gelhaften Gegenstand produziert hat und daher auch der eigentlich Verantwortliche sein sollte.

Eine Lösung, die den unterschiedlichen Interessen der an der Lieferkette beim Streckengeschäft Beteiligten gleichermaßen gerecht wird, muss an den Besonderheiten dieser Form des Warenabsatzes ansetzen. Die Art des Geschäfts führt dazu, dass von der Handelsstufe keine Untersuchung der Kaufsache gefordert werden kann. Dafür ist sie verpflichtet, Informationen über Mängel, die beim Endkunden auftreten, unverzüglich weiterzugeben. Den berechtigten Interessen des Herstellers wird damit Rechnung getragen. Auf diese Weise wird nicht der Adressatenkreis des § 377 HGB verändert. Vielmehr wird dessen Pflichtenkatalog wegen der Art der Geschäftsdurchführung modifiziert, die Herstellern und Händlern gleichermaßen Vorteile bescheren kann. Ein solches Verständnis würde zahlreiche Schwierigkeiten in der Praxis vermeiden helfen und zugleich den Regelungen des Handels- ebenso wie denjenigen des Verbrauchsgüterkaufs systemgerecht entsprechen.

Professor Dr. **Thomas Hoeren**, Münster*

Die Umsetzung der Richtlinie zur Vorratsdatenspeicherung – Konsequenzen für die Privatwirtschaft

Die neuen Vorschriften zur Vorratsdatenspeicherung haben für die Adressaten aus der Privatwirtschaft insbesondere Speicherungs- und Auskunftspflichten eingeführt. Die Rechtslage ist aber derzeit angesichts der anhängigen Verfahren vor dem BVerfG und dem EuGH unsicher.

I. Neue Regelungen im TKG und in der StPO

Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG ist am 1. 1. 2008 in Kraft getreten.[1] Neben der Umsetzung der RiL zur Vorratsdatenspeicherung,[2] die die verdachtsunabhängige Speicherung von Telekommunikationsdaten vorsieht, werden durch die Novelle die strafprozessualen Regelungen zur Telekommunikationsüberwachung nach §§ 100a, 100b StPO, zur Abfrage von Verkehrsdaten nach § 100g StPO, zum so genannten IMSI-Catcher nach § 100i StPO sowie zur Beschlagnahme von elektronischen Speichermedien nach § 110 Abs. 3 StPO erheblich ausgeweitet bzw. reformiert. Dies ist zum einem auf den ungebremsten Reformwillen des Gesetzgebers im Bereich der staatlichen Überwachung zurückzuführen, dient aber auch der Umsetzung eines Übereinkommens des Europarats über Computerkriminalität (Cybercrime-Konvention)[3] sowie der Anpassung der Regelungen an die Rechtsprechung des *BVerfG* hinsichtlich des Kernbereichs der privaten Lebensgestaltung.[4] An dieser Stelle sollen die in das Telekommunikationsgesetz (TKG) eingeführten Vorschriften zur Speicherungspflicht (vor allem §§ 111, 113a, 113b TKG), aber auch die diese flankierenden Ermittlungsbefugnisse, die sich aus dem TKG und der StPO ergeben, im Hinblick auf deren Bedeutung für die Privatwirtschaft untersucht werden.

II. Anwendungsbereich der Vorratsdatenspeicherung

Der Adressat der Vorratsdatenspeicherung ergibt sich aus § 113a TKG. Hiernach richtet sich die Speicherungspflicht an denjenigen, der öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt. Ausweislich der Gesetzesbegründung wird hierdurch der nichtöffentliche Bereich wie etwa unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail-Server von Universitäten, die ausschließlich für dort immatrikulierte Studenten betrieben werden, von der Verpflichtung zur Speicherung ausgenommen.[5]

Der Begriff des öffentlich zugänglichen Telekommunikationsdienstes ist in § 3 Nr. 17 TKG legaldefiniert. Hiernach handelt es sich um einen der Öffentlichkeit zur Verfügung stehenden Dienst für das Führen von Inlands- und Auslandsgesprächen einschließlich der Möglichkeit, Notrufe abzusetzen. Maßgebliches Kriterium für den Anwendungsbereich der Vorratsdatenspeicherung ist damit der Begriff der Öffentlichkeit. Zur Auslegung kann der Begriff des Telekommunikationsdienstes für die Öffentlichkeit nach § 3 Nr. 19 TKG 1996 herangezogen werden.[6] Unter den Begriff der Öffentlichkeit fällt jeder unbestimmte Personenkreis.[7] Ausgeschlossen sind damit Telekommunikationsdienste, die nur einem *begrenzten Kreis von Personen* zugänglich gemacht werden bzw. von diesem in Anspruch genommen werden können.[8] Öffentlich zugänglich sind damit alle Telekommunikationsdienste, die für beliebige natürliche oder juristische Personen und nicht lediglich für die Teilnehmer einer geschlossenen Benutzergruppe erbracht wurden. Damit ist für die Abgren-

* Der Autor lehrt Informations- und Telekommunikationsrecht an der Universität Münster.

