Generalstaatsanwaltschaft Frankfurt am Main
- Zentralstelle zur Bekämpfung der Internetkriminalität -

HESSEN

Internetermittlungen

- Ein Leitfaden für die Praxis -

Stand: 20.06.2013

Nur für den Dienstgebrauch!

Autoren:

OStA May
OStA Franosch
StA Dr. Krause

Generalstaatsanwaltschaft Frankfurt am Main
- Zentralstelle zur Bekämpfung der Internetkriminalität-

Außenstelle Gießen
Ostanlage 7
35390 Gießen

Telefon: 0641 / 934 - 3650 bis 3654
Telefax: 0641 / 934 - 3659
E-Mail: ZIT@GStA.Justiz.Hessen.de

Stand:

20.06.2013

Verwendungshinweis:

Der Inhalt ist nur für den dienstlichen Gebrauch bestimmt (NfD).
Jede kommerzielle Verwertung sowie die Weitergabe an Personen oder Stellen außerhalb von Strafverfolgungs-, Sicherheitsbehörden und der Bundeswehr sind untersagt.

Inhaltsverzeichnis

Teil 1 – Daten nach dem TKG/TMG und Voraussetzungen für ihre Beauskunftung durch die Diensteanbieter

Durch den Wegfall der Vorratsdatenspeicherung aufgrund des Urteils des BVerfG vom 02.03.2010 können im Rahmen von Internetermittlungen (bzw. durch die Auswertung sichergestellter Datenträger) gewonnene IP-Adressen über den Internet-Access-Provider (wie z.B. Telekom) häufig nicht mehr zum jeweiligen Anschlussinhaber zurückverfolgt werden, es sei denn es erfolgt eine Ausleitung der IP-Adressen in Echtzeit (s.u. Ziffer III.).

Ansatzpunkte für eine Täterermittlung ergeben sich jedoch regelmäßig durch vom Täter verwendete E-Mail-Adressen, Kennungen von sozialen Netzwerken, Chat- oder Messengerdiensten.

Zu Beginn der Ermittlungen muss der ermittelnde Polizeibeamte/Staatsanwalt klären, welchen telekommunikationsrechtlichen Vorschriften diese unterschiedlichen Dienste jeweils unterfallen, da diese Einordnung nicht nur von rein akademischem Interesse ist, sondern vielmehr Auswirkungen auf die möglichen Ermittlungsmaßnahmen hat.

I. Anwendungsbereiche und Abgrenzung von TMG und TKG

Die vorgenannten Dienste unterfallen allesamt entweder dem Telemedien- und/oder dem Telekommunikationsgesetz.

Das **Telemediengesetz (TMG)** hat am 01.03.2007 das Teledienstegesetz (TDG) und den Mediendienstestaatsvertrag (MDStV) ersetzt. Nach § 1 Abs. 1 TMG findet das Gesetz Anwendung auf Telemedien, also auf alle elektronischen Informations- und Kommunikationsdienste, die keine Telekommunikationsdienste (§ 3 Nr. 24 TKG), telekommunikationsgestützte Dienste (§ 3 Nr. 25 TKG) oder Rundfunk (§ 2 RStV) darstellen.

Darunter fallen

- **Onlineangebote von Waren/Dienstleistungen** (z.B. Angebot von Verkehrs-, Wetter-, Umwelt- oder Börsendaten, elektronische Presse, Fernseh-/Radiotext, Teleshopping)
- **Internet-Auktionshäuser** (z.B. ebay) / **Onlineversandhäuser** (z.B. Amazon)
- **Social-Community-Webseiten** (Facebook, VZ-Netzwerke, WKW u.a.)
- Betreiber von **Newsgroups**
- **Chatdienste**
- **Video-on-Demand** (verschlüsselte TV-und Hörfunkprogramme, sowohl in Abonnementform oder durch Einzelabruf)
- Onlinedienste, die Instrumente zur Datensuche, zum Zugang zu Daten oder zur Datenabfrage bereitstellen (z.B. **Internet-Suchmaschinen** wie google, bing oder yahoo)
- die kommerzielle Verbreitung von Informationen über Waren-/Dienstleistungsangebote mit elektronischer Post (z.B. Werbe-E-Mails)
- (grds.) **Access-Provider und E-Mail-Dienste** (soweit sie auf ihren Onlineportalen/Zugangsportalen neben dem reinen Internet-/E-Mail-Zugang auch weitere der o.g. Dienste anbieten, was regelmäßig der Fall ist)

Das TMG findet Anwendung auf alle Diensteanbieter einschließlich der öffentlichen Stellen, unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

Das **Telekommunikationsgesetz (TKG)** von 1996 (zuletzt geändert am 24.03.2011) ist der Nachfolger des früheren Fernmeldeanlagengesetzes (FAG) und regelt Telekommunikationsdienste.

Dies sind nach der Legaldefinition von § 3 Nr. 24 TKG „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen".
Das TKG betrifft daher im Wesentlichen die Telekommunikationsinfrastruktur sowie die hierüber erbrachten Telekommunikationsdienstleistungen.

Die **Abgrenzung zwischen TMG und TKG** wird dementsprechend weit überwiegend anhand der jeweiligen Funktion der Dienste vorgenommen:

Sind die Infrastruktur, das Leitungsnetz oder andere technische Belange betroffen, gilt das TKG. Stehen hingegen die übertragenen Inhalte im Vordergrund und nicht der reine Übertragungsvorgang, ist das TMG anwendbar.

Das bedeutet, dass bei jeder einzelnen Dienstleistung eines Anbieters zu prüfen ist, ob die Transportleistung im Vordergrund steht oder der transportierte Inhalt.[1]

In der Informatik werden Kommunikationsprotokolle in ein Schichtenmodell eingeordnet; Protokolle einer Schicht bauen auf denen der darunterliegenden Schicht auf. Die Strukturierung anhand eines solchen Modells hat den Vorteil, dass bei der Betrachtung einer spezifischen Aufgabenstellung von (internen) Details darunter- und darüberliegender Schichten abstrahiert werden kann. Am geläufigsten ist das aus sieben Schichten (Bitübertragung, Sicherung, Vermittlung, Transport, Kommunikationssteuerung, Darstellung, Anwendung) bestehende ISO/OSI-Referenzmodell. Daneben ist in der Praxis das TCP/IP-Modell relevant, in dem nur vier Schichten (Rechner-Netzanschluss, Vermittlung, Transport, Anwendung) betrachtet werden. In der juristischen Literatur wird die Auffassung vertreten, die Grenze zwischen TKG und TMG lasse sich zwischen Transport- und Anwendungsschicht des TCP/IP-Modells (bzw. zwischen Transport- und Kommunikationssteuerungsschicht des ISO/OSI-Modells) ziehen. Auch leicht abweichende Grenzziehungen finden sich. Problematisch ist dies jedoch, weil alle Schichten beider Modelle sich mit rein technischen Aspekten der Kommunikation befassen; die Diensterbringung, an der der Benutzer letztlich interessiert ist, bilden sie nicht ab.

TMG und TKG können aber auch parallel zur Anwendung kommen, zumal das TKG gemäß § 1 Abs. 3 TMG von der Anwendung des Telemediengesetzes unberührt bleibt. Dies ist etwa dann der Fall, wenn zusätzlich zum reinen Netzzugang auch o.g. inhaltliche Dienstleistungen nach dem TMG angeboten werden. Bei diesen „doppelfunktionalen" Diensten ist die rechtliche Einordnung im Einzelfall problematisch.

<u>Grundsätzlich gilt:</u>
Dienste mit Doppelnatur (=gleichzeitig Telekommunikationsdienst und Telemediendienst) fallen unter das TKG wie auch das TMG.

Für die Abgrenzung, auf welcher Gesetzesgrundlage im Einzelfall die Speicherung und Herausgabe von Daten an die Ermittlungsbehörden erfolgt, kommt es auf den jeweiligen **Schwerpunkt** an. Gem. § 11 Abs. 3 TMG sind die speziellen Auskunftsverpflichtungen der TMG-Dienste auf Telemedien, die **überwiegend** in der Übertragung von Signalen über Telekommunikationsnetze bestehen, nicht anwendbar. Insoweit muss dann auf die nach dem TKG gespeicherten Daten i.V.m. den allgemeinen Auskunftsverpflichtungen des Diensteanbieters nach den Vorschriften der StPO zurückgegriffen werden.

[1] Banholzer, Speicherrechte nach dem Telemediengesetz (TMG) und dem Telekommunikationsgesetz (TKG), abrufbar über die Webseite des DFN

Besonders problematisch ist diese Doppelnatur im Bereich der **E-Mail-Dienste**. Aus der Gesetzesbegründung zum TMG geht hervor, dass die Datenschutzvorschriften des TMG für diese deshalb nicht in vollem Umfang gelten müssten, da sie ohnehin unter die des TKG fielen.

Angesichts der Tatsache, dass E-Mail-Dienste heute selbst bei Freemail-Angeboten umfangreiche inhaltliche Leistungen anbieten (Nachrichtenportal, Verschlüsselung, E-Mail-Siegel, Virenschutz, Spamschutz, Navigator zu Shops, Anrufbeantworter, Online-Kalender, Online-Chat, etc.) wird man aber in der Regel nicht mehr davon ausgehen dürfen, dass der Dienst überwiegend in der Übertragung von Signalen besteht, sodass die E-Mail-Diensteanbieter nach hiesiger Auffassung auch den Auskunftsverpflichtungen des TMG unterfallen.
Dagegen unterfallen Access-Provider und Dienste der Internet-Telefonie (z.B. „Skype“) den Auskunftsverpflichtungen des TKG.

II. Befugnisse zur Datenspeicherung nach TMG und TKG / Auskunftsansprüche der Ermittlungsbehörden

1. Datenspeicherung und Auskunftsansprüche für Telemediendienste

Das TMG differenziert zwischen zwei Arten von personenbezogenen Daten – **Bestandsdaten** und **Nutzungsdaten** – und stellt an die Erhebung und Verwendung der jeweiligen Daten unterschiedliche Anforderungen:

a) Bestandsdaten

Bestandsdaten sind Daten, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind (§ 14 Abs. 1 TMG), beispielsweise **Name und Anschrift des Kunden, Kontoverbindung, (verschlüsseltes) Passwort, Nutzername bzw. -kennung („User-ID“) oder Art des kontrahierten Dienstes**. Bestandsdaten betreffen daher nicht einen konkreten Kommunikationsvorgang, sondern lediglich die vertraglichen Rahmenbedingungen für die legale Nutzung eines Telemediendienstes. Der Bestandsdatenbegriff entspricht der Bestandsdatendefinition des § 3 Nr. 3 TKG.

Die Voraussetzungen, unter denen der Diensteanbieter zur Weitergabe der erhobenen Bestandsdaten befugt ist, sind in § 14 Abs. 2 TMG geregelt. Demnach darf der Diensteanbieter auf Anordnung der zuständigen Stellen im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies u.a. für Zwecke der Strafverfolgung erforderlich ist. Da Bestandsdaten nicht zu den näheren Umständen der Telekommunikation gehören, mithin nicht unter den Schutzbereich des Fernmeldegeheimnisses des Art. 10 GG fallen, ist ihre Beauskunftung aufgrund der Ermittlungsgeneralklauseln der §§ 161, 163 StPO möglich.

Die Bestandsdaten nach dem TMG unterliegen jedoch (wie die des TKG) keinerlei Echtheits-Prüfungsverpflichtung durch den Telemedien-Diensteanbieter, d.h. ihre Aussagekraft ist - jedenfalls bei kostenlosen Diensten - zumeist sehr begrenzt. Um valide Aussagen zu erhalten sind daher Anfragen nach Daten erforderlich, deren Wahrheitsgehalt der Diensteanbieter stets oder im Bedarfsfall überprüft.

➡***Muster: Bestandsdatenabfrage nach TMG: Anlage 1***

b) Nutzungsdaten

Nutzungsdaten sind hingegen Daten, die erforderlich sind, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (§ 15 Abs. 1 TMG). Diese Daten, die es lediglich bei den Telemediendiensten gibt, sind für die Strafverfolgungsbehörden derzeit von großem Interesse.

Beispielhaft werden in § 15 Abs. 1 TMG als Nutzungsdaten Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien aufgeführt. Nutzungsdaten dürfen zu Abrechnungszwecken über das Ende des Nutzungsvorgangs hinaus gespeichert werden und – wenn zu diesem Zweck erforderlich – mit Nutzungsdaten über die Inanspruchnahme anderer Telemedien zusammengeführt werden. Der Diensteanbieter darf mit den Nutzungsdaten zu Werbe- und Forschungszwecken oder zur bedarfsgerechten Gestaltung der Telemedien zwar auch Nutzungsprofile erstellen, er muss aber Pseudonyme verwenden und der Nutzer darf der Erstellung eines Profils nicht widersprochen haben.

Auch **(dynamische) IP-Adressen** stellen Nutzungsdaten dar und unterfallen daher den Bestimmungen von § 15 TMG. (*Es ist derzeit heftig umstritten, ob die von den Telemediendiensten gespeicherten IP-Adressen „personenbezogene" Daten darstellen, denn dann würde deren Erhebung, Verarbeitung und Nutzung den datenschutzrechtlichen Vorschriften unterliegen, sodass dies ohne die ausdrückliche, aktiv erklärte Einwilligung des Nutzers nur bis zum Ende des jeweiligen Nutzungsvorgangs oder zu Abrechnungszwecken erhoben, verarbeitet und genutzt werden dürften. Weite Teile des Schrifttums[2] sowie der Rechtsprechung[3] sehen jedoch derzeit dynamische IP-Adressen nicht per se als personenbezogen an, sodass deren Speicherung durch die Telemediendienste als rechtmäßig zu beurteilen ist*.)

Nutzungsdaten gem. § 15 TMG sind zusammenfassend:

bei kostenlosen Diensten:

- (**dynamische) IP-Adressen des Nutzers**, Passwort, (frei wählbarer) Nutzername
- besuchte Subsites oder Mitgliedschaft in Nutzergruppen

bei Bezahldiensten (zusätzlich):

- Dauer der Nutzung
- einzelne kostenpflichtige Seitenabrufe oder Downloads

Auf diese Nutzungsdaten können die Ermittlungsbehörden durch ein einfaches Auskunftsersuchen gem. §§ 161, 163 StPO i.V.m. §§ 15 Abs. 5 S. 4, 14 Abs. 2 TMG zugreifen und damit auch **retrograde Login-IP-Adressen** des Nutzers erhalten. Zudem ist es hierüber bei einigen E-Mail-Diensten auch möglich, gem. §§ 161,163 StPO i.V.m. § 15 TMG Auskünfte darüber zu erhalten, welche weiteren Dienste (bspw. Zugriff auf weitere E-Mail-Konten) mit den dort mitgeloggten IP-Adressen in Anspruch genommen wurden.

➡***Muster: Nutzungsdatenabfrage nach TMG: Anlage 2***

[2] Krüger/Maucher MMR 2011, 433 Rn. 92

[3] AG München MMR 2008,860 ; LG Wuppertal MMR 2011,65 ; OLG Köln BeckRS 2010,10822 ; OLG Hamburg MMR 2011, 281

Die Abfrage von Nutzungsdaten wird auch zukünftig von eminenter praktischer Wichtigkeit sein, da

- die Nutzungsdatenabfrage (Erhalt der Login-IP) nicht den erhöhten Eingriffsvoraussetzungen des § 100 g StPO unterliegt

- nach der eindeutigen Aussage des BVerfG vom 02.03.2010 auch weiterhin bei bekannter IP-Adresse (nebst Zeitstempel) ein Rückgriff auf die Vorratsdaten unabhängig von begrenzenden Rechtsgüterkatalogen zulässig ist

- zu erwarten ist, dass die Vorratsdatenspeicherung deutlich weniger als 6 Monate betragen wird, sodass weiterhin Eilbedürftigkeit bestehen wird

c) Plattformübergreifende Recherche (mittels Bestands- oder Nutzungsdaten)

Falls eine Datenabfrage bei dem für die ermittelte E-Mail-Adresse, die Nutzerkennung oder das Passwort zuständigen Dienstanbieter erfolglos bleibt, bietet es sich in geeigneten Fällen an, zu prüfen, ob diese Daten – was erfahrungsgemäß häufig der Fall ist – auch auf anderen Plattformen genutzt werden und sodann über diese weitergehende Nutzerinformationen zu erhalten sind.

So werden z.B. E-Mail-Adressen, die für kriminelle Zwecke genutzt werden, auch bei sozialen Netzwerken oder bei Skype hinterlegt oder eingesetzt. Auch werden – gerade komplexe und damit individualisierbare – Passworte häufig mehrfach verwendet. Abfragen nach Passworten sollten jedoch, da diese bei den Diensteanbietern häufig verschlüsselt abgelegt werden, die Hashwerte der gebräuchlichsten Verschlüsselungsmethoden beigefügt werden.

Beispiel:

Passwort	Hashwert MD 5	Hashwert SHA-1	Hashwert CRC 32

Passwort	MD5	SHA-1	CRC32
ra17.5el	05C8165CD9CC119AE82D8550FD5C815D	77778E4C024D87D4ABE5727944C612F9FD14A354	4472F3AC
bo12.5le	A194D443948498CCF3256AC3DC7CD9FB	3103B1669CD7FB19F1FA44EF172B68A9C59D3270	08083547
RA!/:%EL	D835CF68271F34EE0BB494B62BE6DA0F	5004DE109C5F3F3B28B691A1CDD94C3BC5DE9495	4C48116C
ma24.7ke	00003E3133A114FED6A88AD4EB76AB0F	5CDD1060E8013470C752F37A9CDC3E302612C1C2	C4069911
derkeller0815 (1)	E56409F3B4C2AC25F1A3A62D9B3D21C7	E35A0785F9F97780CEAF8613909CDC10BA478413	C0D11A46
koenig	22123CB23FC6C93B5FD5C387A238121B	617D1703C8B160C078F1953413B024813BA021BF	E1CB7BA8

2. Datenspeicherung und Auskunftsansprüche für Telekommunikationsdienste

Für die Erhebung und Beauskunftung von (Kunden-) und **Bestandsdaten nach dem TKG** (bei den Access-Providern oder Diensten der Internet-Telefonie) gelten keine wesentlichen Abweichungen. Der Bestandsdatenbegriff des § 95 i.V.m. § 3 Nr. 3 TKG entspricht dem des TMG.

Lediglich die Auskunftsverfahren sind besonders geregelt:

a) Kundendaten, § 111 TKG

Die Kundendaten des § 111 TKG, also

- Rufnummern
- Name und Anschrift des Rufnummerinhabers
- Datum des Vertragsbeginns
- bei Festnetzanschlüssen: Anschrift des Anschlusses
- Datum des Vertragsendes

zu deren Speicherung der geschäftsmäßige Anbieter von TK-Diensten verpflichtet ist und die er bei Bekanntwerden von Änderungen (auch bei prepaid-Produkten) aktualisieren muss, hat der TK-Diensteanbieter in Kundendateien zu speichern, damit diese gem. **§ 112 TKG i.V.m. §§ 161, 163 StPO** für kostenfreie, behördliche Auskunftsersuchen im Wege **automatisierter Abfrage** zur Verfügung stehen.

b) Bestandsdaten, § 95 TKG

Darüber hinaus hat der geschäftsmäßige TK-Anbieter gem. **§ 100j StPO i.V.m. § 113 TKG** unverzüglich über Kundendaten und die **Bestandsdaten gem. § 95 TKG**, die er erheben und verwenden darf, also

- Daten des Nutzers (Name, Geburtsdatum, Anschrift, Bankverbindung)
- Angaben zum Zahlungsverkehr, bestellte Dienstemerkmale
- Feste IP-Adressen (nicht dynamische)
- Namen zu E-Mail-Adressen

Auskunft zu erteilen.

Die manuelle Auskunftserteilung – die sich bei allen spezifischen Fragestellungen anbieten wird – ist kostenpflichtig.

➡***Muster: Bestandsdatenabfrage nach § 100j StPO: Anlage 1***

aa) Sonderfall der Bestandsdatenabfrage I (bei dynamischen IP-Adressen)

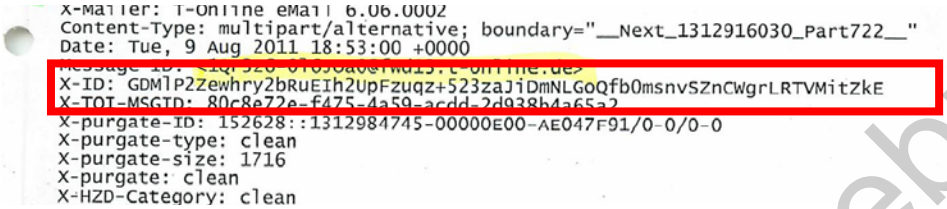
Bei der Abfrage dynamischer IP-Adressen, welche grds. Verkehrsdaten nach § 96 TKG darstellen, ist folgende Besonderheit zu beachten:

- Soweit ein konkreter **Telekommunikationsvorgang noch nicht bekannt** ist, wenn also z.B. hinsichtlich eines Anschlussinhabers sämtliche an diesen dynamisch vergebenen IP-Adressen abgefragt werden sollen, ist hierfür ein Beschluss gem. § 100g StPO erforderlich.

