Generalstaatsanwaltschaft
München

Leitfaden zum Datenzugriff

insbesondere für den Bereich der Telekommunikation

Stand: Juni 2013

A) Vorwort:

Aufgrund des technischen Fortschritts gilt es bei der Überwachung der Telekommunikation und beim Zugriff auf in elektronischen Medien gespeicherten Daten immer wieder neue Herausforderungen zu bewältigen. Die nachfolgenden Ausführungen sollen dazu Hilfestellung geben, ohne dass es möglich ist, alle tatsächlichen und rechtlichen Fragen vertieft und abschließend zu behandeln. Der Leitfaden wird regelmäßig aktualisiert.

Als Ansprechpartner für Änderungs- oder Aktualisierungsvorschläge steht der Leiter der Abteilung C der Generalstaatsanwaltschaft München (Telefonnr.: 089/5597-4469) und für Fragen im Zusammenhang mit konkreten Maßnahmen das Kompetenzzentrum TKÜ-BY, Bayerisches Landeskriminalamt, Sachgebiet 633) zur Verfügung

Telefonnummern:

- 089/1212-3355 allgemeine Anfragen
- 089/1212-3351 konkrete Fragen zu 100a-Maßnahmen

Der Leitfaden ist in Bayern im Intranet-Portal der Staatsanwaltschaften eingestellt.

Aktuelle Entwicklungen:

Der Gesetzgeber hat den Anforderungen des Bundesverfassungsgerichts, die sich aus dem Beschluss vom 24. Januar 2012 (1 BvR 1299/05) ergeben, durch eine Änderung verschiedener Gesetze, insbesondere des § 113 TKG und die Einfügung von § 100 j StPO, umgesetzt. Die Änderungen treten am 01.07.2013 in Kraft.

Ab diesem Zeitpunkt haben Telekommunikationsanbieter auf schriftlichen Anfrage der Ermittlungsbehörden (Staatsanwaltschaften, Polizei, Zoll usw.) gem. § 100j Abs. 1 Satz 1 StPO Auskünfte zu Bestandsdaten und gem. § 100j Abs. 2 StPO zu Internetprotokolladressen (dynamische IP) zu erteilen.

§ 100j Abs.1 Satz 2 StPO betrifft Daten, die als Zugangssicherungscodes (z.B. Passwörter, PIN, PUK) dienen. Auskunftsersuchen für diese Daten bedürfen, sofern

B) Inhaltsverzeichnis

C) **Übersicht über Ermittlungsmaßnahmen:**

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
Aufzeichnung und Überwachung von Telekommunikation	Überwachung und Aufzeichnung des **Inhalts** eines **Telekommunikationsvorgangs** (z.B. Telefongespräche, SMS, MMS, E-Mail, Internetkommunikation)	§ 100a StPO	eri 100a 1	eil 100a 1
Auswertung Gerätespeicher/ SIM-Karte	Sicherung und Auswertung von Daten aus Gerätespeicher oder SIM-Karte	§ 94 StPO	eri db 1 eri db 2	eri db 4
Datenauskunft	**Bestandsdaten**	• § 100j Abs. 1 Satz 1 StPO bzgl. Tele**kommunikations**diensteanbietern (Deutsche Telekom AG, Vodafone, Telefonica O2, E-Plus) • § 161 Abs.1, 163 Abs. 1 StPO i.V.m.§ 14 Abs. 2 TMG bzgl. Tele**medien**diensteanbieter (eBay, YouTube, Facebook, Webmail u.a.)	Anfrage erfolgt in der Regel durch die Ermittlungspersonen der Staatsanwaltschaften	

[1] Die Länder Baden-Württemberg, Bayern, Bremen, Niedersachsen, Saarland, Sachsen, Sachsen-Anhalt, Thüringen und Rheinland-Pfalz arbeiten in der EDV im web-sta-Verbund zusammen. Hier sind die im mit web.sta verbundenen Textsystem TV-StA eingestellten Bausteine/Formulare aufgeführt.

Stichwort	Durchzuführende Maßnahme		Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
	Nutzungsdaten		§§ 15 Abs. 1, Abs. 5 Satz 4 i.V.m. 14 Abs. 2 TMG bzgl. Telemediendiensteanbieter bei Nutzungsdaten	Hier verlangen die Telemediendienste-anbieter meist eine staatsanwaltschaftliche Anfrage gem. §§ 161, 163 StPO. Ggf. ist auch ein Durchsuchungs- und Beschlagnahmebe-schluss gem. §§ 94,98, 103 StPO (eri db 2) erforderlich.	
	Online-Zugangsdaten (z.B. für E-Mail-Postfach, soziale Netzwerke etc.)		• entweder aus Überwachung des DSL- oder Breitbandkabelanschlusses bekannt • oder Erhebung beim Diensteanbieter des E-Mail-, Chat- oder Onlinedienstes gemäß § 100j Abs. 1 Satz 2 StPO (bis 30.06.2013: §§ 113 Abs. 1 S. 2 TKG, 161 StPO)	Beschluss gem. § 100j Abs. 3 StPO Formblatt/Textbaustein wird entwickelt	
	Online-Zugangsdaten für Tele-medien (z.B. Ebay oder andere Online-Dienste)		gemäß §§ 14 Abs. 2 TMG, 161 StPO (Beachte: § 100j StPO gilt nur für TK-Anbieter, nicht für Telemedien)	w.o.	
	Personenaus-kunft	zu vorhandener Rufnummer	• § 100j Abs. 1 Satz 1 StPO	**Anfrage erfolgt in der Regel durch die Ermittlungspersonen derStaatsanwaltschaften**	
		zu vorhandener dynamischer IP-Adresse	• **§ 100j Abs. 1 Satz 1 i.V.m. Abs. 2 StPO** • bzgl. der Speicherfristen siehe Übersichten unten G	w.o.	
		zu vorhandener E-Mail-Adresse oder statischer IP-Adresse	§ 100j Abs. 1 Satz 1 StPO	w.o.	

Stichwort	Durchzuführende Maßnahme		Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
Datenauskunft	**Standortdaten von Mobiltelefonen**	über Mobilfunknetz	§§ 100a oder 100g StPO Die Erhebung von Standortdaten in Echtzeit über die Funkzelle gemäß § 100g Abs. 1 S. 3 StPO ist nur im Falle des Satzes 1 Nr. 1 dieser Vorschrift zulässig. **Hinweis**: bei Mobiltelefon im Stand-By-Betrieb ist nur der LAC [location area code] feststellbar; dieser wird jedoch nicht gespeichert; eine retrograde Abfrage nach § 100g StPO ist daher nicht sinnvoll; Zur Gefahrenabwehr können die Standortdaten nach § 20k BKAG bzw. nach jeweiligem Landespolizeigesetz präventiv-polizeilich (Bayern: Art. 34a i.V.m. 34b BayPAG; BW: § 23a PolGBW) ermittelt werden.	eri 100a 1 eri 100g 1	eil 100a 1 eil 100g 1
		mittels **GPS-Empfänger**, die serienmäßig in modernen Mobiltelefonen eingebaut sind	Auf GPS-Daten, die beispielsweise in Smartphones gespeichert werden, kann derzeit online nicht zugriffen werden. Derartige Daten können nur nach Beschlagnahme eines solchen Gerätes ausgelesen werden. Online-Standortdaten können nur über die aktuell genutzte Funkzelle erhoben werden (siehe oben)	(-)	**(-)**
	Rechnungsdaten		Erhebung bei TK-Unternehmen: §§ 100g StPO,96, 97 TKG	eri 100g 1	eil 100g 1
			Im Rahmen von Durchsuchungen beim Betroffenen aufgefundene Unterlagen können nach §§ 94, 98 StPO sichergestellt/beschlagnahmt werden.	eri db 1 eri db 2	eri db 4

Stichwort	Durchzuführende Maßnahme		Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
Datenauskunft	**Verkehrsdaten**	Auskunft über künftig anfallende Verkehrsdaten	Gem. § 100g Abs. 1 S. 3 StPO können künftig anfallende Verkehrsdaten erhoben werden. Das Urteil des BVerfG v. 2.3.2010 zur Vorratsdatenspeicherung steht dem nicht entgegen. Diese Daten werden als Nebenprodukt auch bei TKÜ-Maßnahmen nach § 100a StPO ausgeleitet.	eri 100g 1 eri 100a 1	eil 100g 1 eil 100a 1
		Auskunft über in der Vergangenheit angefallene Verkehrsdaten	• § 100g Abs. 1 S. 1 Nr. 1 u. Nr. 2 StPO • Auskunft bzgl. **Verkehrsdaten i.S. der § 96, 97, 100 TKG, (Rechnungsdaten, Betriebsdaten zur Störungsbeseitigung)** weiterhin zulässig. • Auswirkungen des Urteils des BVerfG v. 2.3.2010: §§ 113a, 113b TKG u. §100g StPO, wurden nur soweit für nichtig erklärt, als diese den Abruf nach § 113a TKG gespeicherter Daten (sog. Vorratsdaten) erlaubten, Die Vorratsdatenspeicherung findet entgegen dem geltendem EU-Recht in Deutschland derzeit nicht statt. Daher werden derzeit nur die oben genannten Rechnungs- und Betriebsdaten gespeichert.	eri 100g 1	eil 100g 1
Datenauskft	**PIN/PUK**		• **§ 100j Abs. 1 Satz 2 StPO (statt bisher § 113 Abs. 1 Satz 2 TKG i.V.m. §§ 161, 163 StPO)** • Anlässlich einer Durchsuchung (bei Betroffenem) aufgefundene Unterlagen können nach §§ 94, 98 StPO sichergestellt/beschlagnahmt werden.	Beschluss gem. § 100j Abs. 3 StPO Formblatt/Textbaustein wird entwickelt eri db 1	**eri db2**

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
	Vertragsverhältnisse	§ !00j Abs. 1 Satz 1 StPO: Auskunft über sämtliche zum Vertragsverhältnis gespeicherte Daten, z.B. Rechnungsadresse, Kontoverbindung, Personalausweisdaten, Referenzerreichbarkeit, Vertragsvermittler	Anfrage erfolgt in der Regel durch die Ermittlungspersonen der Staatsanwaltschaften	
Durchsicht von räumlich getrennten Speichermedien	Durchsicht eines **räumlich getrennten Speichermediums** im Rahmen einer Durchsuchung bei dem Betroffenen, soweit hierauf von einer während der Durchsuchung aufgefundenen EDV-Anlage zugegriffen werden kann. Dies gilt auch für das Abrufen von E-Mails beim Provider während der Durchsuchung. • **Passwort** Wird dieses bei der Durchsuchung aufgefunden, ist der Zugriff auf die dortigen Informationen zulässig • **Speicherung auf ausländischem 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., S. 55). Im Rahmen der Anwendbarkeit	§§ 102, 103, 110 Abs. 3 StPO	eri db 1 eri db 2	eri db 4