1 Gesetz vom 21. 12. 2007 – BGBl. I Nr. 70, S. 3198.

2 RiL 2006/24/EG des Europäischen Parlaments und des Rates vom 15. 3. 2006 über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden und zur Änderung der RiL 2002/58/EG – ABl. L 105, S. 54 ff.

3 Convention on Cybercrime vom 23. 11. 2001 – ETS No. 185: nach dieser muss den Ermittlungsbehörden im Gegensatz zu der Auskunftsregelung nach §§ 100g, h StPO a. F. selbst die Befugnis zur Erhebung von Verkehrsdaten zustehen (hierzu unten IV.1.). Allerdings sieht die Convention im Gegensatz zur Richtlinie die Einführung eines „Quick Freeze"-Verfahrens vor.

4 *BVerfGE* 113, 368 (391).

5 BT-Drs. 16/5846, S. 69.

6 *Bock*, in: Beck'scher TKG-Kommentar, 3. Aufl. 2006, § 112 Rdnr. 12.

7 BT-Drs. 15/2316, S. 60.

8 Dies gilt etwa für Funknetze in einer Hausgemeinschaft (*Gietl* K&R 2007, 545 (547)).

zung des öffentlich zum nicht-öffentlich zugänglichen Dienstes auf den Begriff der geschlossenen Benutzergruppe abzustellen.[9] Dieses Kriterium liegt auch der Begründung zum Regierungsentwurf zugrunde, da mit unternehmensinternen Netzen und Email-Servern von Universitäten ausschließlich für dort immatrikulierte Studenten[10] auf typische geschlossene Benutzergruppen abgestellt wird. Firmeninterne Netze stehen für die so genannten Corporate Networks, unter denen man Telekommunikationsnetze, durch die Kommunikationsleistungen für eine begrenzte Nutzerzahl erbracht werden und die an die Bedürfnisse von Unternehmen oder Unternehmensgruppen speziell angepasst sind, versteht.

Die Diensteerbringung in einer geschlossenen Benutzergruppe kann die Herstellung einer Verbindung zwischen den Teilnehmern einer geschlossenen Benutzergruppe, aber auch die Kommunikation eines Teilnehmers der geschlossenen Benutzergruppe mit einem beliebigen anderen Teilnehmer (Öffentlichkeit) sein. Maßgeblich ist allein, dass an der Kommunikation ein Mitglied der geschlossenen Benutzergruppe beteiligt ist.[11] Hieraus ergibt sich, dass Unternehmen der Privatwirtschaft, die ihren Mitarbeitern den Zugang zum Internet gewähren und damit funktional als Zugangsprovider zu qualifizieren sind, von der Vorratsdatenspeicherung nicht erfasst werden. Der Telekommunikationsdienst wird in diesem Fall nur einem begrenzten Kreis von Personen zugänglich gemacht. Dies gilt auch dann, wenn die private Nutzung des Internet nicht ausgeschlossen ist oder geduldet wird. In diesem Fall ist der Kommunikationspartner des Teilnehmers der geschlossenen Benutzergruppe zwar als Dritter im Sinne des TKG anzusehen,[12] für die Geschlossenheit der Benutzergruppe ist jedoch die Zugehörigkeit eines Kommunikationspartners ausreichend.

Durch das Merkmal der Erbringung des Dienstes für Endnutzer werden zudem Vermittler von Telekommunikationsdiensten – wie etwa Internet-Backbone-Provider – von der Vorratsdatenspeicherung ausgenommen.[13]

III. Umfang der Speicherungspflicht

1. Verkehrsdaten nach § 113a TKG

Die Neufassung des TKG sieht eine sechsmonatige Speicherungspflicht für bestimmte Verkehrsdaten vor. Verkehrsdaten sind nach § 3 Nr. 30 TKG solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Sie stehen damit in einem unmittelbaren Zusammenhang mit einem individuellen Kommunikationsvorgang und werden vom Fernmeldegeheimnis nach Art. 10 GG geschützt.