- Soweit ein konkreter **Telekommunikationsvorgang** (bestehend aus einer dynamischen IP-Adresse in Verbindung mit einem konkreten Zeitstempel [Datum, Uhrzeit, Zeitzone]) jedoch **bereits bekannt** ist, und nur noch bei dem Internet-Access-Provider den Bestandsdaten eines Kunden zugeordnet werden soll, bedarf es hierfür keines 100g-Beschlusses, sondern es genügt ein Auskunftsersuchen gem. § 100j StPO.

bb) Sonderfall der Bestandsdatenabfrage II (X-ID's)

Nutzt ein Täter die Deutsche Telekom sowohl als Access-Provider als auch als E-Mail-Provider, so ist dessen Ermittlung bei einer durchaus möglichen Veränderung der E-Mail-Adresse im E-Mail-Header – trotz Ablauf der 7-tägigen Speicherfrist – über eine Kennung (bei der Telekom: **X-ID**) in den Kopfzeilen der E-Mail möglich. Nach welchem Zeitraum diese X-ID's gelöscht werden, ist derzeit nicht bekannt, jedoch kann die Telekom über diese eine Aussage treffen, von welchem Anschluss aus die E-Mail versendet wurde. Die Telekom erteilt diese Auskünfte ebenfalls über eine Bestandsdatenabfrage gem. **§ 100j StPO.**



cc) Sonderfall der Bestandsdatenabfrage III (HotSpots)

HotSpots werden üblicherweise von klassischen Telekommunikationsanbietern (Access-Providern) betrieben, bei McDonald's etwa von T-Mobile. Dort müssen die Kunden bei der Registrierung für die kostenlose Nutzung des HotSpot (z.B. täglich eine Stunde) lediglich ihre Mobilfunknummer angeben. An diese Mobilfunknummer wird von dem Betreiber eine Zugangs-PIN per SMS übersendet.

Sofern die Nutzung des HotSpots per Zeitstempel individualisierbar ist, kann die angegebene Mobilfunknummer gemäß § 100j StPO abgefragt werden.

Bei dieser Mobilfunknummer handelt es sich um ein Kunden- bzw. Bestandsdatum gem. §§ 95, 111 TKG. Die Angabe der Mobilfunknummer ist für die Übersendung der Zugangs-PIN und damit für die Begründung des Vertrages über die Nutzung des HotSpot erforderlich. Dies gilt nicht nur für die kostenlose Nutzung, sondern auch und gerade für die folgende kostenpflichtige Nutzung des HotSpot, da dann üblicherweise die Abrechnung über die angegebene Mobilfunknummer erfolgt.

Ein Verkehrsdatum gem. § 96 TKG stellt diese Mobilfunknummer schon deshalb nicht dar, weil diese Nummer nicht bei der Nutzung eines Telekommunikationsdienstes anfällt und gespeichert wird, sondern - wie bereits beschrieben - zur Begründung des Vertragsverhältnisses erhoben und gespeichert wird. Ein Beschluss nach § 100g StPO ist daher nicht erforderlich.

dd) Sonderfall der Bestandsdatenabfrage IV (Unternehmensnetzwerke)

Wenn bei den Ermittlungen über eine IP-Adresse Hinweise auf das Netzwerk eines Unternehmens bekannt werden, stellt sich zunächst die Frage, ob auch Bestandsdaten von Unternehmen angefragt werden können.

§ 100j StPO verpflichtet diejenigen zur Auskunft, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken. Ein geschäftsmäßiges Erbringen von Telekommunikationsdiensten ist nach § 3 Nr. 10 TKG das „nachhaltige Angebot von Telekommunikationsdiensten für Dritte mit oder ohne Gewinnerzielungsabsicht". Nicht erforderlich ist, dass der Verpflichtete seine Telekommunikationsdienste der Öffentlichkeit zugänglich macht, sofern Dritte auf diesen Dienst zurückgreifen können und eine gewisse Nachhaltigkeit vorhanden

ist. § 100j StPO verpflichtet daher grundsätzlich auch die Betreiber von **Corporate Networks für Unternehmen** und Behörden, Auskünfte über ihre Teilnehmer zu erteilen[4].

Daneben kann sich das Problem stellen, dass eine reine Abfrage der bekannten IP-Adresse mit Zeitstempel nicht zielführend ist, wenn diese IP-Adresse zeitgleich mehreren Personen (Mitarbeitern) zugeordnet werden kann.

Eine Zuordnung etwa des Zugriff auf eine verfahrensgegenständliche URL ist insofern nur über Log-Daten der lokalen (internen) IP-Adressen möglich. Für diese Art der Abfrage ist ein **Beschluss nach § 100g StPO** zur Verpflichtung des Unternehmens erforderlich, da insoweit originär Verkehrsdaten erhoben werden müssen.

III. Erhebung von Verkehrsdaten (§ 100g StPO, § 96 TKG)

Trotz der dargestellten Ermittlungsmöglichkeiten über Kunden-, Bestands- und Nutzungsdaten bleibt der Rückgriff auf IP-Adressen der wichtigste Ansatzpunkt zur Täterermittlung, da über diese jedenfalls i.d.R. nachvollzogen werden kann, von welchem Anschluss die Einwahl erfolgt ist.

1. Retrograde Erhebung von Verkehrsdaten

Gemäß § 96 Abs. 1 Nr. 1 TKG sind die Diensteanbieter grds. berechtigt, Nummern oder Kennungen der an einem Telekommunikationsvorgang beteiligten Anschlüsse zu erheben und zu verwenden. Nummern sind hierbei nicht nur die Rufnummern des klassischen Telefondienstes, sondern auch **IP-Adressen**. Der ursprüngliche Regelfall einer Speicherung von IP-Adressen mit Beginn und Ende der jeweiligen Verbindung gem. § 96 Abs. 1 Nr. 2 TKG zur Entgeltabrechnung (§ 97 TKG), ist aufgrund der inzwischen meist vorhandenen „Flatrate"-Verträge nicht mehr gegeben: Eine Verkehrsdatenspeicherung zu Abrechnungszwecken erfolgt bei den TK-Anbietern gegenwärtig vielfach nicht oder nur sehr kurzzeitig.

Neben der Entgeltermittlung ist aber auch eine Verkehrsdatenverwendung gem. § 96 Abs. 2 TKG vor allem zur Störungs- und Missbrauchsbekämpfung (§ 100 TKG) zulässig. Die Rspr. hat insoweit eine 7-tägige Speicherfrist der Diensteanbieter für zulässig erachtet (BGH MMR 2011, 341), welche z.B. von der Deutschen Telekom auch ausgeschöpft wird.

Alle Ermittlungshandlungen, die auf die **Erlangung von retrograden Verkehrsdaten** abzielen oder unter deren Verwendung erfolgen, sind daher nunmehr stets eilbedürftig, weil eine Speicherung auf der Grundlage des § 96 TKG in der Regel nur für kurze Zeiträume erfolgt und die Daten sodann von den Providern gelöscht werden.

Datenerhebungen sind daher grundsätzlich beschleunigt durchzuführen, in Fällen drohenden Beweismittelverlustes sind Eilanordnungen zu treffen.

[4] Säcker, in: Säcker, Berliner Kommentar zum TKG, 2. Aufl., § 3 Rn. 19 ff.; Bock, in: Beck'scher TKG-Kommentar, 3. Auflage, § 113 Rn. 2.

2. Erhebung von Verkehrsdaten in Echtzeit bei TK-Diensten

Da retrograde Verkehrsdatenermittlungen aufgrund fehlender oder nur kurzfristiger Speicherung durch die Access-Provider häufig nicht erfolgreich sein werden, ist zur Täterermittlung – soweit die rechtlichen Voraussetzungen gegeben sind – eine **Echtzeitüberwachung gem. § 100g StPO bei TK-Diensten** erforderlich, um eine Abfrage der IP-Adresse (bei dem diese nicht speichernden Access-Provider) während der laufenden Session/Verbindung vornehmen zu können.

§ 100g Abs. 1 StPO stellt seit dem 01.01.2008 eine allgemeine Befugnis zur Erhebung von Verkehrsdaten dar, sodass nunmehr diese Echtzeiterhebung von Verkehrsdaten möglich ist, wobei die Erhebungsbefugnis keine bestehende Kommunikationsverbindung voraussetzt.

Gem. § 100g StPO können mithin auch Diensteanbieter zur Erhebung und Echtzeitausleitung von Verkehrsdaten verpflichtet werden, die normalerweise solche Verkehrsdaten weder erheben noch speichern. In den Beschlüssen ist darauf zu achten, dass die Erhebung und Ausleitung der Verkehrsdaten in Echtzeit zur Klarstellung in den Beschlusstext aufgenommen wird.

➡***Muster: Echtzeitüberwachung eines Telekommunikationsdienstes: Anlage 3***

3. Erhebung von Verkehrsdaten in Echtzeit bei TM-Diensten

Zwar enthält § 100g StPO – im Unterschied etwa zu § 20 m II BKAG – keinen (ausdrücklichen) Auskunftsanspruch auf Nutzungsdaten gem. § 15 TMG.

Gleichwohl wird die Anwendung des § 100g StPO auf Telemediendienste für zulässig erachtet[5], sodass auch Betreibern von Telemediendiensten wie Chats, Foren, sozialen Netzwerken etc. gem. § 100g StPO verpflichtet werden können, Verkehrsdaten (also IP-Adressen) in Echtzeit zu erheben und an die Strafverfolgungsbehörden auszuleiten.

➡***Muster: Echtzeitüberwachung eines Telemediendienstes: Anlage 3***

4. Erhebung von Verkehrsdaten in Echtzeit in anderen Fällen

Gem. § 100g Abs. 3 StPO bestimmt sich die Erhebung von Verkehrsdaten, sofern sie nicht beim Telekommunikationsdiensteanbieter erfolgt, nach Abschluss des Kommunikationsvorgangs nach den allgemeinen Vorschriften, d.h. für den Zugriff auf alle Daten, die auf PCs, Festplatten, Servern o.ä. abgespeichert sind, ist ein Beschluss gem. § 100g StPO nicht erforderlich. Die Daten/Datenträger können –ggf. im Rahmen von Durchsuchungsmaßnahmen – vorläufig sichergestellt bzw. beschlagnahmt werden (näheres s.u.).

[5] Bär, TK-Überwachung Vorb. § 100a Rn 32; Karlsruher-Kommentar, § 100a Rn 12

IV. Erhebung von Inhaltsdaten (§ 100a StPO)

1. DSL-Überwachung

Unter dem gesetzlich nicht definierten Begriff der „**Inhaltsdaten**“ kann man insbesondere den eigentlichen Inhalt der übermittelten Nachrichten subsumieren. Der Zugriff auf den Inhalt während der Nachrichtenübermittlung ist bei strafprozessualen Maßnahmen nur nach § 100a StPO möglich. Neben den Kommunikationsinhalten umfasst 100a aber auch die übertragenen Verkehrs- bzw. Nutzungsdaten, sodass ein ergänzender Beschluss gem. § 100g StPO nicht erforderlich ist. Die Überwachung des Internet-Verkehrs bei einem bekannten Internetanschluss erfolgt in der Regel durch eine „klassische“ DSL-Überwachungsmaßnahme.

➡***Muster: Beschluss DSL-Überwachung: Anlage 4***

2. Quellen-TKÜ

Da Internet-Kommunikation (VoIP, HTTPS) in zunehmendem Maß verschlüsselt stattfindet und eine „Entschlüsselung“ der kryptierten Daten praktisch nicht möglich ist, liefert eine „herkömmliche“ TK-Überwachungsmaßnahme in diesen Fällen keine verwertbaren Ergebnisse.

Es ist daher zwingend erforderlich, die Daten im Rechner vor dem Kommunikationsvorgang selbst aufzuzeichnen, zu übertragen oder auf andere Art und Weise auszuleiten oder auszulesen.

Eine solche **„Quellen-Telekommunikationsüberwachung“** wird in Rechtsprechung und Literatur nahezu einhellig als zulässig gem. § 100a StPO angesehen[6]. Hinsichtlich etwaiger ergänzender Maßnahmen, z.B. Aufbringung der Übertragungssoftware auf dem zu überwachenden Rechner über Datenleitung ist eine zusätzliche Anordnung (bspw. nach § 100c StPO) nicht notwendig; diese ist vielmehr als Begleitmaßnahme zur Umsetzung der Überwachung gemäß § 100a StPO im Wege der Annexkompetenz zulässig. Das Betreten von Wohnungen ist hingegen von der Annexkompetenz nicht umfasst, da hier nicht Art. 10 GG, sondern Art. 13 GG betroffen ist.

Bei der Überwachung verschlüsselten E-Mail-Verkehrs ist allerdings darauf zu achten, dass die Übertragungssoftware so konfiguriert ist, dass keine „Entwürfe“ per Screen-shots gesichert werden[7].

➡***Muster: Beschluss „Quellen-TKÜ“: Anlage 5***

3. Analoge Anwendung des § 100a StPO bei TM-Diensten

Für eine Überwachung von Inhaltsdaten bei Telemediendiensten (bspw. Überwachung des Chatverkehrs bei ICQ) ist § 100a StPO ebenfalls (analog) anwendbar.

[6] Meyer-Goßner, § 100a Rdn. 7 a m.w.N.
[7] LG Landshut; Beschl. v 20.1.2011 – Az 4 Qs346/10

Teil 2 – Weitergehende Möglichkeiten der Täteridentifizierung

I. Rechtsgrundlage für den Zugriff auf zwischengespeicherte Nachrichten auf dem Server eines E-Mail-Providers

Nach einer Entscheidung des BVerfG[8] und zwei Entscheidungen des BGH[9] sind die Voraussetzungen für den Zugriff auf Inhalte der Mailbox eines E-Mail-Diensteanbieters geklärt.

Nach der Entscheidung des BGH vom 31.03.2009 können E-Mails beim E-Mail-Provider entsprechend den Voraussetzungen des **§ 99 StPO** mit der Herausgabepflicht nach § 95 Abs. 2 StPO beschlagnahmt werden.

Auch das BVerfG hat in der Entscheidung von 16.06.2009 bestätigt, dass die **§§ 94 ff. StPO** den verfassungsrechtlichen Anforderungen, die an eine gesetzliche Ermächtigung für die Sicherstellung und Beschlagnahme von E-Mails auf dem Server des Providers zu stellen sind, genügen. Damit sind sowohl § 99 StPO, als auch §§ 94, 98 StPO anwendbar.

Der BGH hat allerdings in der Entscheidung vom 24.11.2009 darauf hingewiesen, dass es sich bei der **Beschlagnahme gem. §§ 94 ff. StPO** um eine offene Ermittlungsmaßnahmen handelt, deren Anordnung den Betroffenen und Verfahrensbeteiligten bekannt zu machen ist (§ 33 Abs. 1, § 35 Abs. 2 StPO). Eine Zurückstellung der Benachrichtigung wegen Gefährdung des Untersuchungszwecks sieht die Strafprozessordnung für diese Untersuchungshandlung nicht vor. Darüber hinaus ist zu beachten, dass die Anordnung der Beschlagnahme des gesamten auf dem Mailserver des Providers gespeicherten E-Mail-Bestandes eines Beschuldigten regelmäßig gegen das **Übermaßverbot** verstößt. Als weniger eingriffsintensive Maßnahme kann etwa die Beschlagnahme eines Teils des Datenbestands unter Eingrenzung der ermittlungsrelevanten E-Mails anhand bestimmter Sender- oder Empfängerangaben oder anhand von Suchbegriffen in Betracht kommen. Dies wird in aller Regel nicht praktikabel sein. Dem Verhältnismäßigkeitsgrundsatz kann jedoch auch die **vorläufige Sicherstellung des gesamten E-Mail-Bestandes** im Rahmen einer **Durchsuchung beim Provider nach § 103 StPO** genügen, an die sich zunächst eine **Durchsicht des sichergestellten Datenmaterials nach § 110 Abs. 1 bzw. Abs. 3 StPO** zur Feststellung der Beweiserheblichkeit und -verwertbarkeit anzuschließen hat. Erst dann sind gemäß § 98 StPO lediglich die beweiserheblichen E-Mails zu beschlagnahmen.

Die Beschlagnahme nach § 99 StPO kann auch in die Zukunft gerichtet werden. Eine Echtzeitausleitung neu ein- und ausgehender Mails ist jedoch nur nach § 100a StPO möglich, da über § 99 StPO nur solche Mails erlangt werden können, die auf dem Mailserver des Providers abgespeichert sind. Daher sollten in einem in die Zukunft gerichteten Beschluss Intervalle für die Herausgabe angegeben werden. Je kürzer die Intervalle gewählt werden, desto höher ist der Aufwand für den jeweiligen E-Mail-Provider.

Die Beschlagnahme der Inhalte auf den Servern der E-Mail-Provider ist ermittlungstaktisch vor allem deshalb wichtig, weil die Täter über diese kommunizieren können, ohne E-Mails versenden und empfangen zu müssen. Die Täter nutzen einfach denselben E-Mail-Account und tauschen ihre Nachrichten dadurch aus, dass sie abwechselnd Nachrichteninhalte als Entwürfe im Entwurfsordner abspeichern (Prinzip „toter Briefkasten“). Beschränkt man sich ermittlerseitig also auf eine einmalige Beschlagnahme nach § 99 StPO und eine spätere Echtzeitausleitung nach § 100a StPO, besteht die Gefahr, dass die Nutzung des Entwurfsordners als toter Briefkasten unentdeckt bleibt. Zur Gewährleistung einer lückenlosen E-Mailüberwachung empfiehlt es sich daher in Fällen, in denen mit einem solchen Täterhan-

[8] BVerfG 2. Senat,16.06.2009 (2 BvR 902/06)

[9] BGH 1. Strafsenat vom 31.03.2009, 1 StR 76/09; BGH 3.Strafsenat, 24.11.2009, StB 48/09

deln zu rechnen ist, die Maßnahmen zu kombinieren und neben einer 100a-Echtzeitüberwachung die Postfachinhalte wiederholt ausleiten zu lassen. Wegen des hohen damit verbundenen Aufwandes sollte dieses Vorgehen sorgfältig geprüft und nur in bedeutsamen Fällen angewendet werden.

Folgerung:

Wenn die Maßnahme offen erfolgen kann:

- Beschluss gemäß § 103 StPO beim Provider für den gesamten Mailbestand, anschließend Durchsicht gemäß § 110 StPO sowie Beschlagnahme lediglich der beweiserheblichen E-Mails gemäß § 98 StPO.

Wenn prozessuale Folgemaßnahmen (Telefonüberwachung, Durchsuchung) beabsichtigt sind:

- Beschluss gemäß § 99 StPO mit Übertragung der Durchsicht des Postfachinhaltes auf die Staatsanwaltschaft gemäß § 100 Abs. 3 StPO. Eine Übertragung auf deren Ermittlungspersonen entsprechend § 110 Abs. 1, 2. Hs. StPO ist nicht möglich.

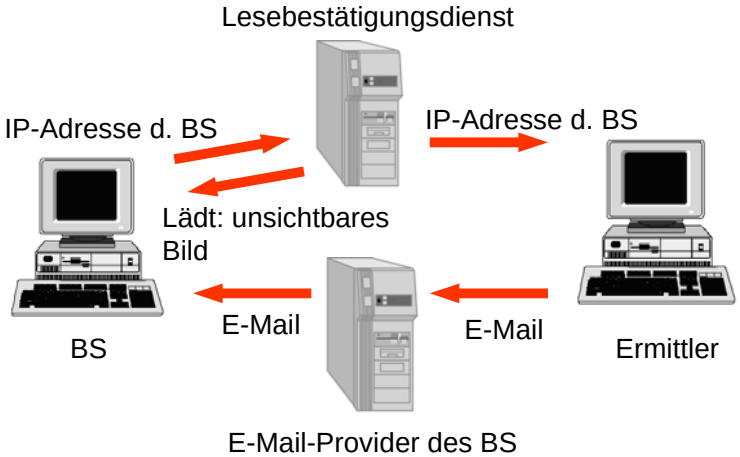
Wenn eine verdeckte, dauernde lückenlose E-Mail-Überwachung erforderlich ist:

- Kombinierter 99- und 100a-Beschluss mit Übertragung der wiederholten Durchsicht des Postfachinhaltes auf die Staatsanwaltschaft gemäß § 100 Abs. 3 StPO (Katalogtat erforderlich, sehr aufwendig in der Umsetzung).

