Leitfaden zum Datenzugriff

insbesondere für den Bereich der Telekommunikation

Generalstaatsanwaltschaft München

Verfasser: OStA [redacted]

Stand: Juni 2011

Mit Kommentaren der ZOK und ZIK der GenStA Stuttgart und des TKÜ-Zentrums des LKA BW
für die Anwendung in Baden-Württemberg (Stand: Juli 2011)

Ansprechpartnerin GenStA Stuttgart: [redacted]
Ansprechpartner LKA BW: TKÜ-Zentrum LKA BW

VS - Nur für den Dienstgebrauch!

Inhaltsverzeichnis

I. Literatur und nützliche Links

Arndt/Fetzer/Scherer	Telekommunikationsgesetz Kommentar, 2008, Erich Schmidt Verlag
Bär, Wolfgang	• TK-Überwachung, §§ 100a – 101 StPO mit Nebengesetzen, 2010, Carl Heymanns Verlag • „Transnationaler Zugriff auf Computerdaten“ in Zeitschrift für Internationale Strafrechtsdogmatik (ZIS) Nr. 2/2011, S. 53 ff.(www.zis-online.com)
www.a-i3.org	Arbeitsgruppe Identitätsschutz im Internet
www.antiphishing.org	
www.cyberfahnder.de	
www.dnstools.ch	

II. Übersicht über Ermittlungsmaßnahmen

Stichwort	Durchzuführende Maßnahme		Gesetzliche Grundlage
Aufzeichnung v. Telekommunikation	Überwachung u. Aufzeichnung des **Inhalts** eines **Telekommunikationsvorgangs**		§ 100a StPO
Auswertung Gerätespeicher/SIM	Sicherung u. Auswertung von Daten aus **Gerätespeicher** od. **SIM-Karte**		§ 94 StPO
Datenauskunft	**Bestandsdaten**		§§ 161 Abs.1, 163 Abs. 1 StPO i.V.m. • § 113 Abs. 1 TKG bzgl. Telekommunikationsdiensteanbieter (Telekom, Arcor u.a.) • § 14 Abs. 2 TMG bzgl. Telemedien (eBay, YouTube, Facebook, Webmail u.a.)
	Personenauskunft	zu **vorhandener Rufnummer**	§ 112 TKG (Online-Auskunft) oder § 113 TKG (Manuelle Auskunft)
		zu **vorhandener dynamischer IP-Adresse**	• § 113 TKG; • bzgl. der Speicherfristen sh. Übersichten unten VI.
		zu **vorhandener E-Mail-Adresse od. statischer IP-Adresse**	§ 113 TKG
	Standortdaten von **Mobiltelefonen**	**über Mobilfunknetz**	§§ 100a od. 100g StPO Standortdaten in Echtzeit nach § 100g Abs. 1 S. 3 nur unter den Voraussetzungen der Nr.1; **Hinweis**: bei Mobiltelefon im Stand-By-Betrieb ist nur die LAC [location area code] feststellbar; diese wird jedoch nicht gespeichert; eine retrograde Abfrage

			nach § 100g StPO ist daher nicht sinnvoll;
		mittels GPS-Empfänger, die serienmäßig in modernen Mobiltelefonen eingebaut sind	Bisher keine gesetzliche Grundlage Es handelt sich nach überwiegender Auffassung nicht um Verkehrsdaten; zulässig nur präventiv-polizeilich nach § 20k BKAG bzw. Landespolizeigesetz (Bayern: Art. 34d BayPAG)
	Rechnungsdaten		§§ 96, 97 TKG, 100g StPO
	Verkehrsdaten	Auskunft über **künftig anfallende Verkehrsdaten**	§ 100g Abs. 1 StPO; künftige Verkehrsdaten können weiterhin erhoben werden, das Urteil des BVerfG v. 2.3.2010 zur Vorratsdatenspeicherung steht nicht entgegen.
		Auskunft über in der **Vergangenheit angefallene Verkehrsdaten**	• § 100g Abs. 1 S. 1 Nr. 1 u. Nr. 2 StPO; • nur noch bzgl. **Verkehrsdaten i.S. der §§ 96 ff. TKG (z.B. Rechnungsdaten)** möglich, nachdem durch Urteil des BVerfG v. 2.3.2010 die §§ 113a, 113b TKG u. § 100g StPO, soweit dieser den Abruf nach § 113a TKG gespeicherter Daten erlaubte, für nichtig erklärt wurden. • vor Erlass des Urteils des BVerfG nach § 100g Abs. 1 Nr. 1 StPO rechtmäßig erhobene und übermittelte Verkehrsdaten durften im Strafverfahren verwertet werden; durch das Urteil des BVerfG entsteht insoweit auch kein nachträgliches Beweisverwertungsverbot (BGH, Beschl. v. 4.11.2010, Az. 4 StR 404/10 (NJW 2011, 467), OLG München, Beschl. v. 27.05.2010, Az. 2 Ws 404/10).
	PIN/PUK		§§ 113 Abs. 1 S. 2 TKG, 161, 163 StPO

	Vertragsverhältnisse	§ 113 TKG
Durchsicht v. räumlich getrennten Speichermedien	Durchsicht eines **räumlich getrenntes Speichermediums** im Rahmen einer Durchsuchung bei dem Betroffenen, soweit hierauf von einer während der Durchsuchung aufgefundenen EDV-Anlage zugegriffen werden kann • **Passwort** Wird dieses bei der Durchsuchung aufgefunden, ist der Zugriff auf die dortigen Informationen zulässig; • **Speicherung auf ausländischen Server** Für Zugriff auf Daten, die auf einem ausländischen Server gespeichert sind, ist in der Regel ein Rechtshilfeersuchen erforderlich (bei Eilfällen im Bereich der EU: Art. 20 Abs. 4 EuRHÜbk) (Näheres hierzu s.u. VIII.)	§§ 102, 103, 110 Abs. 3 StPO
E-Mail	Aufzeichnung des **E-Mail**-Verkehrs während der **Übertragungsphase** (Absender-Provider od. Provider-Empfänger)	§ 100a StPO
	Kontrolle des **E-Mail**-Verkehrs während **Zwischenspeicherung beim Provider** im **Postfach des Empfängers**	§§ 94 ff. bzw. § 99 StPO (BGH, 1 StR 76/09 v. 31.3.2009 u. BVerfG, 2 BvR 902/06 v. 16.6.2009) **Achtung**: **Beschluss BGH v. 24.11.2009**, StB 48/09 (NJW 2010, 1297): Sicherstellung/Beschlagnahme muss verhältnismäßig sein. Die **Beschlagnahme sämtlicher gespeicherter Daten** ist nur dann mit dem Verhältnismäßigkeitsgrundsatz vereinbar, wenn konkrete Anhaltspunkte vorliegen, dass der gesamte Datenbestand potenziell für das Verfahren beweiserheblich ist. Bei E-Mail-Postfach ist dies **nur ausnahmsweise** der Fall. Ansonsten **muss bereits in der Durchsuchungsanordnung der Beschränkung Rechnung getragen werden, z.B. durch zeitliche**

		Eingrenzung od. Bezugnahme auf bestimmte Inhalte bzw. bestimmte Sender/Empfänger. Ist eine **Sichtung u. Trennung der E-Mails am Zugriffsort nicht möglich**, kann die vorläufige Sicherstellung größerer Teile od. gar des gesamten E-Mail-Bestandes erfolgen, an die sich die **Durchsicht gem. § 110 StPO zur Feststellung der beweiserheblichen E-Mails** anschließen muss. Die **irrelevanten E-Mails** sind danach herauszugeben bzw. **zu löschen**.
	Sicherstellung des E-Mail **auf Computer des Empfängers**	§§ 94 ff. StPO (zum Umfang der Sicherstellung sh. obigen Hinweis)
IMSI (-Catcher)	Ermittlung der IMSI zur **Identifizierung oder Lokalisierung** mittels **IMSI-Catcher**	§ 100i StPO (**Bayern**: nach **Art. 34a Abs. 4 PAG** ist im präventiven Bereich durch den IMSI-Catcher auch die **Unterdrückung der Kommunikation** eines **einzelnen Teilnehmers** oder einer **gesamten Funkzelle** möglich, z.B. im Falle der beabsichtigten Fernauslösung einer Bombe mittels eines Mobiltelefonsignals)
IMEI	Ermittlung der IMEI	§ 113 TKG (hier werden nur Bestandsdaten mitgeteilt, z.B. über ursprünglich mit Vertrag überlassenes Gerät; jedoch keine Aktualisierung)
Funkzelle	**Funkzellenabfrage** Feststellung, welche Mobiltelefone sich zu einer bestimmten Zeit in einer Funkzelle befunden haben	§ 100g Abs. 2 S. 2 StPO (nur über Rechnungsdaten)
GPS-Technik	Einsatz von **GPS-Technik** zur Observation	§ 100h Abs. 1 Nr. 2 StPO mit Annexkompetenz für Maßnahmen zum Einbau der technischen Mittel