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
	der Cyber Crime Convention (CCC) ist gem. Art. 32b CCC bei Einverständnis des Berechtigten keine Rechtshilfe erforderlich			
E-Mail	Aufzeichnung und Überwachung des E-Mail-Verkehrs **während der Übertragungsphase** • Absenden der Nachricht bis zum Ankommen im Speicher des Providers • Abrufen der Nachricht durch den Empfänger beim Provider	§ 100a StPO	eri 100a 1	eil 100a 1
	Sicherstellung von E-Mails auf **Computer des Empfängers**	**§§ 94 ff. StPO** Hinweis zum Umfang der Sicherstellung siehe nachfolgende Ausführungen unter “Beschränkung der Durchsuchungsanordnung“, S. 14	eri db 1 eri db 2	eri db 4

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
	Zugriff auf E-Mails beim **Provider** im **Postfach des Empfängers**	Der Gesetzgeber hat mit den gesetzlichen Neureglungen zum 01.01.2008 dazu keine gesetzliche Klarstellung vorgenommen, so dass die Rechtsgrundlage für den Zugriff weiterhin strittig ist.		
E-Mail		1. **§§ 94, 98, 103 StPO – offene Maßnahme** (BGH, NJW 2010, 1297, BVerfG, NJW 2009, 2431): • Die Maßnahme richtet sich gegen den Provider. Es kommt nicht darauf an, ob der Empfänger von dem E-Mail bereits Kenntnis genommen hat, sondern auf seine Möglichkeit des sofortigen Zugriffs auf die Mailbox (KK-StPO/Nack §100a Rn. 22). Die Beschlagnahme ist den Betroffenen, also auch dem Beschuldigten, und Verfahrensbeteiligten bekannt zu machen (§§ 33 Abs. 1, 35 Abs. 2StPO), *ohne* dass es eine Möglichkeit der Rückstellung gibt (BGH NJW 2010, 1297). • **Beschränkung der Durchsuchungsanordnung:** Die Beschlagnahme sämtlicher gespeicherter Daten gem. § 98 StPO ist allenfalls dann mit dem Grundsatz der Verhältnismäßigkeit vereinbar, wenn konkrete Anhaltspunkte dafür vorliegen, dass der gesamte Datenbestand, auf den zugegriffen werden soll, für das Verfahren potenziell beweiserheblich ist. Bei	eri db 1 eri db 2	**eri db 4**

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
E-Mail		einem E-Mail-Postfach wird dies in aller Regel nicht der Fall sein. Ansonsten muss bereits in der **Durchsuchungsanordnung** der **Beschränkung** Rechnung getragen werden, z.B. durch zeitliche Eingrenzung od. Bezugnahme auf bestimmte **I**nhalte bzw. bestimmte Sender/Empfänger. • **Durchführung der Maßnahme am Zugriffsort:** **I**st eine **Sichtung u. Trennung der E-Mails am Zugriffsort nicht möglich**, kann die vorläufige Sicherstellung größerer Teile oder 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**. Ggfls. kann auch bei Durchsuchung beim Betroffenen gem. § 110 Abs. 3 StPO auf E-Mail-Postfach zugegriffen werden, wenn Zugangsdaten bekannt sind.		

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
E-Mail		2. **§§ 99, 95, 100 Abs.3 StPO - verdeckte Maßnahme** (BGH -1 StR 76/09 - vom 31.03.2009 und BeckOK-StPO/Graf, § 99 Rn. 9-11): • Anordnung gem. § 99 StPO und Herausgabeverlangen gem. § 95 Abs.2 StPO; • Benachrichtigung kann gem. § 101 Abs.5 StPO zurückgestellt werden. • **Hinweis:** • § 99 StPO umfasst alle gesendeten und empfangenen E-Mails. • Durchsicht des Postfachinhaltes h.M.: Bei dieser Maßnahme gem. § 99 StPO, kann nach dem Wortlaut des § 100 Abs. 3 StPO die Durchsicht des Postfachinhaltes nur auf die Staatsanwaltschaft übertragen werden (str.). a.A.(Kochheim, Verdeckte Ermittlungen im Internet, S. 32): Auf die Durchführung der Maßnahme sind nicht die Formvorschriften des § 100 Abs. 2 bis 6 StPO anzuwenden, sondern ein gestaffeltes Verfahren, das sich an den §§ 95 Abs. 1 und 110 Abs. 1 StPO orientiert. Danach kann die Durchsicht des Postfachinhaltes gem. § 110 Abs. 1 StPO auf Ermittlungspersonen der Staatsanwaltschaft übertragen werden.	Formblatt /Textbaustein wird entwickelt	Formblatt /Textbaustein wird entwickelt

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
		3. § 100a StPO - verdeckte Maßnahme Vertreten wird auch folgendes (Meyer-Goßner, StPO, § 100a Rn. 6b, m.w.N.): • Für den Fall heimlicher Ermittlungen stellt BVerfG besonders hohe Anforderungen an Bedeutung der zu verfolgenden Tat und den Grad des Tatverdachts. Daher nur § 100a StPO geeignete Rechtsgrundlage. • Hinweis: Erfahrungsgemäß verlangt Telekom für nicht gelesene E-Mails einen § 100a Beschluss.	eri 100a 1	eil 100a
		4. Beschlagnahme von E-Mails gem. §§ 94, 98, StPO gegenüber Beschuldigten – offene Maßnahme: Erfolgt der Zugang zu dem E-Mail-Postfach nicht über den Provider, sondern über erlangte Zugangsdaten (z.B. TKÜ oder freiwillige Herausgabe), richtet sich die Maßnahme gegen den Beschuldigten. Rechtsgrundlage hierfür sind §§ 94, 98 StPO.	eri db1	eri db 4

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
Funkzelle	**Funkzellenabfrage**: • Feststellung, welche mobilfunkfähigen Endgeräte (insbes. Mobiltelefone, Smartphones, Tablet-PC`s) zu einer bestimmten Zeit in einer Funkzelle kommuniziert haben. • Gespeichert sind nur die Mobilfunkteilnehmer, die kommuniziert haben (Telefonie, SMS, Daten). Sog. Stand-by-Daten werden nicht gespeichert. • Von Smartphones werden Verkehrsdaten von den Netzbetreibern nur gespeichert, wenn über Apps tatsächlich Daten gesendet oder geladen werden.	§ 100g Abs. 2 S. 2 StPO **Hinweis:** Die Bestimmung der ermittlungsrelevanten Funkzellen erfolgt durch das BLKA München, wenn die bayerische Polizei ermittelt. Nur wenn diese Bestimmung erfolgt ist, ist im Gegensatz zu einer Adressanfrage beim Netzbetreiber ein sehr genaues Ergebnis der Abfrage zu erwarten (vgl. E, Stichwort Standortermittlung über Funkzelle , Seite 37)	eri 100g 1	eil 100g 1

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
GPS-Technik	Einsatz von GPS-Technik zur Observation	§ 100h Abs. 1 Nr. 2 StPO mit Annexkompetenz für Maßnahmen zum Einbau der technischen Mittel	Anordnung der StA – ggfls. in Kombination mit Observation eri obs 1	eil etm 7
IMSI-Catcher	Ermittlung der IMSI zur Identifizierung oder Lokalisierung mittels IMSI-Catcher	§ 100i StPO für repressive Zwecke zur Identifizierung und Lokalisierung Daneben präventiv-polizeilich: • **Bayern**: nach **Art. 34a Abs. 4 PAG** kann die Polizei (nicht die Staatsanwaltschaft) im präventiven Bereich durch den IMSI-Catcher auch die **Kommunikation** eines **einzelnen Teilnehmers** oder einer **gesamten Funkzelle** unterdrücken, z.B. im Falle der beabsichtigten Fernauslösung einer Bombe mittels eines Mobiltelefonsignals; • **Baden-Württemberg**: nach §23a PolGBW)	eri 100i 1 **ACHTUNG:** Beschluss bzw. Anordnung darf nur an ausführende Ermittlungsdienststelle, **nicht** an Provider geschickt werden	eil 100i 1 **ACHTUNG:** Beschluss bzw. Anordnung darf nur an ausführende Ermittlungdienststelle, **nicht** an Provider geschickt werden

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
IMEI	Ermittlung der IMEI	§ 100j Abs. 1 Satz 1 StPO Es werden aber nur Bestandsdaten mitgeteilt, soweit im Rahmen des ursprünglichen Vertrages ein Mobiltelefon überlassen wurde (§ 111 Abs. 1 Satz 1 Nr. 5 TKG); jedoch keine Aktualisierung der Daten	Anfrage erfolgt i.d.R. durch die Ermittlungspersonen der Staatsanwaltschaften	
		Aktuell genutzte IMEI-Nummer (zu bekannter Rufnummer): § 100g StPO	eri 100g 1	eil 100g 1
Internetforen	Zugriff auf Daten in geschlossenen Internetforen mittels Zugangsdaten, die ohne od. gegen den Willen der Kommunikationsbeteiligten erlangt wurden.	**§ 100a StPO <u>bei Liveüberwachung</u>** über Netzbetreiber (auch bei Einsatz virtueller Ermittler, siehe unten), gegebenenfalls ist zusätzlich § 110a StPO zu beachten.	eri 100a 1	eil 100a 1
		§§ 94, 98 StPO (offene Maßnahme) oder § 99 StPO (verdeckte Maßnahme) gegenüber Telemediendiensten nach Abschluss des Telekommunikationsvorgangs (z.B. Inhalt von Chat, eingestellte Fotos)	eri db 2 eri post 1	eri db 2 eil post 1
IP-Catching	Es soll eine bisher **unbekannte Person** ermittelt werden, die eine veränderte IP-Adresse bei der Einwahl verwendet. Dazu wird über IP-Catching die dahinter stehende IP-Adresse ermittelt. Beispiele: Anonymisierungsdienste, Verwendung gefälschter E-Mail-Adressen	Erhebung von Verkehrsdaten gem. § 100g Abs. 1 S.3 StPO für die Zukunft, weil von der Maßnahme eine Vielzahl von Personen betroffen sein kann	eri 100g 1 Formblatt wird angepasst	eil 100g 1 Formblatt wird angepasst