➡***Muster: Beschlagnahme bzgl. E-Mail-Postfach gem. § 99 StPO: Anlage 6***

II. Bestandsdatenerhebung durch verdeckte Teilnahme der Ermittlungsbehörden an einem Telekommunikationsvorgang („IP-Tracking“)

Neben den Möglichkeiten zur Abfrage und Erhebung von IP-Adressen bei einzelnen Telekommunikations- und Telemediendiensteanbietern (retrograd oder in Echtzeit) besteht in geeigneten Fällen auch die Möglichkeit, aktuelle IP-Adressen eines Beschuldigten durch den Einsatz von sog. Lesebestätigungsdiensten zu erhalten. Hierbei werden E-Mails mit funktionslosen, 1x1-Pixel kleinen, transparenten Bildern versehen. Bei bestehender Internetverbindung werden diese beim Öffnen der E-Mail von einem externen Server nachgeladen und erlauben somit eine Kontrolle, wann welches Dokument geöffnet wurde. Dabei wird die aktuelle IP-Adresse des Internetanschlusses, an welchem die E-Mail geöffnet wurde, aus technischen Gründen jeweils an den Server übertragen. Der bekannteste private Anbieter derartiger Lesebestätigungsdienste heißt „ReadNotify“.



1. Rechtliche Voraussetzungen des IP-Tracking

Hinsichtlich der rechtlichen Zulässigkeit des Einsatzes von Lesebestätigungsdiensten gilt, dass die Kommunikation von Ermittlungsbehörden mit Dritten unter einer fiktiven E-Mail-Adresse oder einer sonstigen Legende grundsätzlich erlaubt ist[10].

Nach der hier vertretenen Auffassung, sowie nach Meyer-Goßner[11] und Bär[12], handelt es sich bei der Verwendung derartiger Bestätigungsdienste durch Ermittlungsbehörden um den Einsatz eines sonstigen technischen Mittels gem. **§ 100h Abs. 1 Nr. 2 StPO**, der durch Polizei und Staatsanwaltschaft angeordnet werden kann.

Je nach der Ausgestaltung des eingesetzten Tools kann der Einsatz von Lesebestätigungsdiensten bereits auf Grundlage der **§§ 161 oder 163 StPO** zulässig sein, weil die Einordnung als „technisches Mittel“ i.S.v. § 100h StPO in Fällen, in denen die angewendete Maßnahme offen erkennbar ist, zu weitgehend sein könnte:

- Das Einbetten von unsichtbaren Bildern ist als Marketing-Methode beim Versand von Werbe-E- Mails üblich.
- Der Download von Bildern ist normale Internet-Nutzung.
- Der Einsatz eines Lesebestätigungsdienstes ist nicht vollständig verdeckt, zwar sind die Bilder unsichtbar, in den Kopfzeilen der Nachricht ist deren Verwendung aber häufig erkennbar.

Frühere untergerichtliche Entscheidungen, wonach für den Einsatz von Lesebestätigungsdiensten ein richterlicher Beschluss gemäß § 100g StPO erforderlich sein soll, sind überholt und übersehen, dass ein Eingriff in das Grundrecht aus Art. 10 GG nicht gegeben ist. Das Telekommunikationsgeheimnis gilt nämlich nicht zwischen den Teilnehmern an einem TK-Vorgang. Erfasst sind Nachrichten während des technischen Übermittlungsvorgangs; der Grundrechtsschutz endet am Endgerät des TK-Teilnehmers[13]. Die staatliche Wahrnehmung von Inhalten oder Umständen der Telekommunikation ist daher nur dann am Telekommunikationsgeheimnis zu messen, wenn eine staatliche Stelle eine Telekommunikationsbeziehung von außen überwacht. Das Grundrecht schützt dagegen nicht davor, dass eine staatliche Stelle selbst eine Telekommunikationsbeziehung zu einem Grundrechtsträger aufnimmt[14].

Das gilt auch in Fällen, in denen an eine E-Mail bspw. Bilder, PDF-Dateien oder Anhänge mit Dateiformaten aller Art angehangen werden, die entsprechende Einbettungen (sog. iFrames) enthalten, durch deren Ausführen die IP-Adresse des Empfängers übermittelt wird, sofern er den Anhang aktiv öffnet.

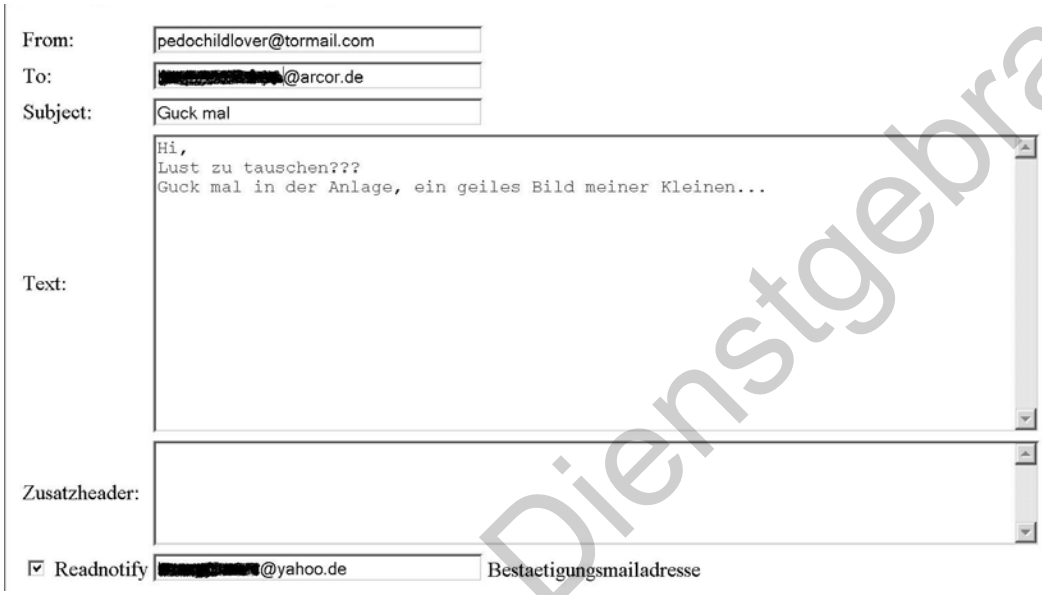
Gerade in diesen Fällen kann ein Vorgehen bereits auf der Grundlage der §§ 161 oder 163 StPO zulässig sein, da das Öffnen der E-Mail-Anhänge von einer bewussten Entscheidung des Empfängers abhängt und allgemein bekannt ist, dass das Öffnen von Dateianhängen Datenspuren verursacht, die beim Absender oder Dritten erfasst werden können.

[10] Vgl. BVerfG NJW 2008, 822-837, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 290
[11] Meyer-Goßner, StPO, 54. Aufl. 2011, § 100h Rn. 2
[12] Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren, Rn 306-310
[13] Vgl. BGHSt 42, 139 ff
[14] BVerfG NJW 2008, 822-837, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 272

2. IP-Tracking bei E-Mail-Diensten

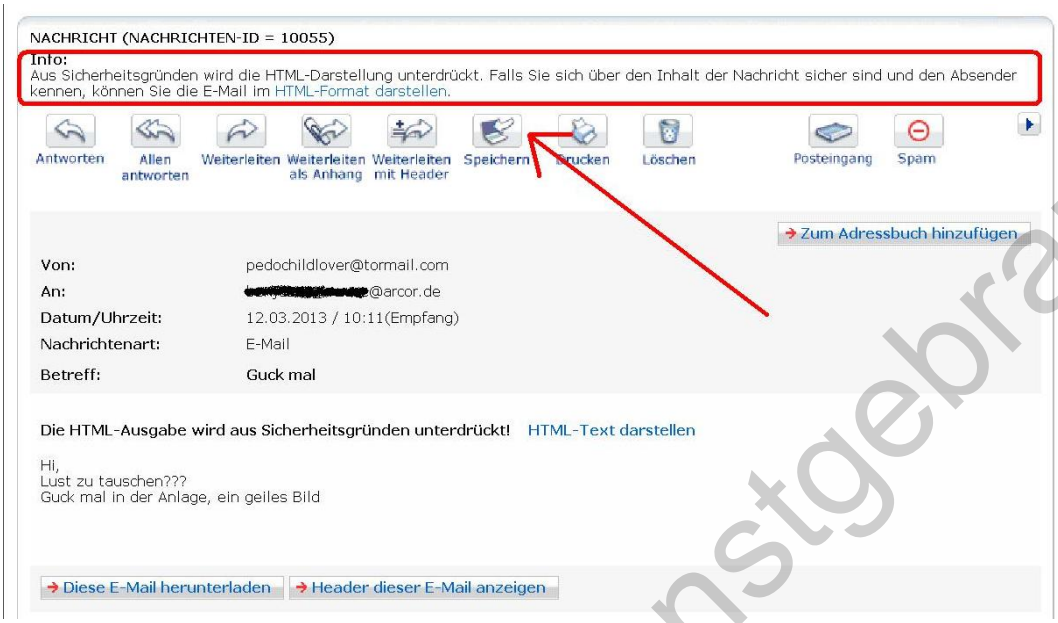
Es ist technisch ohne weiteres möglich, bei der Versendung von E-Mails die Absenderangaben in dem E-Mail-Header zu ändern, so dass nicht die von den Ermittlern tatsächliche genutzte E-Mail-Adresse, sondern eine fiktive E-Mail-Adresse bei dem Beschuldigten angezeigt wird (so genannte Fake-Mail).

Eine entsprechende Fake-Mail (hier: pedochildlover@tormail.com) mit Einbindung der Read-notify-Technik könnte etwa so aussehen:



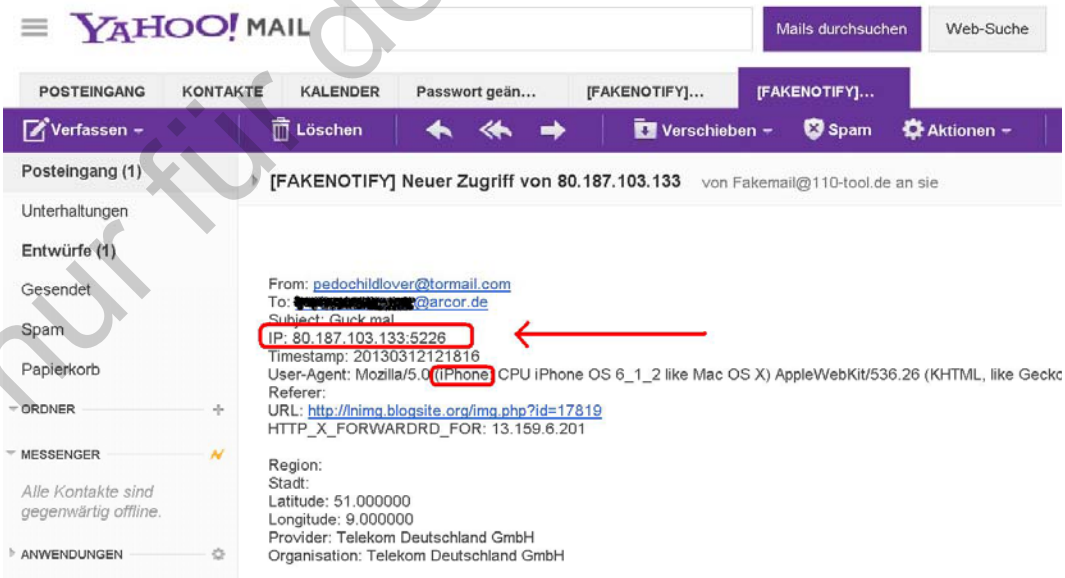
Bei dem Empfänger wird die Fake-Mail mit dem (transparenten) Bild im Anhang so dargestellt.

Je nach Konfiguration des betroffenen PCs bzw. Mail-Programms kann die Kontaktaufnahme zu dem externen Server durch den Empfänger der Fake-Mail aber auch verhindert werden, so dass die Maßnahme ins Leere läuft und ein gewisses Entdeckungsrisiko besteht.



Durch das Nachladen des Anhangs wird von dem Readnotify-Dienst die aktuelle IP-Adresse des Empfängers mitgeloggt.

Bei der **mobilen Internetnutzung** wird auch der **Port der IP-Adresse** (hier: :5226) mitgeloggt, so dass insofern auch die Möglichkeit besteht, die IP-Adresse bei dem entsprechenden Provider anzufragen.

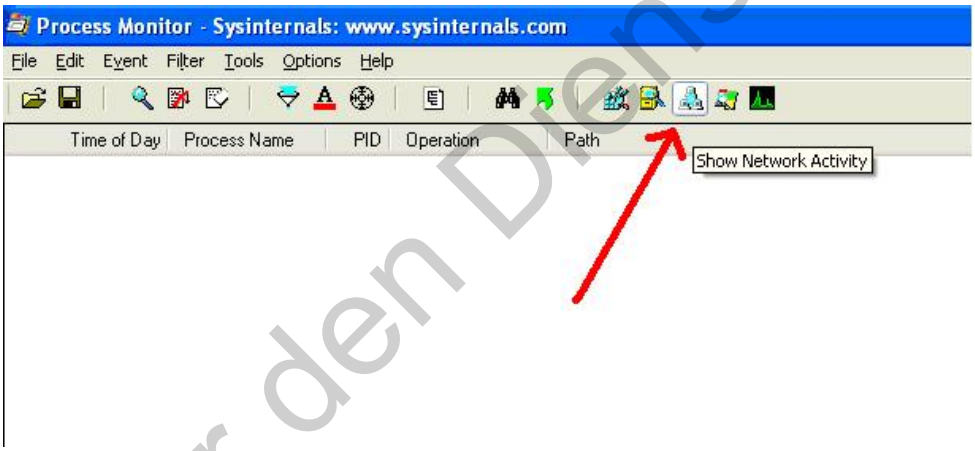


3. IP-Tracking bei Messenger-Diensten

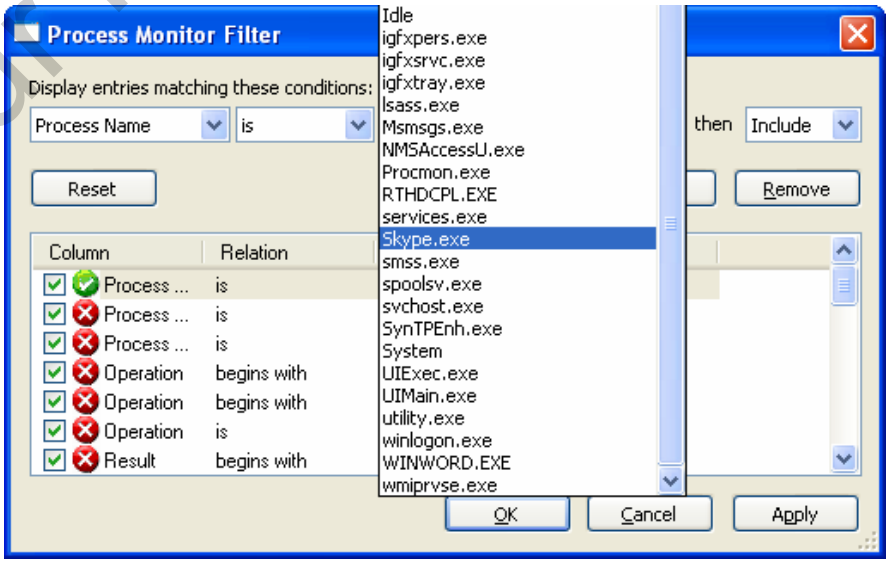
Die bei dem Einsatz von E-Mail-Lesebestätigungsdiensten verwendete Technik („IP-Tracking“) kann prinzipiell auch bei anderen Kommunikationsarten über Internet eingesetzt werden, so z.B. beim peer-to-peer- Dateienaustausch via Chat (z.B. ICQ) sowie bei der Internettelefonie mittels „Skype“ oder ähnlichen Diensten. Rechtlich stellt sich die Situation dabei genauso dar, vorausgesetzt, dass die Erhebung der IP-Adresse des Kommunikationspartners im Zusammenhang mit einem TK-Vorgang erfolgt, an dem die Ermittlungsbehörden teilnehmen.

Beim Normalfall des **Messenger-Tracking**, in dem die Ermittlungsbehörde selbst den Beschuldigten offen via Messenger anruft, wird die IP-Adresse des Kommunikationspartners (also des Beschuldigten) in einem Datenpaket, welches als Antwort nach einem Anruf versendet wird, an die Behörde übermittelt. Das bedeutet, dass insoweit ein Beschluss nach § 100g StPO **nicht** erforderlich ist, weil kein Eingriff in das TK-Geheimnis gegeben ist (s.o.).

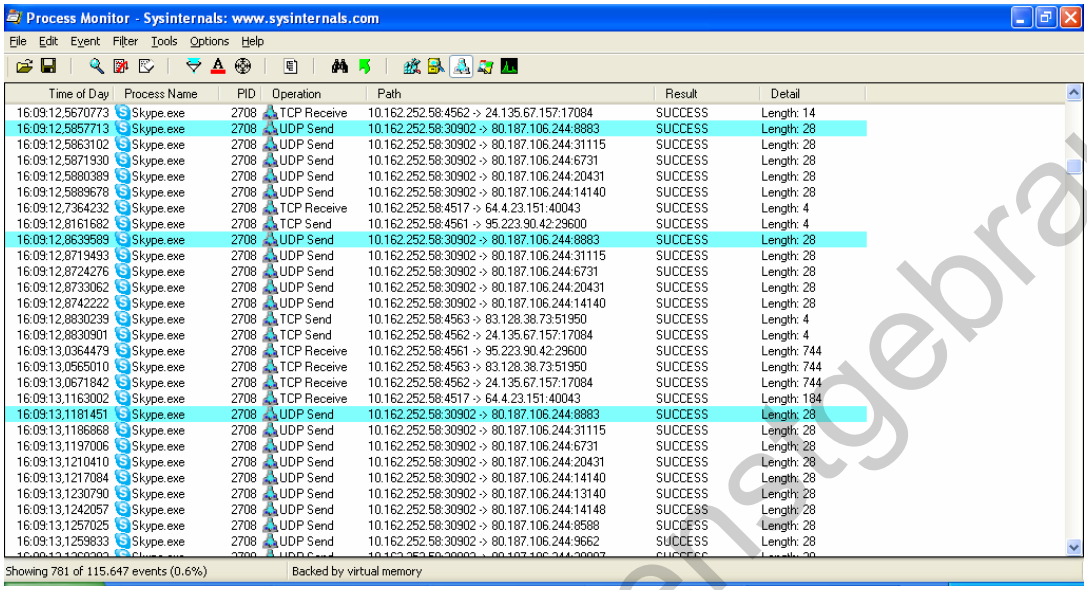
Zur entsprechenden beweissicheren Protokollierung kann etwa das kostenlose Programm **Process-Monitor von Microsoft** genutzt werden. Dieses ist Bestandteil der Freeware Microsoft Sysinternals-Suite. Mit diesem Tool können die laufenden Netzwerkzugriffe angezeigt werden.



Dabei bietet es sich an, nach den jeweiligen Prozessen (hier: Skype.exe) zu filtern, um nur relevante Netzwerkzugriffe anzeigen zu lassen.



Nach einem (auch erfolglosen) offenen Anruf bei dem Kommunikationspartner, wird die IP-Adresse des Kommunikationspartners im Process-Monitor angezeigt und kann abgespeichert sowie ausgewertet werden. Die Anzeige der IP-Adresse des Kommunikationspartners beruht darauf, dass eine peer-to-peer- Kommunikation nur möglich ist, wenn die jeweiligen IP-Adressen der Kommunikationspartner bekannt sind.



Es ist allerdings derzeit überwiegend so, dass **Skype-Tracking** in der Praxis unter Nutzung des sog. „**Skype Public API**“ ausgeführt wird. Das Skype Public API macht offene und verdeckte Anrufe bei der Zielperson entbehrlich. Sobald ein Skype-Nutzer online ist, sind seine relevanten Daten einschließlich seiner aktuellen IP-Adresse im dezentralen Skype-Netzwerk bekannt und können unter Nutzung spezieller Software technisch erhoben und gelesen werden. Dabei wird auf frei zugängliche Informationen von Skype zugegriffen und insbesondere keine Kommunikationsverbindung zum Ziel-Account aufgebaut. Auch hier ist kein 100g-Beschluss erforderlich.

Lediglich bei einem Zugriff auf einen TK-Vorgang des Beschuldigten mit Dritten oder unterdrückter Anrufe vergleichbar der „stillen SMS“, kann ein Beschluss gemäß § 100g StPO nötig sein. In diesen Fällen liegt kein TK-Vorgang vor, an dem die Ermittlungsbehörden teilnehmen (s.o.). Ein solcher 100g-Beschluss muss dabei nicht zwingend zur Umsetzung an den Provider gesandt werden, vielmehr können die Ermittlungsbehörden den Beschluss auch mit eigenen technischen Mitteln (auch Software) umsetzen, §§ 100g Abs. 2 S. 1 i.V.m. § 100b Abs. 3 StPO[15]. Das Muster Anlage 8 ist für diese Ausnahmefälle gedacht.

<u>Zusammenfassung</u>:
Der Einsatz von IP-Tracking im Zusammenhang mit der Versendung von Nachrichten durch die Ermittlungsbehörden an den Beschuldigten ist <u>immer</u> zulässig auf der Grundlage des § 100h StPO. Es bedarf niemals eines Beschlusses nach § 100g StPO, da Artikel 10 GG nicht berührt ist.
In den Konstellationen, in denen die Datei, die den Tracking-Vorgang auslöst, für den Beschuldigten offen erkennbar ist oder bei Nutzung der Skype Public API kann auch ein Vorgehen auf der Grundlage der §§ 161 oder 163 StPO zulässig sein.