Für die Vorratsdatenspeicherung ist zu beachten, dass sich die Speicherungspflicht nach § 113a Abs. 1 TKG nur auf die bei der Nutzung des Dienstes erzeugten oder verarbeiteten Verkehrsdaten bezieht. Es werden nur solche Daten erfasst, die bei dem Telekommunikationsdiensteanbieter im Rahmen der Erbringung des Dienstes ohnehin anfallen.[14] Zusätzliche Erhebungspflichten begründet die Vorratsdatenspeicherung hingegen nicht. Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten sind nach § 113a Abs. 8 TKG nicht zu speichern. Zudem ist durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu vom Diensteanbieter ermächtigten Personen möglich ist. Die gespeicherten Daten sind innerhalb eines Monats nach Ablauf der Sechsmonatsfrist zu löschen. Im Ergebnis ist damit ein Zugriff von bis zu sieben Monaten möglich.

Internetzugangsdienste, Dienste der elektronischen Post und Internettelefondienste trifft die Speicherungspflicht nach § 150 Abs. 12b TKG erst ab dem 1. 1. 2009. Eine vorsätzliche oder fahrlässige Verletzung der Speicherpflichten, der Verpflichtung zur Einrichtung von technischen und organisatorischen Schutzvorkehrungen oder der Löschungspflichten ist nach § 149 Abs. 1 Nr. 36–39 TKG mit einem Bußgeld in Höhe von bis zu 500 000 Euro (Speicherpflichten) bzw. bis zu 300 000 Euro (technische und organisatorische Schutzvorkehrungen) bewehrt. Den Bescheid erlässt die Bundesnetzagentur. Verstöße gegen die Speicherungspflicht werden nach § 150 Abs. 12b Satz 1 TKG auch für Telefondiensteanbieter erstmalig ab dem 1. 1. 2009 verfolgt.

Im Einzelnen bestehen folgende Speicherungspflichten:

a) Anbieter von Telefondiensten

Zu den Anbietern von Telefondiensten zählen nach § 113a Abs. 2 TKG neben den Festnetzanbietern auch Mobilfunk- und Internettelefondienste. Für die Dauer von sechs Monaten sind zu speichern: die Telefonnummer des anrufenden und angerufenen Anschlusses unter Angabe des Zeitpunkts von Beginn und Ende der Verbindung, gegebenenfalls andere Kennungen der Anschlüsse (etwa aus dem Bereich der Internettelefonie, soweit nach einem anderen als dem herkömmlichen E-164-Nummerierungsplan bezeichnet), die Art des genutzten Dienstes (etwa Sprach-, Telefax- oder Datenübertragung, SMS oder MMS) sowie für Mobilfunkanbieter die Karten- (IMSI) und Gerätekennung (IMEI) des anrufenden und angerufenen Anschlusses und die Bezeichnung der bei Beginn der Verbindung genutzten Funkzelle (Standortdaten). Im Falle der Um- oder Weiterschaltung müssen zudem die Rufnummern der weiteren beteiligten Anschlüsse gespeichert werden. Bei erfolglosen Anrufversuchen oder Emailübermittlungen sind die genannten Daten nur dann zu speichern, wenn der Diensteanbieter sie ohnehin speichert.

b) Internetzugangsdienste

Internet-Access-Provider haben die dem Teilnehmer für eine Internetnutzung zugewiesene IP-Adresse zu speichern. Bei der Vergabe von dynamischen IP-Adressen bedeutet dies, dass für jeden einzelnen Nutzungsvorgang die divergierenden IP-Adressen zu speichern sind. Zudem muss eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, und der Zeitpunkt der Nutzung des Dienstes gespeichert werden. Eine Speicherung der aufgerufenen Internet-Adressen ist nach der Neufassung hingegen nicht vorgesehen.

c) Email-Provider

Auch EMail-Provider fallen unter die Speicherungspflicht. Nach § 113a Abs. 4 TKG haben sie bei der Versendung von Nachrichten die IP-Adresse des Absenders sowie die Kennung des Postfaches des Absenders und jedes Empfängers zu speichern. Bei eingehenden Nachrichten tritt an die Stelle der IP-Adresse des Absenders die der absendenden Telekom-

9 So auch *Bizer* Datenschutz und Datensicherheit (DuD) 2007, 586 (587).
10 BT-Drs. 16/5846, S. 69.
11 *Berger/Gramlich* CR 1999, 150 (154); *Simon* ArchivPT 1996, 142 (144); *Bock*, in: Beck'scher TKG-Kommentar (Fn. 6), § 112 Rdnr. 12.
12 Die Anwendbarkeit des Fernmeldegeheimnis nach § 88 TKG und der datenschutzrechtlichen Vorschriften der §§ 91 ff. TKG ist von der geschäftsmäßigen Erbringung von Telekommunikationsdiensten für Dritte abhängig. Hier ist im Gegensatz zum Öffentlichkeitsbegriff die Anzahl der berechtigten Nutzer unerheblich.
13 *Gietl* K&R 2007, 545 (547).
14 BT-Drs. 16/5846, S. 69.

