Transnationaler Zugriff auf Computerdaten

Von RiOLG Dr. **Wolfgang Bär**, Bamberg

Seit dem Einzug der Personalcomputer in allen Bereichen der Wirtschaft und des Privatlebens sowie der ständig weiter zunehmenden Vernetzung der EDV-Anlagen mit der rasanten Ausbreitung des Internets bestimmen schon heute die Informationstechnologien und das Internet unsere Arbeitsabläufe und Arbeitsweisen. Die mit diesen neuen Techniken verbundene Digitalisierung aller Tätigkeiten birgt aber auch vielfältige neue Gefahren und Risiken in sich und eröffnet Straftätern neuartige Missbrauchsmöglichkeiten, wenn Computerdaten und -systeme in qualitativ und quantitativ stark zunehmender Weise zu Tatmittel oder Tatobjekt werden. Dabei setzen Straftäter technisch immer weiter fortentwickelte Methoden zur Tatbegehung ein, mit denen es heute möglich ist, gesamte Bereiche der Wirtschaft lahm zu legen und vor allem auch hohe Schäden anzurichten. Dabei ist es den Straftätern über die weltweiten Datennetze in zunehmendem Maße möglich, die jeweiligen Taten auch vom Ausland aus zu begehen, aber gleichwohl einen strafrechtlich relevanten Taterfolg im Inland herbeizuführen. Zur Tataufklärung muss daher häufig auch auf Beweismittel im Ausland zugegriffen werden. Im Folgenden sollen daher – ausgehend von den eigenen nationalen Ermittlungsbefugnissen – die rechtlichen Möglichkeiten aufgezeigt werden, die sich bei der transnationalen Sicherung von Computerdaten ergeben. Dabei wird hinsichtlich der relevanten Eingriffsbefugnisse zwischen Durchsuchungs- und Beschlagnahmemaßnahmen, Eingriffen in die Telekommunikation und Ermittlungsmöglichkeiten in Datennetzen differenziert, wobei abschließend auch Fragen der Verwertung im Ausland erlangter Beweismittel zu erörtern sind.

I. Durchsuchung und Beschlagnahme

1. Begriff „Durchsuchung“

Mit § 102 und § 103 StPO wird den Ermittlungsbehörden die Befugnis eingeräumt, Wohnungen oder andere Räume von Verdächtigen sowie auch anderen Personen nach Beweismitteln zu durchsuchen und in einem zweiten Schritt etwaige vorgefundene Beweise nach §§ 94 ff. StPO sicherzustellen oder zu beschlagnahmen. Während bei herkömmlichen Durchsuchungen die relevanten Beweismittel regelmäßig in Papierform vorgefunden wurden, ist dies beim Einsatz der modernen EDV-Techniken eher der Ausnahmefall. Die Ermittlungsbehörden müssen deshalb vorhandene EDV-Anlagen und Speichermedien zum einen zur Sichtung und Sichtbarmachung der gespeicherten Daten verwenden. Zum anderen kann die EDV-Anlage aber auch dazu dienen, bisher noch nicht gefundene beweisrelevante Daten erst auf internen oder externen Speichermedien zu suchen, die sich physikalisch an einem anderen Speicherort im In- oder Ausland befinden können.

Unter dem Durchsuchungsbegriff ist nach seinem sprachlichen Verständnis als eine Tätigkeit zu verstehen, die einer Sache nachspürt, sie sorgfältig untersucht und durchforscht, und sich darum bemüht, etwas aufzufinden, indem ein Objekt bis in den letzten Winkel abgesucht wird. Sinnverwandte Ausdrücke sind damit das Durchforschen, Erforschen, Nachsehen, Auskundschaften, Durchstöbern und „Filzen“.[1] Kennzeichnend für die Durchsuchung ist damit ein Verhalten, dem inhaltlich nur Grenzen durch die Zweckbestimmung der jeweiligen Handlung und die zu durchsuchenden Räumlichkeiten gezogen sind. Es ist daher mit dem Zweck des Eingriffs vereinbar, eine in den durchsuchten Objekten vorgefundene EDV-Anlage in Betrieb zu nehmen oder weiter zu benutzen. Kommt es bei einer Benutzung der fremden EDV-Anlage oder bei einer Auswertung sichergestellter Unterlagen auf vorgefundenen Datenträgern oder auf der Zentraleinheit bzw. dem Server zum Aufruf vorhandener Computerprogramme oder zur Kopie solcher Anwendungen, ist die darin ggf. zu sehende Verletzung fremder Urheberrechte i.S.d. §§ 16 ff. UrhG in jedem Fall durch die gesetzlichen Schranken des Urheberrechts abgedeckt, da in § 45 UrhG eine Herstellung einzelner Vervielfältigungsstücke von Werken zur Verwendung in Verfahren vor einer Behörde oder einem Gericht ausdrücklich zugelassen wird.[2]

2. Externe Datenhaltung im Inland

Besteht von den Computeranlagen aus, die in den durchsuchten Objekten vorgefunden werden, die Möglichkeit, neben lokal gespeicherten Daten auch weitere Dateien abzurufen, die physikalisch auf einem externen Speicher vorgehalten werden, der sich nicht in den primär durchsuchten Räumlichkeiten befindet, muss die Frage einer Reichweite der Durchsuchungsmaßnahme erörtert werden. Da es sich bei der Durchsuchung um eine offen gegenüber dem Beschuldigten bzw. Dritten ausgeführte Zwangsmaßnahme handelt,[3] kann eine Durchsuchung über Netzwerke nicht allein auf § 102 StPO bzw. § 103 StPO gestützt werden. Vielmehr werden durch die konkrete Bezeichnung des Durchsuchungsobjekts im Anordnungsbeschluss auch die räumlichen Grenzen für die Umsetzung festgelegt. Diese Begrenzungen führen zu erheblichen Beschränkungen bei einer Suche nach beweisrelevanten Daten in Computernetzwerken. Dies hat eine große praktische Relevanz, weil durch neue technische Möglichkeiten wie „Cloud Computing“ oder „Cloud Storage“ viele Firmen und private PC-Anwender dazu übergegangen sind, beweisrelevante Daten und Programme nicht mehr auf dem eigenen Rechner vorzuhalten, sondern extern auf einem oder mehreren Servern von Fremdanbietern abzuspeichern. Der Ausbau entsprechender Speichermedien wird derzeit in erheblichem Umfang von der Industrie forciert, wobei sogar von einem abermaligen Strukturwandel der Computerwelt ausgegangen wird, so dass Experten davon ausgehen, dass sich hier innerhalb weniger Jahre ein Milliarden-Markt in

[1] Vgl. näher: *Bär*, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007, Rn. 361-354.
[2] Vgl. näher: *Bär* (Fn. 1), Rn. 365 f.
[3] Vgl. nur BGHSt 51, 211 sowie näher *Bär* (Fn. 1), Rn. 367-371.