Internetforen	Zugriff auf Daten in **geschlossenen Internetforen mittels Zugangsdaten**, die ohne od. gegen den Willen der Kommunikationsbeteiligten erlangt wurden	• § 100a StPO bei Liveüberwachung über Netzbetreiber • §§ 94, 98 StPO gegenüber Telemediendiensten nach Abschluss des Telekommunikationsvorgangs (z.B. Inhalt von Chat, eingestellte Fotos)
Kfz-Ortung	Ist in einem **Kfz** ein **SIM-Modul** (z.B. BMW-Assist/ ConnectedDrive, Audi-Ortungsassistent Cobra, ebenso bei Porsche und Renault, ab 2011 auch bei Opel) eingebaut, so ist dessen **Ortung** möglich (sowie darüber hinaus alle Varianten des TKÜ-Instrumentariums wie Inhaltsdatenüberwachung od. Verkehrsdatenerhebung)	• bei Katalogtat: § 100a StPO; seit 12/2009 ist BMW selbst Netzprovider; ist die FIN (Fahrzeugidentifikationsnummer) bekannt, erfolgt eine Bestandsdatenabfrage bei BMW nach § 113 TKG; mittels dieser Daten kann eine TKÜ Maßnahme nach § 100a StPO veranlasst werden; • keine Katalogtat: liegen Einverständniserklärungen des Herstellers (z.B. BMW) u. des Eigentümers vor, handelt es sich bei der Ortung des SIM-Moduls um keinen Rechtseingriff i.S. des Art. 10 GG (Fernmeldegeheimnis) (rechtl. streitig); folgende Vorgehensweise: auf privatrechtlicher Schiene wird ein GSM-Tracking über einen LocationBasedService-Dienst (z.B. Fa. Ubinam) realisiert. Der LBS-Diensteanbieter erhält die aktuellen Standortdaten über privatrechtliche Verträge zur Funkzellenortung mit den Netzbetreibern.
Mautdaten	**Mautdaten**, die gem. § 4 Abs. 3 Autobahnmautgesetz (ABMG) beim automatisierten Abrechnungssystem mittels GPS u. **On Board Unit** anfallen	Es handelt sich um Verkehrsdaten, die bei der Betreibergesellschaft **TollCollect** anfallen, jedoch einem strengen Verarbeitungs- u. Verwertungsverbot unterliegen, d.h. die Verwendung der Daten ist auf die Zwecke des ABMG beschränkt.

		Auskunftserteilung ist aber **bei Einverständnis** des Betroffenen (z.B. des Spediteurs) mit der Verwertung der Daten zulässig (Antragsformular an TollCollect ist beim LKA vorhanden). TollCollect teilt in diesem Fall die Rufnummer des Moduls und die gespeicherten Streckendaten mit (Achtung: Auskunft ist gebührenpflichtig: 300 EUR/1. Tag im Trefferfall; 200 EUR, wenn keine Daten vorhanden). Mittels dieser Rufnummer können Verkehrsdaten (aufgrd. Urteils d. BVerfG v. 2.3.2010 derzeit nur Verkehrsdaten i.S. der §§ 96 ff. TKG, z.B. Rechnungsdaten) beim Mobilfunknetzbetreiber (z.B. T-Mobile) erhoben, § 100g StPO, od. eine Überwachung nach § 100a StPO durchgeführt werden.
Mailbox	Feststellung von **Nachrichten**, die **auf einer Mailbox gespeichert** sind (z.B. T-Net-Box)	§§ 94, 98 bzw. 99 StPO analog **Hinweis**: Nachrichten, die auf eine Mailboxfunktion gesprochen werden, werden bei einer Telekommunikationsüberwachungsmaßnahme nach § 100a StPO nicht ausgeleitet. Der Umstand, dass eine Nachricht auf die Mailbox gesprochen wurde, kann bei einer § 100a-Maßnahme ggf. über die zusätzlich mitgeteilten Verkehrsdaten erkannt werden.
Online-Durchsuchung	Ermittlung von **gespeicherten Daten** eines **Computers über Online-Verbindung**	Bisher keine gesetzliche Grundlage für sog. „Online-Durchsuchung“ (zulässig nur präventiv-polizeilich nach § 20k BKAG bzw. in Bayern gem. Art. 34d BayPAG)
Spionagesoftware	Installation von **Spionagesoftware** (korrekte Bezeichnung: Überwachungssoftware) in Form von „Trojanern“, Keyloggern u.a. (sh. auch Stichwort VoIP)	keine gesetzliche Grundlage, § 100 h Abs. 1 Nr. 2 StPO nicht ausreichend.

„Stille SMS“	(auch als „*Silent Message*, S*tealth SMS* od. *steathly ping“* bezeichnet); dient der **Ermittlung des Aufenthaltsortes** sowie ggf. der Erstellung von Bewegungsbildern von Personen, die Mobiltelefone nutzen. Es handelt sich um ein Signal (sog. „ping“), das von den Ermittlern an eine ihnen bekannte Mobilfunknummer gesandt wird. Beim Mobilfunkbetreiber wird hierdurch ein Datensatz mit Verbindungsdaten erzeugt, u.a. mit Angaben zur Funkzelle, in der sich das Handy befindet. Auf entsprechende Anordnung werden diese Daten vom betreffenden Mobilfunkbetreiber an die Ermittlungsbehörde übermittelt. Für den Handybesitzer ist dieser Vorgang nicht wahrnehmbar (weder Anzeige auf dem Display noch akustisches Signal)	Rechtsgrundlage ist strittig; § 100 i StPO reicht allein nicht aus. Diese Vorschrift lässt zwar die Aussendung des Signals („ping“) zu, nicht jedoch die nachfolgende Datenabfrage beim Mobilfunkbetreiber (Meyer-Goßner, § 100i Rn. 4); daher nach überwiegender Ansicht nur in Verbindung mit § 100a StPO. Da Standortdaten nach § 100g Abs. 1 S. 3 StPO auch in Echtzeit erhoben werden können, mache dies nach Auffassung des Gesetzgebers (BT-Drucks. 16/5846 S. 51) die Übersendung einer „stillen SMS“ weitgehend entbehrlich (vgl. auch KK-Nack § 100a Rn.11 [Beck online Kommentar]; dies ist jedoch in der Praxis nicht zutreffend: sh. hierzu unten „Technische Tipps: Standortermittlung über Funkzellen“
VoIP	Aufzeichnung v. verschlüsselter **VoIP** (Voice over IP) unter Verwendung entsprechender Überwachungssoftware (sog. Quellen-TKÜ)	§ 100a StPO mit Annexkompetenz zum Einsatz technischer Mittel zur Umsetzung der Anordnung (in der Praxis: zahlreiche verschiedene Anbieter mit unterschiedlichen technischen Voraussetzungen).
W-LAN-Catcher (WiFi-Catcher)	**Gerät zur Feststellung kabelloser Datenströme**; (vergleichbar mit dem IMSI-Catcher, jedoch mit dem Unterschied, dass W-LAN-Catcher keine Funkzelle, sondern einen Zugang ins Internet simuliert) **Einsatzmöglichkeiten**: a) Ausmessung der exakten geographischen Ausbreitung des funktechnisch versorgten Bereichs eines WLAN; b) Identifizierung aller mit dem Access Point verbundenen Endgeräte (z.B. WLAN-fähiges Notebook, PDA, Handy) c) Überwachung/Aufzeichnung des Datenverkehrs über WLAN eines bestimmten Telekommunikationsgerätes	zu a) §§ 161, 163 StPO zu b)Voraussetzungen wie bei IMSI-Catcher, s.o. zu c) § 100a StPO
Zielwahlsuche	Ermittlung von **Rufnummern**, von denen Verbindungen zu einem bekannten Anschluss hergestellt wurden	§ 100g Abs. 1 StPO (Verkehrsdaten i.S. der §§ 96 ff. TKG, z.B. Rechnungsdaten)

	Hinweis: eine Zielwahlsuche ist derzeit nur sehr eingeschränkt möglich, da die entsprechende Technik von den Providern mit Einführung der Vorratsdatenspeicherung ab 1.1. 2008 zurückgebaut worden war. Die Dt. Telekom AG teilte mit Schreiben vom 29.09.2010 mit, dass die Zielwahlsuche zwar nunmehr wieder eingerichtet sei; zur it sei es aber nur möglich, festzustellen, von welchem Festnetzanschluss der Telekom ein beliebiger Anschluss innerhalb der letzten 3 Tage angerufen worden sei.	