➡***Muster für Anordnung nach § 100h StPO: Anlage 7***
➡***Muster für Skype-Tracking gem. § 100g StPO: Anlage 8***

[15] Meyer-Goßner, a.a.O., § 100a Rn 8

Teil 3 – Beschlagnahme, Durchsuchung und Festnahme

I. Vorbereitung und Durchführung der Durchsuchungsmaßnahme

Vielfach erbringt die der Durchsuchungsmaßnahme in aller Regel vorgeschaltete DSL-Überwachung, dass der Täter die Dateien auf seinem Rechner (bspw. mittels „TrueCrypt“ oder „Steganos“) verschlüsselt oder es ist eine solche Verschlüsselung zu erwarten, da dies aus vorherigen Ermittlungsverfahren gegen den Beschuldigten bekannt ist oder weil er verschlüsselt im Internet kommuniziert bzw. Proxy-Server oder TOR nutzt. Um die im Rahmen der Durchsuchung sicherzustellenden Beweismittel überhaupt auswerten zu können, ist es daher erforderlich, den Beschuldigten unmittelbar vor laufendem Rechner zu einem Zeitpunkt aufzugreifen, an dem die ansonsten verschlüsselten Datencontainer geöffnet sind und damit entschlüsselt vorliegen. Sollte der Rechner zum Zeitpunkt des Zugriffs dagegen außer Betrieb sein, besteht die Gefahr, dass die Rechner und Datenträger trotz moderner IT-Forensik aufgrund von nicht zu überwindender Verschlüsselungstechnik nicht ausgewertet werden können.

Es ist daher erforderlich, dass die DSL-Überwachungsmaßnahme zur Feststellung des „Online-Status“ des Beschuldigten bis zur Durchsuchung fortgeführt wird oder eine solche Maßnahme zu diesem Zweck eingeleitet wird. Finden die Internet-Sitzungen des Beschuldigten zumeist nachts statt, so ist auch die Durchsuchung zur Nachtzeit zu beantragten.
Ferner ist darauf zu achten dass die vorl. Festnahme des Beschuldigten so rasch (wenn möglich durch Spezialkräfte) erfolgt, dass dieser seine verschlüsselten Container nicht wieder schließen kann.

In einigen Fällen hat es sich zudem als sinnvoll erwiesen, in Vorbereitung der Durchsuchung auch die Mobiltelefone des Beschuldigten (inkl. der Standortdaten) zu überwachen und ihn (gem. § 163f StPO) zu observieren.

➡***Muster: Durchsuchungsbeschluss beim Beschuldigten gem. § 102 StPO: Anlage 9***

II. Die „vorläufige Sicherstellung“ der Beweismittel

Staatsanwaltschaftliche Musterformulare sehen häufig kombinierte Durchsuchungs- und Beschlagnahmeanträge vor. Im Rahmen von Internetermittlungen ist in den meisten Fällen vom Gebrauch dieser Formulare dringend abzuraten.

Die potentiell beweisrelevanten Datenträger werden im Rahmen von Durchsuchungen gem. §§ 102, 103 StPO vielmehr zunächst „vorläufig sichergestellt“. Die sich anschließende Auswertung gehört prozessual zur Durchsuchung (§ 110 StPO: Sichtung der Papiere), d.h. entsprechend § 98 Abs. 2 S. 2 StPO ist bei einem „Widerspruch“ die *richterliche Bestätigung* der vorläufigen Sicherstellung zu beantragen[16]. Dagegen ist die *Beschwerde* statthaft, § 105 StPO, § 304 StPO. Einwände gegen die *Art und Weise der Durchsicht* und die Behauptung des Verstoßes gegen § 110 Abs 2 S 1 StPO sind ebenfalls entsprechend § 98 Abs 2 S 2 StPO überprüfbar. Die *Dauer der Durchsicht* muss zwar zügig[17], aber nicht in dem vom BVerfG für die zeitliche Geltung von Durchsuchungsbeschlüssen festgelegten Rahmen (ca. 6 Monate) erfolgen, da es in der Phase der Durchsicht nach § 110 StPO zu keinem Eingriff in den Schutzbereich des Art 13 GG kommt.

[16] BVerfG, Beschl v 18.3.2009 – Az 2 BvR 1036/08 Rn 51 = NJW 2009, 2518; BVerfG NStZ-RR 2002, 144; BGH NStZ 2003, 670
[17] BGH NStZ 2003, 670, BVerfG NStZ 2002, 377

Dies ist deshalb so wichtig, da es (nur) in der Phase der Sichtung die Möglichkeit des Zugriffs auf externe Daten gem. § 110 Abs. 3 StPO gibt. Findet man während der Auswertung Hinweise auf externen Speicherplatz, E-Mail-Konten etc. ist es zulässig, diese Inhalte sofort zu sichern.

Finden sich auf dem ausgewerteten PC oder den über ihn abrufbaren externen Speicherorten beweisrelevante Dateien, so ist der PC (bei Widerspruch) nach Abschluss der Sichtung zu beschlagnahmen; einer (gesonderten) Beschlagnahme der extern gesicherten Datenbestände bedarf es nicht mehr.

Dabei ist jedoch auf § 110 Abs. 3 Satz 2, 2. HS StPO zu achten, wonach der Inhaber des externen Speichermediums entsprechend § 98 Abs. 2 Satz 2 StPO jederzeit Antrag auf gerichtliche Entscheidung stellen kann, wonach er entsprechend § 98 Abs. 2 Satz 6 StPO zu belehren ist, sofern Daten gesichert wurden.[18]

➡***Muster: Ersuchen Vollstreckung Durchsuchungsbeschluss: Anlage 10***

➡***Muster: Nachweis über vorläufig sichergestellte Speichermedien: Anlage 11***

➡***Muster: Antrag richterliche Bestätigung analog § 98 Abs. 2 Satz 2 StPO: Anlage 12***

[18] Meyer-Goßner § 110 Rn. 11.

III. Das Herausgabeverlangen nach § 95 StPO

In Ermittlungsverfahren fallen beweisrelevante Verkehrs- und Inhaltsdaten nicht nur bei Telekommunikationsprovidern, sondern auch bei sog. Content-Providern und sog. Host-Service-Providern an. Content-Provider ist derjenige, der eigene Inhalte auf einer Internetseite anbietet (§ 7 TMG). Host-Service-Provider ist derjenige, der fremde Informationen und Inhalte auf seinem eigenen Webserver und den eigenen Seiten einstellt (§ 10 TMG). Grundsätzlich unterfällt das schlichte Hosting und das Betreiben eines eigenen Internetangebots nicht dem TKG, weil der technische Vorgang des Übertragens der Daten nicht durch die Hostprovider, sondern durch die Accessprovider (z.B. T-Online, 1&1 etc.) vorgenommen wird.

Häufig benutzen z.B. Täter für Ihre tatbezogene Kommunikation Server, die sie bei Host-Service-Providern anmieten. Auch werden dort z.B. ausgespähte Kreditkartendaten abgelegt. Die auf diesen Servern anfallenden Log-Dateien sind demzufolge regelmäßig von Beweisbedeutung. Ferner kann es etwa in Verfahren wegen des Verbreitens von Kinderpornographie von Bedeutung sein, welche Personen auf ein bestimmtes Internetangebot zugegriffen haben.

In diesen und allen anderen Fällen, in denen beweiserhebliche Daten sich nicht im Gewahrsam von Beschuldigten, sondern in solchem von herausgabebereiten und –verpflichteten Dritten, also Zeugen, die nicht Telekommunikationsdiensteanbieter sind, befinden, kann anstelle der Beschlagnahme das mildere Mittel der Herausgabeanordnung gemäß § 95 StPO gewählt werden. Dies gilt auch für Verkehrsdaten, ein Beschluss nach § 100g StPO ist nicht erforderlich. Gemäß § 100g Abs. 3 StPO gilt diese Norm nämlich nicht, wenn Verkehrsdaten nicht bei TK-Diensteanbietern erhoben werden und der zugrundeliegende TK-Vorgang bereits abgeschlossen ist. Vielmehr greifen dann die allgemeinen Vorschriften.

Zuständig für die Anordnung nach § 95 StPO sind Polizei, Staatsanwaltschaft und Gericht. Danach ist derjenige, der einen als Beweismittel in Betracht kommenden Gegenstand in seinem Gewahrsam hat, verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern. Diese Verpflichtung ist nicht von einem Gerichtsbeschluss abhängig und kann mit den Zwangsmitteln des § 70 StPO durchgesetzt werden, § 95 Abs. 2 StPO. Vor dem Hintergrund, dass die Polizei keine Zwangsmittel androhen kann, ist es angezeigt, dass der Staatsanwalt das Herausgabeverlangen stellt.

In bestimmen Fallkonstellationen ist die Anwendung des § 95 StPO zielführender als ein Beschlagnahmebeschluss nach § 98 StPO. Dies gilt vor allem dann, wenn es sich um eine geringe relevante Datenmenge in einem viel größeren Gesamtbestand überwiegend unbedeutender Daten handelt, dessen komplette Beschlagnahme, Sicherung und Auswertung sehr viel Zeit in Anspruch nehmen würde.

Der historische Gesetzgeber, der die überkommenen Normen über die Beschlagnahme geschaffen hat, konnte noch nicht mit der Möglichkeit rechnen, dass elektronische Daten als nichtkörperliche Informationen für die Beweisführung im Strafverfahren Bedeutung erlangen könnten. §§ 94 ff. StPO erlauben daher auch die Sicherstellung von Daten auf behördeneigenen Datenträgern. Der Wortsinn gestattet es, als "Gegenstand" des Zugriffs auch nichtkörperliche Gegenstände zu verstehen. Der Wortlaut wird durch die Annahme, auch unkörperliche Gegenstände seien von §§ 94 ff. StPO erfasst, schon im Hinblick auf die Unterscheidung gegenüber dem engeren Begriff der (körperlichen) Sache nicht überschritten (vgl. BVerfG NJW 2005, 1917-1923).

Die Auslegung von § 95 Abs. 1 StPO i.V.m. § 94 Abs. 1 StPO, wonach sich das Herausgabeverlangen auch auf einen Beweisgegenstand beziehen kann, der nicht bereits vorhanden ist, sondern erst aufgrund des Herausgabeverlangens geschaffen werden muss (z.B. durch

Zusammenstellung von Einzeldaten nach konkreten Kriterien aus einem Gesamtdatenbestand), überschreitet nicht die Wortlautgrenze der Norm. Sie ist auch nicht willkürlich, da sie gegenüber der Beschlagnahme des Gesamtdatenbestandes das mildere Mittel darstellt (vgl. BVerfG NStZ-RR 2003, 176-177). Betroffene sind demgemäß verpflichtet, die Ihnen in elektronischer Form vorliegenden Daten auch in elektronischer Form heraus zu geben bzw. zu übermitteln.

Über die Art und Weise der Herausgabe von Daten enthält § 95 StPO keine Regelung. Eine nähere gesetzliche Eingrenzung ist wegen der Vielgestaltigkeit möglicher Sachverhalte auch nicht geboten. Dies führt jedoch nicht dazu, dass der Betroffene die Herausgabe von Daten verweigern kann, die entweder auf einem räumlich entfernten Speichermedium liegen oder entschlüsselt werden müssen (a.A. Sieber, Straftaten und Strafverfolgung im Internet, 2012, C 115).

Sofern der Betroffene tatsächlich Zugriff auf die räumlich entfernt gespeicherten Daten hat, hat er die Daten in seinem (Mit-)Gewahrsam gemäß § 95 Abs. 1 StPO, so dass es auf den Ort der physikalischen Speicherung nicht ankommt. Dass eine Herausgabeanordnung nicht mit dem Hinweis auf eine räumlich entfernte Speicherung abgelehnt werden kann, ergibt sich auch aus der gesetzlichen Wertung des § 110 Abs. 3 StPO. Eine Speicherung der Daten vor Ort ist in Zeiten des „Cloud Computing“ ohnehin eher die Ausnahme.

Verschlüsselte Daten sind von dem herausgabepflichtigen Betroffenen zu entschlüsseln. Nur die entschlüsselten und damit lesbaren bzw. verwertbaren Daten sind Beweismittel im Sinne der §§ 94, 95 StPO. Nur auf diese entschlüsselten Daten bezieht sich die Herausgabepflicht. Sofern der Betroffene einer Herausgabeanordnung ein Kaufmann im Sinne von § 1 HGB ist, ist er zudem nach § 261 HGB verpflichtet, auf seine Kosten diejenigen Hilfsmittel zur Verfügung zu stellen, die erforderlich sind, um die Unterlagen lesbar zu machen und ggf. die Unterlagen auf seine Kosten auszudrucken oder ohne Hilfsmittel lesbare Reproduktionen beizubringen (Meyer-Goßner, StPO, § 95 Rn. 8). Eine solche Pflicht zur Herausgabe stellt zudem einen geringeren Eingriff dar, als die Herausgabe von verschlüsselten Daten und die Erlangung des Zugangscodes durch die Inanspruchnahme der Wahrheitspflicht bei der Vernehmung von Zeugen.

Diese Ergebnisse entsprechen auch einer europarechtskonformen Auslegung von § 95 StPO im Hinblick auf Artikel 18 Abs. 1a Cybercrime-Konvention. Danach müssen die zuständigen Behörden ermächtigt werden anzuordnen, dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat. Eine solche Auslegung scheitert – wie die genannte Rechtsprechung des BVerfG zeigt – auch nicht an der Wortlautgrenze.

➡***Muster: staatsanwaltschaftliches Herausgabeverlangen nach § 95 StPO: Anlage 13***

Teil 4 – Verdeckte personale Ermittlungen im Internet

I. Problemdarstellung

Verdeckte technische Ermittlungen im Internet allein sind nur begrenzt erfolgversprechend:

Hochprofessionell arbeitende Täter verschleiern ihre IP-Adresse mittels Anonymisierungstechniken. Der Einsatz von Botnetzen liefert IP-Adressen von unbeteiligten Personen, deren Rechner ohne ihr Wissen mit Schadprogrammen infiziert und zur Begehung von Straftaten verwendet wurde. Das „Darknet“, die „Hidden Services“ im TOR-Netzwerk sind nur über den Anonymisierungsdienst TOR (Abk. für „The Onion Router“) erreichbar, der physikalische Standort der Daten nicht ermittelbar.

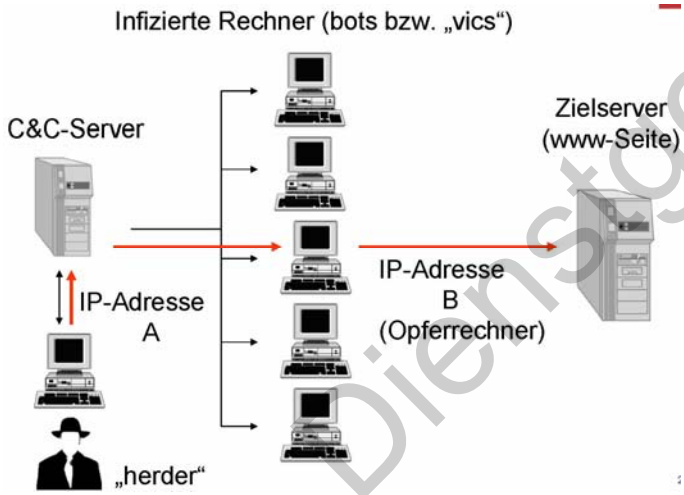
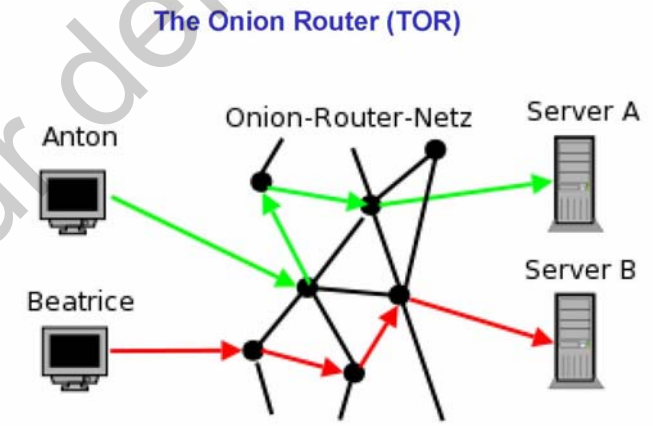


Schaubild: Botnetz



Es müssen also verdeckte personale Ermittlungen hinzutreten.

Bei der Frage der rechtlichen Möglichkeiten und Grenzen sind die Besonderheiten des Mediums Internet zu beachten.

Soweit es sich um herkömmliche Kriminalität mit Kommunikation und Zusammentreffen der Täter mit den Ermittlern im wahren Leben und außerhalb des Internets handelt und das Internet dabei nur ein weiteres Kommunikationsmittel darstellt, gelten die allgemeinen Grundsätze.

Für verdeckte personale Ermittlungen unter Nutzung des Internets – ohne ein reales Zusammentreffen des Beamten mit dem Beschuldigten – ist hingegen zu prüfen, inwieweit die bisherige Rechtsprechung zum herkömmlichen NoeP (Nicht offen ermittelnden Polizeibeamter)- und VE (Verdeckter Ermittler)-Einsatz überhaupt zu den tatsächlichen Rahmenbedingungen passt. Hinsichtlich verdeckter personaler Ermittlungen im Internet fehlt ober- und höchstrichterliche Rechtsprechung nahezu vollständig. Die Rechtsprechung zu verdeckten technischen Internetermittlungen ist deshalb auszuwerten und nutzbar zu machen.

Grundsätzlich sind verdeckte Ermittlungen – egal ob technischer oder personaler Art – als kriminalistische List erlaubt:

*„**Die Heimlichkeit von Maßnahmen der Strafverfolgung verstößt als solche auch nicht gegen das im Gebot des fairen Verfahrens wurzelnde Täuschungsverbot.** Das heimliche Abhören nutzt zwar eine Fehlvorstellung des Betroffenen in Bezug auf die Abgeschirmtheit der Wohnung aus. Die Äußerung des Beschuldigten beruht vielmehr auf seiner freiwilligen Entscheidung. Nicht freiwillig ist allerdings die Kenntnisgabe dieser Äußerung an die Staatsgewalt. Ermittlungen in Heimlichkeit sind aber eine unabdingbare Voraussetzung des Erfolgs einer Reihe von Maßnahmen der Strafverfolgung, die nicht allein deshalb rechtsstaatswidrig sind.“*
BVerfG, Urteil vom 03.03.2004 - 1 BvR 2378/98 Rn 161

und

„*Die Heimlichkeit eines polizeilichen Vorgehens ist kein Umstand, der nach der Strafprozessordnung für sich allein schon die Unzulässigkeit der ergriffenen Maßnahmen begründet. Es gilt der Grundsatz der freien Gestaltung des Ermittlungsverfahrens, der auch das verdeckte Führen von Ermittlungen erlaubt. **Ermittlungen in Heimlichkeit sind eine unabdingbare Voraussetzung des Erfolgs einer Reihe von Maßnahmen der Strafverfolgung, die nicht allein deshalb rechtsstaatswidrig sind.**“*
BVerfG, Beschluss vom 17.02.2009 - 2 BvR 1372/07 Rn 28

Dabei gilt, dass auch für verdeckte personale Ermittlungen grundsätzlich die **Ermittlungsgeneralklauseln der §§ 161, 163 StPO** in Betracht kommen:

*„§ 161 Abs. 1 StPO stellt als Ermittlungsgeneralklausel die **Ermächtigungsgrundlage für Ermittlungen jeder Art dar, die nicht mit einem erheblichen Grundrechtseingriff verbunden sind und daher keiner speziellen Eingriffsermächtigung bedürfen**. Sie ermächtigt die Staatsanwaltschaft zu den erforderlichen Ermittlungsmaßnahmen, die weniger intensiv in Grundrechte des Bürgers eingreifen (...). **Die Staatsanwaltschaft kann auf dieser Grundlage in freier Gestaltung des Ermittlungsverfahrens die erforderlichen Maßnahmen zur Aufklärung von Straftaten ergreifen.**“*
BVerfG, Beschluss vom 17.02.2009 - 2 BvR 1372/07, Rn 26

Vor diesem Hintergrund ist für die Zulässigkeit von verdeckten personalen Ermittlungen im Internet zunächst zu betrachten, in welche Grundrechte wie intensiv eingegriffen wird. Dabei gilt:

*„Indem der Beschuldigte die Telekommunikationsanlage zum Tatmittel seiner strafbaren Handlungen einsetzt, **mindert sich sein Anspruch auf Wahrung des Schutzes** des von ihm missbrauchten Mediums.“*
BVerfG, Urteil vom 17.06.2006 - 2 BvR 1085/05, Rn 17

Als Grundrechte, in die durch verdeckte personale Internetermittlungen eingegriffen wird, kommen Art. 10 GG (Fernmeldegeheimnis) und Art. 2 GG (in der Form des Rechts auf informationelle Selbstbestimmung) in Betracht.

