material/themen/presse/anonip4.htm.
59 Siehe dazu auch die Besprechung von Krasemann, JurPC Web-Dok. 140/2004, abrufbar unter http://www.jurpc.de/aufsatz/20040140.htm.
60 LG Ravensburg, MMR 2003, 679; *Bär*, Anm. zu LG Ravensburg, MMR 2003, 681; *Nack* in KK-StPO, § 100a, Rn. 8; *Meyer-Goßner*, § 100a, Rn. 2.
61 BGH, NJW 1997, 1934; LG Hanau, NJW 1999, 3647.
62 *Meyer-Goßner*, § 100a, Rn. 2; *Nack* in Karlsruher Kommentar, § 100a, Rn. 8; *Bär* MMR 2003, 680 mwN.
63 Bejahend BGH, NJW 1997, 1934.
64 LG Hanau, NJW 1999, 3647.
65 LG Mannheim, StV 2002, 242.
66 Zustimmend *Meyer-Goßner*, § 100a, Rn. 2.
67 LG Hanau, NJW 1999, 3647.
68 *Büchner* in Büchner/Ehmer/Geppert, § 85 TKG, Rn. 16.
69 LG Ravensburg, MMR 2003, 679.
70 *Bär*, Anm. zu LG Ravensburg, MMR 2003, 681; *Nack* in KK-StPO, § 100a, Rn. 8.
71 Siehe hierzu *Bäumler* in Roßnagel, Teil 8.3, Rn. 17 ff.
72 Siehe etwa §§ 27 ff. BrPolG, §§ 13 ff. HSOG, §§ 9 ff. PolGNW, §§ 25a ff. PolGRhPf, 3 25 ff. SPolG.
73 Z.B. §§ 5,6 BKAG.
74 §§ 1 ff. BGSG.
75 *Bäumler* in Roßnagel, Teil 8.3, Rn. 21, 34.
76 *Bäumler* in Roßnagel, Teil 8.3, Rn. 26.

dürfen. Mangels einer Befugnis in den Online-Datenschutzgesetzen – TKG, TDSV und TDDSG/MDStV – muss eine Übermittlung durch die allgemeinen Datenschutznormen im BDSG bzw. für Hochschulen im jeweiligen LDSG legitimiert sein. Zwar lassen die Datenschutzgesetze die zweckentfremdende Nutzung personenbezogener Daten für Strafverfolgung und Gefahrenabwehr mehr oder weniger pauschal zu[77]. Das BDSG erlaubt die Unterrichtung der Polizei durch öffentliche Stellen in § 14 Abs. 2 Nr. 6, 7, 8, durch nicht-öffentliche Stellen in § 28 Abs. 3 S. 1 Nr. 2. Parallelregelungen finden sich in zahlreichen Landesdatenschutzgesetzen[78], so z.B. §§ 13 Abs. 2 Satz 1 d), h), 14 DSG NW, §§ 11 Abs. 2 Satz 1 Nr. 2 und 3, 12 BerlinerDSG oder §§ 13 Abs. 2, 12 Abs. 2 Nr.4 HDSG. Allerdings beziehen sich diese Gesetze durchwegs auf „Offline-Daten"; problematisch ist bereits, ob diese Erlaubnisnormen auf „Online-Daten", also Daten der Telekommunikation oder der Dienstenutzung, überhaupt anwendbar sind. Jedenfalls aber bedeutet eine solche Datenübermittlung eine Zweckentfremdung, die im Hinblick auf das informationelle Selbstbestimmungsrecht des Betroffenen erforderlich und verhältnismäßig sein und daher sorgfältig abgewogen werden muss[79]. Zu bedenken ist schließlich, dass – anders als bei einer Anfrage durch die Strafverfolgungsbehörden – bei einer eigeninitiierten Datenweitergabe an die Behörden die Verantwortlichkeit allein bei der übermittelnden Stelle liegt. Damit haftet ausschließlich das übermittelnde Rechenzentrum für die Zulässigkeit der Datenweiterleitung[80].