III. Gesetzliche Grundlagen

§ 100a Abs. 1 StPO	
Eingriffsvoraussetzungen:	
Form der Telekommunikation, die der Überwachung und Aufzeichnung zugänglich ist	• Begriff „Telekommunikation“ umfasst alle modernen Formen der Datenkommunikation, wie z.B. auch SMS, MMS, E-Mail über Internet-Anbindung (mit ISDN od. DSL), Internet Telefonie (Voice over IP) nebst den mitübertragenen Bildern einer webcam (Beschl. d. LG Hamburg v. 13.09.2010, Az. 608/Qs 17/10), drahtlose Verbindungen unter Einsatz von WLAN-Technik od. Hotspots, Satelliten- und Laserkommunikation, Übermittlung mittels Breitband- und Kabelnetzen einschließlich des Stromnetzes • Zur Mitwirkung verpflichtet sind nicht nur geschäftsmäßige Telekommunikationsdiensteanbieter, sondern auch Betreiber geschlossener Benutzergruppen (Corporate Networks, Intranets) oder in Eigenregie betriebenen Nebenstellenanlagen (Kliniken, Hotels, Haustelefonanlagen); aus der TKÜV ergeben sich aber Einschränkungen bei der Verpflichtung zur technischen Umsetzung • verwertbar sind neben dem eigentlichen Gespräch auch Hintergrundgespräche bzw. –geräusche sowie Aufzeichnungen, die während des Wählvorgangs oder beim Ertönen des Freizeichens gemacht werden (BGH NStZ 08, 473) • verwertbar sind auch Erkenntnisse aus einer Überwachung, wenn der Beschuldigte eine zuvor von ihm selbst hergestellte Telekommunikationsverbindung eines Mobiltelefons versehentlich nicht beendet hat (BGH NStZ 2003, 668) • die Überwachungsanordnung kann sich neben der Rufnummer auch auf die IMEI, die IMSI, ein E-Mail-Account (z.B. paul.mueller@gmx.de od. andere Zugangskennung) oder die Zugangskennung eines (entbündelten) DSL-Anschlusses beziehen (vgl. § 100b Abs. 2 S. 1 Nr. 2 StPO)

durch bestimmte Tatsachen konkretisierter Verdacht auf Katalogtat nach § 100a Abs. 2	• Aufzählung der Katalogtaten des § 100a Abs. 2 StPO ist abschließend • es genügt „einfacher“ Tatverdacht, der aber auf hinreichend sicherer Tatsachenbasis beruhen muss • Teilnahme in Form der Beihilfe od. Anstiftung wird der Täterschaft gleichgestellt
Tat wiegt im Einzelfall schwer	• Einzelfallabwägung erforderlich • im Gesetz genannte minder schwere Fälle sind nicht von vornherein auszuschließen
Subsidiaritätsgrundsatz	• Erforschung d. Sachverhalts od. Ermittlung d. Aufenthalts muss auf andere Weise erschwert od. aussichtslos sein
Anordnungskompetenz:	
Richtervorbehalt nebst Eilkompetenz der Staatsanwaltschaft bei Gefahr in Verzug mit richterlicher Bestätigung binnen drei Werktagen	• § 100b Abs. 1 S. 1 – 3 StPO • Dauer: 3 Monate, mit Verlängerungsmöglichkeit, § 100b Abs. 1 S. 4 u. 5 StPO

§ 100g Abs. 1 StPO	
Eingriffsvoraussetzungen	**Hinweis**: • Bei § 100g StPO geht es nicht um den Inhalt der Telekommunikation (dazu dient § 100a StPO), sondern **Feststellung technischer Daten** (Anschlussstelle, Zeit u. Ort des Gesprächs usw.). • Das **BVerfG hat mit Urteil vom 2.3.2010** die **§§ 113a, 113b TKG und § 100g StPO, soweit dieser den Abruf der nach § 113a TKG zu speichernden Daten erlaubt, für nichtig** erklärt. Damit können insoweit nur noch die **Verkehrsdaten nach §§ 96 ff. TKG** erhoben werden (**z.B. Rechnungsdaten**).
Abs. 1 S. 1 **Nr. 1**: Straftat von auch im **Einzelfall erheblicher Bedeutung**,	• Verweisung auf ‚Katalogtaten“ des § 100a Abs. 2 StPO ist nicht abschließend • **Standortdaten in Echtzeit** dürfen nur nach Nr. 1 erhoben werden (vgl. Abs. 1

insbes. **Katalogtat** nach § 100a Abs. 2 StPO **oder**	S. 3)
Abs. 1 S. 1 **Nr. 2**: **mittels Telekommunikation begangene** Straftat	z.B. mittels Telefon, Fax, Internet od. E-Mail begangene Beleidigung, Bedrohungen od. Ausspähung von Daten
bestimmte Tatsachen müssen Verdacht begründen	• Für eine **Funkzellenabfrage** müssen hinreichend **konkrete Anhaltspunkte** für die **Verwendung eines Mobiltelefons bei der Straftat** gegeben sein (Bär, § 110g Rn. 9, 24;). Allein der Hinweis auf **kriminalistische Erfahrung** genügt nicht. **Ausreichend** ist es aber beispielsweise, wenn ein Beschuldigter bei seiner **Festnahme** im **Besitz eines eingeschalteten Mobiltelefons** war u. im fraglichen Zeitraum auf Mittäter wartete**.** • **Funkzellenabfrage** zur Ermittlung von **Zeugen** ist **unzulässig** (Funkzellenabfrage muss sich immer gegen Beschuldigten bzw. Nachrichtenmittler richten, §§ 100g Abs. 2 S. 1 i.V.m. § 100a Abs. 3 StPO)
Subsidiaritätsgrundsatz: • bzgl. **Nr. 1**: zur Erforschung des Sachverhalts od. Ermittlung des Aufenthaltsorts d. Beschuldigten erforderlich • bzgl. **Nr. 2**: Erforschung des Sachverhalts od. Ermittlung des Aufenthaltsorts d. Beschuldigten auf andere Weise aussichtslos u. angemessenes Verhältnis zur Bedeutung der Sache	

§ 100i Abs. 1 StPO	
Eingriffsvoraussetzungen:	
Durch bestimmte Tatsachen konkretisierter Verdacht	
Straftat von auch im Einzelfall erheblicher Bedeutung	• Verweis „insbesondere“ auf Straftatenkatalog des § 100a Abs. 2 ist nicht abschließend • notwendig ist Täterschaft od. Teilnahme in Bezug auf die erhebliche Straftat, strafbarer Versuch reicht aus;
zur Erforschung des Sachverhalts oder Ermittlung des Aufenthaltsorts des Beschuldigten erforderlich	
Anordnungskompetenz:	
Richtervorbehalt nebst Eilkompetenz der Staatsanwaltschaft bei Gefahr in Verzug mit richterlicher Bestätigung binnen drei Werktagen	• § 100i Abs. 3 S. 1 i.V.m. § 100b Abs. 1 S. 1 – 3 StPO • Dauer: 6 Monate, mit Verlängerungsmöglichkeit, § 100i Abs. 3 S. 2 u. 3 StPO

IV. Tipps für die Praxis:

Hinweise für die Bearbeitung	**Abfassung** von gerichtlichen **Beschlüssen**	• Zur besseren Lesbarkeit, insbesondere im Falle mehrfacher Übermittlung per Telefax, ist auf eine **ausreichende Schriftgröße** zu achten (mindestens Schriftgrad 12); **Fettdruck**, gerade von Anschlussnummern sollte **vermieden**, werden, da auch hierdurch die Lesbarkeit beeinträchtigt wird. • In der Textzeile „Ermittlungsverfahren gegen….. wegen…..“ sollte die Straftat möglichst konkret bezeichnet werden, z. B. „Betrug“, „Mord“; die bloße Angabe „wegen Straftat“ ist nicht ausreichend, da das LKA entsprechende statistische Auswertungen vornehmen muss und ansonsten in einer Vielzahl von Einzelfällen Rückfragen bei der sachbearbeitenden Staatsanwaltschaft nötig werden. • Bei einer **Verkehrsdatenabfrage** (Rechnungsdaten i.S. des § 96 TKG), insbesondere wenn sie sich **auf mehrere Rufnummern/Anschlüsse bezieht**, sollte nur ein **einheitlicher, gesamter Zeitraum angegeben werden**. Da im Falle einer Stückelung nach Tagen oder Stunden die Beauskunftung jedes gesonderten Zeitabschnitts extra in Rechnung gestellt wird.
	Änderung von gerichtlichen **Beschlüssen**	• Ist eine gerichtliche Anordnung über TKÜ-Überwachungsmaßnahmen **zu berichtigen**, sollte nicht der gesamte Beschluss aufgehoben und neu erlassen werden, sondern **nur eine Berichtigung/Ergänzung des bestehenden Beschlusses vorgenommen werden**. Hierdurch können erheblich Kosten gespart werden, da nicht erst komplett abgeschalten und dann wieder neu angeschalten werden muss. Dies kann insbesondere dann eine Rolle spielen, wenn aufgrund richterlicher Anordnung eine Vielzahl von Anschlüssen überwacht wird und z.B. nur eine einzelne Rufnummer berichtigt werden muss. • Wird ein **Beschluss durch den Richter handschriftlich ergänzt**, sollte der Richter die Ergänzung zusätzlich **durch seine Unterschrift am Rand und den Namensstempel autorisieren**. In einigen Fällen wurde ansonsten von den Providern bereits die Umsetzung der Beschlüsse abgelehnt.
	Angabe des **Überwachungs-zeitraums**	Anordnungen nach **§ 100a StPO** sind auf **höchstens drei Monate zu befristen**,, § 100b Abs. 1 S. 4 StPO. Dabei ist darauf zu achten, dass der 3 Monatszeitraum nicht überschritten wird. Die **Frist mit beginnt mit dem Tag der Anordnung**, d.h. das Beschlussdatum ist maßgeblich, nicht erst der im Beschluss angegebene, ggf. abweichende Anfangszeitpunkt. Wird der Anfangs- bzw. Endzeitpunkt durch den Richter im Beschluss handschriftlich eingesetzt, sollte diese handschriftliche Ergänzung durch den Richter am Rand des Beschlusses