Der Schutzbereich von Art. 10 GG ist bei Ermittlungen unter Geheimhaltung der Identität als Polizeibeamter jedoch regelmäßig nicht betroffen:

*„Es [das Fernmeldegeheimnis] schützt das Vertrauen des Einzelnen darin, dass eine Fernkommunikation, an der er beteiligt ist, nicht von Dritten zur Kenntnis genommen wird, also den technischen Vorgang als solchen**, nicht aber die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner.**“*
BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 290

Damit sind Eingriffe nur an Art. 2 GG zu messen. Auch hier ist jedoch der Schutzbereich bei internetbasierter Kommunikation durch die Rechtsprechung des BVerfG stark eingeschränkt:

*„Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt nicht schon dann vor, **wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung** zu einem Grundrechtsträger begibt, wohl aber, wenn sie dabei **ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt**, um persönliche Daten zu erheben, die sie ansonsten nicht erhalten würde.“*
BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 310

und

*„Die Kommunikationsdienste des Internet ermöglichen in weitem Umfang den Aufbau von Kommunikationsbeziehungen, **in deren Rahmen das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner nicht schutzwürdig ist, da hierfür keinerlei Überprüfungsmechanismen bereitstehen**. Dies gilt selbst dann, wenn bestimmte Personen - etwa im Rahmen eines Diskussionsforums - über einen längeren Zeitraum an der Kommunikation teilnehmen und sich auf diese Weise eine Art "elektronische Gemeinschaft" gebildet hat. **Auch im Rahmen einer solchen Kommunikationsbeziehung ist jedem Teilnehmer bewusst, dass er die Identität seiner Partner nicht kennt oder deren Angaben über sich jedenfalls nicht überprüfen kann. Sein Vertrauen darauf, dass er nicht mit einer staatlichen Stelle kommuniziert, ist in der Folge nicht schutzwürdig.**“*
BVerfG, Urteil vom 27.02.2008 - 1 BvR 370/07, 595/07, Rn 311

Bei Kommunikation über Internet besteht in der Regel kein personengebundenes Vertrauen, weil man den Kommunikationspartner zumeist nur als „Nickname“ kennt. Die Benutzung falscher Identitäten im Netz ist die Regel. Das weiß jeder Internetnutzer.

Gerade in kriminellen Internetforen und Boards ist die Nennung von Echtpersonalien verpönt bzw. untersagt. Oft werden in diesen Kreisen bewusst unwahre, vermeintlich aber reale Details zu den Lebensumständen mitgeteilt, um Ermittler zu täuschen.

Weil es unerwünscht ist, dass Täter private und echte Informationen über sich preisgeben, ist eine Legendierung im herkömmlichen Sinne i.d.R. entbehrlich. Das Zusammentreffen von Ermittlern und Beschuldigten außerhalb des Netzes sind die absolute Ausnahme. Inkriminierte Waren werden über Packstationen oder Hausdrops ausgeliefert. Eine begehrte Tatbeute sind Daten, die über Zwischenschritte und schließlich über anonyme Zahlungsmittel „ausgecasht“ werden und zu deren Weitergabe bzw. Verwertung keine Realkontakte erforderlich sind.

Der wichtigste Unterschied zu verdeckten personalen Ermittlungen außerhalb des Internets ist aber, dass ein über Internet verdeckt kommunizierender Beamter **keine fremden Wohnungen betreten muss**. Das sog. „virtuelle Betreten“ von Chaträumen, Foren, Boards etc. ist nicht von Art. 13 GG geschützt.

Schließlich ist weiterhin zu berücksichtigen, dass bei Ermittlungen gegen einen unbekannten Beschuldigten häufig nur ein Nickname, eine Emailadresse o.ä. bekannt ist. Diese sind oft, aber nicht immer mit lediglich einer Person verknüpft.

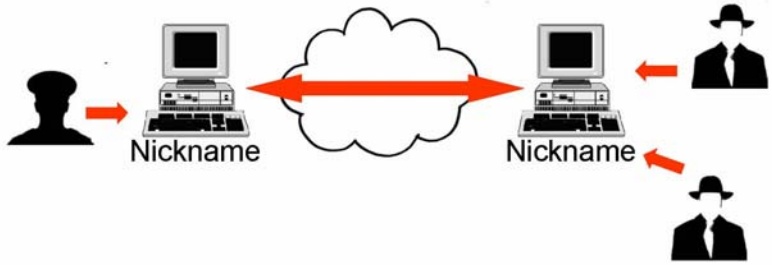


Schaubild: Mehrere Täter nutzen einen Account

Ferner ist bei der Abwägung der Zulässigkeit des Eingriffs in Art. 2 GG aufgrund der Ermittlungsgeneralklauseln zu berücksichtigen, dass es Bereiche gibt, in denen die Anwendung technischer Ermittlungsmethoden nahezu ohne Aussicht auf Erfolg ist, etwa, wenn die Täter Anonymisierungstechniken anwenden. In diesen Fällen, in denen wegen fehlender Vorratsdaten oder von den Tätern benutzter Anonymisierungsdiensten ohne die Anwendung verdeckter personaler Ermittlungen Strafverfolgungsfreie Räume entstünden, muss beachtet werden, dass das Interesse an einer leistungsfähigen Strafjustiz in den Gewährleistungsbereich des Rechtsstaatsprinzips (Art. 20 Abs. 3 GG) gehört. Soweit der Grundsatz der Rechtsstaatlichkeit die Idee der Gerechtigkeit als wesentlichen Bestandteil enthält, verlangt er auch die Aufrechterhaltung einer funktionstüchtigen Rechtspflege, ohne die Gerechtigkeit nicht verwirklicht werden kann (vgl. BVerfG, Beschluss vom 24.05.1977 - 2 BvR 988/75, Rn 65).

Danach gilt als

➡ **<u>Zwischenergebnis 1</u>**,
dass bei verdeckten personalen Internetermittlungen regelmäßig kein oder nur ein sehr geringer Grundrechtseingriff vorliegt, der durch §§ 161, 163 StPO gedeckt ist:

Die allgemeine Informationsbeschaffung, Nutzung von Fake Accounts und Kommunikation in Sozialen Netzwerken, Foren und Boards sind von der Ermittlungsgeneralklausel abgedeckt, auch wenn sie längerfristig aufrecht erhalten werden.

Die Kommunikation mit einem Beschuldigten, um Scheingeschäfte über Internet abzuwickeln oder ihn anhand von auch längerfristigen Internet-Kontakten zu identifizieren, ist ebenfalls von der Ermittlungsgeneralklausel gedeckt.

Für den Polizeibeamten, der außerhalb des Internets unter Verheimlichung seiner Identität ermittelt, hat die Rechtsprechung bereits vor Inkrafttreten der §§ 110a ff. StPO die Figur des „Nicht offen ermittelnden Polizeibeamten“ (NoeP) entwickelt.

Ein NoeP ist ein Beamter, der nur gelegentlich verdeckt auftritt, seine Funktion nicht offen legt und nicht unter einer dauerhaft angelegten Legende ermittelt (vgl. dazu BGHSt 41, 64; BGH StV 1995, 398; NStZ 1996, 450; NJW 1997, 1516; NStZ 1997, 294; s. auch Anl. D II 2.9 RiStBV).
Sein Einsatz richtet sich grundsätzlich nach §§ 161, 163 StPO (vgl. BGH NJW 1997, 1516).
Auf Seiten der Polizei ist der Einsatz eines NoeP mit bestimmten formalisierten Zustimmungserfordernissen und Abläufen verbunden.

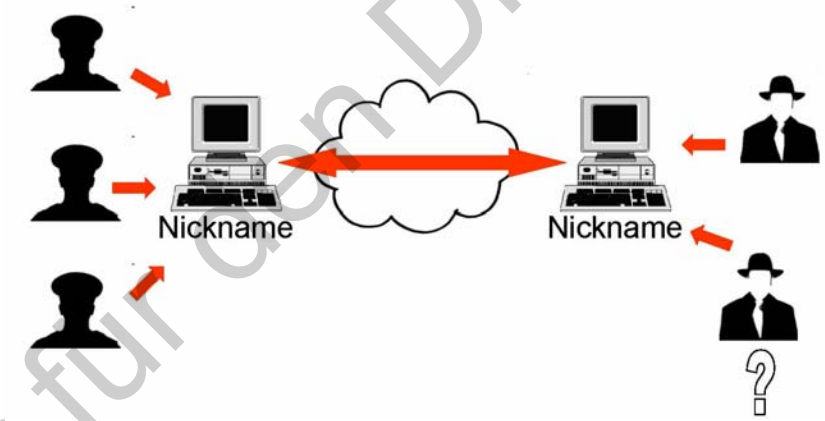
Nach der Erlasslage in Hessen – und wohl auch nach derjenigen in den meisten anderen Bundesländern – dient ein NoeP grundsätzlich der Erlangung inkriminierter Gegenstände durch Scheinkäufe (Gemeinsamer Rd.Erl. v. HMdJIE u. HMdIuS v. 30.12.2009).
Hier findet die Figur des NoeP außerhalb des Internets auch den häufigsten Anwendungsbereich: als Scheinaufkäufer von BtM.

Der Einsatz eines NoeP, der unter Verheimlichung oder Verschleierung seiner Identität im Internet mit Tatverdächtigen kommuniziert, ist zulässig (vgl. Karlsruher Kommentar zur StPO, 6. Auflage 2008, § 110a Rn. 7).

Betrachtet man die oben zitierte **Rechtsprechung**, muss man jedoch festhalten, dass **nicht jede Benutzung von Fake Accounts ein NoeP-Einsatz im Sinne des „Gemeinsamen Runderlasses" darstellt, denn Voraussetzung für die Erreichung der Schwelle eines NoeP-Einsatzes ist die Täuschung des Beamten über seine Identität. Wenn aber jeder an der Kommunikation Beteiligten weiß, dass keinerlei echte Identitäten verwendet werden, entfällt dieses Kriterium.**

Bei den NoeP-Einsätzen außerhalb des Internets im wahren Leben ist ggf. zudem die **Sicherheit des Beamten** ein entscheidendes Kriterium, ebenso die Notwendigkeit der **Geheimhaltung seiner Identität im Strafverfahren**. Dies sind die Hauptgründe für die Regelung des formalisierten NoeP-Einsatzes im Erlasswege.

Anders bei internetbasierten verdeckten Ermittlungen. Hier muss nicht die Person des Ermittlers geheim gehalten werden, da **ein Fake Account von mehreren Beamten bedient werden kann**.



Auch wenn ein Polizeibeamter vor Gericht als Zeuge auftritt und dessen Gesicht in der Szene bekannt ist, kann er weiterhin mittels anderer Fake Accounts im Internet ermitteln, ohne identifiziert zu werden. Zudem **entfällt das Problem der Dokumentation der Beweisergebnisse in der Hauptverhandlung**, welches sich bei Ermittlungen außerhalb des Internets immer dann stellt, wenn die Identität des NoeP geheim gehalten werden soll und nur der Führungsbeamte als Zeuge vom Hörensagen vernommen werden soll. Bei Internet-Ermittlungen durch Polizeibeamte **wird die gesamte Kommunikation unter dem Fake Account immer beweissicher durch Screenshots oder das Abspeichern der Inhalte dokumentiert**. Häufig wird man die Beamten, die den Fake Account bedient haben, nicht als Zeugen benötigen, da Chatprotokolle, E-Mailverkehr u. ä. als Urkunden oder Augenscheinsobjekte zur Verfügung stehen. Dies stellt einen ganz wesentlichen Unterschied zu verdeckten Ermittlungen außerhalb des Internets dar und verdeutlicht, warum sich eine undifferenzierte Übernahme der BGH-Rechtsprechung zum Scheinaufkäufer-NoeP verbietet.

➡**Zwischenergebnis 2:**
Nicht jeder Polizeibeamte, der unter einem Fake Account im Internet ermittelt und kommuniziert, ist ein NoeP im Sinne des herkömmlichen rechtlichen Sprachgebrauchs und vor allem im Sinne der einschlägigen Erlasse. Diese dienen vor allem dem Schutz von Beamten, die als Scheinaufkäufer in der BtM-Szene Realkontakte haben. Dieses Schutzbedürfnis besteht bei einem einfachen Internetchat nicht.

II. Wann ist der Einsatz eines VE erforderlich?

Wie bei Ermittlungen in der realen Welt stellt sich auch bei Internetermittlungen die Frage, ab welcher Intensität der verdeckten polizeilichen Maßnahmen es eines Beschlusses nach §§ 110a ff. StPO, also des Einsatzes eines verdeckten Ermittlers im rechtstechnischen Sinne, bedarf.

In Abgrenzung zum NoeP sind verdeckte Ermittler gemäß § 110a Abs. 2 StPO Beamte des Polizeidienstes, die unter einer ihnen verliehenen**, auf Dauer angelegten, veränderten Identität (Legende)** ermitteln. Sie dürfen unter der Legende am Rechtsverkehr teilnehmen.

In der Praxis handelt es sich um Beamte,

- die aus dem allgemeinen Ermittlungsbereich ausgegliedert,
- dauerhaft ausschließlich verdeckt operierend tätig sind und
- über eine auf Dauer angelegte Legende verfügen und grundsätzlich als Zeuge in einer Hauptverhandlung nicht zur Verfügung stehen.

Mit dem Instrument des Verdeckten Ermittlers ist die **dauerhafte Legendierung** der Beamten **ohne Bezug zu einem einzelnen Ermittlungsverfahren** verbunden. Dabei dürfen sämtliche personenbezogenen Daten durch fiktive Daten ersetzt werden und, soweit es für den Aufbau oder die Aufrechterhaltung der Legende unerlässlich ist, **entsprechende Urkunden hergestellt, verändert und gebraucht werden** (§ 110a Abs. 3 StPO).

Der Einsatz verdeckter Ermittler ist gem. § 110a I 1 Nr. 3 StPO zulässig bei gewerbs- oder gewohnheitsmäßiger sowie gem. § 110a I 1 Nr. 4 StPO bei bandenmäßiger oder sonstiger organisierter Begehungsweise.
§ 110a I 1 Nr. 4 StPO liegt regelmäßig vor, sobald sich Internet-Teilnehmer in geschlossenen Benutzergruppen abschotten. Bei Verbrechen ist der Einsatz von VE auch zulässig, wenn eine besondere Bedeutung der Tat vorliegt und andere Mittel aussichtslos sind.

Gemäß § 110a I 3 StPO ist jeder Einsatz eines VE jedoch nur zulässig, soweit die Aufklärung auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Der Einsatz eines VE, der sich **nicht gegen einen bestimmten Beschuldigten richtet, wird gemäß § 110b Abs. 1 StPO durch den Staatsanwalt angeordnet.** Richtet sich der Einsatz gegen einen **bestimmten Beschuldigten, ist gemäß § 110b StPO ein richterlicher Beschluss** erforderlich. Hierfür ist es nicht erforderlich, dass der Beschuldigte namentlich bekannt sein muss. Es reicht aus, dass der Beschuldigte aufgrund seines Verhaltens oder Aussehens **"identifizierbar"** ist. Zu denken ist etwa an den unter einem Spitznamen bekannten Drogendealer, von dem man weiß, wo er wohnt und wie er telefonisch erreichbar ist, nicht jedoch, wie er tatsächlich heißt. Tatsächlich wäre eine solche Person auch ohne Kenntnis ihres Namens als Person individualisierbar. Ein Zugriff auf die Person wäre jederzeit möglich. Dies ist jedoch bei demjenigen, der unter einem Pseudonym oder einer E-Mailadresse im Internet operiert, nicht möglich. Man weiß über ihn in der Regel wenig mehr als das, was mit dem Internetverkehr zusammenhängt. Selbst wenn dabei gelegentlich Mit-

teilungen privaten Inhalts gemacht werden, hebt ihn noch nicht aus der Anonymität eines Internetnutzers heraus. **Daher ist ein richterlicher Beschluss für den VE-Einsatz bei verdeckten Internetermittlungen gegen nur nach Nickname oder E-Mail-Adresse bestimmte Beschuldigte i.d.R. nicht erforderlich.**

III. Abgrenzung zum NoeP-Einsatz

Für den Scheinaufkäufer im wahren Leben gilt als Faustformel der polizeilichen und justiziellen Praxis, dass die Grenze bei drei bis fünf Kontakten zwischen Polizeibeamten und Zielperson liegen dürfte.

Für die Ermittlungen außerhalb des Internets hat der BGH folgende Abgrenzungskriterien zum NoeP entwickelt:

*„Entscheidend ist, ob der Ermittlungsauftrag über einzelne wenige, konkret bestimmte Ermittlungshandlungen hinausgeht, ob es erforderlich werden wird**, eine unbestimmte Vielzahl von Personen über die wahre Identität des verdeckt operierenden Polizeibeamten zu täuschen, und ob wegen der Art und des Umfanges des Auftrages von vornherein abzusehen ist, daß die Identität des Beamten in künftigen Strafverfahren auf Dauer geheimgehalten werden muß**.*

*Dabei ist darauf abzustellen, ob **der allgemeine Rechtsverkehr oder die Beschuldigtenrechte in künftigen Strafverfahren eine mehr als nur unerhebliche Beeinträchtigung** durch den Einsatz des verdeckt operierenden Polizeibeamten erfahren können."*
BGH, Urteil vom 07.03.1995 - 1 StR 685/94, BGHSt 41, 64-69

und

*„Die Anforderungen des § 110b Abs. 2 Nr. 1 StPO finden ihren Grund also […] in einem **gravierenden Eingriff in die Belange des Beschuldigten**.*
Ein solcher liegt erst vor bei einer durch veränderte Identität bewirkten Gefährdung des allgemeinen Rechtsverkehrs und der erheblichen Beeinträchtigung der Rechte von Betroffenen durch schwerwiegende Täuschung, wie sie sich bei einem auf Dauer nach außen angelegten Auftreten gegenüber konkret Beschuldigten ergeben kann.
*Die erhöhten Anforderungen stellt das Gesetz an den Einsatz, der den Beschuldigten in seinem Umfeld oder **in seiner Privatsphäre erfaßt und begleitet**, ihm auf Dauer vorspiegelt, mit einer ganz anderen Person zu tun zu haben, die ihn so **in seiner Lebensführung ausforscht.**"*
BGH, Urteil vom 06.02.1996 - 1 StR 544/95, NStZ 1996, 450

Ein wesentliches Kriterium zur Abgrenzung, dass auch für Internetermittlungen gilt, ist mithin der Umfang der Legendierung:

Wird der Beamte mit einer Identität ausgestattet, die nicht nur im Verhältnis zu dem/den Beschuldigten oder etwa anderer Chat- bzw. Forenteilnehmer im Internet als Täuschung über seine Eigenschaft als Polizeibeamter, sondern eine Einbeziehung des allgemeinen Rechtsverkehrs – d.h. z. B. bei rechtserheblichem Handeln wie etwa Vertragsschlüssen - zur Folge hat, ist der Status eines Verdeckten Ermittlers im Sinne des § 110a StPO erreicht.

Ferner erfordert ein Einsatz, der den Beschuldigten in seinem Umfeld oder in seiner Privatsphäre erfasst und begleitet, ihm auf Dauer vorspiegelt, es mit einer ganz anderen Person zu tun zu haben, die ihn so in seiner Lebensführung ausforscht, einen VE im Sinne von § 110a StPO.

Schließlich ist wegen des **Richtervorbehalts in Art. 13 GG** jede verdeckte Ermittlung, bei der der **ermittelnde Beamte unter seiner Legende Wohnungen betreten muss, ein VE-Einsatz, weil es der richterlichen Zustimmung gemäß § 110b Abs. 2 StPO bedarf**.

Mit anderen Worten: Die Notwendigkeit des Einsatzes eines VE bei Ermittlungen im Internet ist **nur in seltenen Fällen** gegeben. Regelmäßig ist die Schwelle der §§ 110a ff. StPO nicht erreicht. Dies sieht auch der BGH so, der zusätzlich darauf hinweist, dass die Subsidiarität des VE-Einsatzes (keine anderen Mittel vorhanden) beachtet werden muss (Beschluss v. 24.06.2010, StB 15/10, n. veröff.). Dieser **wichtigen, weil einzigen höchstrichterlichen Entscheidung zum Thema verdeckte personale Ermittlungen im Internet**, lag folgender Sachverhalt zugrunde:

Die Ermittlungsbehörde beabsichtigte, mit dem nicht identifizierten Beschuldigten in der Weise in Kontakt zu treten, dass auf deren an eine E-Mail-Adresse eines anderen Beschuldigten, der mit der Polizei kooperierte, gerichtete Anfrage durch einen Polizeibeamten geantwortet und dabei der Eindruck erweckt werden sollte, es handele sich um eine E-Mail des Beschuldigten. Sollte der noch unbekannte Beschuldigte darauf reagieren, war eine Fortsetzung des Austausches von E-Mails beabsichtigt. Weitere Einsatzmöglichkeiten waren nicht gegeben. Ein persönlicher Kontakt mit dem unbekannten Beschuldigten war mangels näherer Kenntnisse zu deren Identität nicht möglich. Der Polizeibeamte sollte weder eine Wohnung betreten noch Dritten gegenüber mit einer Legende in Erscheinung treten müssen. Es war allein eine Kommunikation im Internet unter Verschleierung der Identität des Polizeibeamten geplant.