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
IP-Tracking	Feststellung des **geographischen Standorts eines Internetzugangs**, der von einer Zielperson benutzt wird; durch Ermittlung der IP-Adresse zu einer konkreten Kennung Beispiel: Einsatz von" ReadNotify"	**§ 100g Abs. 1 S.3 StPO**	eri 100g 1 Formblatt wird angepasst.	eil 100g 1 Formblatt wird angepasst.
Kfz-Ortung	Ist in einem Kfz ein SIM-Modul eingebaut, so ist dessen Ortung möglich (sowie darüber hinaus alle Varianten des TKÜ-Instrumentariums wie Verkehrsdatenerhebung)	**Katalogtat**: § 100a StPO	eri 100a 1	eil 100a 1
		Nichtkatalogtat/en Liegen bei Diebstahl eines Fahrzeugs Einverständniserklärungen des Berechtigten mit der Ortung seines Fahrzeugs durch den Hersteller vor, können die Ortungsdaten den Ermittlungsbehörden, i.d.R. der Polizei, freiwillig zur Verfügung gestellt oder ggf. von diesen beschlagnahmt werden. Berechtigter ist derjenige, dessen Daten von der Abfrage betroffen sind (z.B. Eigentümer).	(-) eri db 2	(-) eri db 4

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
Mautdaten	Mautdaten, die gem. § 4 Abs. 2 Autobahnmautgesetz (ABMG) beim automatisierten Abrechnungssystem mittels GPS und On Board Unit (OBU) anfallen	Die gem. § 4 Abs. 2 ABMG bei der Betreibergesellschaft TollCollect erhobenen Mautdaten dürfen ausschließlich für die Zwecke dieses Gesetzes (ABMG) verarbeitet und genutzt werden. Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften (StPO, PAG)ist unzulässig	(-)	(-)
Online-Durchsuchung	Ermittlung von gespeicherten Daten eines Computers über Online-Verbindung	Die heimliche Durchsuchung der im Computer eines Beschuldigten gespeicherten Dateien mit Hilfe eines Programms, das ohne Wissen des Betroffenen aufgespielt wurde (verdeckte Online-Durchsuchung), ist nach der Strafprozessordnung unzulässig. Es fehlt an der für einen solchen Eingriff erforderlichen Ermächtigungsgrundlage (BHG NJW 2007,930). Die verdeckte Online-Durchsuchung ist insbesondere nicht durch § 102 StPO (Durchsuchung beim Verdächtigen) gedeckt, weil die Durchsuchung in der Strafprozessordnung als eine offen durchzuführende Ermittlungsmaßnahme geregelt ist. Auf die im Bund und in einzelnen Ländern bestehenden präventiv-polizeilichen Regelungen wird besonders hingewiesen (BKA: § 20k BKAG, Bayern Art. 34d BayPAG)	(-)	(-)

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
„Stille SMS“	Stille SMS (auch als „*Silent Message*, S*tealth SMS* od. *stealth ping*“ bezeichnet) dienen 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 Verkehrsdaten 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 in der Regel nicht wahrnehmbar (weder Anzeige auf dem Display noch akustisches Signal, allerdings möglicherweise Störgeräusche im Radio, PC-Lautsprecher usw.)	Die Rechtsgrundlage ist strittig. Das StPO enthält für die „stille SMS“ keine ausdrückliche Ermächtigung. Bei der Begründung zu dem am 1.1.2008 in Kraft getretenen "Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG" ging der Gesetzgeber davon aus, dass die Maßnahme mit der Reform überflüssig geworden sei (BT-Drucks. 16/5846 S. 51) Da das Erfordernis "im Falle einer Verbindung" in § 100g StPO gestrichen wurde, soll es nun möglich sein, Standortdaten auch ohne aktive Verbindung in Echtzeit zu erheben. Die Übersendung einer „stillen SMS“ sei weitgehend entbehrlich (vgl. auch KK-StPO/Nack, § 100a Rn.11). Dies ist jedoch in der Praxis nicht zutreffend: siehe hierzu unten „Technische Tipps: Standortermittlung über Funkzellen“		

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
"Stille SMS"		**Rechtsgrundlage für die Datenabfrage sind §§ 100a, 100g StPO** • In der Versendung der stillen SMS liegt kein eigenständiger Grundrechtseingriff, daher Rechtsgrundlage §§ 161, 163 StPO oder Annexkompetenz zu §§ 100g, 100a StPO • Achtung: keine Anwendbarkeit der TKÜV bei Maßnahmen gem. § 100g StPO (vgl. § 1 TKÜV)! • Die rechtlich mögliche Abfrage der Standortdaten in Echtzeit nach § 100g StPO scheitert jedoch aus technisch-organisatorischen Gründen. Die Provider sind nach der TKÜV weder dazu verpflichtet Standortdaten in Echtzeit technisch auf die TKÜ-Anlage des Kompetenzzentrums TKÜ-BY auszuleiten, noch müssen sie hierzu außerhalb der Regelarbeitszeiten einen Bereitschaftsdienst zur Entgegennahme derartiger Anordnungen installieren. • <u>Ausnahme (auf freiwilliger Basis):</u> Deutsche Telekom – Mobilfunk (zu deren Bürozeiten)	eri 100a 1 eri 100g 1	eil 100a 1 eil 100g1

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
		• Bei den übrigen Mobilfunknetzbetreibern ist eine Beauskunftung von Standortdaten in Echtzeit im von der Anordnung betroffenen Zeitraum nur jeweils wöchentlich retrograd über die Elektronische Schnittstelle Behörden (ESB/ Leitstelle Verkehrsdaten) möglich.		
Überwachung verschlüsselter Telekommunikation (z.B. Skype, googlemail, https usw.)	Um eine sichere Kommunikation zwischen den Kommunikations-teilnehmern zu gewährleisten, kann Telekommunikationsübertragung verschlüsselt werden (z.B. Skype). Dazu gibt es unterschiedliche Verschlüsselungssoftware. Hinweis: Derzeit ist eine Überwachung meist technisch nicht möglich!	**Anordnung der Überwachung** Rechtsgrundlage dafür sind die gesetzlichen Vorschriften der StPO, insbes. § 100a StPO, oder im präventiven Bereich des Polizeirechts des Bundes oder der Länder (z.B. Bayern: Art 34 a PAG) **Technische Umsetzung der Überwachung** • Entschlüsselung der verschlüsselten Telekommunikation während des Übertragungsvorgangs in der Regel aufgrund der hochwertigen Verschlüsselungstechniken nicht möglich. Bei einer herkömmlichen Telefonüberwachung werden daher nur verschlüsselte Daten abgefangen. Sie sind in Unkenntnis des Schlüssels wertlos. Daher: • **Quellen-TKÜ** „Quellen-TKÜ“ ist die Überwachung von Telekommunikation „an der Quelle“ und somit vor ihrer Verschlüsselung bzw. nach ihrer	eri 100a 3	Eilanordnung nicht sinnvoll

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
Überwachung verschlüsselter Telekommunikation		Entschlüsselung. Auf dem Computer, mit der die zu überwachende Kommunikation getätigt wird, wird eine Überwachungssoftware (z.B. Keylogger, Trojaner) installiert, welche die Kommunikation vor der Verschlüsselung mitschneidet und an die Ermittlungsbehörde Telekommunikationsdaten während eines aktiven Telekommunikationsvorgangs übermittelt. • § 100a StPO beinhaltet die Annexkompetenz zum Einsatz technischer Mittel zur Umsetzung der Anordnung. • Quellen-TKÜ ist ausschließlich auf Telekommunikationsvorgänge zu beschränken. Unzulässig wäre eine „Online-Durchsuchung“ (s.o. Stichwort „Online-Durchsuchung“). Die ausdrückliche Beschränkung auf die Überwachung der Telekommunikation sollte bereits in den Anordnungsbeschluss des Gerichts aufgenommen werden. Durch technische Mittel ist ferner sicherzustellen, dass die Überwachungssoftware tatsächlich nur die Telekommunikation überwachen sowie ggf. aufzeichnen kann und nicht zugleich auch ein Zugriff auf sonstige gespeicherte Daten möglich ist. Das Bundeskriminalamt ist derzeit mit der Entwicklung einer geeigneten Software beauftragt.		

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
Virtuelle Ermittler (Cybercops)	Polizeibeamte, die in Internet-Foren, auf Vermittlungs-Plattformen oder in Tauschbörsen, ermitteln und ggf. an der Kommunikation teilnehmen (z.B. Mitlesen, Mit-Chatten usw.)	1. **§§ 161, 163 StPO** (Benutzergruppe ohne schutzwürdiges Vertrauen in die Identität und Motivation der Nutzer) Kein Eingriff in Grundrechte bei Teilnahme unter einer Legende an offener Kommunikation in sozialen Netzwerken, solange der Betroffene nicht schutzwürdig auf die Identität des Kommunikations-partners vertraut (vgl. BVerfGE 120, 274, 346). Maßgeblich sind die äußeren Umstände, wie etwa Anmeldung im sozialen Netzwerk, ggf. unter einem Pseudonym problemlos für Vielzahl von Teilnehmern möglich. **§§ 161, 163 StPO erlauben** • Verschaffung und Auswertung allgemeiner Informationen, z.B. zur Identifizierung von Personen • Teilnahme an Kommunikation, z.B. chatten • einfache Legendierung (**einfacher Fake Account** beispielsweise Verwendung eines Pseudonyms ohne Offenlegung der Identität bzw. Verwendung eines fremden Accounts mit Zustimmung des Inhabers) • **kurzfristige Beobachtung von Beschuldigten und Verdächtigen** • **Einsatz noeP** (nicht offen ermittelnder Polizeibeamter) sachlich umgrenzter Einsatz eines NoeP mit	**(-)**	

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
		Zustimmung der Staatsanwaltschaft, beispielsweise im Zusammenhang mit einem Scheingeschäft (z.B. eBay) oder zur Identifizierung eines Täters durch eine direkte Kontaktaufnahme;		
Virtuelle Ermittler (Cybercops)		**2. §§ 100a, 100b, 110a ff. StPO** (Benutzergruppe mit schutzwürdigem Vertrauen in die Identität und Motivation des Nutzers) Bei Teilnahme an der Kommunikation in einem sozialen Netzwerk • einer Benutzergruppe mit schutzwürdigem Vertrauen in die Identität und Motivation des Nutzers oder • Nutzung eines Zugangsschlüssel ohne Zustimmung eines anderen Kommunikationsteilnehmers kann dies unter den Voraussetzungen der §§ 100a, 100b, 110a StPO zulässig sein. **a. § 100a StPO** • Aufzeichnung der Kommunikation zu Beweiszwecken • Verschaffung des Zugangsschlüssels durch technische Mittel b. **§ 110a StPO Verdeckter Ermittler** • auf Dauer angelegte, veränderte Identität (anderenfalls ggf. NoeP)	eri ve 1 eri 100a 1	eil ve 1 eil 100a 1