munikationsanlage. Einzelne Zugriffe auf das Postfach sind ebenfalls unter Angabe der Kennung und IP-Adresse des Abrufenden zu speichern. Ausreichend ist das Öffnen der persönlichen Posteingangsseite. Ein Zugriff auf den Inhalt der Emails ist nicht vorausgesetzt. Das Herunterladen der Nachrichten vom Server des Providers gilt als Zugriff im Sinne der Vorschrift.[15] Sämtliche Zeitpunkte der genannten Nutzungen müssen gespeichert werden.

d) Anonymisierungsdienste

Die Vorratsdatenspeicherung betrifft auch Internet-Anonymisierungsdienste wie TOR oder AN.ON. Für diese Dienste ist anerkannt, dass es sich um Telekommunikationsdienste, die der Vorratsdatenspeicherung unterliegen, und nicht etwa um Telemediendienste handelt.[16] Nach § 113a Abs. 6 TKG haben Diensteanbieter, die speicherungspflichtige Angaben verändern, sowohl die ursprüngliche Angabe als auch die neue Angabe sowie den Zeitpunkt der Umschreibung zu speichern.

Der Bereich des NAT-Routing ist von der Vorschrift ebenfalls erfasst.[17] Allerdings gilt zu beachten, dass dies nur für Dienste gilt, die der Öffentlichkeit zugänglich sind. Dem Betrieb von NAT-Routern in Studentenwohnheimen für ausschließlich dort immatrikulierte Studenten steht die Vorratsdatenspeicherung daher auch dann nicht entgegen, wenn eine Speicherung von Zugriffsdaten nicht erfolgt.

e) Zweckbindung der gespeicherten Verkehrsdaten

§ 113b TKG regelt die zulässigen Verwendungszwecke der durch die Vorratsdatenspeicherung erhobenen Daten. Nach dem so genannten Zweckbindungsgrundsatz, der im gesamten Datenschutzrecht Anwendung findet, dürfen personenbezogene Daten nur zu gesetzlich eindeutig bestimmten Zwecken verarbeitet werden.

Die Vorschrift begründet aber lediglich eine datenschutzrechtliche Erlaubnisnorm. Auskunft darf nur aufgrund einer weiteren gesetzlichen Anspruchsgrundlage, die auf § 113a TKG verweist, erteilt werden. Derzeit ist ein solches Auskunftsrecht nur in § 100g StPO vorgesehen,[18] der Gesetzgeber ist aber nicht gehindert, weitere Anspruchsgrundlagen zu schaffen.

Zulässig ist die Verwendung der gespeicherten Daten zur Verfolgung von Straftaten, zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit und zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des BND und des MAD. Damit geht die nationale Umsetzung deutlich über die Vorgaben der Richtlinie zur Vorratsdatenspeicherung hinaus. Diese sieht lediglich die Ermittlung, Feststellung und Verfolgung von schweren Straftaten als zulässigen Verwendungszweck vor.[19] Auf der anderen Seite ist der Zugriff auf die im Rahmen der Vorratsdatenspeicherung gespeicherten Daten für den geplanten zivilrechtlichen Auskunftsanspruch[20] entgegen Forderungen des Bundesrats[21] ausgeschlossen. Der Verwendungszweck zur Verfolgung von Straftaten ist zudem durch eine einstweilige Anordnung des *BVerfG* vorläufig ausgesetzt worden. Bis zu einer abschließenden Entscheidung dürfen die aufgrund von § 113a TKG erhobenen Daten nur zur Verfolgung von schweren Straftaten verwendet werden.[22]

2. Bestandsdaten nach § 111 TKG

Im Zuge der Umsetzung der Richtlinie zur Vorratsdatenspeicherung ist ebenfalls die Verpflichtung zur Erhebung von Bestandsdaten nach § 111 TKG erweitert worden. Bestandsdaten sind dabei nach § 3 Nr. 3 TKG Daten, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden.