		durch seine Unterschrift und den Namensstempel nochmals ausdrücklich zusätzlich autorisiert werden, da in einigen Fällen die Provider ansonsten die Umsetzung bereits abgelehnt haben.
	Angabe der zu überwachenden Anschlüsse: Übergang von der Mobilfunknummer auf die Festnetzkennung; internet accounts	• Es werden zunehmend Handyverträge angeboten, aufgrund derer **unterwegs** über eine **Mobilfunknummer** telefoniert werden kann und die z.B. **zu Hause („homezone“)** über eine **Festnetznummer** verfügen. Wird die Funkzelle der „homezone“ erreicht, **wechselt das Handy meist automatisch in den Festnetzmodus**. Handelt es sich um solche Anschlüsse, was in der Regel durch das LKA mitgeteilt wird, ist im Beschluss nach § 100a StPO sowohl die **Überwachung der Mobilfunknummer als auch der Festnetznummer anzuordnen**. • Insbesondere bei **IPhones** wird zunehmend auch der Zugang zum Internet genutzt (Apps u.a.); der entsprechende **internet-account** muss in diesem Fall **im § 100a-Beschluss ebenfalls angegeben** werden; für die Praxis bedeutet dies, dass künftig z.T. erst im Laufe der Ermittlungen vom LKA festgestellt werden wird, welche der verschiedenen Dienste genutzt werden, mit der Folge, dass § 100a-Beschlüsse ggf. mehrfach erweitert werden müssen.
	Übersendung von **„§ 100a Beschlüssen“**	TKÜ-Maßnahmen werden nach Vorliegen der **§ 100a StPO-Anordnung in Bayern über das Kompetenzzentrum TKÜ-BY** (beim LKA) **bei den Verpflichteten (Netzbetreibern) beantragt**. Der **Originalbeschluss** oder eine beglaubigte Abschrift muss **binnen 1 Woche beim Verpflichteten** vorliegen (§ 12 Abs. 2 S. 2 TKÜV. Dies ist **durch die StA sicherzustellen**. Die Übersendung einer Kopie ist nicht ausreichend. Diese wird von den Providern nicht akzeptiert. **Achtung, Hinweis**: • Übersendung von Originalbeschlüssen ist bei **Verkehrsdatenüberwachung** u.a. nicht erforderlich. Die „Abwicklung“ erfolgt hier **nur über das Kompetenzzentrum TKÜ-BY.** • Netzbetreiber Telefonica **O2 Germany** unterhielt bisher mit **T-Mobile** einen **Roaming-Vertrag**. Dieser wurde jedoch zum 05.01.2010 **gekündigt.** Folglich ist seitdem bei TKÜ-Maßnahmen gegenüber einen Telefonica O2 Kunden keine Doppelanschaltung bei T-Mobile mehr erforderlich. Damit erübrigt sich auch der Versand entsprechender Beschlüsse an T-Mobile.

technische Tipps	**„Auslandskopf-überwachung“**	• Die Zusammenschaltung inländischer u. ausländischer Telekommunikationsnetze erfolgt über diverse Schnittstellen, den sog. **„Auslandsköpfen“.** Überwacht werden können nur im Inland lokalisierte Auslandsköpfe. • Mit **„Auslandskopfüberwachung“** ist die Kommunikation vom Inland zum ausländischen Festnetz- bzw. Mobilfunkanschluss oder umgekehrt gemeint. • **Nicht überwacht** wird die **Telekommunikation des ausländischen Anschlusses im Ausland** und des **inländischen Mobilfunktelefons im Ausland** (4 I, II TKÜV); dies ist nur über ein förmliches RH-Ersuchen möglich; • eine **Live-Ausleitung** ist **derzeit nur 4 Auslandskopfbetreibern** möglich; alle anderen liefern nur Verkehrsdaten. Die meisten Auslandsköpfe betreibt die **Telekom**. Aufgrund **geringer Kapazitäten** ist deren Auslandskopfüberwachung auf Jahre hinaus ausgebucht. Um deshalb **Überwachungslücken** gering zu halten, sollten parallel zur Inhaltsdatenüberwachung die rückwirkenden Verkehrsdaten (Rechnungsdaten) gem. § 100g StPO mittels Zielsuchlaufs bei allen gängigen Festnetz- und Mobilfunknetzbetreibern angefordert werden. Unterstützung hierbei leistet das TKÜ-Kompetenzzentrum des LKA. Bei einer Sachbearbeitung des Verfahrens durch die BPol, muss die StA dafür Sorge tragen, dass die entsprechenden Beschlüsse an alle Provider übersandt werden.
	Ausländische Provider **Alternativen zur Ermittlung der Rufnummer**	• **Bestandsdaten von ausländischen Providern** können nur über **Rechtshilfeersuchen** erlangt werden. • In der Praxis kann sich jedoch auch folgendes Vorgehen anbieten: falls bei der Identifizierung mittels IMSI Catcher eine ausländische IMSI festgestellt wird, empfiehlt sich in **Eilfällen** –statt einer Ermittlung der Rufnummer im Rechtshilfeweg - eine **Anordnung nach § 100a StPO**, weil die IMSI überwacht werden kann und auf die Weise auch die Rufnummer festgestellt wird. Die Ermittlung der Rufnummer wäre in diesem Fall auch über § 100 g StPO möglich, Abfrage dauert aber einige Tage. • Im **präventiven Bereich** können **Bestandsdaten** eines Dienstenutzers bzw. eines E-Mail-Accounts auch von **bestimmten ausländischen Providern** sehr schnell mittels **spezieller Antragsformulare**, die u.a. beim LKA München vorhanden sind, erlangt werden (so für Google, YouTube, Skype, Microsoft [emergency disclosure request])
	eTicketing	In neueren Mobiltelefonen (z.B. von Vodaphone) werden Speicherchips verbaut, welche die Teilnahme am **Elektronischen-Ticket-System (e-Ticketing)** ermöglichen. Das System befindet sich noch in der Aufbauphase. Marktreife ist ab 2011 beabsichtigt.

		Beispiel: Der Nutzer meldet sich in München am Hauptbahnhof an einem **Touchpoint der Bahn** vor Betreten eines Zuges an. Am Fahrtziel in Berlin meldet er sich an einem weiteren Toupoint ab. Der Fahrpreis wird berechnet und elektronisch abgebucht. Die Rechnung wird, spätestens nach 35 Tagen, mittels E-Mail versandt. Hieraus ergeben sich folgende Überwachungsmöglichkeiten: die DeutscheBahn verfügt über die **Daten sämtlicher Funkzellen, die der Nutzer durchfahren hat**. Dabei handelt es sich um **Verkehrsdaten**, da die Daten vom Mobiltelefon gesendet werden und nicht vom Touchpoint. Diese Verkehrsdaten können nach § 100g StPO herausverlangt werden. Aufgrund der Abrechnung mittels E-Mail, ist auch die E-Mail-Adresse hinterlegt. Diese kann von der Deutschen Bahn herausverlangt werden und ggf. anschließend überwacht werden. Neben der Deutschen Bahn wird e-Ticketing derzeit zum Teil auch im Öffentlichen Personennahverkehr (z.B. Verkehrsverbund Rhein-Ruhr, Verkehrsverbund Rhein-Sieg, Verkehrsgemeinschaft Niederrhein, KreisVerkehr Schwäbisch Hall) angeboten. Sh. auch www.eticket-deutschland.de; www.touchandtravel.de.
	GSM bzw. UMTS-Netz; **unterschiedliche Funkzellen**	Mobilfunkendgeräte wurden bisher häufig im GSM-Netz betrieben, neuere Geräte verfügen jedoch über den UMTS-Standart. Das **GSM-Netz** ist vom **UMTS-Netz** zu **unterscheiden**. Beide Netze verfügen über **gesonderte Funkzellen**. Die UMTS-Endgeräte buchen sich bevorzugt im UMTS-Netz ein. Ist keine (oder eine unzureichende) UMTS-Netzversorgung verfügbar, erfolgt die Einbuchung in das GSM-Netz. Daher ist insbesondere bei einer Funkzellenerhebung/-auswertung dafür Sorge zu tragen, dass sowohl die entsprechende GSM- als auch die UMTS-Funkzelle überprüft wird.
	UMTS-Datenkarten	IP Adresse lässt **keinen Rückschluss auf Anschlussinhaber** zu, da zugehörige Ports nicht gespeichert werden müssen (Stichwort: NAPT, network access port translation) (Ausnahme Vodafone). Folge: Ermittlung der Internetnutzer ist nicht möglich.
	IMEI **Manipulations-möglichkeiten**	Die **IMEI** muss nicht immer eindeutig einem bestimmten Gerät zugewiesen sein. Es gibt Computerprogramme, die eine Manipulation ermöglichen. Normalerweise wird beim Verkauf von Mobiltelefonen mit Vertrag eine Bindung von z.B. 12 Monaten festgelegt, d.h. in diesem Zeitraum kann das Endgerät nicht mit der SIM-Karte eines anderen Providers betrieben werden. Durch technische Manipulation kann diese Sperre aufgehoben werden (Stichwort: **SIM-Lock-Entsperrung**). Das **Manipulationsprogramm überschreibt die IMEI und vergibt eine neue IMEI**. In der Praxis ist dies immer die gleiche IMEI, welche in der Software programmiert ist. Auf diese Weise können viele Geräte auf dem Markt