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
		• (ggf.) Teilnahme am Rechtsverkehr • Vertrauen der geschlossenen Gruppe in Identität des VE **c. § 110 b StPO:** Die auf Dauer angelegte Kontaktaufnahme des verdeckten Ermittlers zu einem bestimmten Beschuldigten bedarf der gerichtlichen Zustimmung.		
VoIP – unverschlüsselt	Telefonieren über Computernetzwerke, welche nach Internet-Standards aufgebaut sind. (nicht Skype)	§ 100a StPO Entscheidend für eine standardmäßige Ausleitung ist, ob der entsprechende VoIP-Anbieter zur Ausleitung verpflichtet ist! Eine aktuelle Liste der VoIP-Betreiber, die Inhaltsdaten ausleiten können, ist über das BLKA, SG 633, erhältlich. Falls keine Ausleitung möglich ist, sollte DSL-/ bzw. Breitbandüberwachung des Internetzugangs gem. § 100a StPO als Ausgleichsmaßnahme zur fehlenden Audioüberwachung und zusätzlich eine rückwirkende Verkehrsdatenerhebung gem. § 100g StPO erfolgen	eri 100a 1	eil 100a 1

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
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:			
	Ausmessung der exakten geographischen Ausbreitung des funktechnisch versorgten Bereichs eines WLAN;	§§ 161, 163 StPO	Ausmessung erfolgt durch die Ermittlungs-personen der Staats-anwaltschaften	
	Identifizierung (anhand MAC-Adresse) aller mit dem Access Point verbundenen Endgeräte (z.B. WLAN-fähiges Notebook, PDA, Handy)	§ 100i StPO	eri 100i 1	eil 100i 1
	Überwachung/Aufzeichnung des Datenverkehrs über WLAN eines bestimmten Telekommunikationsgerätes, anhand dessen MAC-Adresse.	§ 100a StPO	eri 100a 1	eri 100a 1

Stichwort	Durchzuführende Maßnahme	Gesetzliche Grundlage	**TV-StA-Formblatt**[1] Beschluss	**TV-StA-Formblatt** Eilanordnung
Zielwahlsuche	Ermittlung von **Rufnummern**, von denen Verbindungen zu einem bekannten Anschluss hergestellt wurden **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 Deutsche Telekom AG teilte mit Schreiben vom 29.09.2010 mit, dass die Zielwahlsuche zwar nunmehr wieder eingerichtet sei; zurzeit sei es aber nur möglich, festzustellen, von welchem Festnetzanschluss der Telekom ein beliebiger Anschluss innerhalb der letzten 3 Tage angerufen worden sei. Für sogenannte homezone-Tarife siehe Hinweis S. 32	§ 100g Abs. 1 StPO (Verkehrsdaten i.S. der §§ 96, 97, 100 TKG, Rechnungs- und Betriebsdaten) Der Verhältnismäßigkeitsgrundsatz ist besonders zu beachten. **beachte:** Zielwahlsuche zur Ermittlung von Zeugen ist unzulässig. Die Maßnahmen dürfen sich nur gegen den Beschuldigten bzw. den Nachrichtenmittler richten (§§ 100g Abs. 2 S. 1 i.V.m. § 100a Abs. 3 StPO).	eri 100g 1	eil 100g 1

D) **Gesetzliche Grundlagen:**

§ 100a Abs. 1 StPO	**Überwachung der Telekommunikation** (eri 100a 1, eil 100a1)
1. Eingriffsvoraussetzungen:	
a. 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 von 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, einen 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)
b. 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

c. Tat wiegt im Einzelfall schwer	• Einzelfallabwägung erforderlich • Im Gesetz genannte minder schwere Fälle sind nicht von vornherein auszuschließen
d. Subsidiaritätsgrundsatz	Erforschung d. Sachverhalts od. Ermittlung d. Aufenthalts muss auf andere Weise erschwert od. aussichtslos sein
2. 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	Allgemeine Erhebungsbefugnis für Verkehrsdaten
1. Eingriffsvoraussetzungen	**Hinweis** **Bei § 100g StPO geht es nicht um den Inhalt der Telekommunikation (dazu dient § 100a StPO), sondern nur um die Feststellung technischer Daten (Teilnehmernummern, Anschlussstelle, Zeit u. Ort des Gesprächs usw.).** **Das BVerfG hat mit Urteil vom 2.3.2010 die §§ 113a, 113b TKG und § 100g StPO, soweit diese den Abruf der nach § 113a TKG zu speichernden Daten (sogenannte Vorratsdaten) erlaubten, für nichtig erklärt. Damit können insoweit nur noch die Verkehrsdaten nach §§ 96, 97, 100. TKG erhoben werden (Rechnungs- und Betriebsdaten).**
a. Abs. 1 S. 1 Nr. 1: Straftat von auch im Einzelfall erheblicher Bedeutung, insbes. Katalogtat nach § 100a Abs. 2 StPO oder	• Verweisung auf ‚Katalogtaten" des § 100a Abs. 2 StPO ist nicht abschließend • Standortdaten **in Echtzeit** dürfen nur nach Nr. 1 erhoben werden (vgl. Abs. 1 S. 3)
b. Abs. 1 S. 1 Nr. 2: mittels Telekommunikation begangene Straftat	c. z.B. mittels Telefon, Fax, Internet od. E-Mail begangene Beleidigung, Bedrohungen od. Ausspähung von Daten
c. bestimmte Tatsachen müssen Verdacht begründen	d. Für eine Funkzellenabfrage müssen hinreichend konkrete Anhaltspunkte für die Verwendung eines mobilfunkfähigen Endgeräts bei der Straftat gegeben sein (Bär, § 100g 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 mobilfunkfähigen Endgerätes war u. im fraglichen Zeitraum auf Mittäter wartete. e. 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)
d. 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. Beschuldigte auf andere Weise aussichtslos u. angemessenes Verhältnis zur Bedeutung der Sache. Der Verhältnismäßigkeitsgrundsatz ist besonders zu beachten.

2. Anordnungskompetenz	
Richtervorbehalt nebst Eilkompetenz der Staatsanwaltschaft bei Gefahr in Verzug (mit richterlicher Bestätigung binnen drei Werktagen)	§ 100g Abs. 2 S. 1 mit Verweis auf § 100b StPO: Regelungen zur TKÜ gelten entsprechend
§ 100i Abs. 1 StPO	**IMSI-Catcher** (eri 100 i, eil 100i)
1. 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	
2. 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

§ 100j Abs. 1 StPO	
1. Eingriffsvoraussetzungen:	
Durch bestimmte Tatsachen konkretisierter Verdacht	
zur Erforschung des Sachverhalts oder Ermittlung des Aufenthaltsorts des Beschuldigten erforderlich	
2. Anordnungskompetenz:	
Ermittlungsbehörden für §§ 100j Abs. 1 Satz 1 (Bestandsdaten) und Abs. 2 StPO (dynamische IP-Adressen): Richtervorbehalt nebst Eilkompetenz der Staatsanwaltschaft bei Gefahr in Verzug(mit richterlicher Bestätigung für § 100j Abs. 1 Satz 2 (Zugangscodes) i.V.m. § 100j Abs. 3 StPO:	

E) Bearbeitungshinweise für die Praxis

Leitlinien für verdeckte Ermittlungsmaß-nahmen	Eine gemeinsame Arbeitsgruppe Polizei/Justiz hat Leitlinien für verdeckte Ermittlungsmaßnahmen, insbesondere für TKÜ-Maßnahmen erarbeitet, auf die Bezug genommen wird. Besonders wird auf den Kernbereichsschutz und die grundrechtssichernden Verfahrensregelungen (z.B. Mitteilungs-, Löschungspflichten) hingewiesen. GAG_Leitfaden.pdf
Abfassung von gerichtlichen Beschlüssen	• Zur besseren Lesbarkeit, insbesondere im Falle mehrfacher Übermittlung per Telefax, ist auf eine **ausreichende Schriftgröße** zu achten (**empfohlen ARIAL, mindestens Schriftgrad 11, kein Fettdruck**; gerade kein Fettdruck von Anschlussnummern, 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 BLKA entsprechende statistische Auswertungen vornehmen muss und ansonsten in einer Vielzahl von Einzelfällen Rückfragen bei der sachbearbeitenden Staatsanwaltschaft nötig werden.
	• 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 abgeschaltet und dann wieder neu angeschaltet 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 Über-wachungszeitraums	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 beginnt mit dem Tag der Anordnung**, d.h. das Beschlussdatum ist maßgeblich, nicht erst der im Beschluss angegebene, ggf. abweichende Anfangszeitpunkt. Das **Enddatum** (Achtung aus Praktikabilitätsgründen weder Wochenende noch Feiertag) sollte im Beschlussantrag festgelegt werden. 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 Festnetz-kennung; 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**. Zur Überwachung reicht jedoch die Angabe der Mobilfunknummer im Beschluss nach § 100a StPO aus (soll jedoch eine Zielwahlsuche nach § 100g StPO erfolgen, so ist zwischen Mobilfunknummer und Festnetznummer zu unterscheiden). • Bei. **Smartphones** werden zunehmend auch weitere Arten der mobilen Datenkommunikation wie Zugang zum Internet oder Zugriff auf Daten via Apps genutzt. Bei einer Mobilfunküberwachung ist bei Beschlussvollzug durch das BLKA in Bayern automatisch der Datenverkehr (Internetverkehr über UMTS) enthalten. Zur Überwachung reicht auch hierfür die Angabe der Mobilfunknummer im Beschluss nach § 100a StPO aus.
Übersendung von § 100a -Beschlüssen	TKÜ-Maßnahmen werden nach Vorliegen der **§ 100a StPO-Anordnung in Bayern über das Kompetenzzentrum TKÜ-BY** des LKA, SG 633, **bei den Verpflichteten (Netzbetreibern/Providern) beantragt**. Der **Originalbeschluss** oder **eine beglaubigte Abschrift (ohne Gründe)** muss **binnen 1 Woche beim Verpflichteten** vorliegen (§ 12 Abs. 2 S. 2 TKÜV). Bei ausländischen Mobilfunknummern, ausländischen IMSI-Überwachungen und IMEI-Überwachungen muss der Originalbeschluss an alle 4 Mobilnetzfunkbetreiber (T-Mobil, Vodafone, 02, E-Plus) versandt werden Dies ist **durch die Staatsanwaltschaft sicherzustellen**. Die Übersendung einer Kopie ist nicht ausreichend. Diese wird von den Providern nicht akzeptiert. **Achtung, Hinweise**: • Übersendung von Beschlüssen an die Netzbetreiber/Provider ist bei 100g-Beschlüssen (**Verkehrsdatenüberwachung** u.a.). **nicht** erforderlich. Die „Abwicklung" erfolgt hier **nur über das Kompetenzzentrum TKÜ-BY** (Elektronische Schnittstelle Behörden, ESB). Nur dorthin (BLKA, SG 633, Kompetenzzentrum TKÜ Bayern) ist eine beglaubigte Abschrift d. Beschlusses zu faxen. • 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.
Auslandskopf-überwachung (AKÜ)	• Die Zusammenschaltung inländischer u. ausländischer Telekommunikationsnetze erfolgt über diverse Schnittstellen, sog. „**Auslandsköpfe".** Überwacht werden können nur im Inland lokalisierte Auslandsköpfe. • Mit „**Auslandskopfüberwachung"** ist die Kommunikation vom Inland zum ausländischen Festnetz- bzw.