Nach § 111 TKG trifft denjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die Verpflichtung, bestimmte Kundendaten (der Begriff der Bestandsdaten geht über die nach § 111 TKG zu erhebenden Daten hinaus) vor der Freischaltung des Anschlusses zu erheben und unverzüglich zu speichern. Im Gegensatz zur Vorschrift des § 113a TKG und zu dem in § 110 TKG geregelten Anwendungsbereich der Telekommunikationsüberwachungsverordnung (TKÜV) sieht die Norm keine Beschränkung auf öffentlich zugängliche Dienste vor. Geschlossene Benutzergruppen wie etwa die Betreiber von Corporate Networks, Hotels oder Krankenhäuser unterliegen daher der Erhebungs- und Speicherungspflicht. Zudem handelt es sich um eine echte Erhebungspflicht, die unabhängig davon besteht, welche Daten beim Diensteanbieter verarbeitet werden.

Nach bisherigem Recht umfasste die Vorschrift Name und Anschrift des Rufnummerninhabers, das Datum des Vertragsbeginns, bei natürlichen Personen deren Geburtsdatum, bei Festnetzanschlüssen die Anschrift des Anschlusses sowie bei Bekanntwerden das Ende des Vertragsverhältnisses. Neu hinzugekommen ist zum einen die Verpflichtung zur Speicherung anderer Anschlusskennungen. Die Regelung trägt dem Umstand Rechnung, dass neuere Technologien – wie etwa DSL – andere Kennungen als die Rufnummer zur Bezeichnung des Anschlusses verwenden. Zum anderen begründet § 111 Abs. 1 Nr. 5 TKG eine Speicherungspflicht der Gerätenummer (IMEI) bei der Überlassung von Mobilfunkgeräten.

Email-Provider sind nunmehr nach § 111 Abs. 1 Satz 3 TKG verpflichtet, die Email-Adressen sowie Namen und Anschrift des Postfachinhabers zu speichern. Dies gilt allerdings nur für öffentlich zugängliche Dienste der elektronischen Post, so dass Server von Universitäten ausschließlich für dort immatrikulierte Studierende oder Bedienste hiervon ausgenommen sind. Zudem sieht die Vorschrift für Email-Provider keine Erhebungspflicht vor, sondern ist nur dann anzuwenden, wenn die Daten durch den Diensteanbieter für eigene Zwecke ohnehin erhoben werden.

Die Daten sind nach § 111 Abs. 4 TKG nach Ende des Vertragsverhältnisses mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. Bei der Vorschrift handelt es sich um eine Speicherverpflichtung im Interesse der Öffentlichen Sicherheit und nicht etwa um eine Höchstspeicherungsfrist.[23]

---

15 BT-Drs. 16/5846, S. 71.

16 *Gietl* K&R 2007, 545 (548); *Golembiewski* DuD 2003, 134 (136).

17 Hierzu kritisch *Gietl* K&R 2007, 545 (548 f.).

18 Hierzu unten IV. 1.

19 Art. 1 Abs. 1 RiL 2006/24/EG.

20 Regierungsentwurf eines Gesetzes zur Verbesserung der Durchsetzung der Rechte des geistigen Eigentums vom 26. 1. 2007 – BT-Drs. 16/2930; dort insbesondere § 101 UrhG-E.

21 Stellungnahme des Bundesrates, BT-Drs. 16/5846, S. 86; ablehnend die Gegenäußerung der Bundesregierung, BT-Drs. 16/5846, S. 96.

22 Hierzu unten V. 1.

23 *Bock*, in: Beck'scher TKG-Kommentar (Fn. 6), § 111 Rdnr. 14.

IV. Der Zugriff auf die Daten

1. Verkehrsdaten nach § 100g StPO

Nach bisherigem Recht waren die §§ 100g, 100h StPO a. F. als reiner Auskunftsanspruch der staatlichen Ermittlungsbehörden gegenüber Telekommunikationsunternehmen ausgestaltet. Auskunftspflichtig waren solche Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbrachten oder daran mitwirkten, also etwa Access-Provider, aber auch Mailbox-Betreiber oder andere Online-Dienste. Die Anwendung der Vorschriften setzte eine Straftat von erheblicher Bedeutung oder aber eine mittels Telekommunikationsendeinrichtung begangene Straftat voraus. Zu letzteren zählten mittels Telefon, Internet oder Email begangene Straftaten. Hintergrund dieser gegenüber der 1. Alternative geringeren Eingriffsschwelle war die technisch bedingte fehlende anderweitige Aufklärungsmöglichkeit der Taten.

Inhaltlich war der Auskunftsanspruch auf einzelne in § 100g Abs. 3 StPO a. F. aufgezählte Verbindungsdaten, nach neuerer Terminologie Verkehrsdaten, gerichtet. Der Auskunftsanspruch stand unter Richtervorbehalt, bei Gefahr im Verzug stand auch der Staatsanwaltschaft die Anordnungsbefugnis zu. Auskunftsersuchen konnten auch über in der Zukunft anfallende Gesprächsdaten angeordnet werden.