Der BGH hat hierzu entschieden:

„(…) Zur Durchführung der geplanten Ermittlungsmaßnahmen bedarf es des Einsatzes eines Verdeckten Ermittlers nicht, vielmehr reicht ein nicht offen ermittelnder Polizeibeamter aus (zur Abgrenzung vgl. BGHSt 41, 64, 65 f.; Nack in KK 6. Aufl. § 110a Rdn. 5 f.; Hegmann in Graf, StPO § 110a Rdn. 2 f.). Der Maßnahme steht daher § 110a Abs. 1 Satz 3 StPO entgegen. (…)“

➡**Zwischenergebnis 3:**
Die Notwendigkeit des Einsatzes eines formell gemäß § 110a StPO eingesetzten Verdeckten Ermittlers im Internet ist nur in seltenen Ausnahmefällen gegeben. Regelmäßig kann aufgrund von §§ 161, 163 StPO verdeckt ermittelt werden.

IV. Sonderproblem: Stellt die Einrichtung eines Fake Accounts durch Polizeibeamte ein Vergehen nach § 269 StGB dar?

Diese Rechtsfrage stellt sich ausschließlich für den verdeckt operierenden Beamten, der nicht Verdeckter Ermittler im Sinne von § 110a StPO ist, weil für Letztere § 110a Abs. 3 StPO eine Ermächtigungsgrundlage enthält, die die Anlage von Fake Accounts ausdrücklich rechtlich legitimiert.

Die Einrichtung eines Fake-Accounts durch Ermittlungsbeamte ist nach der Rspr. des BGH zur sog. „Namenstäuschung“ nicht strafbar, vgl. BGHSt 33, 159-163:

„ (…) Im Rahmen der Täuschungshandlung ist zusätzlich darauf abzustellen, welchen Zweck der Täter mit der falschen Namensnennung verfolgt. ***Wollte er nur seinen wirklichen Namen ungenannt lassen und steht er im übrigen zu der abgegebenen Erklärung, so handelt er nicht zur Täuschung im Rechtsverkehr****; wollte er sich jedoch der Beweiswir-*

kung der Urkunde in bezug auf seine Person entziehen, so ist das subjektive Unrechtselement gegeben (vgl. RGSt 3, 337, 339, 342; 48, 238, 242; RG JW 1934, 3064; insoweit in der Literatur umstritten - vgl. hierzu Seier aaO S. 137 m.w.N.) (…)“

Vgl. ferner BGH StraFo 2003, 253-254:
*„ (…) Der Angeklagte, der seinem Vermieter gegenüber unter dem falschen Namen "M." auftrat, hatte eine Selbstauskunft und den Mietvertrag mit dem falschen Namenszug "M." unterzeichnet. Der Senat folgt im Ergebnis den Ausführungen des Generalbundesanwalts in seiner Antragsschrift vom 13. Januar 2003 dahin, daß der Angeklagte im vorliegenden Fall **naheliegend nur über seinen Namen und nicht über seine Identität getäuscht hat. Danach kommt hier eine Urkundenfälschung nicht in Betracht** (vgl. u.a. BGH NStZ-RR 1997, 358, 359; BGHSt 33, 159 f.) (…)“*

Ein Polizeibeamter, der ein Benutzerkonto unter einem Phantasienamen anlegt, täuscht ebenfalls nur über seinen Namen und nicht über seine Identität. Er steht immer zu seinen Erklärungen, diese werden sogar Bestandteil der Ermittlungsakte. Damit liegt das TB-Merkmal „Zur Täuschung im Rechtsverkehr“, welches bei § 267 StGB und § 269 StGB den gleichen Inhalt hat, nicht vor.

Vgl. ferner OLG Hamm StV 2009, 475 zur Anmeldung unter Falschpersonalien bei eBay:
„Allein die Angabe eines (falschen) Namens und einer (Schein-) Adresse im Rahmen einer Internet-Anmeldung reicht hierzu jedoch nicht aus, da der Name als solcher keine rechtserhebliche Gedankenerklärung enthält und auch nicht hinreichend geeignet ist , für ein Rechtsverhältnis Beweis zu erbringen. (…)
Die bloße Eingabe des Namens und der Adresse geben aber keinen hinreichenden garantierten Rückschluss auf die Authentizität, da es jedem Internet-Nutzer im offenen Medium "Internet" möglich ist, auch unter einem fiktiven Namen den Zugang zu einer Internet-Plattform zu erlangen.“

Die Entscheidung des KG Berlin (NStZ 2010, 576-579) zu einem ähnlich gelagerten Fall ebenfalls eBay betreffend steht dem nicht entgegen. Das KG konnte im zugrundeliegenden Fall mangels geeigneter Feststellungen zur Täuschungsabsicht kein Urteil in der Sache fällen, sondern hat den Fall zurückverwiesen:

„ (…) Der Angeklagte kann auch vorsätzlich und zur Täuschung im Rechtsverkehr gehandelt haben (…) Dies und ob der Angeklagte sonst vorsätzlich in Bezug auf alle Merkmale des Tatbestands handelte, vermag der Senat angesichts des Fehlens jeglicher Feststellungen zum subjektiven Tatbestand indessen nicht zu entscheiden.(…)“

Mithin kann diese Entscheidung nicht als Argument für eine Strafbarkeit von Fake Accounts herangezogen werden.

Auch die Allgemeinen Geschäftsbedingungen (AGB) der Telemediendienste oder sozialen Netzwerke, die häufig das Anlegen von Fake Accounts als Vertragsverstoß werten und die Kündigung solcher Konten in Aussicht stellen, hindern die Maßnahme rechtlich nicht. **Zwar könnte der vorsätzliche Verstoß gegen die AGB theoretisch als ein staatlicher Eingriff in Art. 12 GG (Recht am eingerichteten und ausgeübten Gewerbebetrieb) gewertet werden. Dieser wäre jedoch durch §§ 161, 163 StGB rechtlich legitimiert.** Die Unternehmen können ihre Rechtsposition zudem durch Kündigung und Sperren der Accounts ausreichend wahrnehmen.

Grundsätzlich können Private staatliche Ermittlungshandlungen, die auf Grundlage von §§ 161, 163 StPO oder anderer strafprozessualer Normen erfolgen, nicht mit Hilfe von AGB verhindern.

Fazit:

- **Die allgemeine Informationsbeschaffung, Nutzung von Fake Accounts und Kommunikation in Sozialen Netzwerken, Foren und Boards sind von der Ermittlungsgeneralklausel abgedeckt, auch wenn sie längerfristig aufrecht erhalten werden. Regelmäßig wird dabei die Schwelle eines formalen NoeP- Einsatzes im Sinne des „Gemeinsamen Runderlasses“ nicht erreicht.**

- **Die Kommunikation mit einem Beschuldigten, um ein Scheingeschäft abzuwickeln oder ihn anhand von auch längerfristigen Internet-Kontakten zu identifizieren, ist von der Ermittlungsgeneralklausel gedeckt. Ob es schon ein NoeP-Einsatz nach den entsprechenden Richtlinien ist, hängt vom Einzelfall ab (Identitätstäuschung oder unüberprüfte Identität? Gefährdung des Beamten?).**

- **Nur tatsächlich legendierte längerfristige Aktionen und Kommunikation in Foren und Boards erfordern den Einsatz eines Verdeckten Ermittlers i.S.v. § 110a Abs. 1 StPO. Die „3-5-Kontakte-Regel“ des Scheinaufkäufers im wahren Leben gilt im Internet nicht, weil man ohnehin nie weiß, wie viele Personen eine/n Nickname/E-Mailadresse/User Account benutzen.**

- **„Legendiert“ bedeutet dabei, dass der Kommunikationspartner tatsächlich ernsthaft Vertrauen in eine vermeintlich real existierende Person fassen soll, deren Echtpersonalien mit entsprechenden Maßnahmen (§ 110a Abs. 2 StPO, z.B. falsche Personaldokumente) vorgetäuscht werden müssen, weil sie von den Tätern überprüft werden. Dies ist im Internet fast nie der Fall.**

- **Ein VE ist ferner nötig, wenn die Wohnung des Beschuldigten real betreten werden soll.**

- **Der Grundsatz der Subsidiarität des VE-Einsatzes gegenüber dem NoeP ist zu beachten.**

➡***Muster: staatsanwaltschaftliche Zustimmung zum VE-Einsatz bei nicht bestimmten Beschuldigten und nicht Betreten von Wohnungen gem. § 110b I StPO: Anlage 14***

➡***Muster: Beschluss für einen VE-Einsatz bei einem bestimmten Beschuldigten oder Betreten von Wohnungen gem. § 110b II StPO: Anlage 15***

Teil 5 – Grenzüberschreitende Internetermittlungen

I. Einleitung

Die Nutzung von weltweit operierenden Telemediendiensten (TMD)/Internetserviceprovidern (ISP) ist heute die Regel, siehe Facebook, Google, Twitter etc. Internetermittlungen, die Global Player betreffen oder sonst grenzüberschreitend sind, kommen daher häufig vor.

Zwei Konstellationen sind dabei grundsätzlich zu unterscheiden:

1) Der Ermittler erlangt im Rahmen einer Durchsuchung o.ä. Kenntnis von beweiserheblichen Daten des Beschuldigten, die möglicherweise im Ausland liegen (z.B. Inhalt eines E-Mail-Postfachs). Kann man die Daten ohne Rechtshilfeersuchen sichern?

2) Der Ermittler benötigt Informationen über den Kunden eines ausländischen Telemediendienstes (z.B. Kundendaten oder Login-IP-Adressen). Ist zur Einholung einer Auskunft ein Rechtshilfeersuchen erforderlich?

II. Fallkonstellation 1 (Sicherung möglicherweise im Ausland liegender Daten)

Der Ermittler erlangt im Rahmen einer Durchsuchung o.ä. Kenntnis von beweiserheblichen Daten des Beschuldigten, die möglicherweise im Ausland liegen (z.B. Inhalt eines E-Mail-Postfachs). Kann man die Daten ohne Rechtshilfeersuchen sichern?

Für Daten, die sich physikalisch in Deutschland befinden gilt insoweit § 110 Abs. 3 StPO:

„Die Durchsicht eines elektronischen Speichermediums bei dem von der Durchsuchung Betroffenen darf auch auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden, wenn andernfalls der Verlust der gesuchten Daten zu besorgen ist. Daten, die für die Untersuchung von Bedeutung sein können, dürfen gesichert werden; § 98 Abs. 2 gilt entsprechend.“

Die Daten dürfen also ohne weiteres gesichert werden.

Der Online-Zugriff auf ausländische Daten über Internet ist rechtlich komplizierter.

1. Zugriff auf im Ausland liegende Daten

a) Online-Zugriff auf frei zugängliche Daten

Er ist zulässig, wenn es sich um frei zugängliche Informationen handelt, die von Jedermann - ggf. auch im Rahmen eines privatrechtlichen Benutzungsverhältnisses - abrufbar sind.

Beispiel:
Aufruf einer Homepage

b) Online-Zugriff mit Zustimmung des Berechtigten

Ebenfalls zulässig ist der Zugriff ins Ausland, wenn die rechtmäßige und freiwillige Zustimmung der Person, die rechtmäßig zur Datenweitergabe befugt ist, vorliegt.

Beispiel:
Abruf von E-Mails aus dem Ausland mit Zustimmung des Account-Inhabers oder bei Zustimmung einer deutschen Niederlassung des ausländischen Providers.
Diese Regeln gelten inzwischen völkergewohnheitsrechtlich. Für die Vertragsparteien des Übereinkommens des Europarats über Computerkriminalität (Cybercrime Convention, CCC) ist dies auch kodifiziert:

Art. 32 CCC
„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."

In anders gelagerten Fällen, in denen sicher feststeht, dass sich die Daten physikalisch in solchen Ländern befinden, die nicht zum Schengen-Raum gehören und Art. 52 SDÜ nicht zur Anwendung kommen kann, ist grundsätzlich ein Rechtshilfeersuchen erforderlich.

c) Ad-hoc-Sicherung bei drohendem Datenverlust

Eine grenzüberschreitende vorläufige ad-hoc Sicherung (wie im Beispiel während laufender Durchsuchung) zugangsgeschützter Datenbestände im Ausland mit nachträglichem Rechtshilfeersuchen ist jedoch zulässig (Burhoff, ErmVerf., Rdnr. 579i; Meyer-Goßner, 53. Aufl. 2010, § 110 Rdnr. 7a; a.A. ebda. 54. Aufl. 2011).

d) Vorabsicherung nach Art. 29 CCC

Falls **kein sofortiger Datenverlust droht**, also etwa, wenn der Beschuldigte von dem Verfahren noch keine Kenntnis hat, können Daten im Ausland, insbesondere in den USA auch auf einem Weg, welcher schneller ist als derjenige der Rechtshilfe, vorab gesichert werden. Hierzu ist ein **formloses staatsanwaltschaftliches oder polizeiliches Ersuchen nach Art. 29 CCC zur Vorabsicherung der Daten** erforderlich.

Der notwendige Inhalt ergibt sich aus Art. 29 Abs. 2 CCC. Danach sind anzugeben:

- die Behörde, die um die Sicherung ersucht;
- die Straftat, die Gegenstand der strafrechtlichen Ermittlungen oder Verfahren ist, und eine kurze Sachverhaltsdarstellung;
- die gespeicherten Computerdaten, die zu sichern sind, und der Zusammenhang zwischen ihnen und der Straftat;
- alle verfügbaren Informationen zur Ermittlung des Verwahrers der gespeicherten Computerdaten oder des Standorts des Computersystems;
- die Notwendigkeit der Sicherung und
- die Erklärung der Absicht der ersuchenden StA, ein Rechtshilfeersuchen um Durchsuchung oderähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der gespeicherten Computerdaten zu stellen.

Das Ersuchen kann **per Fax oder Email** übermittelt werden. Die beiderseitige Strafbarkeit ist keine Voraussetzung. Die gesicherten Daten müssen vom ersuchten Staat 60 Tage aufbewahrt werden.
Die Übermittlung des Ersuchens erfolgt gem. Art. 35 CCC **über das „G8 High Tech Crime"-Netzwerk (= polizeilicher Weg, eine 24/7- Bereitschaft ist international sichergestellt).** Zuständig für die Weiterleitung ins Ausland ist das **BKA, Referat SO41 (G8-Dienststelle in Dtl., E-Mail: cyberintelligence@bka.bund.de)**. Es ist die **ausdrückliche Zusicherung der Übersendung eines späteren RH- Ersuchens durch die zust. StA erforderlich**. Ein vorherige telef. Verkehrsaufnahme mit SO 41 ist empfehlenswert.

Die entscheidende Frage im Beispielsfall 1 ist jedoch eine andere. Bevor sich ein Ermittler vor einem laufenden Computer während einer Durchsuchung den Kopf über eventuelle Rechtshilfeerfordernisse zerbricht, muss er sich doch fragen:

2. Standortproblematik

<u>Woher weiß ich, an welchem Ort in der Welt ein Server steht / sich die Daten befinden?</u>

Die **Länderkennung (.DE, .RU etc.) hilft i.d.R. nicht**, weil diese nicht mit dem Standort der Server korrespondieren muss. Die IP-Adresse des Ziel-Servers liefert lediglich einen Ansatz und ist unzuverlässig. **Deswegen sind visuelle Darstellungen eines Serverstandorts mittels Visualroute o.ä. für eine exakte, rechtssichere Ortsbestimmung ungeeignet**.

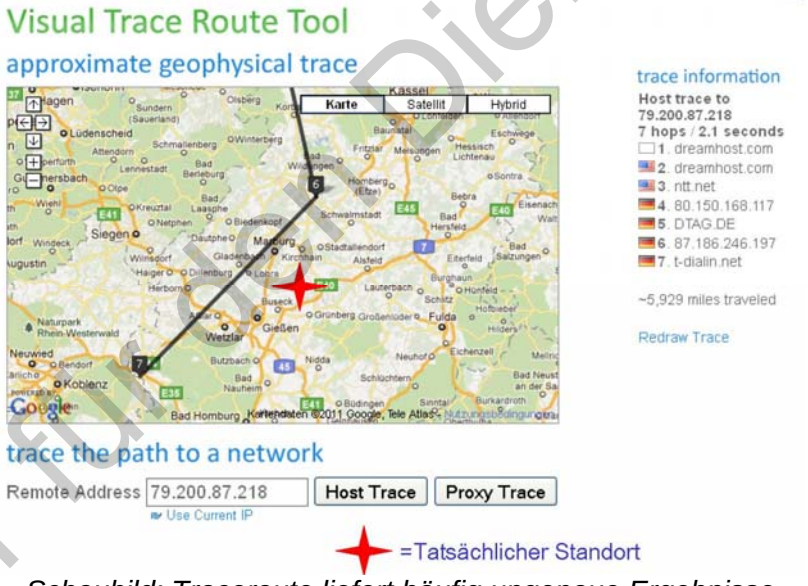


Schaubild: Traceroute liefert häufig ungenaue Ergebnisse

So nutzt z.B. die Amazon-Cloud Host-Server auf der ganzen Welt. Inhalte werden je nach Aufkommen und Herkunft der Anfragen dynamisch von Server zu Server, von Land zu Land verlegt, teilweise in kurzen zeitlichen Abständen. Technisch bedeutet dies, dass eine Homepage z.B. (reales Beispiel aus einem Verfahren der ZIT) eine IP-Adresse aufweist, die zu einem schwedischen Provider gehört, die Daten physikalisch also in Schweden zu liegen scheinen. Tatsächlich liegen die Daten physikalisch aber (auch) in Frankfurt am Main und der Datenabruf erfolgt mithin rein national.

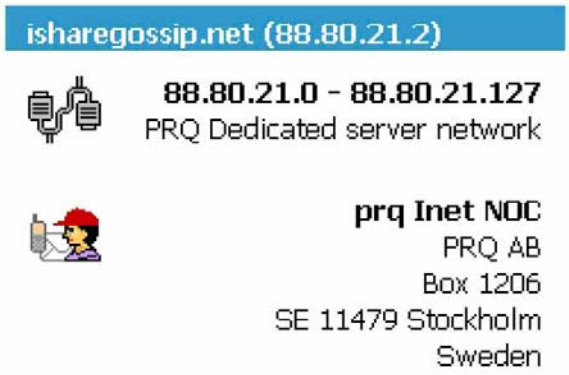


Schaubild: Die Seite „isharegossip.net“ scheint in Schweden zu liegen.

(4) Please inquire at Amazon, where the content of isharegossip.com is stored physically.

The customer is currently using the Amazon CloudFront CDN service to cache a small amount of data. That data is cached locally at a CloudFront data center in Frankfurt, Germany, served from Amazon Web Services S3 data storage service in Dublin, Ireland. We do not know what sort of data is cached.

Schaubild: Tatsächlich lagen die Daten (auch) in Frankfurt/M

Auch andere Clouddienste wie z.B. Google benutzen Host-Server in Deutschland**. Es kann also gut möglich sein, dass die Abfrage eines Email-Postfachs von Google beweiserhebliche Daten physikalisch nicht aus den USA, sondern aus Deutschland oder aus einem anderen Schengen-Land transportiert.**

Unabhängig von der Nutzung von Cloud-Diensten ist die Struktur des Internets dezentral, d.h. mittels Proxy-Servern (Zwischenspeicher) wird der Datenverkehr beschleunigt. **Nicht jeder Abruf des Angebots eines ausländischen TMD führt somit zu einem tatsächlichen Datenzugriff im Ausland:**

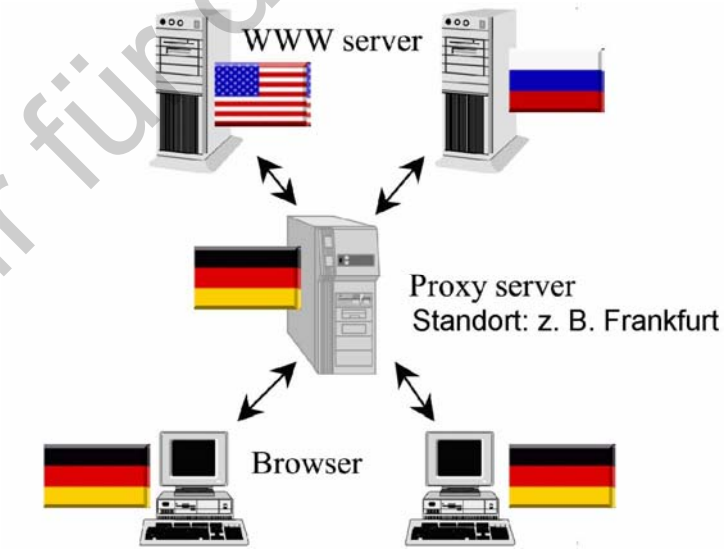


Schaubild: Ausländische Inhalte werden auf Proxy-Servern vorgehalten, der Datenabruf geschieht national

Lösung für die Praxis:

Bei externen Datenspeichern lässt sich häufig nicht klären, wo ihr physikalischer Standort ist. Aufgrund der Technik des Internets (Einsatz von Proxy-Servern und Cloud-Diensten) ist die Wahrscheinlichkeit sehr groß, dass sie jedenfalls auch in Deutschland (oder einem anderen Schengen-Land) liegen.