	Mobilfunkanschluss oder umgekehrt gemeint. • § 4 Abs. 2 TKÜV bezieht sich nur auf die Kommunikation vom unbekannten inländischen zu bekannten ausländischen Anschlüssen. Nicht ausgeschlossen ist jedoch, nach § 100a StPO auch die Überwachung und Aufzeichnung von aus dem Ausland stammender, aber im Inland eingehender Telekommunikation anordnen zu lassen. Es empfiehlt sich daher die TKÜ-Maßnahmen unbegrenzt anordnen zu lassen und nicht nur „in dem nach der TKÜV zulässigen Umfang“. Zur Klarstellung für den Netzbetreiber sollte aufgenommen werden, dass die Maßnahme am im Inland befindlichen Auslandskopf des jeweiligen Betreibers durchzuführen ist. Soll daneben auch die Inlandsüberwachung des ausländischen Anschlusses erfolgen, sollte (zur Klarstellung für den Netzbetreiber) ein weiterer Beschluss eingeholt werden. • **Soll ein ausländischer Provider zur TK-Überwachung verpflichtet werden,** ist ein förmliches RH-Ersuchen nötig. • Es gibt inzwischen **12 Betreiber von Auslandsköpfen**. Davon können 10 Live-Ausleitungen einrichten. Zwei (Verizon Business und Cable & Wireless) können nur Verkehrsdaten übersenden. Die Deutsche Telekom AG hat zum 01.02.2011 ein neues System in Betrieb genommen. Gleichwohl bestehen immer noch (bzw. inzwischen wieder) Kapazitätsprobleme. Es ist daher zu empfehlen, Verlängerungsbeschlüsse für eine Überwachungsmaßnahme frühzeitig zu erwirken, um eine Abschaltung zu verhindern, da die Verpflichteten die Maßnahmen nach Eingang abarbeiten und daher eine „Warteliste“ entstehen kann. Ferner sollten, um **Überwachungslücken** gering zu halten, parallel zur Inhaltsdatenüberwachung in Echtzeit die Verkehrsdaten gem. § 100g StPO mittels Zielsuchlaufs bei allen gängigen Festnetz- und Mobilfunknetzbetreibern angefordert werden.
Ausländische Provider/ Alternativen zur Ermittlung der Rufnummer	• **Bestandsdaten von ausländischen Providern** können in der Regel 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 diese Weise auch die Rufnummer festgestellt wird. Die Ermittlung der Rufnummer wäre in diesem Fall auch über § 100g StPO möglich, die 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 BLKA München vorhanden sind, erlangt werden (so für Google, YouTube, Skype, Microsoft [emergency disclosure request])

<table>
<tr><td>Ausländische Provider</td><td colspan="4">U.S.-amerikanischen Internetproviderfirmen
(vgl. Schreiben des Bundesamts für Justiz vom 30. März 2012 und 8. Oktober 2012, , Gz.: III1-9360 E-A5-B 3601/2012)</td></tr>
<tr><td></td><td>Art der Daten</td><td>Optionen</td><td colspan="2">Hinweis</td></tr>
<tr><td></td><td>Inhaltsdaten</td><td>förmliches Rechtshilfeer-suchen</td><td colspan="2">Provider dürfen diese Daten nicht freiwillig herausgeben;
Sonderregelung bei Notfällen (z.B. Terrorismus/Amoklauf usw.)
Vorläufige Sicherung von Internetdaten über das G8 24/7-Netzwerk (weitere Ausführungen Kapitel 7)</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">Übersendung eines deutschen Gerichtbeschlusses oder einer Anfrage gem. § 113 TKG mit englischer Übersetzung an Provider mit dem Ziel der freiwilligen Herausgabe der Daten
Hinweis:
Die US-Behörden legen Wert darauf, dass mitgeteilt wird, auf welchem Weg die ermittelnde Behörde tatsächlich Kenntnis darüber erlangt hat, dass der zu beschlagnahmende Account von der in Rede stehende Person tatsächlich genutzt worden ist (z.B. Beschlagnahme eines Computers, Zeugen- bzw. Beschuldigtenvernehmung).</td></tr>
<tr><td></td><td>Bestands- und Verkehrs-daten</td><td>direktes Heran-treten an US-amerikanische Provider oder deren Töchter-firmen mit dem Ziel der freiwilli-gen Herausgabe möglich</td><td>Google</td><td>Google.Inc und You Tube LLC gehören zu Google.</td></tr>
<tr><td></td><td></td><td></td><td></td><td>Bestandsdaten:
E-mail-Dienste: 113 TKG
YouTube: § 15 Abs. 5 S.4, § 14 Abs. 2 TMG, § 95 StPO</td></tr>
</table>

				Verkehrsdaten: § 100g StPO, wenn IP-Adresse aus Deutschland bzw. der Region kommt, (anderenfalls ist ein Rechtshilfeersuchen notwendig) Google Inc. 1600 Amphitheatre Parkway 94043 Mountain View CA 94043 USA via Google Hamburg E-Mail: lis-global@google.de Fax-Nr.: 001-650-469-0622
			Facebook	**Normalfall** (gestempeltes und unterschriebenes Ersuchen in englischer Sprache gem. 15 Abs. 5 S.4, § 14 Abs. 2 TMG, 161 StPO i.V.m. 95 StPO): Facebook Inc. 1601 S. California Avenue 94304 California **USA** an E-Mail Adresse: subpoena@fb.com Fax:040/30187621 Notrufhotline:+1 650 543 49 48 **Besonders eilbedürftige Ersuchen** (Amokläufe/Attentatsdrohung/Gefahr für Leib und Leben) Verwendung der Emergency- Disclosure-Form (https://www.eff.org/sites/default/files/filenode/social_network/facebook2009_SN_LEG-DOJ.pdf) an oben genannte E-Mail-Adresse mit Wichtigkeit „hoch“.

				Auszug Infoblatt Facebook des Hessischen Landeskriminalamts Ersuchen auf Bestandsdatenauskunft können bei Facebook über das Records-Portal unter www.fachebook.com/record gestellt werden. Die Auskunft erfolgt ausschließlich über einen Internetrechner und NICHT über den Standortarbeitsplatz, siehe Infoblatt Facebook des Hessischen Landeskriminalamts, Link S. 68 Über das Records-Portal kann ein Beweissicherungsantrag zum Einfrieren von Inhaltsdaten gestellt werden. Facebook sichert zu, nach Eingang des Beweissicherungsantrags die Profilinhalte im Zusammenhang mit strafrechtlichen Ermittlungen bis zur Erlangung einer formellen gerichtlichen Verfügung (höchstens 90 Tage) zu speichern (einzufrieren). Der Beweissicherungsantrag darf nur gestellt werden, wenn kein Beschluss vorliegt. Dieser muss dann über den Rechtshilfeweg in die USA gesendet werden. Erfahrungswerte haben ergeben, dass es ca. 1 Jahr dauert, bis eine Antwort kommt.
			Microsoft	Microsoft Corporation One Microsoft Way, 98052 Redmont,WA 98052-6399 USA über Microsoft Deutschland GmbH, Konrad-Zuse-Straße 1 85716 München Fax-Nr.: 0800-6738329
			Ebay	Vereinigtes Königreich (Fraud Investigation Team FIT) Ebay kooperiert mit ausländischen Strafverfolgungsbehörden.
			Whatsapp	WhatsApp Inc.

				3561 Homestead Avenue , #416, Santa Clara, CA 95051, Voraussetzungen • deutsche Rufnummer • Person mit Wohnsitz in Deutschland
eTicketing	In neueren Mobiltelefonen (z.B. von Vodafone, Samsung) werden Speicherchips verbaut, welche die Teilnahme am **Elektronischen-Ticket-System (e-Ticketing)** ermöglichen. Alternativ können auf Smartphones entsprechende Apps zur Teilnahme am e-Ticketing installiert werden. Die Deutsche Bahn AG bietet diese Technik seit November 2011 im Fernverkehr an. 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 Touchpoint 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 Deutsche Bahn verfügt über die **Daten sämtlicher Funkzellen, die der Nutzer durchfahren hat (Geodaten)**. Dabei handelt es sich um **Verkehrsdaten**, da die Daten vom Mobiltelefon gesendet werden und nicht vom Touchpoint. Diese Daten können nach §§ 161, 163 StPO herausverlangt werden. Beschluss nach § 100g StPO ist nicht erforderlich, weil die Daten nicht beim Telekommunikationsdiensteanbieter, sondern bei der Deutschen Bahn abgefragt werden, vgl. § 100g Abs. 3 StPO. 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. Siehe auch: www.eticket-deutschland.de ; www.touchandtravel.de			