		sein, mit immer der gleichen IMEI.
	PrePaid-Karten **Ermittlungsansätze bzgl. des tatsächlichen Nutzers**	• bei Prepaidkarten werden (bis auf wenige Ausnahmen) keine Verkehrsdaten gespeichert. • Häufig werden **PrePaid-Karten** verkauft, **ohne Verifizierung der (wahren) Personalien des Erwerbers**, da § 95 Abs. 4 TKG nur eine Kann-Vorschrift ist. Eine Bestandsdatenabfrage führt daher hier häufig nicht zum wahren Nutzer. Ein Ermittlungsansatz kann in diesen Fällen sein, über die Aufladevorgänge der PrePaid-Karten zu ermitteln, wer diese vornimmt (häufig zugleich auch Nutzer). Die Provider/Netzbetreiber verfügen über **Daten, wo bzw. an welchen Terminals die Aufladung erfolgte**. Diese Daten werden auf staatsanwaltschaftliche Auskunftsersuchen nach §§ 161 StPO herausgegeben. Falls eine Bezahlung über EC-Karte erfolgte, können die Bankverbindungen im weiteren Verlauf festgestellt werden. Falls die Aufladung bar bezahlt wurde, können eventuell Ermittlungen über installierte Videokameras (z.B. bei Tankstellen) weiterführen. **Muster** eines **Auskunftersuchens**: sh. **unten IX**.
	Rechnungsdaten	Da rückwirkende Verkehrsdaten aufgrund des Urteils des BVerfG vom 2.3.2010 nach der derzeit bestehenden Gesetzeslage nicht erlangt werden können (Nichtigkeit des § 113a TKG), ist daran zu denken, die **Rechnungsdaten nach § 96, 97 TKG** i.V.m. § 100g StPO heraus zu **verlangen**. Die Herausgabe der Rechnungsdaten wird **von dem Urteil des BVerfG nicht berührt**. Hierauf ist bei der Abfassung des richterlichen Beschlusses durch präzise Angabe der derjenigen Daten zu achten, die herausverlangt werden (z.B. „Rechnungsdaten“) und Angabe der Rechtsgrundlage (z.B. §§ 96, 97 TKG, 100g Abs. 1 StPO). Für die Speicherung dieser Rechnungsdaten gelten die in der unten angefügten Tabelle angegebenen, unterschiedlichen Fristen. Mittels der **Rechnungsdaten** lassen sich auch **Funkzellendaten feststellen**! Über die Rechnungsdaten ist ferner eine **Zielwahlsuche möglich**!
	Standortermittlung über Funkzelle	Nach § 100g Abs. 1 S. 3 StPO ist die Erhebung von **Standortdaten in Echtzeit** möglich. **Achtung: Entgegennahme** einer solchen **Anordnung** ist **nur zu den Geschäftszeiten** der Netzbetreiber möglich. Zum Teil auch Schwierigkeiten bei der techn. Umsetzung durch Netzbetreiber. **Empfehlung**: **Anordnung nach § 100a StPO** (sofern die rechtl. Voraussetzungen vorliegen), da bei einer solchen Maßnahme auch die Standortdaten mitgeteilt werden.

V. Definitionen und Begriffsbestimmung

Begriff	Fundstelle	Definition/Bedeutung	Hinweise
Account-Takeover		Engl. für *Benutzerkontoübernahme;* Szenebegriff; die Zugangsdaten (z.B. Benutzername [username] und Passwort) für fremde Benutzerkonten [accounts] werden durch Phishing oder Hacking ausgespäht und anschließend für illegale Zwecke genutzt.	Dient häufig zu Betrugs-/Warenkreditbetrugshandlungen im Umfeld des Onlinehandels
Cache		**Cache** [kæʃ] bezeichnet in der EDV eine Methode, um Inhalte, die bereits einmal vorlagen, beim nächsten Zugriff schneller zur Verfügung zu stellen. Caches sind als Puffer Speicher realisiert, die Kopien zwischenspeichern.	
Cell-ID		Eigene Kennung eines Mobilfunk-Sendemastes; eindeutige Zuordnung nur in Verbindung mit „LAC“ möglich	
Cloud Computing		IT-Infrastrukturen (z.B. Rechenkapazitäten, Datenspeicher, fertige Programmpakete) werden, dynamisch an den Bedarf angepasst, über Netzwerke zur Verfügung gestellt.	Dokumente, Internetseiten, Fotos, Videos werden nicht mehr auf dem heimischen Rechner gespeichert, sondern irgendwo in der „Wolke“, d.h. in Datenzentren, die irgendwo auf der Welt sein können. Die Internetnutzer können dann überall u. mit allen Geräten auf ihre Daten zugreifen und diese mit anderen Nutzern teilen. Der weitere Grundgedanke beim Cloud Computing ist, dass alle Anwendungen von einfacher Software bis hin zu kompletten Betriebssystemen dezentral im Web laufen. Alle Programme lagern auf den Anbieterservern und werden je nach Bedarf geladen (weiterführend: Obenhaus, Cloud Computing als neue Herausforderung für

			Strafverfolgungsbehörden, NJW 2010, 651 ff.)
Daten	**Bestands-daten** (Benutzer-daten)	§ 3 Nr. 3 TKG: „Bestandsdaten“ Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden; §14 Abs. 1 TMG: Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit sie für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (**Bestandsdaten**).	Rufnummer, Anschlusskennung, Name, Anschrift u. Geburtsdatum des Anschlussinhabers; örtliche Lage des Festnetzanschlusses; Gerätenummer (IMEI) des Mobiltelefons, soweit dem Kunden bei Vertragsschluss ein Handy überlassen wurde, statische IP-Adresse.
	Inhalts-daten	Im Rahmen der Telekommunikation (§ 3 Nr. 22 TKG) übertragene bzw. ausgetauschte Informationen und Nachrichten	z.B. Gesprächsinhalte, übertragene Töne, Bilder, Signale aller Art
	Standort-daten § 3 Nr. 19 TKG	Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines Telekommunikationsdienstes für die Öffentlichkeit angeben	
	Verkehrs-daten § 3 Nr. 30 TKG	Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden	Nummer u. Kennung (IMSI; IMEI) des anrufenden u. des angerufenen Teilnehmers sowie zusätzlich bei mobilen Anschlüssen die Standortdaten; Beginn u. Ende der jeweiligen Verbindung nach Datum u. Uhrzeit; vom Nutzer in Anspruch genommene Telekommunikationsdienste; Beginn und Ende der Internet-Nutzung sowie die zugewiesene dynamische IP-Adresse

Download		Herunterladen von Dateien von einem fremden Rechner über eine Netzwerkverbindung	
DSL		Abkürzung für **D**igital **S**ubscriber **L**ine	Breitband-Technologie, um insbes. das Internet mit höherer Geschwindigkeit betreiben zu können; möglich sind auch sog. **entbündelte DSL-Anschlüsse**, dies bedeutet, dass die Zugangskennung nicht mehr über die Rufnummer definiert ist
GPS		Abkürzung für **G**lobal **P**ositioning **S**ystem, satellitengestütztes Ortungssystem	**GPS bei Mobiltelefonen:** **Onboard-Lösung** Navigation erfolgt wie bei einem separaten Navigationsgerät „an Bord“ des Mobiltelefons. Nutzer erwirbt ein Programmpaket samt Kartenmaterial, das auf das Mobiltelefon aufgespielt wird und eine Navigation ermöglicht. **Offboard-Lösung** Navigation wird als Dienstleistung angeboten und je nach Nutzung bezahlt. Die Routenberechnung findet „offboard“ auf dem Rechner des Diensteanbieters statt. Auch für die Datenübertragung entstehen gesonderte Kosten.
GSM		Abkürzung für **G**lobal **S**ystem for **M**obile Communications	Zweite Generation („2G“) der volldigitalen Mobilfunknetze als Nachfolger der analogen Systeme der ersten Generation (in Deutschland: A-Netz, B-Netz und C-Netz);derzeit noch der weltweit am meisten verbreitete Mobilfunk-Standard.
IMEI		Abkürzung für: **I**nternational **M**obile **E**quipment **I**dentity	Hardware-Kennung des Mobiltelefons; IMEI ist eine grundsätzlich einmalig vergebene **mehrstellige Ziffernfolge** (15 bis 17 Ziffern)
IMSI		Abkürzung für: **I**nternational **M**obile **S**ubscriber **I**dentity	**Teilnehmerkennung** mit der ein Mobilfunkteilnehmer in den weltweiten Funknetzen eindeutig identifiziert werden kann. Nicht zu verwechseln mit der eigentlichen

			Mobiltelefonnummer. Die IMSI besteht aus einem **15-stelligen Code**, gebildet aus dem dreistelligen „Mobile Country Code“ (MCC) für Deutschland 262, dem zweistelligen „**Mobile Network** Code“ (MNC) für den nationalen Netzbetreiber (z.B. Dt. Telekom: 01; Vodafone (D2): 02; O2: 07) u. der 10-stelligen „Mobile Subscriber Identification Number“ (MSIN)
IMSI-Catcher		Technisches Gerät zur Simulation einer Funkzelle beim Mobilfunkverkehr, um die IMSI der in Reichweite befindlichen, eingeschalteten Mobiltelefone festzustellen	
Internet-Breitband-Anschluss		Oberbegriff für Internetzugang, z.B. DSL, aber auch Breitbandanschluss über Kabelnetze (z.B. Kabel Deutschland) oder Mobilfunk (UMTS)	
IP-Adresse	**Dynamische IP-Adresse**	IP steht für „**i**nternet **p**rotocol“; elektronische Adresse für Kommunikation im Internet. Die **dynamische IP-Adresse** wird vom Provider aus einem ihm zustehenden Vorrat einem bestimmten Nutzer **nur für die Dauer** seiner **Kommunikation im Internet** zur Verfügung gestellt u. kann nach Beendigung der Verbindung einem anderen Nutzer zugewiesen werden.	Wird den **Verkehrsdaten,** §§ 96 Abs. 1, 113 a Abs. 4 Nr. 1 TKG, zugerechnet, da sie durch den Provider an seinen Internet-Nutzer nur für die Dauer eines konkreten Kommunikationsvorgangs vergeben wird und schon Informationen enthält, wer wann mit wem einen Informationsaustausch vorgenommen hat (Bär Vorb. Rn. 11)
	Statische IP-Adresse	Die **statische IP-Adresse** wird einem **Rechner auf Dauer zugeordnet**	Gehört zu den **Bestandsdaten** i.S.d. § 111 Abs. 1 Nr. 1 TKG, da sie - wie eine Rufnummer – unabhängig von einem konkreten Kommunikationsvorgang vergeben wird u. den Nutzer eindeutig identifiziert (Bär, Vorb. Rn. 11)
LAC		Abkürzung für **L**ocation **A**rea **C**ode, verwaltet mehrere Funkzellen (s.o. Cell ID)	
LAN		Abkürzung für **L**ocal **A**rea **Network**, lokales Netzwerk	
LINK		Englische Bezeichnung für Verknüpfung od. Verbindung, insbes. Verweisung von einer Internet-Seite auf eine andere, um so Zugang und Auffinden der Information zu erleichtern	
Phishing		Gebildet aus den engl. Wörtern *password* und *fishing*. Oberbegriff für eine Vielzahl von Methoden zur Erlangung	