Deutschland entwickeln wird.[4] Dabei kann sich der jeweilige Server mit den Daten sowohl im Inland als auch auf einem ausländischen Server befinden.[5]

Vor diesem Hintergrund hatte deshalb bereits die Cyber-Crime-Konvention des Europarats vom 23.11.2001[6], die mit Zustimmungsgesetz vom 5.11.2008[7] ratifiziert wurde, in Art. 19 Abs. 2 im Rahmen der nationalen strafprozessualen Bestimmungen vorgesehen, dass durch entsprechende Regelungen bei Durchsuchungen eines Computersystems im Strafverfahrensrecht sicherzustellen ist, dass auch auf Daten in einem anderen Computersystem im eigenen Hoheitsgebiet zugegriffen werden kann. Diesen Anforderungen hat der Gesetzgeber zum 1.1.2008 durch die Schaffung eines neuen § 110 Abs. 3 StPO Rechnung getragen. Die dort vorgesehene Online-Sichtung von Daten führt damit quasi zu einer „Online-Durchsuchung light“,[8] jedoch ohne Einsatz technischer Mittel. Danach darf nunmehr die Durchsicht elektronischer Speichermedien auch auf räumlich getrennte Speichermedien erstreckt werden, wenn darauf vom Speichermedium des Betroffenen aus zugegriffen werden kann. Durch diese Regelung soll ein Verlust beweiserheblicher Daten vermieden werden, die sich auf räumlich getrennten Speichermedien im Internet oder Intranet befinden. Da dem § 110 Abs. 3 StPO keine weiteren Einschränkungen hinsichtlich der zu sichernden Daten entnommen werden können, ist ein Zugriff auf alle externen Dateien möglich. Voraussetzung ist nur, dass der externe Speicherplatz von einer während der Durchsuchung vorgefundenen EDV-Anlage aus zugänglich ist, d.h. dieses Computersystem so konfiguriert ist, dass eine Erweiterung der Durchsicht auf andere über ein Netzwerk angeschlossene Speichermedien technisch möglich ist.[9] Von § 110 Abs. 3 S. 1 StPO erfasst werden damit Fallgestaltungen, bei denen der Betroffene z.B. von einem entsprechenden Anbieter (sog. filehoster) Speicherplatz gemietet hat, auf den nur online – etwa über einen am Rechner vorgefundenen Hyperlink – über Datennetze zugegriffen werden kann.[10] Werden im Rahmen der Durchsuchung Passwörter für den Zugang zu solchen externen Speichermedien des Betroffenen gefunden, ist ein Abruf der dortigen Informationen ebenfalls zulässig, so dass hier auch ein Abruf von gespeicherten E-Mails des von der Durchsuchung Betroffenen in Betracht kommt, wenn dies die konkrete Konfiguration des vorgefundenen Rechners gestattet.[11] Ggf. können insoweit durch ein Auskunftsverlangen beim Provider gem. § 113 Abs. 1 S. 2 TKG i.V.m. §§ 161, 163 StPO zur Durchführung der Durchsicht auch vorab die entsprechenden Zugangsdaten herausverlangt werden. Eine Anwendung des § 110 Abs. 3 StPO ist auch nicht deshalb ausgeschlossen, weil die Durchsuchung zu einer heimlichen Maßnahme gegenüber dem Gewahrsamsinhaber der online zugänglichen Daten wird. Dessen Interessen wird nach § 110 Abs. 3 S. 2 Hs. 2 StPO durch die entsprechende Anwendung von § 98 Abs. 2 StPO Rechnung getragen, indem dieser bei einem Zugriff auf seine Daten durch die Möglichkeit zur Beantragung einer richterlichen Bestätigung der Beschlagnahme Gelegenheit zum Rechtsschutz erhält. Die Durchsicht ist zulässig, wenn andernfalls mit einem Daten- bzw. Beweismittelverlust zu rechnen ist. Da eine Sicherstellung am Ort der Datenhaltung meist mit zeitlichen Verzögerungen verbunden sein wird, besteht diese Gefahr des Datenverlustes bei Computerdaten regelmäßig. Die Hauptschwierigkeit in der Praxis bei Maßnahmen nach § 110 Abs. 3 StPO besteht aber darin, dass jeweils der Standort des Servers mit den beweisrelevanten Daten im In- oder gar im Ausland geklärt werden muss, um festzustellen, ob der Eingriff über den nationalen Hoheitsbereich hinaus ausgedehnt wird. Dies kann z.B. durch trace-routing erfolgen, wobei aus den Top-Level-Domains und Länderkennungen des jeweiligen Internet-Angebots nicht notwendig auf den Standort des Rechners geschlossen werden kann. Vielmehr entfalten diese Angaben – ebenso wie eine verwendete IP-Adresse – nur eine Indizwirkung. Erfolgt in diesen Fällen eine Sicherung der beweisrelevanten Daten und wird nachträglich festgestellt, dass die jeweiligen Dateien nicht im Inland, sondern auf einem ausländischen Server gespeichert waren, führt dies zur Frage, ob von einem Beweisverwertungsverbot in Bezug auf die sichergestellten Daten auszugehen ist.[12]

3. Externe Datenhaltung im Ausland

In jeden Fall lässt sich der nationalen Befugnis zur Online-Sichtung von Daten keine Rechtsgrundlage für einen Zugriff auf im Ausland gespeicherte Daten entnehmen. Durch derartige Online-Ermittlungen kann es vielmehr zu einer Verletzung fremder Souveränitätsrechte kommen, wobei durch solche Direktermittlungen im Ausland etwaige bestehende Rechtshilfeübereinkommen unterlaufen werden können. Befinden sich die beweisrelevanten Daten tatsächlich im Ausland, kann hier auf die entsprechenden Regelungen in Art. 29 und 32 der Cyber-Crime-Konvention zurückgegriffen werden. Ein „transborder-search“ ist als einseitiger Zugriff auf ausländische gespeicherte Daten im Fall des Art. 32 in

[4] Bis zum Jahr 2015 wird von einem jährlichen Durchschnittswachstum bei „Cloud Computing“ von 48 % ausgegangen. Vgl. näher den Bericht dazu unter http://www.heise.de/newsticker/meldung/Steve-Ballmer-und-Rene-Obermann-Offene-Plattformen-und-Standards-fuers-Cloud-Computing-1102732.html.