GSM bzw. UMTS-Netz; unterschiedliche Funkzellen	Mobilfunkendgeräte wurden häufig im GSM-Netz betrieben, aktuelle Geräte verfügen über den UMTS-Standard bzw. bereits über den LTE-Standard. 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. Künftig wird ferner das LTE-Netz, mit entsprechenden Funkzellen, zu berücksichtigen sein. Daher ist insbesondere bei einer Funkzellenerhebung/-auswertung dafür Sorge zu tragen, dass (derzeit) sowohl die entsprechende GSM- als auch die UMTS-Funkzelle überprüft wird. Dies ist in Bayern und Baden-Württemberg regelmäßig der Fall.
IMEI Manipulations-möglichkeiten	Die **Gerätenummer eines Mobilfunkgeräts (IMEI**), z.B. eines Handys oder Smartphones, kann im Einzelfall eindeutig einem bestimmten Gerät zugewiesen sein. Es gibt jedoch Computerprogramme, die eine Manipulation ermöglichen. (gehört nicht hier her!)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. Erforderlich ist daher die vorherige Klärung einer Mehrfachvergabe durch Anfrage bei den TK-Dienstleistern gem. §§ 161 StPO, § 113 TKG, Live-Auswertung und bei Feststellung von Mehrfachaufkommen sofortige Abschaltung.
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, die aber über § 149 Abs. 1 Nr. 30 TKG bußgeldbewehrt ist. Eine Bestandsdatenabfrage führt daher hier häufig nicht zum wahren Nutzer. Ein Ermittlungsansatz kann in diesen Fällen sein, über die Auflade Vorgänge 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 **Auskunftsersuchens**: siehe unten ;
Rechnungsdaten	Rückwirkende Verkehrsdaten können aufgrund der Außerkraftsetzung der Vorratsdatenspeicherung durch das Urteil des BVerfG vom 2.3.2010 (Nichtigkeit des § 113a TKG) nur noch in Form der **Rechnungs- Betriebs- und Störungsdaten nach § 96, 97,100TKG** i.V.m. § 100g StPO herausverlangt werden. 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. „Rechnungs- und Betriebs- sowie Störungsdaten“) und Angabe der Rechtsgrundlage (z.B. §§ 96, 97 TKG, 100g Abs. 1 StPO). Für die Speicherung dieser Rechnungs-, Betriebs- und Störungsdaten gelten die in der unten angefügten Tabelle angegebenen, unterschiedlichen Fristen. Die von den Verpflichteten selbst gesetzten Fristen können in Baden-Württemberg unter http://tkue.lka.bwl.de festgestellt werden (siehe Verkehrsdaten). Mittels der **Rechnungs-, Betriebs- und Störungsdaten** lassen sich auch **Funkzellendaten feststellen**! Über diese Daten ist ferner eine **Zielwahlsuche möglich**!
Standortermittlung über Funkzelle	Nach § 100g Abs. 1 S. 3 StPO ist die Erhebung von **Standortdaten in Echtzeit** möglich. Technisch ist die Verkehrsdatenabfrage in Echtzeit bei fast allen Betreibern noch nicht möglich. Lediglich die Deutsche Telekom, Mobilfunk (= T-Mobile) schaltet eine TKÜ ohne Inhaltsdaten und leitet in Echtzeit aus. **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. Beweiskräftige, nur schwer angreifbare Erkenntnisse aus einer Funkzellenabfrage liegen nur dann vor, wenn die Funkzelle vor der Abfrage aktuell vermessen und - wegen der Speicherfristen der Netzbetreiber - die Daten innerhalb von sieben Kalendertagen nach der relevanten Tatzeit erhoben wurden. Anordnungen sollten daher am sechsten Tag, spätestens am siebten Tag rechtzeitig vor Arbeitsende bei den Netzbetreibern eingegangen sein. In die Anregung sind die

	Daten der aktuellen Vermessung aufzunehmen Die einmalige Standortfeststellung kann im ausschließlich präventiven Bereich mittels der sog. „Leib & Leben“ Faxe über den Netzbetreiber selbst angefragt werden. Als Ergebnis erhält man die Funkzelle der letzten bekannten Einbuchung des Mobiltelefons
UMTS-Datenkarten	IP Adresse lässt keinen Rückschluss auf Anschlussinhaber zu, da zugehörige Ports nicht gespeichert werden müssen (Stichwort: NAPT, Network access port translation). Folge: Ermittlung der Internetnutzer ist nicht möglich.

F) **Definitionen und Begriffsbestimmungen:**

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 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	**Bestandsdaten** (Benutzerdaten)	§ 3 Nr. 3 TKG: „**Bestandsdaten**“ Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden; 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**). Weitere Normen zu den umfassten Daten im Einzelnen: §§ 95, 111 TKG sowie bei Telemedien: § 14 TMG	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.
	Inhaltsdaten	Im Rahmen der Telekommunikation (§ 3 Nr. 22 TKG) übertragene bzw. ausgetauschte Informationen und Nachrichten	z.B. Gesprächsinhalte, übertragene Töne, Bilder, Signale aller Art
	Nutzungsdaten	Nutzungsdaten fallen nur im Bereich der Telemediendienste an. § 15 Absatz 1 TMG Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere	Beispiele: IP-Adresse, „Klickweg“ (alles, was von Nutzern des Telemediendienstes angeklickt wird), gespeicherte Suchkriterien von Angebotsrecherchen (z.B. autoscout24.de)

		1. Merkmale zur Identifikation des Nutzers, 2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien.	
	Standortdaten	§ 3 Nr. 19 TKG Daten, die in einem Telekommunikationsnetz erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben Weitere Normen: §§ 96, 98 TKG §14 Abs. 1 TMG:	**Ermittelbar ist nur, in welcher Funkzelle sich ein Teilnehmer befindet/befunden hat; genaue Ortung ist dann mit IMSI-Catcher möglich**
	Verkehrsdaten	§ 3 Nr. 30 TKG Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Weitere Norm: § 98 TKG	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 **I**nternet 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 (Gerätenummer) des Mobiltelefons; IMEI ist eine grundsätzlich einmalig vergebene **mehrstellige Ziffernfolge** (15 bis 17 Ziffern) zu Manipulationsmöglichkeiten siehe oben Kapitel 1
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 **I**MS**I** der in Reichweite befindlichen, eingeschalteten Mobiltelefone festzustellen bzw. um eine genaue Ortung in einer bekannten Funkzelle durchzuführen	
Internet-Breitband-Anschluss		Oberbegriff für **I**nternetzugang, z.B. DSL, aber auch Breitbandanschluss über Kabelnetze (z.B. Kabel Deutschland) oder Mobilfunk (UMTS)	
IP-Adresse	**Dynamische IP-Adresse**	**I**P steht für „**i**nternet **p**rotocol"; elektronische Adresse für Kommunikation im **I**nternet. 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 bzw. den Nutzungsdaten, § 15 TMG, zugerechnet, da sie durch den Provider an seinen **I**nternet-Nutzer nur für die Dauer eines konkreten Kommunikationsvorgangs vergeben wird und schon **I**nformationen enthält, wer wann mit wem einen **I**nformationsaustausch vorgenommen hat (Bär, TK-Überwachung, Vorb. §§ 100a - 100i, Rn. 11) Rechtsgrundlage für die Auskunft über den Nutzer einer **I**P: §§ 161, 163 StPO, 113 TKG bzw. §§ 161, 163 StPO, 14 TMG

	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 (z.B. 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 **I**dentifikation 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		**I**llegales Ausspähen der Daten von Kreditkarten oder Bankkarten. Mittels technischer Geräte (wie z.B. Magnetstreifenleser u. Videokamera), die verdeckt an Geldausgabeautomaten angebracht werden, um die Daten von Magnetstreifen oder Chipkarten auszulesen und dazu gehörige Geheimnummer (PIN) aufzuzeichnen. 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 **I**nternet, sog. *Carding*, ist möglich und wird praktiziert.	

Skype		**Skype** ist eine kostenlose VoIP-Software des Unternehmens Microsoft, die folgende Funktionen anbietet: • kostenlose VoIP-Telefonate zwischen Skype-Nutzern • gebührenpflichtige Gespräche zu öffentlichen Rufnummern • Erreichbarkeit über eine reguläre Skype-Rufnummer aus dem öffentlichen Netz • Chatfunktionalität, Dateiübertragung und Videokonferenzen Die Kommunikation mittels dieser Software erfolgt verschlüsselt.	**Überwachung ist derzeit nicht möglich!**
Telekommunikationsdienste	§ 3 Nr. 24 TKG	In der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich der Übertragungsdienste in Rundfunknetzen	
Telemediendienste	§ 1 Abs. 1 TMG	Telemedien sind Angebote im Internet, beispielsweise Webshops, Online-Auktionshäuser (wie E-eBay, Amazon) , Suchmaschinen (Immobiliensuche, Ferienangebote, PKW`s) , Webmail-Dienste, Informationsdienste (z. B. zu Wetter, Verkehrshinweise), Podcasts, Chatrooms, Dating-Communities und Webportale. Auch private Websites und Blogs gelten als Telemedien. Das TMG wird daher auch als Internetgesetz bezeichnet.	

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 **I**nternet-Protokolls, indem die Sprache digitalisiert und anschließend im **I**nternet 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 **I**MSI-Catcher, jedoch mit dem Unterschied, dass W-LAN-Catcher keine Funkzelle, sondern einen Zugang ins **I**nternet simuliert)(WiFi steht für: Wireless Fidelity)	

G) Übersicht: Speicherfristen:

In Baden-Württemberg sind die tagesaktuellen Speicherfristen für Polizei und Staatsanwaltschaften unter http://tkue.lka.bwl.de verfügbar.

I) Übersicht über rückwirkende Verkehrsdaten der Netzbetreiber[2]:

Netzbetreiber	§ 96 TKG	Erläuterung
Telekom Deutschland T-Mobile (D1)	1 - 7 Tage	Alle Verkehrsdaten liegen vollständig vor, inkl. IMEI und Zielwahlsuchläufe.
	8 - 80 Tage	Reduzierte rechnungsrelevante Datensätze der T-Mobile Kunden
	8 - 180 Tage	Reduzierte Datensätze von Kunden der Serviceprovider
Vodafone (D2) Mobilfunkbereich	1- 7 Tage	Alle Verkehrsdaten liegen vollständig vor, inkl. IMSI-, IMEI- und Standort-Daten.
	8 - 30 Tage	Alle gebührenpflichtigen ankommenden und alle abgehenden Verkehrsdaten liegen vollständig vor, inkl. IMSI, IMEI, Standort-Daten.
	bis 210 Tage	Es können noch einzelne Verkehrsdaten in den Systemen vorhanden sein.
Vodafone Festnetzbereich (Integration von Arcor)	90 Tage	Alle Verkehrsdaten liegen vollständig vor.
E-Plus	3 Monate + aktueller Monat	Alle Verkehrsdaten liegen vollständig vor.

[2] **Die Speicherfristen können variieren und sind ständigen Änderungen unterworfen.**

Telefónica Germany (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.
	31 - 182 Tage	Verkehrsdaten von Serviceprovidern liegen vor
Deutsche Telekom AG (DTAG)	3 Tage	Zielwahlsuchlauf möglich
	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.
M-Net	180 Tage	Alle Verkehrsdaten liegen vollständig vor.
BT Germany	180 Tage	Netzübergreifend beide Richtungen, ankommende Verbindungen können unvollständig sein.
Kabel Deutschland	14 Tage	Alle Verkehrsdaten liegen vollständig vor.
Verizon	90 Tage	Alle Verkehrsdaten liegen vollständig vor.

II) Übersicht über Funkzellendaten der Netzbetreiber[3]:

Netzbetreiber	Verkehrsdaten kommend	Verkehrsdaten gehend	Zusatzinformationen
Telekom Deutschland T-Mobile (D1)	7 Tage	7 Tage	Telefonie und SMS vollständig
Vodafone (D2)	7 Tage	80 Tage	Telefonie und SMS vollständig
Telefónica Germany (O2)	7 Tage	30 – 182 Tage	Telefonie und SMS vollständig

Übersicht Speicherfristen IP-Adressen Netzbetreiber[4]:

Netzbetreiber/Diensteanbieter	Speicherfrist	Bemerkung
Deutsche Telekom, Bereich Festnetz	7 Tage	-
Deutsche Telekom, Bereich Mobilfunk (Telekom Deutschland, T-Mobile, D1)	30 Tage	Achtung: NAPT (Network Address Port Translation; IP-Adressen-Umsetzung); Wichtige Erläuterungen siehe hierzu Seite 4!
Vodafone (D2), Bereich Festnetz (Arcor Altkundenbestand)	aktueller Login des Kunden	bei aktuellem Login des Kunden ist eine Recherche/Zuordnung der IP-Adresse möglich!