Regelmäßig empfiehlt sich daher, zunächst den Sicherheitsbehörden lediglich einen konkreten Tatverdacht mitzuteilen, ohne dabei personenbezogene Daten weiterzuleiten. Dadurch wird die zuständige Behörde in die Lage versetzt, weitere Ermittlungsschritte wie beispielsweise eine Auskunftsanordnung einzuleiten[81]. Die Verantwortlichkeit für die Datenübermittlung trägt dann die ersuchende Stelle. Keinesfalls sollten Rechenzentren selbsttätig Ermittlungen anstellen. Hierzu sind sie weder verpflichtet noch befugt[82]. Allenfalls können und sollten vorhandene Daten zu Beweiszwecken, durch Ausdruck oder Speicherung, gesichert werden oder Mitarbeiter als Zeugen hinzugezogen werden.

VII. Zusammenfassung der Neuregelungen zur Tk-Überwachung

Die Neuordnung des Telekommunikationsrechts – bei der u.a. TKG und TDSV zusammengefasst werden – bringt auch einige Änderungen im Bereich der Tk-Überwachung mit sich. Beispielsweise trifft jetzt alle Tk-Anbieter die Pflicht zur Speicherung bestimmter Daten wie Namen und Anschrift (ggf. Geburtsdatum) des Nutzers, Anschlusslage und Vertragsbeginn und -ende (§ 111 TKG). Diese Daten müssen von allen Tk-Dienstleistern im Hinblick auf Auskunftsersuchen der Sicherheitsbehörden erhoben und gespeichert werden.

Gestrichen wurde in letzter Minute der Vorstoß des Bundesrats, auch eine Vorratsdatenspeicherung von Verbindungsdaten einzuführen, um auch diese Daten binnen eines Zeitraums von jedenfalls sechs Monaten für Zwecke von Strafverfolgung und Gefahrenabwehr greifbar zu haben.

Die wichtigsten Neuerungen betreffen kurz zusammengefasst:

1. Technische Umsetzung von Überwachungsmaßnahmen

Nach § 110 TKG hat jeder Anlagenbetreiber auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlicher Tk-Überwachungsmaßnahmen vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen. Anders als bisher in der TKÜV geregelt, wären damit nicht nur öffentliche Tk-Anbieter betroffen.

2. Daten für Auskunftsersuchen der Sicherheitsbehörden

In § 111 TKG neu eingeführt wird die Verpflichtung aller Tk-Anbieter, vor der Dienstfreischaltung folgende Daten zu erheben und unverzüglich zu speichern:
- Namen und die Anschrift des Rufnummerninhabers,
- bei natürlichen Personen deren Geburtsdatum,
- bei Festnetzanschlüssen auch die Anschrift des Anschlusses sowie
- das Datum des Vertragsbeginns und
- ggf. das Datum des Vertragsendes.

Die Speicherpflicht besteht unabhängig von der Befugnis der Tk-Anbieter (§ 95 TKG), für Vertragszwecke die erforderlichen Bestandsdaten zu erheben und dient der Identifizierung der Nutzer (erfasst damit insbesondere Prepaid-Kunden). Anbieter öffentlicher Tk-Dienste müssen die Daten in den zu führenden Kundendateien für das automatisierte Abrufverfahren (§ 112 TKG) vorhalten. Nicht-öffentliche Anbieter haben die Daten für einen manuellen Abruf (§ 113 TKG) zu speichern. Bei Verträgen, die beim Inkrafttreten der Regelung bereits bestehen, müssen die Daten nicht nachträglich erhoben werden. Erhebung, Speicherung und Aktualisierungen erfolgen auf eigene Kosten der Provider. Die Daten müssen auch bei der Vermarktung über Vertriebspartner erhoben werden. Gelöscht werden dürfen die Daten erst zum Ende des Jahres, das auf den Vertragsablauf folgt, damit die Auskunftsberechtigten noch nach Vertragsende auf die Daten zugreifen können.

3. Automatisiertes Abrufverfahren

Anbieter öffentlicher Tk-Dienste nehmen am automatisierten Auskunftsverfahren teil, bei dem die Abhörer selbst auf die Daten zugreifen können (§ 112 TKG). Zu den verfügbaren Daten, die in Kundendateien geführt werden müssen, zählen jetzt auch die Daten, die nach Maßgabe von § 111 TKG gespeichert werden müssen. Der Kreis der Auskunftsberechtigten wurde erweitert und umfasst nunmehr nicht nur Gerichte und Strafverfolgungsbehörden sowie Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr, sondern auch Zollkriminalamt und Zollfahndungsämter für Zwecke eines Strafverfahrens sowie das Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 39 des AWG, ferner die Verfassungsschutzbehörden des Bundes und der Länder, MAD und BND. Ferner sind im Rahmen ihrer Aufgaben zur Abfrage berechtigt die Notrufabfragestellen, die Bundesanstalt für Finanzdienstleistungsaufsicht sowie Behörden ihm Rahmen der Schwarzarbeitsbekämpfung.