Unklar war, wie zu verfahren war, wenn die Auskunft suchende Stelle die entsprechende IP-Adresse bereits erhoben hatte und vom Telekommunikationsunternehmen die dahinter stehende Person bzw. deren Anschrift ermitteln wollte. Name und Anschrift einer Person gehören zu den Bestandsdaten, das heißt sie stehen in keinem unmittelbaren Zusammenhang mit einem Telekommunikationsvorgang. Bestandsdaten unterliegen aus diesem Grund nicht dem Fernmeldegeheimnis nach Art. 10 GG bzw. § 88 TKG. Vor diesem Hintergrund wurde in der Rechtsprechung vertreten, dass ein Auskunftsersuchen über die Identität eines Rechtsverletzers im Internet nicht auf §§ 100g, 100h StPO gestützt werden müsse, sondern dass ein Zugriff lediglich eine Auskunft über Bestandsdaten darstelle, für die das manuelle Auskunftsverfahren nach § 113 TKG gelte.[24] Dieses manuelle Auskunftsverfahren unterliegt keinem Richtervorbehalt, die Auskunft ist auch zur Gefahrenabwehr zulässig. In der Literatur stieß diese Rechtsprechung auf Kritik, da der Provider Name und Anschrift des Rechtsverletzers nur unter Verarbeitung der bei ihm gespeicherten Verkehrsdaten (Log-Zeiten und IP-Adresse) ermitteln konnte. Nach dieser Auffassung stellte das Auskunftsverlangen einen Eingriff in das Fernmeldegeheimnis dar, für das § 113 TKG keine ausreichende Ermächtigungsgrundlage darstellte. In der staatsanwaltlichen Praxis setzte sich aber das manuelle Auskunftsverfahren nach § 113 TKG durch.

Im Rahmen der Einführung der Vorratsdatenspeicherung zum 1. 1. 2008 ist der Auskunftsanspruch nach §§ 100g, 100h StPO a. F. novelliert worden. Der neu gefasste § 100g StPO stellt nunmehr die Ermächtigungsgrundlage der staatlichen Behörden zum Zugriff auf die nach § 113a TKG auf Vorrat gespeicherten Daten dar. Die Vorschrift steht nach wie vor unter Richtervorbehalt, ist jedoch nicht mehr als reiner Auskunftsanspruch ausgestaltet. In Zukunft können also die Strafverfolgungsbehörden ohne Mitwirkung der Telekommunikationsanbieter die anfallenden Verkehrsdaten erheben. Über die Vorschrift kann aber auch nach wie vor die Mitwirkung der Unternehmen im Rahmen des Auskunftsverfahrens verlangt werden. Möglich ist aber jetzt die so genannte Echtzeiterhebung von Verkehrsdaten, bei der die Daten zeitgleich mit ihrem Anfallen vom Telekommunikationsdiensteanbieter an die Strafverfolgungsbehörden ausgeleitet werden. Dies war bisher nur unter den Voraussetzungen der Überwachung des Fernmeldeverkehrs nach §§ 100a, 100b StPO möglich. Als Eingriffsvoraussetzung sieht die Vorschrift eine Straftat von auch im Einzelfall erheblicher Bedeutung vor oder – wie bisher – eine Straftat, die mittels Telekommunikation begangen wurde. In letzterem Fall ist die Maßnahme allerdings streng subsidiär zu anderen Ermittlungsmaßnahmen. Eine Echtzeitausleitung ist ebenfalls nicht zulässig.

Für die bisher streitige Frage, ob eine Auskunft über die „hinter einer dynamischen IP-Adresse stehende Person" einer richterlichen Anordnung bedarf, hat die Novellierung keine Klärung geschaffen. Diese Frage zu beantworten wird weiterhin Aufgabe der Rechsprechung sein.