[3] **Die Speicherfristen können variieren und sind ständigen Änderungen unterworfen.**
[4] **Die Speicherfristen können variieren und sind ständigen Änderungen unterworfen.**

Netzbetreiber/Diensteanbieter	Speicherfrist	Bemerkung
Vodafone (D2), Bereich Mobilfunk (GPRS, EDGE, UMTS Technologien) Mobile Breitbandnutzung im Vodafone-Netz	keine Speicherung (in Einzelfällen ist eine Speicherung der IP-Adresse für 4 Stunden möglich)	Einsatz von NAPT (Network Address Port Translation; IP-Adressen-Umsetzung): keine Zuordnung der IP-Adresse zum Kunden möglich! Wichtige Erläuterungen siehe hierzu unter IV.!
Vodafone (D2), Bereich Mobilfunk (LTE Technologie) Stationärer Internetzugang via LTE	keine Speicherung	Derzeit keine technische Möglichkeit zur Zuordnung der dynamisch zugewiesen IP-Adresse zum Kunden!
E-Plus	keine Speicherung (in Einzelfällen ist eine Speicherung der IP-Adresse für 48 Stunden möglich)	keine Zuordnung der IP-Adresse zum Kunden möglich! Wichtige Erläuterungen siehe hierzu unter IV.!
Telefónica Germany **Fusioniert mit Telefónica Deutschland (O_2)** **Fusioniert mit Hanse-Net**	7 Tage	Mobilfunk: ab Beginn der Verbindung Festnetz ehem. Telefónica Deutschland: ab Ende der Verbindung
M-Net	3 Tage	-
Freenet	Keine Speicherung	bei aktuellem Login keine IP-Adressen Feststellung möglich!
1 & 1	10 Tage	Non-Access-Provider; als VoIP

Netzbetreiber/Diensteanbieter	Speicherfrist	Bemerkung
		Anbieter
Kabel Deutschland	2 Tage	Wichtige Erläuterungen siehe hierzu unter IV.!
Net Cologne	4 Tage	-
Versatel Deutschland	2 Tage	-
QSC	7 Tage	-

III) Übersicht Speicherfristen IP-Adressen Diensteanbieter[5]:

Diensteanbieter	Speicherfrist	Bemerkung
Netzquadrat (Sipgate)	2 Tage	IP Adressen können bei Netzquadrat maximal bis zu 2 Tagen vorliegen
AOL	60 – 90 Tage	Bestandsdaten zu AOL Accounts werden von Telefónica O_2 Germany beauskunftet; Wichtige Erläuterungen siehe hierzu unter V.!
Microsoft	Hotmail unbegrenzt Live ID die letzten 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

[5] **Die Speicherfristen können variieren und sind ständigen Änderungen unterworfen!**

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

IV) Zusätzliche Informationen zur Beauskunftung und zur Speicherung von IP-Adressen:

1) Wichtige Information zur Speicherung von IP-Adressen der Mobilfunknetzbetreiber:

a) Generell gilt für alle deutschen Mobilfunknetze:

Die Zuordnung der IP-Adresse zum Kunden erfolgt mit Hilfe der **NAPT-Technologie** (Network Address Port Translation). Eine Zuordnung (IP-Adresse/Kunde) ist über die Standard-Beauskunftung (gem. § 113 TKG) nicht möglich. In speziellen Einsatzfällen können durch operative Maßnahmen **zuordenbare IP-Adressen** festgestellt werden. Informationen hierzu können beim Sachgebiet 633 eingeholt werden.

b) Vodafone (D2) – Stand: Januar 2013, gem. Auskunft der Vodafone Deutschland-

Unter bestimmen Voraussetzung (bei Gefahr für Leib oder Leben) ist eine Zuordnung IP-Adresse zum Kunden möglich. Zuordnungen werden an den Vermittlungsinstanzen (NAPT-Proxies) für max. **4** Stunden gespeichert.

c) E-Plus – Stand: Januar 2013, gem. Auskunft der E-Plus Gruppe-

Unter bestimmen Voraussetzung (bei Gefahr für Leib oder Leben) ist eine Zuordnung IP-Adresse zum Kunden möglich. Zuordnungen werden an den Vermittlungsinstanzen (NAPT-Proxies) für max. **48** Stunden gespeichert.

2) Wichtige Information zur Speicherung von IP-Adressen im Bereich Festnetz:

a) Telefónica O_2 Germany

Die Ermittlung der Bestandsdaten über **I**P-Adressen und Zeitstempel sind im Netz der ehem. **Hanse-Net** nur während einer laufenden Verbindung möglich. Während der allgemeinen Geschäftszeiten der Telefónica O_2 Germany (9 bis 17 Uhr) ist ein sog. **Quickfreeze** zum „Einfrieren" der Daten möglich; siehe Link zum **I**nformationsblatt „Quickfreeze bei **I**P-Adressen" der Telefónica O_2 Germany ehem. Hanse-Net:

V) Zusätzliche Informationen zur Beauskunftung und zu Speicherfristen von IP-Adressen:

1) Wichtige Information zur Speicherung von IP-Adressen der Diensteanbieter:

a) America Online (AOL)

(1) Die Beauskunftung von Bestandsdaten wird durch die Fusion der Hanse-Net in die Telefónica O_2 Germany seit 01.04.2011 ausschließlich von **Telefónica O_2 Germany** durchgeführt; siehe folgenden Link: http://nslk1031:8081/sg643/wp-content/uploads/2011/03/kontaktblatt_02_april_2011.pdf

(2) Für die Beauskunftung von Verkehrsdaten oder die Postfachbeschlagnahme ist eine vollständiges Rechtshilfeersuchen an America Online (AOL US) zu richten, in Deutschland werden **keine** **I**nformationen zu Verkehrs- und **I**nhaltsdaten beauskunftet; siehe dazu folgendes **I**nformationsblatt:

2) Wichtige Information zur Beauskunftung von IP-Adressen bei Kabel Deutschland:

Ab dem **01.10.2011** werden zur **I**dentifikation eines **I**nternetnutzers mit einer **IPv4-Adresse** folgende Angaben benötigt:

a) **I**P-Adresse der **Version 4** (**I**Pv4)

b) Zeitstempel mit Angabe der dazugehörigen Zeitzone

c) Angabe des jeweils genutzten Protokolltyps (TCP oder UDP)

d) Dazugehörige **Port-Nummer** des Quell-Ports (Layer4 – Transportschicht), die von der **I**P-Adresse benutzt wurde

Wichtig: Ohne diese Angaben ist von Kabel Deutschland keine eindeutige Identifizierung des Internetnutzers mehr möglich!

Weiterführende Informationen zur Beauskunftung von IP-Adressen bei KD sind folgendem Dokument zu entnehmen:

VI) 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. Dies gilt auch dann, wenn sich bei externen Datenspeichern nicht klären lässt, wo deren physikalischer Standort ist.

Sind die Daten auf einem Server im Ausland gespeichert und ist dessen Standort bekannt, so ist zu prüfen, ob – gegebenenfalls nachträglich - 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 (Art. 32 Cyber-Crime-Konvention).

24/7-Netzwerk

Gemäß Art. 35 Cyber-Crime-Konvention hat jede Vertragspartei eine **Kontaktstelle** bestimmt , die an sieben Wochentagen 24 Stunden täglich zur Verfügung steht, um für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Computersystemen und -daten oder für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat unverzüglich für Unterstützung zu sorgen. Sie umfasst fachliche Beratung, Sicherung von Daten nach den Artikeln 29 und 30 sowie Erheben von Beweismaterial, Erteilen von Rechtsauskünften und Ausfindigmachen verdächtiger Personen. In Deutschland übt diese Funktion das Bundeskriminalamt in Wiesbaden aus.

Das Bundeskriminalamt Wiesbaden hat für Ersuchen um vorläufige Sicherung von Internetdaten in den USA folgende Kontaktdaten mitgeteilt:

Erreichbarkeit Bundeskriminalamt

Referat SO 41
Erreichbarkeiten innerhalb der Regelarbeitszeit: (8.00 Uhr bis 16Uhr)
Telefon: 0611-5515070 (Kriminaldauerdienst des BKA)
E-Mail: cyber@bka.bund.de
Erreichbarkeiten außerhalb der Regelarbeitszeit:
Telefon: 0611-55 13102 (Kriminaldauerdienst des BKA)

	Fallgruppen	**Rechtshilfeersuchen:**
	Öffentlich zugängliche Daten, die weder durch Passwort noch Benutzerkennung gesichert sind	Bei Zugriff kein Rechtshilfeersuchen erforderlich
	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, falls Standort des Servers bekannt ist und Art. Art. 32 i.V.m. Art 22 Cybercrime Convention nicht anwendbar sind
	Betroffener hält sich aufgrund Durchsuchungsbeschlusses verpflichtet, den Ermittlungsbehörden die Zugangsdaten zu übergeben u. diese greifen ihrerseits auf die Daten zu	Rechtshilfeersuchen erforderlich, falls Standort des Servers bekannt ist und Art. 32 i.V.m. Art 22 Cybercrime Convention nicht anwendbar sind;

Sofern nicht Art. 32 i.V.m. Art 22 Cyber-Crime-Konvention anwendbar ist, kann in **Eilfällen** die Sicherung von Daten auf Servern **in EU-Mitgliedstaaten auf Art. 20 Abs. 4 EURhÜbk (str.) 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) kann als Rechtsgrundlage für diese sog. „transboarder searches“ **herangezogen** werden, auch wenn es zwischen den Unterzeichnerstaaten erhebliche Auslegungsdifferenzen zu Art. 32 gibt.

Artikel 32 – Grenzüberschreitender Zugriff auf gespeicherte Computerdaten mit Zustimmung oder wenn diese öffentlich zugänglich sind

Eine Vertragspartei darf ohne die Genehmigung einer anderen Vertragspartei
a. auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen, gleichviel, wo sich die Daten geographisch befinden, oder
b. auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden,
mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die rechtmäßige und freiwillige Zustimmung der Person einholt, die rechtmäßig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben.