§ 110 Abs. 3 StPO kann zwar die Rechtshilfe nicht außer Kraft setzen, vermittelt aber ein Leitbild:

Im Zweifel ist eine Beweissicherung durchzuführen.

Sollte man sich geirrt haben und sich herausstellen, dass die Daten doch im Ausland lagen, ist dies ebenso bedauerlich wie unschädlich, denn:

Die Nichteinhaltung des Rechtshilfeweges begründet grundsätzlich keine Unverwertbarkeit. (vgl. BVerfG NStZ 2011, 103-106; BGHSt 37, 30-34; BGH NStZ 2010, 351-352; LG Bochum, Beschluss vom 07.08.2009 - 14 Qs-131 Js 150/10-60/10; LG Düsseldorf NStZ 2011, 103-106).

III. Fallkonstellation 2 (Datenerhebung bei ausländischen Diensteanbietern):

Der Ermittler benötigt Informationen über den Kunden eines ausländischen Telemediendienstes (z.B. Kundendaten oder Login-IP-Adressen). Ist zur Einholung einer Auskunft ein Rechtshilfeersuchen erforderlich?

1. Notwendigkeit der Rechtshilfe

Die Vorschriften über die internationale Rechtshilfe schützen **die Souveränität von Staaten**. **Billigt ein Staat stillschweigend die unmittelbare Beantwortung von ausländischen Auskunftsersuchen durch ein in seinem Hoheitsgebiet ansässiges Unternehmen, verzichtet er insoweit konkludent auf die Einhaltung der Vorschriften über die internationale Rechtshilfe.** Bei international agierenden ISP / TMD ist die unmittelbare Beantwortung häufig. Das angeschriebene Unternehmen wird mitteilen, ob es RH benötigt.

Gegen unmittelbare Anfragen bei ausländischen TMD/ISP bestehen daher keine zwingenden Bedenken.

2. Notwendigkeit eines Rechtshilfeersuchen bei Anfragen an US-Firmen

Das Justizministerium der USA hat unmittelbare Anfragen nunmehr auch ausdrücklich gebilligt. US-Firmen dürfen Bestands- und Verkehrsdaten auf freiwilliger Basis mitteilen, sofern es sich bei den Kunden nicht um US- Bürger handelt.

In einem Schreiben vom 30.03.2012 (Az. III 1 - 9360 E - A 5 - B 3601/2012) hat das Bundesamt für Justiz allen Landesjustizverwaltungen folgende Information gegeben:

„Direktes Herantreten an Internetprovider zwecks freiwilliger Herausgabe von Verkehrs- und Bestandsdaten

Das U.S.-amerikanische Justizministerium hat auf eine entsprechende hiesige Anfrage kürzlich Folgendes mitgeteilt:

Bestands- und Verkehrsdaten:
Internetdiensteanbieter (Providerfirmen) dürfen (basierend auf den jeweiligen internen Dienstleitungsbedingungen) freiwillig nicht inhaltsbezogene Informationen (also Bestands- und Verkehrsdaten) an eine ausländische Strafverfolgungsbehörde herausgeben. Insoweit bestehen seitens des amerikanischen Justizministeriums ausdrücklich keine Bedenken gegen ein unmittelbares Herantreten deutscher 5trafverfolgungsbehörden an in den USA ansässige Internetproviderfirmen oder deren Tochterfirmen in Deutschland.

***Notfälle (z.B. Terrorismus. Amokläufe** pp.)*
***In Notfällen kann ein U.S.-amerikanischer Internetdiensteanbieter auch mit dem Ziel der freiwilligen Herausgabe von Inhaltsdaten direkt kontaktiert werden**. In diesem Fall muss allerdings eine Rückleitung der Daten über U.S.-amerikanische Regierungsbehörden erfolgen. Das amerikanische Justizministerium hat hierzu vorgeschlagen, dass deutsche Strafverfolgungsbehörden die amerikanische Seite bzgl. eines solchen Notfallersuchens zeitgleich über das G 8/24/7-Netzwerk informiert in Deutschland über das BKA, dort Referat SO 41, vgl. hierzu auch mein Rundschreiben vom 8. Februar 2007,vgl. Anlage), damit eine schnelle Zurückleitung der erbetenen Informationen an die ersuchende deutsche Behörde gewährleistet ist.“*

Kontaktdaten von US-Firmen:
Die Kontaktdaten der wichtigsten US-amerikanischen TMD lauten:

Facebook, Inc.

Facebook, Inc.
Attn: Facebook Security, Law Enforcement Response Team
18 Hacker Way
Menlo Park, CA 94025
E-Mail: records@facebook.com
Telefax: + 1 650 472-8007
Weitere Informationen: https://www.facebook.com/safety/groups/law/guidelines/

Google, Inc. und YouTube LLC (gehört zu Google):

1600 Amphitheatre Parkway
Mountain View, CA 94043, USA
Fax: 0016504690622
E-Mail: lis-global@google.com

Microsoft Corporation

One Microsoft Way
98052 Redmond, WA
USA

über Microsoft Deutschland GmbH
Konrad-Zuse-Strasse 1
85716 München

a) Anfragen bei Facebook - Bestandsdaten und Verkehrs-/Nutzerdaten

- Facebook akzeptiert zur Herausgabe der Bestands- und Nutzerdaten (inkl. IP-Adressen zu Logins) zu Accounts deutsche Auskunftsersuchen gemäß §§ 161, 163 StPO in direkter Übermittlung ohne justizielle Rechtshilfe.
- Ersuchen ins Englische übersetzen.
- Daten werden nur dann mitgeteilt, wenn der Account nach Deutschland „zeigt".
- Ist es ein nicht-deutsches Benutzerkonto, ist zur Datenerlangung justizielle Rechtshilfe notwendig.
- Speicherfrist bei Facebook laut eigenen Angaben bis zu 90 Tage.
- Rechtsgrundlage: § 161 StPO i.V.m. § 95 StPO oder § 163 StPO, jeweils i.V.m. § 15 Abs. 5 Satz 4; § 14 Absatz 2 TMG
- Anfragen in Englisch formulieren.
- Anfrage auch per E-Mail möglich: Ausdrucken - Unterschreiben! – Einscannen
- Anfragen bei Facebook dauern i.d.R. ca. 4-6 Wochen.
- Facebook bietet nunmehr auch eine Online-Abfragemöglichkeit für Ermittlungsbehörden (wie z.B. eBay) unter https://www.facebook.com/records.

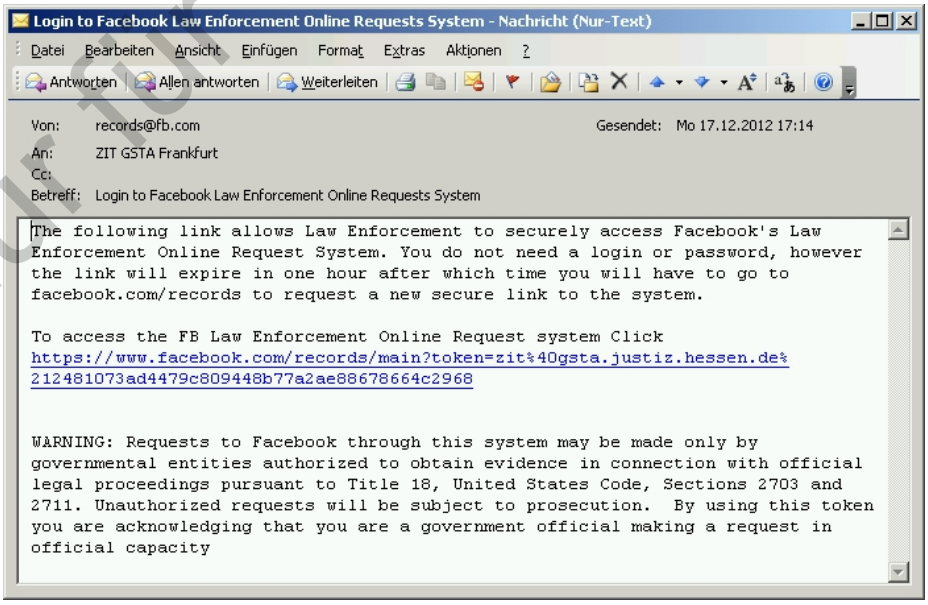


Schaubild: Online-Abfragemöglichkeit von Facebook

b) Anfragen bei Google

Google bietet eine Vielzahl von Diensten an. Nach deutschem Recht ist Google als Telemediendienst anzusehen. Google sieht sich selbst jedoch offenbar in Teilbereichen als Telekommunikationsdienstleister an und verlangt dementsprechend die Angabe von Ermächtigungsgrundlagen nach dem TKG, die aus hiesiger Sicht nicht unbedingt zutreffend sind. Dies ist jedoch unschädlich, da die Standards, die Google verlangt, rechtlich höher sind als tatsächlich erforderlich. Verwertungsprobleme entstehen mithin keine.

Bestandsdaten von Google

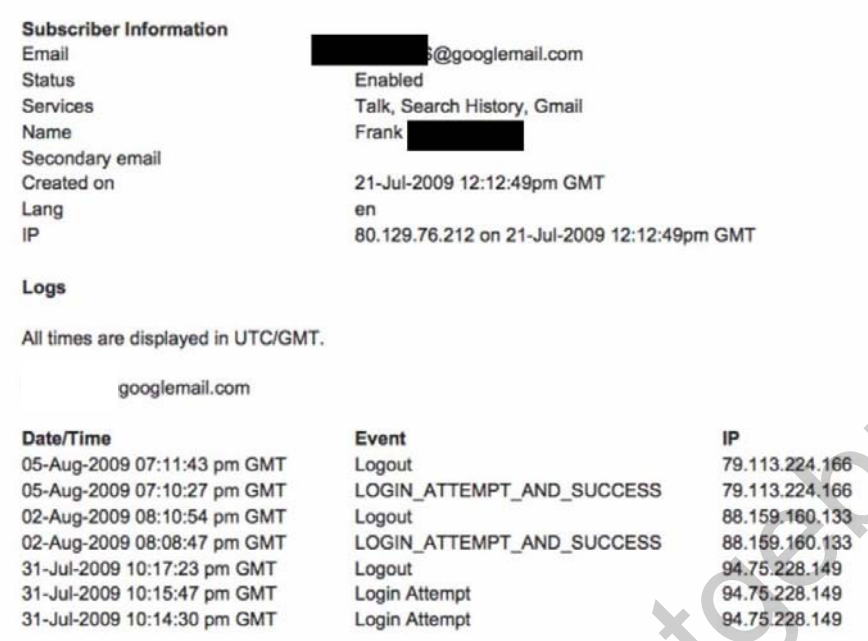
- Anfragen zu Bestandsdaten sind bei Google nach deutschem Recht möglich
- 2 Varianten:
  - Anfrage gem. § 113 TKG (E-Mail-Dienste).
  - Anfrage gem. § 15 Abs. 5 Satz 4; §14 Absatz 2 TMG , § 95 StPO (Youtube).
- Google speichert 28 Tage (allgemein)
- Die Anfragen müssen in englischer Sprache formuliert sein.
- Die Anfragen müssen unterschrieben sein - Nicht unterschriebene Anfragen werden durch Google nicht bearbeitet.
- Antworten seitens Google können mehrere Wochen dauern, da dort viele Anfragen eingehen

```
############### * Google Confidential and Proprietary * ################

GOOGLE SUBSCRIBER INFORMATION

Name: Peter [redacted]er
e-Mail: [redacted]@gmail.com
Status: Enabled
Services: Alerts, Base, Blogger, Co-op, Docs, Gmail, Google profile, Local
business center, Personalized homepage, Profiles, Reader, Search history,
Shopping list, Sites, Spreadsheets, Talk, Toolbar, Toolbar sync,
Transliteration, Web history promo, Webmaster tools, Youtube
Secondary e-Mail: peterr[redacted]@alice-dsl.de
Created on: 2007/09/06-12:22:07-UTC
Language Code: de
SMS: 0176[redacted] [DE]

############### * Google Confidential and Proprietary * ################
```

Schaubild: Ergebnis einer Bestandsdatenabfrage von Google

Verkehrsdaten von Google

- Google akzeptiert zur Herausgabe der IP-Verkehrsdaten zu E-Mailaccounts / Youtube-Accounts deutsche Beschlüsse gemäß § 100g StPO
- auch bzw. gerade in deutscher Sprache
- Adressierung mit Vorblatt wie bei der Bestandsdatenanfrage
- Empfehlung: Englische Sachverhaltsdarstellung im Anschreiben, da Beschluss in deutscher Sprache
- Verkehrsdaten werden nur dann mitgeteilt, wenn die IP-Adressen aus Deutschland bzw. der Region kommen
- Falls dies nicht der Fall ist => Rechtshilfe
- Das Vorblatt zum Beschluss muss in englischer Sprache formuliert sein
- Das Vorblatt muss unterschrieben sein - Nicht unterschriebene Anfragen werden durch Google nicht bearbeitet



Subscriber Information

Email	[redacted]@googlemail.com
Status	Enabled
Services	Talk, Search History, Gmail
Name	Frank [redacted]
Secondary email	
Created on	21-Jul-2009 12:12:49pm GMT
Lang	en
IP	80.129.76.212 on 21-Jul-2009 12:12:49pm GMT

Logs

All times are displayed in UTC/GMT.

googlemail.com

Date/Time	Event	IP
05-Aug-2009 07:11:43 pm GMT	Logout	79.113.224.166
05-Aug-2009 07:10:27 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	79.113.224.166
02-Aug-2009 08:10:54 pm GMT	Logout	88.159.160.133
02-Aug-2009 08:08:47 pm GMT	LOGIN_ATTEMPT_AND_SUCCESS	88.159.160.133
31-Jul-2009 10:17:23 pm GMT	Logout	94.75.228.149
31-Jul-2009 10:15:47 pm GMT	Login Attempt	94.75.228.149
31-Jul-2009 10:14:30 pm GMT	Login Attempt	94.75.228.149

Schaubild: Ergebnis einer Verkehrsdatenabfrage von Google

c) Anfragen bei Microsoft – Bestandsdaten und Verkehrs/-Nutzerdaten

Anfragen an Microsoft sind über die Microsoft Deutschland GmbH zu senden. Auch Microsoft sieht sich offenbar als TK-Dienst.

- Prinzipiell Vorgehen wie bei Google
- Microsoft akzeptiert für Bestandsdaten-Anfragen gemäß § 113 TKG und für Herausgabe der IP-Verkehrsdaten zu E-Mail-Accounts deutsche Beschlüsse gemäß § 100g StPO
- Anfragen müssen wie folgt ausgewiesen sein:
  Microsoft Corporation, 1 Microsoft Way, Redmond WA,
  98052-6399, USA
  über Microsoft Deutschland GmbH
- Anfrage an Faxnummer in Deutschland
- 0800-6738329
- Anfrage wird durch Microsoft Deutschland an Microsoft USA weitergeleitet
- Antwort durch Microsoft Deutschland

3. Anfragen zu Inhaltsdaten

Die jeweiligen Diensteanbieter betrachten verschiedene Daten als Content, also Inhaltsdaten. Dies sind Daten, die in Deutschland nur i.d.R. mittels eines Beschlusses gem. §§ 94 ff. oder § 100a StPO zu erlangen sind.

Beispiele
• Inhalt von E-Mailpostfächern
• Chat Protokolle
• Inhalte von Nachrichten bei Facebook oder Nachrichten auf der Pinnwand bei Facebook

Inhaltsdaten (Content) aus Accounts bei im Ausland ansässigen Providern werden i.d.R. nicht ohne die Übermittlung eines justiziellen Rechtshilfeersuchens an den Staat, in dem der

Provider seinen Hauptsitz hat, herausgegeben. Nach U.S.-amerikanischem Recht können Ersuchen um Inhaltsdaten von E-Mail-Accounts o.ä. nur aufgrund eines eigenen Gerichtsbeschlusses ("search-warrant“) eines dortigen Gerichtes umgesetzt werden. Dies gilt insbesondere für Microsoft, Facebook, Google (inkl. seiner Töchter, wie z.B. Youtube). Bei Yahoo! und AOL gibt es Ausnahmen. Im Einzelfall sollte dort angefragt werden, welche Daten freiwillig herausgegeben werden.

Gegen eine direkte Anfrage bei den sogenannten „Global Playern“ durch die Länderpolizeien bestehen diesseits keine Bedenken. Nach § 3 Abs. 2 BKAG ist lediglich bei Anfragen gegenüber „öffentlichen Stellen“ das BKA einzuschalten.

➡***Muster: englischsprachiges Auskunftsersuchen in die USA: Anlage 16***

➡***Muster: Facebook-Anfrage: Anlage 17***

Für Anmerkungen, Ergänzungsvorschläge oder Änderungswünsche zu diesem Skript, das fortlaufend aktualisiert und erweitert wird, sind wir dankbar.
*(**E-Mail: zit@gsta.justiz.hessen.de**).*

Formularbeispiele für Auskunftsersuchen etc.

Anlage 1
Anfrage nach Bestandsdaten eines Telemedien- oder Telekommunikations-Diensteanbieters

Betr.: Ermittlungsverfahren gegen ☐ **Unbekannt z.N.** _____
☐ _____

wegen_____

Sehr geehrte Damen und Herren,

in dem vorbezeichneten Ermittlungsverfahren ist die Herausgabe von Bestandsdaten durch Ihr Unternehmen erforderlich.

Zur Vermeidung einer Vorladung eines Verantwortlichen Ihres Hauses zu einer zeitaufwendigen Zeugenvernehmung bitte ich

☐ gemäß § 100j Abs. 1 S. 1 und Abs. 2 Strafprozessordnung (StPO) in Verbindung mit § 100j Abs. 5 StPO

☐ gemäß § 14 Telemediengesetz (TMG) in Verbindung mit §§ 161, 161a Strafprozessordnung (StPO)

um Mitteilung der nachfolgenden Bestandsdaten zu folgender Person/Kennung:

☐ Vorname:
Name/Geburtsname:
Geburtsdatum/-ort:
Straße, Hausnummer:
PLZ, Wohnort:

☐ Email-Adresse:

☐ IP-Adresse

IP-Adresse	Datum	Uhrzeit	Zeitzone

☐ X-ID

X-ID	Datum	Uhrzeit	Zeitzone

☐ ICQ-Nummer:
☐ AIM-Adresse:
☐ MSN Messenger:
☐ Yahoo-Messenger:
☐ Nutzername im sozialen Netzwerk/Forum etc.:
☐ andere Kennung (bspw. verwendete Passworte)

☒ Welche Angaben hat der Kunde zu seiner Person gemacht?

☒ Wurden diese Angaben auf ihre Richtigkeit überprüft?

☒ Welcher Dienst wurde seit wann in Anspruch genommen?

☒ Handelt es sich hierbei um einen kostenpflichtigen Dienst?

☒ Falls ja, in welcher Form folgte die Bezahlung des Dienstes (Konto, Kreditkartennummer, etc.)

☒ Sind oder waren auf diese Person weitere Accounts registriert?

☐ Beinhaltet der Account

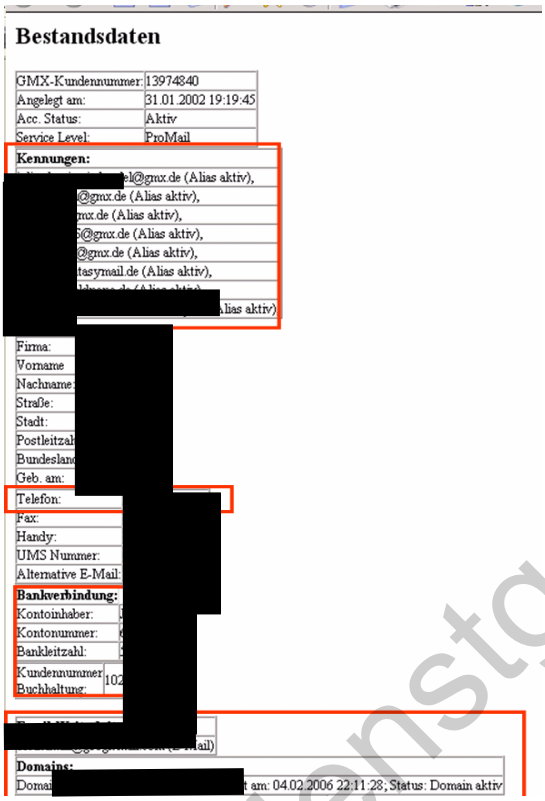
- Email-Weiterleitungen
- Angabe von Kontaktadressen (alternative Email-Adressen, Telefonnummern)

Wurde hierüber Kontakt zum Kunden aufgenommen?