2. Bestandsdaten nach §§ 112, 113 TKG

a) Automatisiertes Auskunftsverfahren

Die im Rahmen des § 111 TKG erhobenen und gespeicherten Bestandsdaten dienen der Auskunftserteilung nach §§ 112, 113 TKG. Im automatisierten Auskunftsverfahren nach § 112 TKG haben Diensteanbieter, die Telekommunikationsdienste für die Öffentlichkeit anbieten (nicht geschlossene Benutzergruppen), die nach § 111 TKG erhobenen Daten in einer Kundendatei zu speichern. Hierbei ist zu gewährleisten, dass die Bundesnetzagentur jederzeit Daten aus den Kundendateien automatisiert im Inland abrufen kann. Hierzu muss die Bundesnetzagentur Zugriff auf die Datei und damit auf die Systeme des Anbieters mittels einer definierten Schnittstelle nehmen können.[25] Vorgesehen ist auch die Abfrage mittels unvollständiger Abfragedaten (Jokerabfrage) und mittels Ähnlichkeitsfunktion. Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass dem Diensteanbieter die Abrufe durch die Bundesnetzagentur nicht zur Kenntnis gelangen. Einzelheiten regelt eine durch das Bundesministerium für Wirtschaft und Arbeit zu erlassende Rechtsverordnung.

Auskunftsberechtigt sind u. a. Gerichte und Strafverfolgungsbehörden, die Polizeivollzugsbehörden des Bundes und der Länder zur Gefahrenabwehr, das Zollkriminalamt, die Verfassungsschutzbehörden des Bundes und der Länder sowie der MAD und der BND. Die Auskünfte werden nicht unmittelbar durch den Telekommunikationsanbieter, sondern durch die Bundesnetzagentur, die die Daten an die Auskunft ersuchende Stelle übermittelt, erteilt.

b) Manuelles Auskunftsverfahren

Im Rahmen des manuellen Auskunftsverfahrens nach § 113 TKG besteht für geschäftsmäßige Anbieter von Telekommunikationsdienstleistungen im Einzelfall eine unverzügliche Auskunftspflicht über die nach § 111 TKG erhobenen Daten, aber auch über sämtliche weiteren Bestandsdaten, die vom Diensteanbieter erhoben wurden. Der Anwendungsbereich ist nicht auf öffentlich zugängliche Dienste begrenzt, so dass auch geschlossene Benutzergruppen unter die Vorschrift fallen. Im Gegensatz zu § 112 TKG steht den auskunftersuchenden Stellen im manuellen Auskunftsverfahren

24 *LG Stuttgart* MMR 2005, 624; MMR 2005, 628; *LG Hamburg* MMR 2005, 711; *LG Würzburg* NStZ-RR 2006, 46; aber a. A. *LG Bonn* DuD 2004, 628; *LG Ulm* MMR 2004, 187.

25 *Bock*, in: Beck'scher TKG-Kommentar (Fn. 6), § 112 Rdnr. 20.

der Anspruch direkt gegen den Telekommunikationsanbieter zu.

Das Auskunftsverfahren ist auf Zwecke der Strafverfolgung und der Verfolgung von Ordnungswidrigkeiten, der Gefahrenabwehr und der Erfüllung der gesetzlichen Aufgaben des Verfassungsschutzes, des BND und des MAD beschränkt. Über die genannten Bestandsdaten hinaus kann nach §§ 161 Abs. 1 Satz 1, 163 Abs. 1 StPO i. V. m. § 113 Abs. 1 Satz 2 TKG Auskunft über Daten, mittels derer ein Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzten Speichereinrichtungen geschützt wird, verlangt werden. Hierzu gehören im Mobilfunkbereich PIN (Personal Identity Number) und PUK (Personal Unblocking Key), aber auch Passwörter.[26]

V. Ausblick

1. Einstweilige Anordnung des BVerfG

Das *BVerfG* hat mit Beschluss vom 11. 3. 2008 Teile der Vorratsdatenspeicherung vorläufig außer Kraft gesetzt. Dies betrifft allerdings nicht die grundsätzliche Speicherungspflicht nach § 113a TKG, sondern die Verwendung der nach § 113a TKG gespeicherten Daten. Nach der amtlichen Fassung des § 113b TKG dürfen die auf Vorrat gespeicherten Daten nur zur Verfolgung von Straftaten, zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden, des BND und des MAD an die zuständigen Stellen übermittelt werden. Eine entsprechende Erhebungsbefugnis der Strafverfolgungsbehörden (§ 113b TKG stellt lediglich die datenschutzrechtliche Erlaubnisnorm dar, gibt aber kein Auskunftsrecht oder eine Erhebungsbefugnis) sieht § 100g StPO für Straftaten von erheblicher Bedeutung und Straftaten, die mittels Telekommunikation begangen werden, vor. Die Zweckbindung der Daten nach § 113b TKG ging dem *BVerfG* nicht weit genug. Aufgrund der einstweiligen Anordnung dürfen bis zur Entscheidung in der Hauptsache die aufgrund von § 113a TKG gespeicherten Verkehrsdaten nur zur Verfolgung von schweren Straftaten übermittelt werden. Der Begriff der schweren Straftat umfasst dabei Straftaten, für die eine gesetzliche Mindestfreiheitsstrafe von fünf Jahren vorgesehen ist, im Einzelfall sollen aber auch die besondere Bedeutung des Rechtsguts oder das besondere öffentliche Interesse an der Strafverfolgung das Vorliegen einer schweren Straftat begründen können. Eine schwere Straftat ist notwendige Voraussetzung für die Anordnung der Telekommunikationsüberwachung nach § 100a StPO.