[5] Vgl. zum Cloud Computing bzw. Cloud Storage näher: *Nägele/Jacobs*, ZUM 2010, 281; *Obenhaus* NJW 2010, 651; *Gercke*, CR 2010, 345; *Niemann/Hennrich* CR 2010, 686.

[6] Vgl. zum Text: http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm.

[7] Vgl. BGBl. II 2008, S. 1242.

[8] *Schlegel*, HRRS 2008, 23.

[9] Vgl. *Bär*, in: von Heintschel-Heinegg/Stöckel (Hrsg.), KMR, Kommentar zur Strafprozeßordnung, 58. Lfg., Stand: August 2010, § 100a Rn. 71; *Hegmann*, in: Graf (Hrsg.), Beck'scher Online-Kommentar, Strafprozessordnung, Stand: 1.8.2010, § 110 Rn. 13 f.; *Schlegel*, HRRS 2008, 23 (28); *Meyer-Goßner*, Strafprozessordnung, Kommentar, 53. Aufl. 2010, § 110 Rn. 6.

[10] Vgl. BT-Drs. 16/5846, S. 64.

[11] Vgl. *Bär* (Fn. 9), § 100a Rn. 71; *Schlegel*, HRRS 2008, 23 (30); *Meyer-Goßner* (Fn. 9), § 110 Rn. 6.

[12] Vgl. dazu näher unter IV.

zwei Fällen zulässig: Zum einen kommt gem. Art 32 lit. a eine Sicherung ausländischer Daten immer dann ohne Rückgriff auf Rechtshilfeersuchen in Betracht, wenn die gesuchten Dateien frei zugänglich sind. Gleiches gilt zum anderen, wenn eine rechtmäßige und freiwillige Zustimmung der zur Datenübermittlung berechtigten Person vorliegt, so dass unter diesen Voraussetzungen etwa auch ein Zugriff auf E-Mail-Konten auf ausländischen Servern oder auf Daten in Betracht kommt, die im Rahmen von „Cloud Computing" ins Ausland ausgelagert wurden.[13] Sollte diese Möglichkeit des unmittelbaren Zugriffs nicht bestehen, kann auf der Grundlage des Art. 29 Cyber-Crime-Konvention eine beschleunigte Sicherung ausländischer Daten ohne vorheriges förmliches Rechtshilfeersuchen erfolgen. Notwendig hierfür ist ein formloses Ersuchen an den anderen Vertragsstaat zur Vorabsicherung der beweisrelevanten Daten, das inhaltlich den Anforderungen des Art. 29 Abs. 2 Cyber-Crime-Konvention entsprechen muss. Nach Eingang des Ersuchens hat der Vertragsstaat gem. Art. 29 Abs. 3 S. 1 Cyber-Crime-Konvention geeignete Maßnahmen zur umgehenden Sicherung der Daten zu treffen, wobei die beiderseitige Strafbarkeit keine Voraussetzung für die Vornahme der Sicherung ist (Art. 29 Abs. 3 S. 2 Cyber-Crime-Konvention). Durch diese vorläufige Maßnahme lässt sich damit eine Sicherung der beweisrelevanten Daten erreichen, die viel schneller und effektiver als traditionelle Rechtshilfehandlungen ist. Die gesicherten Daten müssen zunächst gem. Art. 29 Abs. 7 Cyber-Crime-Konvention mindestens 60 Tage aufbewahrt werden. Neben der Cyber-Crime-Konvention sieht auch der EU-Rahmenbeschluss über die Vollstreckung von Entscheidungen über die Sicherstellung von Vermögensgegenständen oder Beweismitteln vom 22.7.2003[14] entsprechende Regelungen zur Anerkennung von richterlichen Beschlüssen zur Durchsuchung und Sicherstellung von Beweismitteln in anderen EU-Mitgliedsstaaten ohne Anerkennungsverfahren mit schneller Vollstreckung bei 32 Deliktsgruppen vor. Diese Vorgaben wurden mit Gesetz vom 6.6.2008 zur Umsetzung des Rahmenbeschlusses[15] inzwischen in den §§ 94 ff. IRG in nationales Recht umgesetzt.

III. Eingriffe in die Telekommunikation

1. Telekommunikationsdaten

Für das juristische Verständnis und die praktische Umsetzung von Eingriffsmaßnahmen muss zunächst Klarheit über die bei einem Kommunikationsvorgang anfallenden Daten sowie die Befugnisse zu deren Erhebung und Speicherung und über die relevanten gesetzlichen Zugriffsmöglichkeiten bestehen.[16] Abgestuft nach der Eingriffsintensität in die Rechte des Betroffenen ist vom geringsten zum stärksten Eingriff zu unterscheiden zwischen Bestands- oder Benutzerdaten, Verkehrsdaten einschließlich sog. Positions- oder Standortdaten beim Mobilfunk sowie Nutzungsdaten und Inhaltsdaten.

Nachdem sowohl jeder Internetzugang als auch jedes Mobiltelefon nur mit speziellen, dem Nutzer zugewiesenen bzw. überlassenen Kennungen und Passwörtern genutzt werden können, sind diese Informationen als sog. Zugangsdaten für das Ermittlungsverfahren von besonderem Interesse. Durch den Verweis in § 113 Abs. 1 S. 2 TKG auf die Ermittlungsgeneralklausel §§ 161, 163 StPO wird klargestellt, dass ein Zugriff auf diese Daten ohne Eingriff in des Fernmeldegeheimnis zulässig ist.