		fremder Zugangsdaten im Internet (TANs für Onlinebanking, Kreditkartendaten, Benutzernamen und Passwörter für Internetshops u. soziale *Netzwerke*). Es kann beispielsweise über spezielle Viren auf infizierten Computersystemen oder Hacken von Servern, auf denen Daten gespeichert sind, erfolgen.	
PIN und PUK		**P**ersonal **I**dentifikation **N**umber bzw. **P**ersonal **U**nlocking **K**ey	• PIN wird i.d.R. beim Einschalten des Handys abgefragt; • PUK (od. Super-PIN) wird vom Provider zur Verfügung gestellt für den Fall der Sperrung od. des Vergessens der PIN
Router		Technisches Gerät, um zwei räumlich getrennte Netzwerke über eine TK-Leitung miteinander zu verbinden	
SIM		Abkürzung für **S**ubscriber **I**dentity **M**odule;	• es handelt sich um eine Chipkarte, die in ein Mobiltelefon eingesteckt wird und zur Identifikation des Nutzers im Netz dient. Sie ist durch eine veränderbare PIN vor unbefugter Benutzung geschützt. • Achtung: die **Nummer** auf der SIM stellt **nicht die Rufnummer** dar!
Skimming		Illegales Ausspähen der Daten von Kreditkarten oder Bankkarten. Mittels technischer Geräte (wie z.B. Magnetstreifenleser u. Videokamera), die verdeckt an Geldausgabeautomaten angebracht werden, werden die Daten von Magnetstreifen oder Chipkarten ausgelesen und dazu gehörige Geheimnummer (PIN) aufgezeichnet. Die Daten der EC- oder Kreditkarte werden dann typischerweise auf einen leeren Kartenrohling (*White Plastic)* aufgespielt, mit dem dann betrügerisch Bargeld an Geldautomaten abgehoben wird. Auch der direkte Einsatz der Daten im Internet, sog. *Carding*, ist möglich und wird praktiziert.	•
Tele-	§ 3 Nr. 24	In der Regel gegen Entgelt erbrachte Dienste, die ganz oder	

kommuni-kations-dienste	TKG	überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich der Übertragungsdienste in Rundfunknetzen	
UMTS		Abkürzung für **U**niversal **M**obile **T**elecommunication **S**ystem	Mobilfunkstandard der dritten Generation (3G), mit dem deutlich höhere Datenübertragungsraten (bis zu 7,2 Mbit/s) als mit dem Mobilfunkstandard der zweiten Generation (2G), dem GSM-Standard (bis zu 220 kbit), möglich sind.
Upload		Hochladen von Dateien auf einem fremden Rechner	
VoIP		Abkürzung für **Voice over IP**,	Sprachübertragung in Echtzeit mittels des Internet-Protokolls, indem die Sprache digitalisiert und anschließend im Internet übertragen wird
WLAN		Abkürzung für **W**ireless **L**ocal **A**rea **N**etwork	lokales Netzwerk, bei dem die Kommunikation zwischen Router und Client drahtlos über Funkverkehr erfolgt
W-LAN-Catcher (WiFi-Catcher)		**Gerät zur Feststellung kabelloser Datenströme**; (vergleichbar mit dem IMSI-Catcher, jedoch mit dem Unterschied, dass W-LAN-Catcher keine Funkzelle, sondern einen Zugang ins Internet simuliert)(WiFi steht für: Wireless Fidelity)	

VI. Übersicht Speicherfristen

Übersicht rückwirkende Verkehrsdaten der Netzbetreiber

Netzbetreiber	§ 96 TKG	Erläuterung
T-Mobile D1	1 - 30 Tage	Alle Verkehrsdaten liegen vollständig vor
	31 - 180 Tage	T-Mobile-Rufnummern: 80 Tage abgehend - Prepaidkunden: 180 Tage - Serviceprovider: 180 Tage
Vodafone (D2) Mobilfunkbereich	1- 7 Tage	Alle Verkehrsdaten liegen vollständig vor (inkl. IMSI-IMEI-Geo-Daten)
	8 - 30 Tage	Alle gebührenpflichtigen ankommenden und alle abgehenden Verkehrsdaten liegen vollständig vor (inkl. IMSI, IMEI, Geo-Daten)
	31 - 80 Tage	IMEI-Kennungen können bis zu diesem Zeitpunkt vollständig beauskunftet werden
	81 - 180 Tage	Alle noch gespeicherten Verkehrsdaten liegen ohne IMEI, IMSI, Geo-Daten vor mit der Folge, dass die abgehenden Daten zu IMEI-Kennungen ab diesem Zeitpunkt nicht mehr festgestellt werden können
Vodafone Festnetzbereich (Integration von Arcor)	92 Tage	Alle Verkehrsdaten liegen vollständig vor
E-Plus	90 Tage	Alle Verkehrsdaten liegen vollständig vor
Telefonica O2	1 - 7 Tage	Alle Verkehrsdaten liegen vollständig vor
	8 - 30 Tage	Es liegen nur noch abrechnungsrelevante Daten vor Eingehende Anrufe liegen nur vor, sofern sie von einem Fremdnetz kamen

Netzbetreiber	§ 96 TKG	Erläuterung
		Verkehrsdaten von Serviceprovidern liegen vor
Deutsche Telekom AG (DTAG)	0 Tage	Ankommende Verkehrsdaten werden nicht gespeichert
	3 Tage	Abgehende Verkehrsdaten liegen vollständig vor (auch Flatrate)
	4 - 80 Tage	Speicherung ist abhängig vom Kundenwunsch. Es gibt folgende Möglichkeiten: - keine Speicherung - anonymisierte Speicherung - vollständige Speicherung
	80 Tage	Abgehende Verkehrsdaten von Telefonzellen liegen vollständig vor
HanseNet	180 Tage	Alle Verkehrsdaten liegen vollständig vor
M-Net	180 Tage	Alle Verkehrsdaten liegen vollständig vor
BT Germany	180 Tage	netzübergreifend beide Richtungen, ankommende Verbindungen können unvollständig sein

Übersicht Funkzellendaten der Netzbetreiber

Netzbetreiber	Verkehrsdaten kommend	Verkehrsdaten gehend	Zusatzinformation
T-Mobile D1	30 Tage	30 Tage	Telefonie und SMS vollständig

Netzbetreiber	Verkehrsdaten kommend	Verkehrsdaten gehend	Zusatzinformation
Vodafone (D2)	7 Tage	80 Tage	Telefonie und SMS vollständig
E-Plus	90 Tage	90 Tage	Telefonie und SMS vollständig
Telefonica O2	7 Tage	30 – 182 Tage	Telefonie und SMS vollständig

Übersicht Speicherfristen IP-Adressen Diensteanbieter

Netzbetreiber	Speicherfrist	Bemerkung
AOL	14 Tage bei kostenlosen Diensten (AIM und ICQ)	-
Microsoft	Hotmail unbegrenzt Live ID die letzen 5 Login	-
Web	30 Tage	-
1 & 1	60 Tage	-
GMX	Daten werden beim nächsten Login überschrieben	bei aktuellem Login keine IP-Adressen Feststellung möglich; an den zuständigen Internetprovider wenden
Yahoo	Keine Speicherung	bei aktuellem Login keine IP-Adressen Feststellung möglich; zukünftige Login Daten sind vorhanden und werden bei Vorliegen eines Beschlusses nach §§ 100a bzw. 100g StPO beauskunftet

Übersicht Speicherfristen IP-Adressen Netzbetreiber

Netzbetreiber	Speicherfrist	Bemerkung
Freenet	Keine Speicherung	bei aktuellem Login keine IP-Adressen Feststellung möglich
AOL	5 Tage	bei aktuellem Login IP-Adressen Feststellung möglich
1 & 1	60 Tage	Non-Access-Provider; als VoIP Anbieter
Kabel Deutschland	Keine Speicherung	bei aktuellem Login IP-Adressen Feststellung möglich; aber hoher technischer Aufwand
Net Cologne	4 Tage	-
Versatel Deutschland	3 Tage	-

Die Speicherfristen können variieren, insbes. auch in Abhängigkeit von den Vertragsmodalitäten bzw. Speicherwünschen der Kunden, und sind ständigen Änderungen unterworfen. (Stand: 21.04.2010)

Quelle: BayLKA.