Da es sich aber nur um eine vorläufige Entscheidung handelt, ist noch unklar, inwieweit die Vorschriften der Vorratsdatenspeicherung Bestand haben werden. In der einstweiligen Anordnung hat das *BVerfG* angedeutet, dass von der umfassenden und anlassunabhängigen Bevorratung der Daten erhebliche Einschüchterungseffekte ausgehen. Ob dies ein Indiz für eine bevorstehende umfassende Nichtigkeitserklärung ist, lässt sich derzeit nicht absehen.

2. Nichtigkeitsklage vor dem EuGH

Diese unsichere Rechtslage besteht umso mehr, als vor dem *EuGH* in Luxemburg ein Verfahren anhängig ist, das sich ausschließlich mit der formalen Rechtmäßigkeit der Richtlinie zur Vorratsdatenspeicherung befasst.[27] Im Rahmen der von Irland erhobenen Nichtigkeitsklage wird geltend gemacht, die Vorratsdatenspeicherung hätte nicht auf die Wirtschaftskompetenz der Europäischen Gemeinschaften nach Art. 95 EGV gestützt werden dürfen, sondern hätte im Rahmen der dritten Säule, der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, ergehen müssen. Unter Zugrundelegung dieser Rechtsauffassung hätte die Vorratsdatenspeicherung nur durch einen Rahmenbeschluss des Europäischen Rates eingeführt werden können, der eine einstimmige Entscheidung seiner Mitglieder erfordert. In der Literatur wird weitestgehend von der Nichtigkeit der Richtlinie aufgrund des genannten formalen Mangels ausgegangen.[28] Die Vereinbarkeit der Richtlinie mit der Europäischen Menschenrechtskonvention, die nach Art. 6 Abs. 2 EUV zu den allgemeinen Grundsätzen des Gemeinschaftsrechts zählt, bzw. die Vereinbarkeit der Richtlinie mit der Europäischen Grundrechtscharta, ist hingegen nicht Gegenstand des Verfahrens; es ist aber auch nicht auszuschließen, dass hier eine weitere Klage vor dem *EuGH* angestrebt wird.

Der Ausgang des derzeit anhängigen Verfahrens könnte eine erhebliche präjudizielle Wirkung für die Entscheidung des *BVerfG* haben, da hiervon u. U. der Umfang der Prüfungskompetenz des nationalen Gerichts abhängig ist. Sollte die Richtlinie Bestand haben, träfe das *BVerfG* eine Vorlagepflicht nach Art. 234 EGV an den *EuGH* im Vorabentscheidungsverfahren, soweit die Unvereinbarkeit der Richtlinie zur Vorratsdatenspeicherung mit Europäischem Gemeinschaftsrecht in Rede steht. Bei einer Nichtigkeitserklärung durch den *EuGH* fiele hingegen die Prüfungskompetenz umfassend an das *BVerfG* zurück. In der Tendenz wäre eine Nichtigkeitserklärung durch das höchste deutsche Gericht zu erwarten, da das Gericht in seinem Volkszählungsurteil hohe Anforderungen an den datenschutzrechtlichen Zweckbindungsgrundsatz gestellt hat.[29] Hiernach müssen Ziel und Umfang der Datenverarbeitung auf einen gesetzlich bestimmten Verwendungszweck begrenzt werden, dem der pauschale Hinweis auf die Strafverfolgung im nationalen Gesetz nicht genügt. Mit einer abschließenden Entscheidung des *BVerfG* im Hauptsacheverfahren wird bis Ende dieses Jahres gerechnet.

---

26 Zur Frage, ob die Auskunft über die Identität eines Nutzers anhand der dynamischen IP-Adresse unter § 100 g StPO a. F. oder § 113 TKG fällt: oben IV.1.

27 Rechtssache C-301/06.

28 *Gitter/Schnabel* MMR 2007, 411 (413); *Bizer* DuD 2007, 8 (9); *Gietl* K&R 2007, 545 (545); *Leutheusser/Schnarrenberger* ZRP 2007, 9 (11 ff.).

29 *BVerfGE* 65, 1 ff.