Bestandsdaten der Telekommunikation sind in § 3 Nr. 3 TKG legal definiert als die personenbezogenen Daten eines Kunden, die zur Begründung, inhaltlichen Ausgestaltung sowie Änderung oder Beendigung eines Vertragsverhältnisses erhoben werden. Eine fast wortgleiche Definition enthält § 14 Abs. 1 TMG für Bestandsdaten bei Telemedien. Bestandsdaten fallen nicht in den Schutzbereich des Art. 10 GG. Ihre Erhebung ist nur mit einem Eingriff in das Recht auf informationelle Selbstbestimmung i.S.d. Art. 2 Abs. 1 GG verbunden. Der Umfang zu erhebender Bestandsdaten wird mit der datenschutzrechtlichen Befugnis in § 95 Abs. 1 TKG allgemein festgelegt, nur hinsichtlich der in § 111 Abs. 1 TKG aufgeführten Daten wird eine Speicherpflicht für die Provider begründet.[17] Zu den Bestandsdaten gehören gem. § 111 Abs. 1 S. 1 TKG damit Rufnummern und andere Anschlusskennungen (Nr. 1), Name und Anschrift des Anschlussinhabers einschließlich des Geburtsdatums bei natürlichen Personen (Nr. 2, 3), die konkrete örtlichen Lage des Festnetzanschlusses (Nr. 4), die Gerätenummer (IMEI) des Mobiltelefons, soweit dieses – wie in der Praxis üblich – bei Vertragsschluss dem Kunden vom Provider auch ein Handy überlassen wird. Die Speicherpflicht besteht auch bei sog. Prepaid-Produkten (§ 111 Abs. 1 S. 1 TKG). Nach § 111 Abs. 1 S. 3 TKG trifft die Speicherpflicht auch Anbieter der elektronischen Post. Ein Zugriff auf diese Bestandsdaten ist über §§ 112 und 113 TKG zulässig.

Nach der Legaldefinition des § 3 Nr. 30 TKG sind unter Verkehrsdaten alle Daten zu subsumieren, die bei der Erbringung eines TK-Dienstes erhoben, verarbeitet oder genutzt werden. Nach der Legaldefinition des § 96 Abs. 1 TKG gehören dazu u.a. die Nummern oder Kennungen der beteiligten Anschlüsse oder der Endeinrichtungen einschließlich der Standortdaten (Funkzelle) bei mobilen Anschlüssen (Nr. 1), Beginn und Ende der jeweiligen Verbindung nach Datum und Uhrzeit sowie übermittelte Datenmengen (Nr. 2), der vom Nutzer in Anspruch genommene Telekommunikationsdienst (Nr. 3) sowie sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten (Nr. 5). Diese Verkehrsdaten dürfen nur für Abrechnungszwecke erhoben und gespeichert werden. Die ergänzend dazu in § 113a TKG a.F. enthaltene verdachtsunabhängige Vorratsdatenspeicherung der Verkehrsdaten ist verfassungswidrig und damit nichtig.[18] Eine

[13] Kritisch insoweit: *Gercke*, CR 2010, 345 (348).
[14] ABl. EU 2003 Nr. L 196, S. 45.
[15] BGBl. I 2008, S. 995.
[16] Vgl. ausführlich dazu: Vgl. *Bär* (Fn. 9), Vor §§ 100a-100i Rn. 7 ff.; *Bär* (Fn. 1), Rn. 12-46; *Seitz*, Strafverfolgungsmaßnahmen im Internet, 2004, S. 62-68.
[17] Vgl. *Hoeren*, JZ 2008, 668 (670).
[18] Vgl. BVerfG NJW 2010, 833 sowie eingehend dazu *Bär* (Fn. 9), Vor §§ 100a-100i Rn. 6a und 15 ff.

Auskunft über Verkehrsdaten kann nur auf der Grundlage des § 100g StPO verlangt werden.

Soweit den Ermittlungsbehörden demgegenüber bei einem Abruf von inkriminierten Inhalten im Internet eine dynamische IP-Adresse des Täters bereits bekannt ist, bedarf es nur noch die Zuordnung dieser Daten zu einer Person. Welche Rechtsgrundlage für eines solche Personenauskunft zur dynamischen IP-Adresse einschlägig ist, war lange Zeit umstritten.[19] Da sich die vom Provider geforderte Auskunft einerseits nur auf ein Bestandsdatum bezieht, andererseits aber die Auskunft nur durch einen Rückgriff auf die gespeicherten Verkehrsdaten erfolgen kann, liegt die Eingriffsqualität zwischen § 113 TKG und § 100g StPO. Der Gesetzgeber hatte deshalb zur Klarstellung in § 113b letzter Hs. TKG eine ergänzende Regelung aufgenommen, aus der sich eine Anwendung des Auskunftsverfahrens nach § 113 TKG insoweit ergab. Da diese Regelung aber mit dem Urteil des BVerfG vom 2.3.2010[20] für nichtig erklärt wurde, kann darauf seitdem nicht mehr zurückgegriffen werden. Nach Auffassung des BVerfG ist die Personenauskunft zu einer dynamischen IP-Adresse zwar mit einem Eingriff in Art. 10 GG verbunden, jedoch fordert eine solche Ermittlungsmaßnahme keinen Richtervorbehalt und muss auch keinem begrenzenden Rechtsgüter- oder Straftatenkatalog unterstellt werden. Erforderlich ist nur, dass die Auskunft nur bei hinreichendem Anfangsverdacht auf einzelfallbezogener Tatsachenbasis erteilt wird. Unter Berücksichtigung dieser Kriterien genügt auch § 113 TKG für eine solche Personenauskunft den verfassungsrechtlichen Anforderungen für einen Eingriff, soweit ein Anfangsverdacht für eine Straftat besteht.

Nur für Telemedien findet sich in § 15 TMG mit den sog. Nutzungsdaten eine weitere Datenkategorie. Telemedien sind nach der negativen Generalklausel des § 1 Abs. 1 TMG alle elektronischen Informations- und Kommunikationsdienste, die weder dem Bereich der Telekommunikation noch dem Rundfunk zuzuordnen sind.[21] Neben den beim Aufbau der Verbindung anfallenden Verkehrsdaten können hier nach der Legaldefinition des § 15 Abs. 1 S. 2 TMG während der Kommunikation vom jeweiligen Anbieter weitere zusätzliche Informationen erhoben werden, welche die konkrete Nutzung einzelner Angebote von Telemedien oder sogar konkreter Webseiten betreffen, soweit diese Daten für Abrechnungszwecke erforderlich sind. Ein Zugriff auf diese Daten kann regelmäßig über § 100g StPO sowie im Einzelfall auch über § 100a StPO erfolgen.[22]

Unter Inhaltsdaten sind alle bei einem Kommunikationsvorgang anfallenden Informationen und Nachrichten zu verstehen, die im Rahmen der Telekommunikation i.S.d. § 3 Nr. 22 TKG übertragen bzw. ausgetauscht werden. Hierunter fallen neben den Kommunikationsinhalten alle verkehrsbegleitenden Informationen in Form der Verkehrs- bzw. Nutzungsdaten. Dazu gehören neben den konkreten Gesprächsinhalten auch die beim Datenverkehr übertragenen Töne, Bilder oder Signale aller Art oder beim E-Mail- bzw. SMS-Verkehr bzw. bei Voice over IP (VoIP) die individuellen Inhalte der einzelnen übermittelten Nachrichten. Der Zugriff auf diese Daten beinhaltet den weitestgehenden Eingriff in die Rechte des Betroffenen und ist nur unter den engen Voraussetzungen des § 100a StPO zulässig.