VII. Daten auf in- und ausländischen Servern

Die Speicherung von Daten

- **auf transnationalen Netzwerken**
- **im Internet** (beispielsweise Filehoster wie „Rapidshare“),
- **auf einem ausländischen Server**.

ist in der Praxis von hoher Bedeutung.

Soll auf gespeicherte Daten zugegriffen werden, so ist dafür ein Durchsuchungs- und Beschlagnahmebeschluss gem. §§ 102 oder 103 StPO erforderlich. Im Geltungsbereich der Strafprozessordnung kann gemäß § 110 Abs. 3 StPO bei dem von einer Durchsuchung Betroffenen ein elektronisches Speichermedium auch dann durchgesehen werden, wenn dies vom Durchsuchungsobjekt räumlich getrennt und anderenfalls der Verlust der gespeicherten Daten zu besorgen ist.

Sind die Daten auf einem Server im Ausland gespeichert, so ist zu prüfen, ob ein Rechtshilfeersuchen zu stellen ist.
Ein Hinweis auf den Serverstandort kann die Länderkennung des E-Mail Accounts sein (z.B. mustermann@yahoo.de).

Kein rechtshilferelevanter Vorgang liegt vor, wenn öffentlich zugängliche Informationen, die weder durch Passwort noch Benutzerkennung dem allgemeinen Zugriff entzogen sind, im Rahmen einer Durchsuchung gespeichert bzw. gesichert werden sollen.

Fallgruppen	Rechtshilfeersuchen?
1.Öffentlich zugängliche Daten, die weder durch **Passwort noch Benutzerkennung gesichert** sind	Bei Zugriff kein Rechtshilfeersuchen erforderlich

2. Geschützte (private) Daten		
a.	**fehlende Zustimmung** des Betroffenen zur Sicherung der Daten, die sich auf ausländischen Server befinden	Rechtshilfeersuchen erforderlich
b.	**Zustimmung**/Kooperation des Betroffenen	
	Betroffener zieht Daten freiwillig aus Netzwerk u. stellt sie Ermittlungsbehörden zur Verfügung	kein Rechtshilfeersuchen (kein Eingriff in fremde Hoheitsrechte)
	Betroffener sichert aufgrund Durchsuchungsbeschlusses selbst die Daten und überlässt sie in Papierform oder auf Speichermedium den Ermittlungsbehörden	kein Rechtshilfeersuchen
	Betroffener überlässt freiwillig den Ermittlungsbehörden Zugangsdaten, die ihrerseits auf das Dateisystem zugriffen und die Daten sichern	Rechtshilfeersuchen erforderlich
	Betroffener hält sich aufgrund Durchsuchungsbeschlusses verpflichtet, den Ermittlungsbehörden die Zugangsdaten zu übergeben u. diese greifen ihrerseits auf die Daten zu	Rechtshilfeersuchen erforderlich

In **Eilfällen** kann die Sicherung von Daten auf Servern **in EU-Mitgliedstaaten auf Art. 20 Abs. 4 EURhÜbk analog** gestützt werden. Diese Regelung gilt zwar grundsätzlich nur für die Telekommunikationsüberwachung, ist nach h.M jedoch weit auszulegen. Es ist jedoch unverzüglich Kontakt mit den Behörden des Serverstaates aufzunehmen und nach einer vorläufigen Sicherung ein entsprechendes Rechtshilfeersuchen zu stellen.

Art. 32 i.V.m. Art. 23 ff Cybercrime Convention (Übereinkommen des Europarates zur Computerkriminalität, für Deutschland seit 1. Juli 2009 in Kraft) sollte derzeit als Rechtsgrundlage für diese sog. „transboarder searches“ **nicht herangezogen** werden, da es zwischen den Unterzeichnerstaaten erhebliche Auslegungsdifferenzen zu Art. 32 gibt.

Ob aufgrund eines drohenden Beweismittelverlusts eine **vorläufige Datensicherung ohne Rechtshilfeersuchen** und ohne vorherige Zustimmung des Serverstaates in Betracht kommt, ist im Einzelfall zu entscheiden. Nach BGHSt 33, 334 entsteht ein **Beweisverwertungsverbot** dann**, wenn der ersuchte Staat eindeutig zum Ausdruck bringt, dass er der Verwertung einer unter Verstoß gegen völkerrechtliche Prinzipien erhobene Erkenntnisse widerspricht und die Rechtshilfe berechtigt verweigert.**

VIII. Wichtige Rechtsnormen des TKG

§ 96 Verkehrsdaten

(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben und verwenden, soweit dies für die in diesem Abschnitt genannten Zwecke erforderlich ist:

1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,
2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

(2) Die gespeicherten Verkehrsdaten dürfen über das Ende der Verbindung hinaus nur verwendet werden, soweit sie zum Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten oder für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich sind. Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen.

(3) Der Diensteanbieter darf teilnehmerbezogene Verkehrsdaten, die vom Anbieter eines Telekommunikationsdienstes für die Öffentlichkeit verwendet werden, zum Zwecke der Vermarktung von Telekommunikationsdiensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Zeitraum nur verwenden, sofern der Betroffene in diese Verwendung eingewilligt hat. Die Daten der Angerufenen sind unverzüglich zu anonymisieren. Eine zielnummernbezogene Verwendung der Verkehrsdaten durch den Diensteanbieter zu den in Satz 1 genannten Zwecken ist nur mit Einwilligung der Angerufenen zulässig. Hierbei sind die Daten der Anrufenden unverzüglich zu anonymisieren.

(4) Bei der Einholung der Einwilligung ist dem Teilnehmer mitzuteilen, welche Datenarten für die in Absatz 3 Satz 1 genannten Zwecke verarbeitet werden sollen und wie lange sie gespeichert werden sollen. Außerdem ist der Teilnehmer darauf hinzuweisen, dass er die Einwilligung jederzeit widerrufen kann.

§ 112 Automatisiertes Auskunftsverfahren

(1) Wer Telekommunikationsdienste für die Öffentlichkeit erbringt, hat die nach § 111 Abs. 1 Satz 1, 3 und 4 und Abs. 2 erhobenen Daten unverzüglich in Kundendateien zu speichern, in die auch Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere Anbieter von Telekommunikationsdiensten vergeben werden, sowie bei portierten Rufnummern die aktuelle Portierungskennung aufzunehmen sind. Für die Berichtigung und Löschung der in den Kundendateien gespeicherten Daten gilt § 111 Abs. 1 Satz 4 und Abs. 4 entsprechend. In Fällen portierter Rufnummern sind die Rufnummer und die zugehörige Portierungskennung erst nach Ablauf des Jahres zu löschen, das dem Zeitpunkt folgt, zu dem die Rufnummer wieder an den Netzbetreiber zurückgegeben wurde, dem sie ursprünglich zugeteilt worden war. Der Verpflichtete hat zu gewährleisten, dass
1. die Bundesnetzagentur jederzeit Daten aus den Kundendateien automatisiert im Inland abrufen kann,
2. der Abruf von Daten unter Verwendung unvollständiger Abfragedaten oder die Suche mittels einer Ähnlichenfunktion erfolgen kann.

Der Verpflichtete hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen können. Die Bundesnetzagentur darf Daten aus den Kundendateien nur abrufen, soweit die Kenntnis der Daten erforderlich ist
1. für die Verfolgung von Ordnungswidrigkeiten nach diesem Gesetz oder nach dem Gesetz gegen den unlauteren Wettbewerb,
2. für die Erledigung von Auskunftsersuchen der in Absatz 2 genannten Stellen.
Die ersuchende Stelle prüft unverzüglich, inwieweit sie die als Antwort übermittelten Daten benötigt, nicht benötigte Daten löscht sie unverzüglich; dies gilt auch für die Bundesnetzagentur für den Abruf von Daten nach Satz 6 Nr. 1.

(2) Auskünfte aus den Kundendateien nach Absatz 1 werden
1. den Gerichten und Strafverfolgungsbehörden,
2. den Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr,
3. dem Zollkriminalamt und den Zollfahndungsämtern für Zwecke eines Strafverfahrens sowie dem Zollkriminalamt zur Vorbereitung und Durchführung von Maßnahmen nach § 39 des Außenwirtschaftsgesetzes,
4. den Verfassungsschutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst, dem Bundesnachrichtendienst,
5. den Notrufabfragestellen nach § 108 sowie der Abfragestelle für die Rufnummer 124,
6. der Bundesanstalt für Finanzdienstleistungsaufsicht sowie
7. den Behörden der Zollverwaltung für die in § 2 Abs. 1 des Schwarzarbeitsbekämpfungsgesetzes genannten Zwecke über zentrale Abfragestellen nach Absatz 4 jederzeit erteilt, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind und die Ersuchen an die Bundesnetzagentur im automatisierten Verfahren vorgelegt werden.