Ob aufgrund eines drohenden Beweismittelverlusts eine **vorläufige Datensicherung ohne Rechtshilfeersuchen** und ohne vorherige Zustimmung des Serverstaates in Betracht kommt, ist im Einzelfall zu entscheiden. . Eine solche vorläufige Datensicherung wegen drohenden Beweismittelverlusts ist insbesondere angezeigt sein, wenn zum Zeitpunkt der notwendigen vorläufigen Datensicherung der Standort des Servers oder des Orts, an dem die Daten physikalisch gespeichert sind, sich in der Kürze der zur Verfügung stehenden Zeit nicht feststellen lässt. Gegebenenfalls kann ein nachträgliches Rechtshilfeersuchen gestellt werden.

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 (vgl. BVerG NStZ 2011, 103 ff.).**

Ist der Rechtskreis des Betroffenen berührt, kann auch nach allgemeinen Grundsätzen ein Beweisverwertungsverbot entstehen, z. B.

- bewusste und gezielte Umgehung des Rechtshilferechts oder
- Rechtslage wird gröblich verkannt/fehlerhaft beurteilt oder
- zweckwidrige Verwendung offiziell erlangter Erkenntnisse

VII) Wichtige Rechtsnormen:

Zur Abgrenzung des Anwendungsbereichs des Telemedien- und des Telekommunikationsgesetzes wird auf die Ausführungen der Generalstaatsanwaltschaft Frankfurt am Main, Internetermittlungen – Ein Leitfaden für die Praxis-, Bezug genommen (Seite 3 ff).

1) Telemediengesetz

(http://www.gesetze-im-internet.de/tmg/)

§ 1 Anwendungsbereich

Dieses Gesetz gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind (Telemedien). …

§ 14 Bestandsdaten

(1) 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).
(2) **Auf Anordnung der zuständigen Stellen darf der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten erteilen**, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.

§ 15 Nutzungsdaten

(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die

Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

1. Merkmale zur Identifikation des Nutzers,
2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

…

(4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf der Diensteanbieter die Daten sperren.

(5) Der Diensteanbieter darf an andere Diensteanbieter oder Dritte Abrechnungsdaten übermitteln, soweit dies zur Ermittlung des Entgelts und zur Abrechnung mit dem Nutzer erforderlich ist. Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen anonymisierte Nutzungsdaten übermittelt werden. **§ 14 Abs. 2 findet entsprechende Anwendung.**

…

(7) Der Diensteanbieter darf Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers verarbeitet werden, höchstens bis zum **Ablauf des sechsten Monats nach Versendung der Rechnung speichern**

2) Telekommunikationsgesetz

(http://www.gesetze-im-internet.de/tkg_2004/)

§ 3 Begriffsbestimmungen

Im Sinne dieses Gesetzes ist oder sind

…

22. "**Telekommunikation**" der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen

§ 95 Vertragsverhältnisse

(1) Der Diensteanbieter darf **Bestandsdaten** erheben und verwenden, soweit dieses zur Erreichung des in § 3 Nr. 3 genannten Zweckes erforderlich ist. Im Rahmen eines Vertragsverhältnisses mit einem anderen Diensteanbieter darf der Diensteanbieter Bestandsdaten seiner Teilnehmer und der Teilnehmer des anderen Diensteanbieters erheben und verwenden, soweit dies zur Erfüllung des Vertrages zwischen den Diensteanbietern erforderlich ist. Eine Übermittlung der Bestandsdaten an Dritte erfolgt, soweit nicht dieser Teil oder ein anderes Gesetz sie zulässt, nur mit Einwilligung des Teilnehmers

..

§ 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.

§ 111 Daten für Auskunftsersuchen der Sicherheitsbehörden

(1) [1]Wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113

1. die Rufnummern und anderen Anschlusskennungen,
2. den Namen und die Anschrift des Anschlussinhabers,
3. bei natürlichen Personen deren Geburtsdatum,
4. bei Festnetzanschlüssen auch die Anschrift des Anschlusses,
5. in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie
6. das Datum des Vertragsbeginns

vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind; das Datum des Vertragsendes ist bei Bekanntwerden ebenfalls zu speichern. [2]Satz 1 gilt auch, soweit die Daten nicht in Teilnehmerverzeichnisse (§ 104) eingetragen werden. [3]Die Verpflichtung zur unverzüglichen Speicherung nach Satz 1 gilt hinsichtlich der Daten nach Satz 1 Nr. 1 und 2 entsprechend für denjenigen, der geschäftsmäßig einen öffentlich zugänglichen Dienst der elektronischen Post erbringt und dabei Daten nach Satz 1 Nr. 1 und 2 erhebt, wobei an die Stelle der Daten nach Satz 1 Nr. 1 die Kennungen der elektronischen Postfächer und an die Stelle des Anschlussinhabers nach Satz 1 Nr. 2 der Inhaber des elektronischen Postfachs tritt. [4]Wird dem Verpflichteten nach Satz 1 oder Satz 3 eine Änderung bekannt, hat er die Daten unverzüglich zu berichtigen; in diesem Zusammenhang hat der nach Satz 1 Verpflichtete bisher noch nicht erhobene Daten zu erheben und zu speichern, sofern ihm eine Erhebung der Daten ohne besonderen Aufwand möglich ist. [5]Für das Auskunftsverfahren nach § 113 ist die Form der Datenspeicherung freigestellt.

(2) [1]Bedient sich der Diensteanbieter nach Absatz 1 Satz 1 oder Satz 3 eines Vertriebspartners, hat der Vertriebspartner die Daten nach Absatz 1 Satz 1 und 3 unter den dort genannten Voraussetzungen zu erheben und diese sowie die nach § 95 erhobenen Daten unverzüglich dem Diensteanbieter zu übermitteln; Absatz 1 Satz 2 gilt entsprechend. [2]Satz 1 gilt auch für Daten über Änderungen, soweit sie dem Vertriebspartner im Rahmen der üblichen Geschäftsabwicklung zur Kenntnis gelangen.

(3) Für Vertragsverhältnisse, die am Tage des Inkrafttretens dieser Vorschrift bereits bestehen, müssen Daten im Sinne von Absatz 1 Satz 1 oder Satz 3 außer in den Fällen des Absatzes 1 Satz 4 nicht nachträglich erhoben werden.

(4) Die Daten sind mit Ablauf des auf die Beendigung des Vertragsverhältnisses folgenden Kalenderjahres zu löschen

(5) Eine Entschädigung für die Datenerhebung und -speicherung wird nicht gewährt.

§ 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 Ähnlichlichkeitsfunktion 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 d 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 Ähnlichlichkeitsfunktion
   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, darf nach Maßgabe des Absatzes 2 die nach den §§ 95 und 111 erhobenen Daten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. Dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auch Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Verkehrsdaten auch automatisiert ausgewertet werden. Für die Auskunftserteilung nach Satz 3 sind sämtliche unternehmensinternen Datenquellen zu berücksichtigten,

(2) Die Auskunft darf nur erteilt werden, soweit eine in Absatz 3 genannte Stelle dies in Textform im Einzelfall zum Zweck der Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der in Absatz 3 Nummer 3 genannten Stellen unter Angabe einer gesetzlichen Bestimmung verlangt, die ihr eine Erhebung der in Absatz 1 in Bezug genommenen Daten erlaubt; an andere öffentliche oder nichtöffentliche Stellen dürfen Daten nach Absatz 1 nicht übermittelt werden. Bei Gefahr in Verzug darf die Auskunft auch erteilt werden, wenn das Verlangen in anderer Form gestellt wird. In diesem Fall ist das Verlangen unverzüglich nachträglich in Textform zu bestätigen. Die Verantwortung für die Zulässigkeit des Auskunftsverlangens tragen die in Absatz 3 genannten Stellen.
(3) … (5) …

§ 100j StPO

(1) Soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist, darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 11 des Telekommunikationsgesetzes erhobenen Daten verlangt werden (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Absatz 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu bestimmten Zeitpunkten zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3 des Telekommunikationsgesetzes).

(3) Auskunftsverlangen nach Absatz 1 Satz 2 dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr in Verzug auch durch die Staatsanwaltschaft oder ihre Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Sätze 1 bis 3 finden keine Anwendung, wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung

gestattet wird. Das Vorliegen der Voraussetzungen nach Satz 4 ist aktenkundig zu machen.

(4) Die betroffene Person ist in den Fällen des Absatzes 1 Satz 2 und des Absatzes 2 von der Beauskunftung zu benachrichtigen. Die Benachrichtigung erfolgt, soweit und sobald hierdurch der Zweck der Auskunft nicht vereitelt wird. Sie unterbleibt, wenn ihr überwiegend schutzwürdige Belange Dritter oder der betroffenen Person selbst entgegenstehen. Wird die Benachrichtigung nach Satz 2 zurückgestellt oder nach Satz 3 von ihr abgesehen, sind die Gründe aktenkundig zu machen.
(5) Aufgrund des Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln. § 95 Abs. 2 gilt entsprechend.

VIII) 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

H) **Literatur und nützliche Links:**

Arndt/Fetzer/Scherer	Telekommunikationsgesetz Kommentar, 2008, Erich Schmidt Verlag
Marc Geppert	Beck`scher TKG Kommentar, April 2013
Bär, Wolfgang	• **KMR-Kommentar zur StPO, Kommentierungen zu §§ 100a - 101 StPO** • 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
Gemeinsame Arbeitsgruppe Polizei/Justiz (GAG) - Bayern -	Leitlinien für verdeckte Ermittlungsmaßnahmen (StPO-Novelle 2008); Stand: 01.04.2010) GAG_Leitfaden.pdf
LOStA Alfons Obermeier, Generalstaatsanwaltschaft München	Liste zur Überwachung grundrechtssichernder und sonstiger Verfahrensregelungenbei verdeckten Ermittlungsmaßnahmen TÜ-Überwachg.pdf
Bayerisches Landeskriminalamt	Leitfaden Ermittlungen und Recherchen in sozialen Netzwerken, Stand Dez. 2012
Hessisches Landeskriminalamt	Infoblatt Facebook Infoblatt_Facebook.pdf
OStA May/ OStA Franosch, Generalstaatsanwaltschaft Frankfurt a. Main	Internetermittlungen - Ein Leitfaden für die Praxis -, Stand: 08. 10.2012

	 BaWü_Leitfaden.pdf
www.a-i3.org	Arbeitsgruppe Identitätsschutz im Internet mit Sammlung relelvanter Gerichtsentscheidungen zum Phishing
www.antiphishing.org	Amerikanisches Webangebot mit vielfältigen Informationen rund um das Thema Phishing
www.cyberfahnder.de OStA Dieter Kochheim, Staatsanwaltschaft Hannover	Skript zu verdeckten Ermittlungen im Internet http://cyberfahnder.de/doc/Kochheim-Internet-Ermittlungen.pdf
www.dnstools.ch	Webseite mit Tools zur Ermittlung und Zuordnung von IP-Adressen