2. Überwachung der Telekommunikation

Mit der zum 1.1.2008 in wesentlichen Punkten überarbeiteten Regelung des § 100a StPO besteht die Befugnis, alle modernen Kommunikationsformen, die von der Übertragung von Tönen, Bildern, Signalen bis hin zur Daten reichen, zu überwachen. Durch den Wegfall der Beschränkung in § 100b Abs. 3 StPO auf geschäftsmäßige Betreiber, kann eine Überwachung nun auch in geschlossenen Benutzergruppen oder betriebsinternen Netzen erfolgen, wenn eine der in § 100a Abs. 2 StPO abschließend aufgeführten Katalogtaten vorliegt. Eine Überwachungsanordnung kann dabei gem. § 100b Abs. 3 StPO gegenüber dem Beschuldigten, den sog. aktiven oder passiven Nachrichtenmittlern, ergehen oder aber auch gegenüber unbeteiligten Dritten, wenn der Beschuldigte deren Anschluss benutzt.[23] Eine solche Maßnahme darf gem. § 100a Abs. 4 StPO nur dann erlassen werden, wenn allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Dazu zählen nur intime Gespräche, unter Rückgriff auf § 100c Abs. 4 S. 2 und S. 3 StPO aber nicht Kommunikationsvorgänge in Betriebs- und Geschäftsräumen sowie Gespräche über die Planung und Verabredung von Verbrechen.[24]

3. Reichweite der Überwachung mit Auslandsbezug

Für die Umsetzung einer solchen Überwachungsanordnung finden sich detaillierte Regelungen zu den formalen Voraussetzungen in § 100b Abs. 2 StPO sowie eine Verpflichtung der Provider zur Umsetzung solcher Anordnungen gem. § 100b Abs. 3 StPO i.V.m. § 110 TKG einschließlich der Telekommunikationsüberwachungsverordnung (TKÜV). Dort enthält § 4 TKÜV auch wesentliche Regelungen für die TK-Überwachung mit Auslandsbezug. Da ein ausländischer Provider nicht der deutschen Hoheitsgewalt unterliegt, ist eine Überwachung eines TK-Anschlusses eines inländischen Beschuldigten gem. § 4 Abs. 1 TKÜV grundsätzlich ausgeschlossen, wenn sich dieser mit seinem Mobilfunkgerät im Ausland befindet. Dazu finden sich aber in § 4 Abs. 1 letzter Hs. und in Abs. 2 TKÜV zwei wichtige Ausnahmen: Zum

[19] Vgl. näher: *Bär* (Fn. 1), Rn. 205-213; *Bär* (Fn. 9), § 100g Rn. 26-27a.

[20] Vgl. BVerfG NJW 2010, 833.

[21] Gemeint sind z.B. Verteildienste mit Angeboten für Austauschverträge sowie Abrufdienste von Text- oder Bilddarbietungen auf Anforderung (vgl. näher: *Spindler/Schuster*, Recht der elektronischen Medien, 2008, § 1 TMG S. 1402; *Mückl*, JZ 2007, 1077 [1080]; *Hoeren*, NJW 2007, 801 [802]; *Spindler*, CR 2007, 239 [240]).

[22] Vgl. *Bär* (Fn. 9), §100g Rn. 34.

[23] Vgl. näher Vgl. *Bär* (Fn. 9), § 100a Rn. 36-39.

[24] Vgl. BGH NJW 2009, 519; dies gilt auch, wenn Gespräche über Planung und Verabredung von Verbrechen in intime Inhalte (z.B. Gebete) eingebettet werden (BGH NJW 2010, 44 [47]).

einen ist eine Überwachung dann zulässig, wenn die Telekommunikation vom Ausland aus an einen im Inland gelegenen TK-Anschluss um- oder weitergeleitet wird. Ruft der Täter etwa von Ausland aus seine inländische Mobilbox mit gespeicherten Nachrichten ab, findet eine Kommunikation im Inland statt, die dem deutschen Hoheitsrecht unterliegt und deshalb überwacht werden kann. Zulässig ist zum anderen auch die sog. Auslandskopfüberwachung gem. § 4 Abs. 2 TKÜV.[25] Hierbei handelt es sich um einen Kommunikationsvorgang, der von einem unbekannten inländischen Anschluss mit einer bekannten Rufnummer im Ausland geführt wird. In diesem Fall kann der Gesprächsinhalt, der über einen der wenigen Verbindungspunkte des nationalen TK-Netzes zu den internationalen Netzen abgewickelt wird, im Inland aufgezeichnet werden.

Sind diese Möglichkeiten des § 4 TKÜV nicht gegeben, kommt nur eine Überwachung der Telekommunikation im Ausland unter Zuhilfenahme des ausländischen Providers im Wege der Rechtshilfe in Betracht. Eine Rechtsgrundlage für eine solche Erhebung von Inhaltsdaten der Kommunikation in Echtzeit findet sich in Art. 34 der Cyber-Crime-Konvention.[26] Daneben enthält das Übereinkommen über die Rechtshilfe in Strafsachen innerhalb der EU (kurz: EU-RhÜbK) vom 29.5.2000[27] detaillierte Regelungen in Art. 17-22 für die Umsetzung von Überwachungsanordnungen im Wege der Rechtshilfe. Die Durchführung von solchen Maßnahmen richtet sich grundsätzlich nach Art. 4 Abs. 1 EU-RhÜbK nach dem Recht des ersuchenden Staates.[28]