(3) Das Bundesministerium für Wirtschaft und Technologie wird ermächtigt, im Einvernehmen mit dem Bundeskanzleramt, dem Bundesministerium des Innern, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen sowie dem Bundesministerium der

Verteidigung eine Rechtsverordnung mit Zustimmung des Bundesrates zu erlassen, in der geregelt werden
1. die wesentlichen Anforderungen an die technischen Verfahren
    a) zur Übermittlung der Ersuchen an die Bundesnetzagentur,
    b) zum Abruf der Daten durch die Bundesnetzagentur von den Verpflichteten einschließlich der für die Abfrage zu verwendenden Datenarten und
    c) zur Übermittlung der Ergebnisse des Abrufs von der Bundesnetzagentur an die ersuchenden Stellen,
2. die zu beachtenden Sicherheitsanforderungen,
3. für Abrufe mit unvollständigen Abfragedaten und für die Suche mittels einer Ähnlichenfunktion
    a) die Mindestanforderungen an den Umfang der einzugebenden Daten zur möglichst genauen Bestimmung der gesuchten Person,
    b) die Zeichen, die in der Abfrage verwendet werden dürfen,
    c) Anforderungen an den Einsatz sprachwissenschaftlicher Verfahren, die gewährleisten, dass unterschiedliche Schreibweisen eines Personen-, Straßen- oder Ortsnamens sowie Abweichungen, die sich aus der Vertauschung, Auslassung oder Hinzufügung von Namensbestandteilen ergeben, in die Suche und das Suchergebnis einbezogen werden,
    d) die zulässige Menge der an die Bundesnetzagentur zu übermittelnden Antwortdatensätze sowie
4. wer abweichend von Absatz 1 Satz 1 aus Gründen der Verhältnismäßigkeit keine Kundendateien für das automatisierte Auskunftsverfahren vorhalten muss; in diesen Fällen gilt § 111 Abs. 1 Satz 5 entsprechend.

Im Übrigen können in der Verordnung auch Einschränkungen der Abfragemöglichkeit für die in Absatz 2 Nr. 5 bis 7 genannten Stellen auf den für diese Stellen erforderlichen Umfang geregelt werden. Die technischen Einzelheiten des automatisierten Abrufverfahrens gibt die Bundesnetzagentur in einer unter Beteiligung der betroffenen Verbände und der berechtigten Stellen zu erarbeitenden Technischen Richtlinie vor, die bei Bedarf an den Stand der Technik anzupassen und von der Bundesnetzagentur in ihrem Amtsblatt bekannt zu machen ist. Der Verpflichtete nach Absatz 1 und die berechtigten Stellen haben die Anforderungen der Technischen Richtlinie spätestens ein Jahr nach deren Bekanntmachung zu erfüllen. Nach dieser Richtlinie gestaltete mängelfreie technische Einrichtungen müssen im Falle einer Änderung der Richtlinie spätestens drei Jahre nach deren Inkrafttreten die geänderten Anforderungen erfüllen.

(4) Auf Ersuchen der in Absatz 2 genannten Stellen hat die Bundesnetzagentur die entsprechenden Datensätze aus den Kundendateien nach Absatz 1 abzurufen und an die ersuchende Stelle zu übermitteln. Sie prüft die Zulässigkeit der Übermittlung nur, soweit hierzu ein besonderer Anlass besteht. Die Verantwortung für die Zulässigkeit der Übermittlung tragen die in Absatz 2 genannten Stellen. Die Bundesnetzagentur protokolliert für Zwecke der Datenschutzkontrolle durch die jeweils zuständige Stelle bei jedem Abruf den Zeitpunkt, die bei der Durchführung des Abrufs verwendeten Daten, die abgerufenen Daten, ein die abrufende Person eindeutig bezeichnendes Datum sowie die ersuchende Stelle, deren Aktenzeichen und ein die ersuchende Person eindeutig bezeichnendes Datum. Eine Verwendung der Protokolldaten für andere Zwecke ist unzulässig. Die Protokolldaten sind nach einem Jahr zu löschen.

(5) Der Verpflichtete nach Absatz 1 hat alle technischen Vorkehrungen in seinem Verantwortungsbereich auf seine Kosten zu treffen, die für die Erteilung der Auskünfte nach dieser Vorschrift erforderlich sind. Dazu gehören auch die Anschaffung der zur Sicherstellung der Vertraulichkeit und des Schutzes vor unberechtigten Zugriffen erforderlichen Geräte, die Einrichtung eines geeigneten Telekommunikationsanschlusses und die Teilnahme an dem geschlossenen Benutzersystem sowie die laufende Bereitstellung dieser Vorkehrungen nach Maßgaben der Rechtsverordnung und der Technischen Richtlinie nach Absatz 3. Eine Entschädigung für im automatisierten Verfahren erteilte Auskünfte wird den Verpflichteten nicht gewährt.

§ 113 Manuelles Auskunftsverfahren

(1) Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, hat im Einzelfall den zuständigen Stellen auf deren Verlangen unverzüglich Auskünfte über die nach den §§ 95 und 111 erhobenen Daten zu erteilen, soweit dies 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 Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes erforderlich ist. Auskünfte über Daten, mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte Speichereinrichtungen geschützt wird, insbesondere PIN oder PUK, hat der nach Satz 1 Verpflichtete auf Grund eines Auskunftsersuchens nach § 161 Abs. 1 Satz 1, § 163 Abs. 1 der Strafprozessordnung, der Datenerhebungsvorschriften der Polizeigesetze des Bundes oder der Länder zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung, § 8 Abs. 1 des Bundesverfassungsschutzgesetzes, der entsprechenden Bestimmungen der Landesverfassungsschutzgesetze, § 2 Abs. 1 des BND-Gesetzes oder § 4 Abs. 1 des MAD-Gesetzes zu erteilen; an andere öffentliche oder nicht öffentliche Stellen dürfen diese Daten nicht übermittelt werden. Ein Zugriff auf Daten, die dem Fernmeldegeheimnis unterliegen, ist nur unter den Voraussetzungen der hierfür einschlägigen gesetzlichen Vorschriften zulässig. Über die Auskunftserteilung hat der Verpflichtete gegenüber seinen Kundinnen und Kunden sowie Dritten gegenüber Stillschweigen zu wahren.
(2) Der Verpflichtete nach Absatz 1 hat die in seinem Verantwortungsbereich für die Auskunftserteilung erforderlichen Vorkehrungen auf seine Kosten zu treffen.

IX. Musteranordnung (Auskunft über Aufladeverhalten Prepaid-Handy

Staatsanwaltschaft ……..

Geschäftsnummer der StA: , den ……

Ermittlungsverfahren

gegen

wegen

hier: Auskunft über Direktaufladungen

Sehr geehrte Damen und Herren,

im genannten Ermittlungsverfahren ist gemäß § 161 StPO festzustellen, ob für die Anschlüsse

1. Anschluss: Anschlussnummer/ Kennung:
Anschlussinhaber:
Anschrift:
Netzbetreiber/ Provider:

2. Anschluss: Anschlussnummer/ Kennung:
Anschlussinhaber:
Anschrift:
Netzbetreiber/ Provider:

Direktaufladungen und ein damit verbundener Einsatz von EC- Karten und/ oder Kreditkarten erfolgt ist.

Im Einzelnen wird gebeten mitzuteilen:

- Welche Aufladevorgänge sind für die genannten Rufnummern verzeichnet?
- Welche Beträge wurden aufgeladen?

- An welchen Standorten erfolgten die Aufladungen?
- Welche Terminal-ID und welches Aufladegerät wurde verwendet?
- Wer war der Vertragspartner der Aufladung?
- Erfolgte die Aufladung mittels EC-Karte und/ oder Kreditkarte?
- Welche Karten- bzw. Kontonummer wurde für die Aufladung verwendet?

Ich bitte Sie, die Auskunft aus Vereinfachungsgründen direkt an die von mir beauftragte
zu Händen von , mitzuteilen.

Wichtige Hinweise:

Die Ihnen entstehenden Kosten können nach § 7 des Justizvergütungs- und entschädigungsgesetzes (JVEG) in Rechnung gestellt werden.

Die verlangte Auskunft betrifft lediglich personenbezogene Bestandsdaten sowie Rechnungsdaten im Sinne der §§ 95, 97 Abs. 2 Nr. 3 TKG; Sie sind daher zur Erteilung der Auskunft auch ohne Vorliegen eines richterlichen Beschlusses nach § 100g StPO verpflichtet. Auch eine abweichende rechtliche Auffassung berechtigt Sie nicht zur Verweigerung der Auskunftserteilung.
Sollten Sie die Auskünfte nicht fristgerecht oder vollständig erteilen, können in Ihrem Hause tätige Angestellte als Zeugen hierzu vernommen werden. Diese sind gesetzlich verpflichtet, bei dem Staatsanwalt zu erscheinen und anhand von Unterlagen zur Sache auszusagen. Bei unberechtigtem Ausbleiben oder unberechtigter Aussageverweigerung werden Zeugen hierdurch entstandene Kosten auferlegt und ein Ordnungsgeld bis zu EUR 1.000,00 festgesetzt. Auch die zwangsweise Verführung sowie die Anordnung von Erzwingungshaft für einen Zeitraum bis zu 6 Monaten ist zulässig (§§ 161a, 51, 70 Strafprozessordnung). Zur Vorlage der Beweisunterlagen besteht ebenfalls eine gesetzliche Verpflichtung, die notfalls zwangsweise durchgesetzt werden kann (§ 95 Strafprozessordnung).
Sollte innerhalb Ihres Unternehmens eine andere Stelle zur Erteilung der Auskunft zuständig sein, bitte ich um Weiterleitung dieses Schreibens. Für Ihre Mühe bedanke ich mich im Voraus.

Mit freundlichen Grüßen
Staatsanwalt