Ausgeweitet werden die Abfragemöglichkeiten ferner durch die nun zulässige sog. Jokerabfrage, d.h. von Abrufen unter Verwendung von Platzhaltern.

4. Manuelles Auskunftsverfahren

Für geschäftsmäßige Tk-Anbieter gilt das manuelle Auskunftsverfahren des § 113 TKG, der den bisherigen Auskunftsanspruch nach § 89 Abs. 6 TKG ersetzt und erweitert. Im Einzelfall haben geschäftsmäßige Anbieter auf Ersuchen der zuständigen Stellen unverzüglich Auskünfte zu erteilen über
- die gespeicherten Bestandsdaten (§ 95 TKG), die sie zur Vertragsabwicklung speichern dürfen,

77 *Bäumler* in Roßnagel, Teil 8.3, Rn. 1.
78 *Simitis* in Simitis, BDSG, 5. Aufl., § 14, Rn. 79; *Globig* in Roßnagel, Teil 4.7, Rn. 104.
79 *Simitis* in Simitis, § 14, Rn. 80.
80 *Globig* in Roßnagel, Teil 4.7, Rn. 104.
81 *Simitis* in Simitis, § 14, Rn. 80.
82 *Simitis* in Simitis, § 14, Rn. 80.

- und die Daten, die sie im Rahmen der Identifizierungspflicht (§ 111 TKG) speichern müssen (Name und Anschrift des Rufnummerninhabers, Geburtsdatum, Vertragsbeginn, Vertragsende).

Diese Auskünfte dürfen verlangt werden, soweit dies erforderlich ist
- für die Verfolgung von Straftaten oder Ordnungswidrigkeiten,
- zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung
- oder für die Erfüllung der gesetzlichen Aufgaben der Bundes- und Landes-verfassungsschutzbehörden, des BND oder des MAD.

Neu ist auch eine Auskunftspflicht zu Daten, mittels derer der Zugriff auf Inhalte oder auf Umstände der Telekommunikation geschützt ist, d.h. insbesondere Passwörter, PIN und PUK. Auskunftsberechtigt sind insoweit:
- Strafverfolger im Rahmen ihrer Ermittlungen, § 161 Abs. 1 Satz 1, § 163 Abs. 1 StPO,
- Polizei zur Gefahrenabwehr entsprechend den Bundes- und Landesgesetzen,
- Verfassungsschutz, nach den Verfassungsschutzgesetzen des Bundes (§ 8 Abs. 1) bzw. der Länder,
- der BND gemäß § 2 Abs. 1 BNDG sowie
- der MAD nach Maßgabe von § 4 Abs. 1 MADG.

An andere öffentliche oder nicht öffentliche Stellen dürfen diese Daten nicht übermittelt werden. Zu beachten ist, dass für alle „dahinter stehenden" Verbindungsdaten bzw. alle weiteren Verbindungsdaten eine gesonderte Anordnung erforderlich ist, die die Voraussetzungen der einschlägigen Befugnisnorm erfüllt.

Für entstehende Kosten wird eine Entschädigung entsprechend § 17a ZSEG gewährt; Betroffene selbst dürfen über die Auskunft nicht informiert werden.

Wissenschaftlicher Assistent Karsten Gaede, Universitäten Cambridge/Zürich
Wissenschaftlicher Mitarbeiter Tilo Mühlbauer, Universität Dresden

Wirtschaftsstrafrecht zwischen europäischem Primärrecht, Verfassungsrecht und der richtlinienkonformen Auslegung am Beispiel des Scalping

– zugleich Besprechung von BGH wistra 2004, 109 –

Die Autoren treten der Geringschätzung des primären Europarechts und des Verfassungsrechts bei der im Wirtschaftsstrafrecht vermehrt relevanten richtlinienkonformen Auslegung deutscher Strafgesetze entgegen. Der Beitrag kritisiert eine dem Europarecht widersprechende Begründungsmethodik des BGH, die den Schutzbereich der Insiderhandelsverbote unzulässig verkürzt. Beanstandet wird auch die systematische Konfusion der heutigen Verbots- und Sanktionsvorschriften des WpHG im Bereich der Marktmanipulation und der Offenbarungspflichten bei Finanzanalysen sowie das Votum des BGH für die verfassungsmäßige Bestimmtheit der §§ 20a I 1 Nr. 2, 38 I Nr. 4 WpHG. Abschließend wird die Ausblendung richtlinienexterner Legitimitätsmaßstäbe auch des europäischen Rechts, wie etwa der Meinungsfreiheit, gerügt.