4. Überwachung des E-Mail-Verkehrs im In- und Ausland

Besondere Rechtsfragen ergeben sich in Bezug auf die Überwachung des E-Mail-Verkehrs.[29] Hierbei wird herkömmlicherweise zwischen vier Phasen der Kommunikation unterschieden. In der Phase 1 wird die Nachricht vom Absender über dessen Provider an den TK-Anbieter weitergeleitet, bei dem der Empfänger sein elektronisches Postfach hat. Dort wird die jeweilige Nachricht in einer zweiten Phase im jeweiligen elektronischen Postfach so lange zwischengespeichert, bis der Empfänger diese an ihn gerichtete Nachricht in der Phase 3 aus seinem Postfach aufruft. In einer Phase 4 kann dann die angekommene Nachricht beim Empfänger auf seinem Computer weiterhin gespeichert werden. In seiner Entscheidung vom 16.6.2010[30] geht das BVerfG davon aus, dass der zugangsgesicherte Kommunikationsinhalt während der gesamten Übertragung der Nachricht durch Art. 10 GG geschützt ist, da die E-Mail sich auch noch im Stadium der Zwischenspeicherung im Herrschaftsbereich des Providers befindet und der Nutzer keine technische Möglichkeit hat, eine Weitergabe seiner E-Mails zu verhindern. Dieser technisch bedingte Mangel erfordert deshalb den besonderen Schutz durch Art. 10 GG. Dies führt für die Zugriffsmöglichkeiten auf E-Mails dazu, dass in der Phase 1 und 3 während des Übertragungsvorgangs immer nur ein Rückgriff auf § 100a StPO als Eingriffsermächtigung in Betracht kommt. Während der Zwischenspeicherung in Phase 2 genügen demgegenüber die §§ 94 ff. StPO den verfassungsrechtlichen Anforderungen an Eingriffe in Art. 10 GG, so dass auf dieser Grundlage ein einmaliger Zugriff auf gespeicherte E-Mails beim Provider möglich ist.[31] Nach Auffassung des BGH kommt während der Zwischenspeicherung insoweit ein Rückgriff auf § 99 StPO mit einer richterlichen Anordnung gem. § 100 StPO in Betracht.[32] Eine Sicherstellung bzw. Beschlagnahme gespeicherter E-Mails muss aber stets den Grundsatz der Verhältnismäßigkeit berücksichtigen, so dass eine Sicherung des gesamten E-Mail-Bestandes auf dem Mailserver des Providers gegen das Übermaßverbot verstoßen kann, wenn nicht eine Einschränkung des Eingriffs in Bezug auf etwaige Sender- oder Empfängerangaben oder bestimmte Suchbegriffe erfolgt ist.[33] E-Mails auf dem Rechner des Empfängers in der Phase 4 unterliegen demgegenüber nicht mehr dem Schutz durch Art. 10 GG, da dessen Schutzbereich endet, wenn die Nachricht beim Empfänger angekommen ist. Eine Sicherstellung dieser Daten ist daher nach §§ 94 ff. StPO oder 102 ff. StPO jederzeit möglich.[34]

Befindet sich der E-Mail-Server des Providers im Ausland, kommt hier ein Rückgriff auf § 110 Abs. 3 StPO i.V.m. Art. 32 lit. b Cyber-Crime-Konvention in Betracht. Falls die Voraussetzungen hierfür nicht gegeben sind, hat ein vorläufiges Sicherungsverfahren nach Art. 25 Abs. 3 i.V.m. 29 Cyber-Crime-Konvention zu erfolgen. Soweit es sich bei dem E-Mail-Provider um ein im Inland ansässiges Unternehmen handelt, das aber auch im Ausland entsprechende Angebote vorhält, kann auch eine Sicherstellungsanordnung gegenüber dem inländischen Provider erfolgen, wenn dieser mit einem deutschen Web-Angebot auftritt und so den Bezug zum Inland herstellt, auch soweit die relevanten Daten nur aus technischen Gründen ins Ausland ausgelagert werden. Daneben kommt im EU-Bereich auch eine Sicherstellunganordnung auf der Grundlage des EU-Rahmenbeschlusses über die Sicherstellung von Vermögensgegenständen und Beweismitteln vom 22.7.2003[35] in Betracht, dessen Umsetzung in nationales Recht in §§ 94 und 97 IRG erfolgt ist.

5. Erhebung von Verkehrsdaten

Die Regelung zur Erhebung von Verkehrsdaten in § 100g StPO wurde zum 1.1.2008 grundlegend neu gefasst. Statt der vorher nur bestehenden Verpflichtung der Provider, vorhandene Verkehrsdaten an die Strafverfolgungsbehörden zu

[25] Vgl. näher: *Bär* (Fn. 9), § 100b Rn. 17; *Bock*, in: Geppert/Piepenbrock/Schütz/Schuster (Hrsg.), Beck'scher Kommentar, TKG, 3. Aufl. 2006, § 110 TKG Rn. 89; *Reinel*, wistra 2006, 205.
[26] Vgl. *Graf* (Fn. 26), § 100a Rn. 129.
[27] ABl. EG 2000 Nr. C 197, S. 1 ff.
[28] Vgl. dazu näher: *Schuster*, NStZ 2006, 657; *Brodowski*, JR 2009, 402 (410).
[29] Vgl. ausführlich dazu: Vgl. *Bär* (Fn. 9), § 100a Rn. 27-29b.
[30] Vgl. BVerfG NJW 2009, 2431.
[31] Vgl. BVerfG NJW 2009, 2431.
[32] Vgl. BGH NStZ 2009, 397 m. Anm. *Bär*.
[33] Vgl. BGH NJW 2010, 1297.
[34] Vgl. § 100g Abs. 3 StPO für Verkehrsdaten, sowie BVerfG NJW 2006, 976.
[35] ABl. EU 2003 Nr. L 196, S. 45 ff.