A. Einleitung*

Mit dem vorbenannten Urteil wollte der erste Strafsenat des BGH eine klärende Grundsatzentscheidung zum Kapitalmarktphänomen des Scalping treffen.[1] Unter Scalping versteht der BGH die „Vorgehensweise, Wertpapiere in der Absicht zu erwerben, diese anschließend zum Kauf zu empfehlen, um sie dann bei steigendem Kurs – infolge der Empfehlung – mit Gewinn wieder zu verkaufen". Für das Gericht gilt es auf Grund einer richtlinienkonformen Auslegung des WpHG als ausgemacht, dass Scalping selbst bei objektiv vertretbaren Empfehlungen einen Fall der Kurs- und Marktmanipulation (§ 20a I 1 Nr. 2 WpHG) darstellt, nicht hingegen als Insiderhandel (§ 14 I 1 Nr. 1 WpHG) strafbewehrt ist. Das Urteil hat Zustimmung,[2] aber auch bereits Kritik erfahren.[3] Tatsächlich kann der BGH weder verfassungsrechtlich noch europarechtlich überzeugen. Methodologische Schwächen und die Ausblendung des primären Gemeinschaftsrechts machen das Urteil zu einem Musterbeispiel für eine defizitäre richtlinienkonforme Auslegung des deutschen Strafrechts. Die Ausräumung dieser Defizite ist umso mehr angezeigt, als die infolge des Urteilsansatzes drohende Fehlentwicklung über die Frage des Scalping weit hinausreicht: Es droht sowohl die unbegründete Verkürzung des Kapitalmarktschutzes (§ 14 WpHG) als auch seine Entgrenzung (§ 20a WpHG).

B. Die Verwerfung des Insiderhandels

Der BGH nahm davon Kenntnis, dass das Schrifttum hinsichtlich der strafrechtlichen Behandlung des Scalping divergiert: Von der vorherrschenden Erfassung über §§ 14 I Nr. 1, 38 I Nr. 1 WpHG,[4] der Einstufung unter §§ 20a I Nr. 2, 39 I Nr. 2, 38 I

* Zitathinweise: HRRS bezieht sich auf die Referenzausgabe der Onlinezeitschrift unter www.hrr-strafrecht.de. EGMR-Entscheidungen werden mit Prozessgegnern bezeichnet, die amtl. Sammlung des EGMR nach Nr. (Serie A) bzw. Rep. zitiert. Wird das Datum genannt, wird auf die Datenbank Hudoc verwiesen (www.echr.coe.int).

1 Vgl. BGH wistra 2004, 109 (110): „Hier zu Lande *war* die strafrechtliche Beurteilung des ‚Scalping' bislang streitig, insbesondere lag dazu keine höchstrichterliche Entscheidung vor." (Hervorhebung d. Verfasser).

2 *Vogel* NStZ 2004, 252 ff.; z.T. *Fleischer* DB 2004, 51; *Kudlich* JR 2004, 191, 195; *Widder* BKR 2004, 15.

3 Vgl. *Kudlich* JR 2004, 191 (193 ff.); *Pananis* NStZ 2004, 287 ff.; *Schäfer* BKR 2004, 78 (79); *Schmitz* JZ 2004, 526 ff.; *Widder* BKR 2004, 15.

4 Vgl. u.a. LG Stuttgart wistra 2003, 153 (156 ff.); *Assmann*, in: Assmann/Schneider, WpHG, 2. Aufl. 1999, § 14 Rn. 34; *Cahn* ZHR 162 (1998), 1 (20 f.); *Hopt* FS-Heinsius, 289 (295 f.); *Schneider/Burgard* ZIP 1999, 381 (388); *Peters*, Das deutsche Insiderstrafrecht, Frankfurt a.M. 1997, 76.