übermitteln, enthält die Neuregelung – in Umsetzung von Art. 20 der Cyber-Crime-Konvention – eine eigene Befugnis zur Erhebung von Verkehrsdaten in Echtzeit. Eng verbunden mit dem Zugriff auf Verkehrsdaten waren dabei zur Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung[36] die Regelungen über die anlassunabhängige Speicherung von Verkehrsdaten, die in den letzten sechs Monaten angefallen sind, in den bisherigen §§ 113a und 113b TKG. Durch die Nichtigkeit dieser Regelungen auf Grund des BVerfG-Urteils vom 2.3.2010[37] ist auch der Anwendungsbereich des § 100g StPO stark eingeschränkt. Eine Speicherung von Verkehrsdaten der Kommunikation darf nach den §§ 96-101 TKG nur noch für Abrechnungszwecke oder bis zu einem Zeitraum von einer Woche auch zum Erkennen oder Beseitigen von Störungen im Netz erfolgen.[38] Da somit keine starren Mindestspeicherfristen für die Verkehrsdaten mehr gelten, hängt der Erfolg eines Auskunftsersuchens der Ermittlungsbehörden bzgl. retrograder Verkehrsdaten von Zufälligkeiten ab. Dies führt vor allem bei Flatrate-Angeboten, bei Internet- und E-Mail-Diensten sowie bei Anonymisierungsangeboten sowie Prepaid-Mobiltelefonen zu erheblichen Einschränkungen bei den strafprozessualen Ermittlungen. Insoweit bildet die hier in Art. 16 Abs. 2 Cyber-Crime-Konvention vorgesehene „quick freeze"-Anordnung, die nach deutschem Recht auf die Ermittlungsgeneralklausel der §§ 161, 163 StPO gestützt werden kann und darauf abzielt, angefallene Verkehrsdaten nicht zu löschen, sondern aufzubewahren, nur in wenigen Einzelfällen eine Alternative zur Vorratsdatenspeicherung. Dies gilt lediglich dann, wenn innerhalb weniger Tage nach der Tat eine Abfrage der Verkehrsdaten erfolgen kann.

Für den transnationalen Zugriff auf Verkehrsdaten sieht Art. 25 Abs. 3 i.V.m. Art. 29 Cyber-Crime-Konvention ein vorläufiges Sicherungsverfahren vor. Dieses ist kombiniert mit einer Verpflichtung zur umgehenden Weitergabe gespeicherter Verkehrsdaten in Art. 30 Cyber-Crime-Konvention. Ausdrücklich vorgesehen ist in Art. 33 Cyber-Crime-Konvention auch eine Erhebung von Verkehrsdaten in Echtzeit. Da in anderen EU-Staaten die Regelungen zur Vorratsdatenspeicherung entsprechend der Richtlinie 2006/24/EG[39] bereits in nationales Recht umgesetzt wurden und teilweise sogar Speicherfristen für Verkehrsdaten bis zur dort in Art. 6 vorgesehenen Höchstdauer von zwei Jahren vorsehen, besteht auch die Aussicht, entsprechende Verkehrsdaten – je nach dem ersuchten EU-Mitgliedstaat – von den jeweiligen Providern tatsächlich noch zu erhalten.

6. Auskunft über Bestandsdaten

Der daneben im deutschen TKG vorgesehene Auskunftsanspruch in Bezug auf Verkehrsdaten im Online-Auskunftsverfahren nach § 112 TKG oder im manuellen Auskunftsverfahren nach § 113 TKG bietet die Möglichkeit zur Ermittlung der hinter einer Telefonnummer, E-Mail-Adresse oder IP-Adresse stehenden Person. Auch die Personenauskunft zu einer bereits ermittelten dynamischen IP-Adresse kann auf der Grundlage des § 113 TKG erfolgen.[40]

Soweit hier entsprechende Informationen zu einem im Ausland befindlichen Anschluss erforderlich sind, kann dies ebenfalls nur im Wege der Rechtshilfe erfolgen, da durch solche Ermittlungen fremde Souveränitätsrechte tangiert sein können. Ausnahmen können hier aber bei Gefahr in Verzug angenommen werden. Soweit entsprechende Informationen auch in öffentlich zugänglichen Internet-Angeboten zu finden sind, kann hier aber auch auf Art. 32 lit. a Cyber-Crime-Konvention zurückgegriffen werden.

III. Ermittlungen in Datennetzen

Soweit durch die Ermittlungsbehörden im Wege der „Patrouille" in Datennetzen nach strafbaren Inhalten gesucht wird, handelt es sich hierbei um keinen Grundrechtseingriff, wenn der betreffende Anbieter im Netz durch einen offenen Zugang sich auch mit einer Kontrolle durch Sicherheitsbehörden einverstanden erklärt hat. Dies gilt ebenso für Ermittlungen im sog. Web 2.0 bei sozialen Netzwerken aller Art, auch wenn von Seiten der Strafverfolgungsbehörden ein Chat unter einer Legende durchgeführt wird, soweit bei dem jeweiligen angebotenen Dienst keine Überprüfung der Identität des Benutzers erfolgt.[41] Eine anonyme oder pseudonyme Kommunikation von Polizeibeamten in diesen Netzwerken ist damit zulässig und kann auf die Ermittlungsgeneralklausel der §§ 161, 163 StPO gestützt werden. Insoweit kann daher auch hier bei solchen Kontrollen in Datennetzen mit Auslandsbezug auf die Regelung des Art. 32 lit. a der Cyber-Crime-Konvention zurückgegriffen werden, soweit die relevanten Daten in den weltweiten Netzen frei zugänglich sind.

Die Grenze zum Eingriff wird erst dann überschritten, wenn die Ermittlungspersonen sich an geschlossenen Benutzergruppen beteiligen wollen oder von Seiten der jeweiligen Anbieter eine Identitätsprüfung durchgeführt wird. Gleiches gilt auch dann, wenn mit Hilfe entsprechender Software versucht wird, auf Daten in fremden informationstechnischen Systemen zuzugreifen. Eine solche Online-Durchsuchung ist derzeit im nationalen Recht nur auf polizeirechtlicher Grundlage etwa nach § 20k BKAG zulässig. Auch wenn § 20v Abs. 5 BKAG eine Datenweitergabe an die Strafverfolgungsbehörden zulässt, steht einer Verwertung erlangter Erkenntnisse im Strafverfahren § 161 Abs. 2 StPO mit dem Gedanken des hypothetischen Ersatzeingriffs entgegen, da derzeit eine entsprechende strafprozessuale Befugnis hierfür fehlt.[42]

[36] Vgl. Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. EG 2006 Nr. L 105, S. 54 ff.).

[37] BVerfG NJW 2010, 833.

[38] Vgl. dazu eingehend: Vgl. *Bär* (Fn. 9), Vor §§ 100a-100i Rn. 21-27 m.w.N.

[39] ABl. EU 2006 Nr. L 105, S. 54 ff.

[40] S.o. unter I. 1.

[41] Vgl. BVerfG MMR 2008, 315.

[42] Vgl. dazu näher: Vgl. *Bär* (Fn. 9), § 100a Rn. 70 m.w.N.

IV. Verwertung von Beweismitteln

Ob eine Verletzung des Souveränitätsrechts fremder Staaten bei transnationalen Ermittlungen zu einem Beweisverwertungsverbot erlangter Erkenntnisse führt, ist bisher nur wenig geklärt. Ebenso wie bei einer Verletzung anderer Eingriffsnormen ist dem Strafverfahrensrecht aber ein allgemein geltender Grundsatz fremd, dass jeder Verstoß gegen Beweiserhebungsvorschriften ein strafprozessuales Verwertungsverbot nach sich zieht. Die Verwertbarkeit rechtswidrig erlangter Erkenntnisse ist vielmehr nach inzwischen gefestigter Rechtsprechung jeweils nach den Umständen des Einzelfalls zu beurteilen, insbesondere nach der Art des Verbots und dem Gewicht des Verfahrensverstoßes sowie der Bedeutung der im Einzelfall betroffenen Rechtsgüter.[43] Dabei muss beachtet werden, dass die Annahme eines Verwertungsverbotes, auch wenn die Strafprozessordnung nicht auf die Wahrheitserforschung „um jeden Preis" gerichtet ist, eines der wesentlichen Prinzipien des Strafrechts einschränkt, nämlich den Grundsatz, dass das Gericht die Wahrheit zu erforschen und dazu die Beweisaufnahme von Amts wegen auf alle Tatsachen und Beweismittel zu erstrecken hat, die von Bedeutung sind.[44] Die Bejahung eines Beweisverwertungsverbotes ist folglich die Ausnahme, die nur nach ausdrücklicher gesetzlicher Vorschrift oder aus übergeordneten wichtigen Gründen im Einzelfall anzuerkennen ist. Von einem Beweisverwertungsverbot ist deshalb nur dann auszugehen, wenn einzelne Rechtsgüter durch Eingriffe fern jeder Rechtsgrundlage so massiv beeinträchtigt werden, dass dadurch das Ermittlungsverfahren als ein nach rechtsstaatlichen Grundsätzen geordnetes Verfahren nachhaltig geschädigt wird und folglich jede andere Lösung als die Annahme eines Verwertungsverbotes – jenseits des in § 136a Abs. 3 S. 2 StPO normierten – unerträglich wäre.[45] Ein Verbot der Verwertung gewonnener Erkenntnisse ist deshalb nur dann anzunehmen, wenn die Voraussetzungen für einen solchen Eingriff willkürlich angenommen, die relevanten Normen also bewusst und gezielt umgangen bzw. ignoriert werden oder wenn die Rechtslage in gleichgewichtiger Weise gröblich verkannt bzw. fehlerhaft beurteilt wird.[46]

Von einem solchen Beweisverwertungsverbot in Bezug auf Online-Ermittlungen ist daher etwa nur dann auszugehen, wenn der betreffende Staat einer Durchsuchung bzw. Verwertung von erlangten Beweismitteln bereits im Vorfeld widersprochen hat.[47] Im Übrigen ist bei einer etwaigen Verletzung des Territorialitätsgrundsatzes bei Ermittlungen im Ausland ohnehin fraglich, ob der Rechtskreis des Betroffenen überhaupt tangiert ist, da mit dem völkerrechtlichen Souveränitätsrecht keine subjektiven Rechte des unmittelbar Betroffenen geschützt werden.[48] Vor diesem Hintergrund wird daher nur in den seltensten Fällen bei einem ausdrücklichen Widerspruch des fremden Staates gegen eine Verletzung von fremden Hoheitsrechten auch von einem Beweisverwertungsverbot auszugehen sein. Dies umso mehr als die Ermittlungsbehörden in den meisten Fällen bei der Sicherung von beweisrelevanten Daten vor Ort meist gar nicht in der Lage sind, den konkreten physikalischen Speicherort der jeweiligen Dateien festzustellen, so dass eine willkürliche Vorgehensweise nicht angenommen werden kann.[49]

V. Zusammenfassung

Die im immer weiter zunehmende weltweite Vernetzung von Computersystemen mit neuen Formen der externen Datenhaltung in Form von Cloud Computing oder vergleichbaren Speicherformen schaffen zum einen vielfältige neue technische Möglichkeiten zur Begehung von Straftaten vom Ausland aus. Zum anderen müssen die Ermittlungsbehörden in zunehmendem Maße auf Daten zugreifen, die außerhalb des eigenen Hoheitsgebiets erhoben bzw. gespeichert werden. Eine solche transnationale Sicherung von Beweismitteln kann aber nicht durch die jeweiligen nationalen Rechtsordnungen, sondern nur durch internationale Regelungen im Bereich der Europäischen Union oder des Europarats erfolgen. Insoweit bestehen für grenzüberschreitende Ermittlungen mit der Cyber-Crime-Konvention des Europarats und den dargestellten EU-Übereinkommen zwar erste Regelungen in diesem Bereich, doch müssen hier noch weitere Verbesserungen sowohl in Bezug auf die jeweiligen Rechtsgrundlagen – etwa durch eine vorgesehene Europäische Beweisanordnung[50] – als auch in Bezug auf die entsprechenden praktischen Umsetzungsmöglichkeiten im zwischenstaatlichen Bereich geschaffen werden, damit die Grenzen des eigenen Hoheitsbereichs bei Ermittlungsmaßnahmen nicht einen Freiraum für international agierende Straftäter schaffen.

[43] BVerfG NJW 2008, 3053 (3054); 2006, 2684 (2686); NStZ 2006, 46 (47); BGHSt 51, 285 (290); 44, 243 (249); OLG Bamberg NJW 2009, 2146; OLG Hamburg NJW 2008, 2597 (2598); OLG Thüringen, Beschl. v. 25.11.2008 – 1 Ss 230/08; OLG Stuttgart NStZ 2008, 238 (239).

[44] Vgl. BGHSt 51, 285 (290); 44, 243 (249).

[45] Vgl. BGHSt 51, 285 (290).

[46] Vgl. BVerfGE 113, 29 (61); NJW 2008, 3053 (3054); 2006, 2684 (2686) sowie zusammenfassend BGHSt 51, 285 (292) sowie OLG Bamberg NJW 2009, 2146.

[47] Vgl. BGHSt 34, 334; *Hegmann* (Fn. 9), § 110 Rn. 15; *Gercke*, StraFo 2009, 271.

[48] Vgl. *Gercke*, StraFo 2009, 271.

[49] So im Ergebnis auch: *Graf* (Fn. 26), § 100a Rn. 133.

[50] Vgl. Rahmenbeschluss 2008/978/JI des Rates vom 18. Dezember 2008 über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafsachen (ABl. EU 2008 L 350, S 72 ff.).