Die Beantwortung des o.g. Auskunftsersuchens kann eine staatsanwaltschaftliche Zeugenvernehmung von Mitarbeitern Ihres Hauses und Durchsuchungs- bzw. Beschlagnahmemaßnahmen entbehrlich machen. Nur höchst vorsorglich weise ich darauf hin, dass Zeugen gesetzlich verpflichtet sind, auf Ladung vor der Staatsanwaltschaft zu erscheinen und zur Sache auszusagen (§ 161a Abs. 1 StPO). Wer einen als Beweismittel in Betracht kommenden Gegenstand in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern (§ 95 Abs. 1 StPO). Beide Verpflichtungen können mit Zwangsmitteln durchgesetzt werden und sind nicht von einem entsprechenden Gerichtsbeschluss abhängig (§ 95 Abs. 2 i.V.m. § 70 StPO).
Gemäß § 100j Abs. 5 S. 1 StPO hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die für die Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln. Diese Verpflichtung kann mit Zwangsmitteln durchgesetzt werden und ist nicht von einem entsprechenden Gerichtsbeschluss abhängig (§ 100j Abs. 5 S. 2 StPO i.V.m. §§ 95 Abs. 2, 70 StPO).
Von der Benachrichtigung des Nutzers über das vorliegende Schreiben oder allgemein über die Existenz eines Ermittlungsverfahrens bitte ich abzusehen, da dies ein strafrechtlich relevantes Verhalten (z.B. Strafvereitelung, Begünstigung oder Beihilfe zu einer Straftat) darstellen könnte.
Gleiches kann für die unberechtigte Verweigerung oder vorsätzliche Verzögerung der Erteilung von Auskünften gelten.
Um die weiteren Ermittlungen nicht zu gefährden, dürfen auch Dritte über das vorliegende Auskunftsersuchen oder allgemein über die Existenz des laufenden Ermittlungsverfahrens nicht benachrichtigt oder informiert werden. Neben einer direkten Kontaktaufnahme mit einem mutmaßlichen Täter gilt dies namentlich auch für eine öffentliche Bekanntgabe in den Medien (Fernsehen, Rundfunk, Presse, Internet [z.B. in E-Mails, Foren, Chats, Blogs, Twitternachrichten, sozialen Netzwerken, etc.]), da die Möglichkeit besteht, dass der Täter hierüber Kenntnis von den gegen ihn geführten Ermittlungen erlangt und diese dadurch gefährdet werden. Eine Zuwiderhandlung kann ebenfalls ein strafrechtlich relevantes Verhalten (insbesondere eine Strafvereitelung gem. § 258 StGB) darstellen.

Es wird ferner darauf hingewiesen, dass der Verpflichtete gem. § 113 Abs. 4 S. 2 TKG sowohl gegenüber seinen Kundinnen und Kunden als auch gegenüber Dritten über die Auskunftserteilung Stillschweigen zu wahren hat. Zuwiderhandlungen werden gem. § 149 Abs. 1 Nr. 35, 2 TKG mit einem Bußgeld bis zu 10000.- € geahndet.

Bei einer so gestalteten Anfrage bieten die Antwortschreiben teilweise weitere Ermittlungsansätze (beispielhaft Antwort von GMX):



Bestandsdaten

GMX-Kundennummer:	13974840
Angelegt am:	31.01.2002 19:19:45
Acc. Status:	Aktiv
Service Level:	ProMail

Kennungen:

[redacted]@gmx.de (Alias aktiv),
[redacted]@gmx.de (Alias aktiv),
[redacted]mx.de (Alias aktiv),
[redacted]@gmx.de (Alias aktiv),
[redacted]@gmx.de (Alias aktiv),
[redacted]tasymail.de (Alias aktiv),
[redacted]lias aktiv)

Firma:	
Vorname	[redacted]
Nachname:	
Straße:	
Stadt:	
Postleitzah	
Bundesland	
Geb. am:	
Telefon:	
Fax:	
Handy:	
UMS Nummer:	
Alternative E-Mail:	
Bankverbindung:	
Kontoinhaber:	
Kontonummer:	
Bankleitzahl:	
Kundennummer:	102
Buchhaltung:	

[redacted]ail)

Domains:

Domai[redacted] am: 04.02.2006 22:11:28; Status: Domain aktiv

Anlage 2
Anfrage nach Nutzungsdaten (§ 15 TMG) eines Telemediendiensteanbieters

Betr.: Ermittlungsverfahren gegen ☐ **Unbekannt z.N.** _____
☐ _____

wegen_____

Sehr geehrte Damen und Herren,

in dem vorbezeichneten Ermittlungsverfahren ist die Herausgabe von Nutzungsdaten durch Ihr Unternehmen erforderlich.

Zur Vermeidung einer Vorladung eines Verantwortlichen Ihres Hauses zu einer zeitaufwendigen Zeugenvernehmung bitte ich gemäß §§ 15 Abs. 1 und 5 S. 4, 14 Abs. 2 Telemediengesetz (TMG) in Verbindung mit §§ 161, 161a Strafprozessordnung (StPO)

um Mitteilung der dort erhobenen Nutzungsdaten - **insbesondere der dort noch gespeicherten IP-Adressen** - zu folgender Person/Kennung:

☐ Vorname:
Name/Geburtsname:
Geburtsdatum/-ort:
Straße, Hausnummer:
PLZ, Wohnort:

☐ Email-Adresse:
☐ IP-Adresse **<Datum>** um **<Uhrzeit, Zeitzone [z.B. MESZ]>**
☐ ICQ-Nummer:
☐ AIM-Adresse:
☐ MSN Messenger:
☐ Yahoo-Messenger:
☐ Nutzername im sozialen Netzwerk/Forum etc.:
☐ andere Kennung (z.B. verwendetes Passwort):

☐ Ferner bitte ich – soweit technisch möglich – um Überprüfung, ob unter der (den) festgestellten IP-Adresse/n an den jeweiligen Tagen auf weitere Benutzerkonten zugegriffen wurde und ggf. um deren Mitteilung sowie der präzisen Zeitpunkte der Zugriffe.

Gemäß § 1 Abs. 1 TMG sind alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht ausschließlich in der Übertragung von Signalen über Telekommunikationsnetze bestehen bzw. telekommunikationsgestützte Dienste oder Rundfunk darstellen, Telemedien. Gemäß § 15 Abs. 4 S. 4 TMG in Verbindung mit § 14 Abs. 2 TMG in Verbindung mit § 161a StPO sind die Telemediendienste verpflichtet, Nutzungsdaten, also personenbezogene Daten, die erhoben werden um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen, zum Zwecke der Strafverfolgung an die Strafverfolgungsbehörden herauszugeben. Die IP-Adressen, unter denen Kunden Ihr Angebot in Anspruch nehmen, stellen solche Nutzungsdaten gemäß § 15 Abs. 1 Nr. 1 TMG dar.

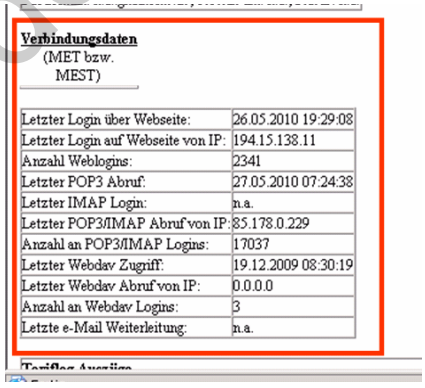
Vorsorglich weise ich darauf hin, dass das Urteil des BVerfG vom 02.03.2010 zur Vorratsdatenspeicherung (Az. 1 BvR 256, 263, 586/08) Ihre Auskunftspflicht über Nutzungsdaten nicht berührt, weil die Entscheidung ausschließlich auf Grundlage der für nichtig erklärten §§ 113a, b Telekommunikationsgesetz gespeicherte Vorratsdaten betrifft.

Vorsorglich weise ich darauf hin, dass das Urteil des BVerfG vom 24.01.2012 (Az. 1 BvR1299/05) Ihre Auskunftspflicht über Nutzungsdaten nicht berührt, weil die Entscheidung ausschließlich Telekommunikationsdienste betrifft.

Die Beantwortung des o.g. Auskunftsersuchens kann eine staatsanwaltschaftliche Zeugenvernehmung von Mitarbeitern Ihres Hauses und Durchsuchungs- bzw. Beschlagnahmemaßnahmen entbehrlich machen. Nur höchst vorsorglich weise ich darauf hin, dass Zeugen gesetzlich verpflichtet sind, auf Ladung vor der Staatsanwaltschaft zu erscheinen und zur Sache auszusagen (§ 161a Abs. 1 StPO). Wer einen als Beweismittel in Betracht kommenden Gegenstand in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern (§ 95 Abs. 1 StPO). Beide Verpflichtungen können mit Zwangsmitteln durchgesetzt werden und sind nicht von einem entsprechenden Gerichtsbeschluss abhängig (§ 95 Abs. 2 i.V.m. § 70 StPO).

Von der Benachrichtigung des Nutzers über das vorliegende Schreiben oder allgemein über die Existenz eines Ermittlungsverfahrens bitte ich abzusehen, da dies ein strafrechtlich relevantes Verhalten (z.B. Strafvereitelung, Begünstigung oder Beihilfe zu einer Straftat) darstellen könnte.
Gleiches kann für die unberechtigte Verweigerung oder vorsätzliche Verzögerung der Erteilung von Auskünften gelten.
Um die weiteren Ermittlungen nicht zu gefährden, dürfen auch Dritte über das vorliegende Auskunftsersuchen oder allgemein über die Existenz des laufenden Ermittlungsverfahrens nicht benachrichtigt oder informiert werden. Neben einer direkten Kontaktaufnahme mit einem mutmaßlichen Täter gilt dies namentlich auch für eine öffentliche Bekanntgabe in den Medien (Fernsehen, Rundfunk, Presse, Internet [z.B. in E-Mails, Foren, Chats, Blogs, Twitternachrichten, sozialen Netzwerken, etc.]), da die Möglichkeit besteht, dass der Täter hierüber Kenntnis von den gegen ihn geführten Ermittlungen erlangt und diese dadurch gefährdet werden. Eine Zuwiderhandlung kann ebenfalls ein strafrechtlich relevantes Verhalten (insbesondere eine Strafvereitelung gem. § 258 StGB) darstellen.

Daraufhin werden von den Telemediendiensten u.a. Auskünfte über die Login-IP-Adressen erteilt:



Verbindungsdaten
(MET bzw. MEST)

Letzter Login über Webseite:	26.05.2010 19:29:08
Letzter Login auf Webseite von IP:	194.15.138.11
Anzahl Weblogins:	2341
Letzter POP3 Abruf:	27.05.2010 07:24:38
Letzter IMAP Login:	n.a.
Letzter POP3/IMAP Abruf von IP:	85.178.0.229
Anzahl an POP3/IMAP Logins:	17037
Letzter Webdav Zugriff:	19.12.2009 08:30:19
Letzter Webdav Abruf von IP:	0.0.0.0
Anzahl an Webdav Logins:	3
Letzte e-Mail Weiterleitung:	n.a.

Anschließend können diese Daten bei dem zuständigen Access-Provider (zu ermitteln mit centralops.net; ripe.net) als Bestandsdaten gem. §§ 161, 163 StPO erfragt werden.

Anlage 3
Antrag Echtzeitüberwachung Telekommunikations-/Telemediendienst gem. § 100g StPO

Urschriftlich mit Akten
dem Amtsgericht – Ermittlungsrichter/in –
in …
unter Hinweis insbesondere auf Bl. … d.A.

mit dem Antrag, einen Beschluss gem. § 100g StPO gem. anliegendem Entwurf zu erlassen:

Beschluss

In dem Ermittlungsverfahren
gegen
wegen (*Straftat von erheblicher Bedeutung oder mittels Telekommunikation*)

wird gemäß § 100 g Abs. 1 StPO

der Diensteanbieter …

verpflichtet,

betreffend

☐ die Anschlussnummer

☐ die Anschlusskennung

☐ Anschlussinhaber (auch gegen Unbekannt möglich)

☐ Anschlussnutzer (auch gegen Unbekannt möglich)

☐ Netzbetreiber

☐ Diensteanbieter

für einen Zeitraum von (bis 3 Monate) ab dem Datum dieses Gerichtsbeschlusses **die anfallenden Verkehrsdaten (§§ 96 Abs. 1, 3 Nr. 30 TKG) bzgl. der o.g Anschlussnummer/-kennung zu erheben und in Echtzeit an …zu übersenden.**

Die Maßnahme wird dem Anschlussinhaber derzeit wegen einer Gefährdung des Untersuchungszwecks nicht mitgeteilt (§ 101 Abs. 5 Satz 1 StPO).

Gründe: Nach den bisherigen Ermittlungen besteht der Verdacht, dass der

☐ Beschuldigte …

☐ bislang unbekannte Beschuldigte

als Täter oder Teilnehmer

☐ folgende Straftat von erheblicher Bedeutung begangen hat:

Die Straftat wiegt auch im Einzelfall schwer, weil…

☐ folgende Straftat mittels Telekommunikation begangen hat:

Verbrechen /Vergehen, strafbar gemäß …

Die
☐ Erforschung des Sachverhalts
☐ Ermittlung des Aufenthaltsortes des/der Beschuldigten
☐ Identifizierung des/der Beschuldigten und Ermittlung seines/ ihres Aufenthaltsortes
ist auf andere Weise aussichtslos oder wesentlich erschwert (§ 100g Abs. 1 Satz 2 StPO).

Die Auskunft ist für die Untersuchung erforderlich (§ 100g Abs. 1 Satz 1 StPO).
Sie ist auch verhältnismäßig (ggf. besonders zu begründen bei Straftat mittels Telekommunikation), weil…

Weniger einschneidende und geeignete Maßnahmen, die den Betroffenen weniger belasten, stehen nicht zur Verfügung.

Eine vorherige Anhörung des Beschuldigten unterbleibt, da sie den Ermittlungszweck gefährden würde, § 33 Abs. 4 S. 1 Strafprozessordnung.

Anlage 4
Muster für DSL-Überwachung

Urschriftlich mit Akten
dem Amtsgericht – Ermittlungsrichter/in –
in …
unter Hinweis insbesondere auf Bl. … d.A.

mit dem Antrag, einen Beschluss gem. § 100a StPO gem. anliegendem Entwurf zu erlassen:

Beschluss

In dem Ermittlungsverfahren
gegen
wegen

wird
gemäß §§ 100a Abs. 1 und 2 Nr. …, 100 b StPO
für die Dauer von 3 Monaten
die Überwachung und Aufzeichnung der Telekommunikation angeordnet für

den DSL-Internetanschluss des …

Nutzerkennung:

Rufnummern:

Provider:

Erfüllungsgehilfe (DSL-Carrier):

Die Maßnahme wird dem Anschlussinhaber derzeit wegen einer Gefährdung des Untersuchungszwecks nicht mitgeteilt (§ 101 Abs. 5 Satz 1 StPO).

Gründe: Aufgrund der bisherigen Ermittlungen besteht der Verdacht, dass der

☐ Beschuldigte …

☐ bislang unbekannte Beschuldigte

als Täter oder Teilnehmer

☐ folgende Straftat gem. § 100a Abs. 1 Nr. 1 i.V.m. Abs. 2 Nr . ... StPO begangen hat:

Die Straftat wiegt auch im Einzelfall schwer, weil…

☐ Die Erforschung des Sachverhalts

☐ Die Ermittlung des Aufenthaltsortes des Beschuldigten

wäre auf andere Weise aussichtslos oder wesentlich erschwert, weil…

Eine vorherige Anhörung des Beschuldigten unterbleibt, da sie den Ermittlungszweck gefährden würde, § 33 Abs. 4 S. 1 Strafprozessordnung.

Anlage 5
Muster für „Quellen-TKÜ“

Urschriftlich mit Akten
dem Amtsgericht – Ermittlungsrichter/in –
in …
unter Hinweis insbesondere auf Bl. … d.A.

mit dem Antrag, einen Beschluss gem. § 100a StPO gem. anliegendem Entwurf zu erlassen:

Beschluss

In dem Ermittlungsverfahren
gegen
wegen

wird

1. gemäß §§ 100a Abs. 1 und 2 Nr. …, 100 b StPO
für die Dauer von <Datum des Beschlusserlasses> bis <3 Monate nach Beschlusserlass>
die Überwachung und Aufzeichnung der Telekommunikation angeordnet für

den DSL-Internetanschluss des …

Nutzerkennung:

Rufnummern:

Provider:

Erfüllungsgehilfe (DSL-Carrier):

2. zur Überwachung der über den oben genannten Telekommunikationsanschluss geführten verschlüsselten Telekommunikation die Vornahme hierzu erforderlicher Maßnahmen angeordnet, um die Telekommunikation vor der Verschlüsselung überwachen zu können.
Zulässig sind hierbei nur solche Maßnahmen, die der Überwachung der Telekommunikation selbst dienen und die für deren Umsetzung zwingend erforderlich sind.
Nicht zugelassen sind insbesondere
- die Durchsicht der Speichermedien, über die der fremde Computer verfügt und an die er angeschlossen ist, nach gespeicherten Daten und Dateien und
- die Überwachung der Datenverarbeitungsvorgänge, die nicht der Telekommunikation dienen (bspw. Screenshots von Entwürfen).

Die Maßnahme wird dem Anschlussinhaber derzeit wegen einer Gefährdung des Untersuchungszwecks nicht mitgeteilt (§ 101 Abs. 5 Satz 1 StPO).

Gründe: …

Nach den derzeitigen Ermittlungserkenntnissen nutzt der Beschuldigte für seine Internetverbindungen überwiegend verschlüsselte

☐ Voice-over-IP-Kommunikation

☐ HTTPS-Kommunikation

Die hierfür eingesetzte Software verschlüsselt die Daten vor der Übertragung, so dass eine „herkömmliche“ TKÜ-Maßnahme keine verwendbaren Daten erbringen würde.
Für die technische Umsetzung der Überwachungsmaßnahme ist es daher zwingend erforderlich, die unverschlüsselten Daten vor der Kryptierung aufzuzeichnen, zu übertragen oder auf andere Art und Weise auszuleiten bzw. auszulesen.

Auch wenn zum Zeitpunkt der Verschlüsselung der Kommunikationsvorgang möglicherweise noch nicht begonnen hat, ist diese als Vorstufe dem Kommunikationsvorgang zuzurechnen, weshalb der Weg für eine Anordnung nach § 100a StPO eröffnet ist (LG Landshut Beschl. v. 20.1.2011 – Az 4 Qs346/10; LG Hamburg Beschl. v. 31.8.2010 – Az 608 Qs 17/10; AG Bayreuth MMR 2010, 266; Meyer-Goßner § 100a Rn 7a; BeckOK-StPO/Graf StPO § 100a Rn 114; KK-StPO/Nack, 6. Aufl., StPO § 100a Rn 27; KMR/Bär StPO § 100a Rn 30).

Die notwendige Installation einer Software auf dem Rechner des Betroffenen, um die noch unverschlüsselten Daten an die Strafverfolgungsbehörden ausleiten zu können, ist als Begleitmaßnahme zur Umsetzung der Überwachung gemäß § 100a Abs. 1 StPO im Wege der Annexkompetenz zulässig, weil andere mildere Mittel nicht zur Verfügung stehen (vgl. BGHSt 46, 266, 273).
Die Überwachungsmaßnahme beschränkt sich nur auf Daten eines laufenden Telekommunikationsvorgangs; sonstige Zugriffe auf dem Rechner des Beschuldigten gespeicherte Daten sind unzulässig, so dass keine Online-Durchsuchung vorliegt (vgl. dazu BVerfG NJW 2008, 822,826). Durch die im Tenor aufgeführten Einschränkungen wird gewährleistet, dass mit der Erweiterung der Maßnahme nur Daten einer aktuellen Telekommunikation erfasst und übertragen werden.

Eine vorherige Anhörung des Beschuldigten unterbleibt, da sie den Ermittlungszweck gefährden würde, § 33 Abs. 4 S. 1 Strafprozessordnung.

Anlage 6
Muster für Beschlagnahme bzgl. E-Mail-Postfach gem. § 99 StPO

Urschriftlich mit Akten
dem Amtsgericht – Ermittlungsrichter/in –
in …
unter Hinweis insbesondere auf Bl. … d.A.

mit dem Antrag, einen Beschluss gem. § 99 StPO gem. anliegendem Entwurf zu erlassen:

Beschluss

In dem Ermittlungsverfahren
gegen
wegen

wird
gem. §§ 99, 100 Abs. 1, Abs. 3 S. 2, 162 StPO

für das elektronische Postfach des Beschuldigten: (e-mail-Adresse)

bei dem Provider:

für die Dauer von 3 Monaten die Beschlagnahme aller in dem elektronischen Postfach gespeicherten Nachrichten inklusive der Nachrichtenanhänge, insbesondere auch der noch nicht endgültig gelöschten Nachrichten sowie der noch nicht abgesendeten Nachrichtenentwürfe, angeordnet.

Das Postfach ist in Intervallen von Tagen / Wochen zu sichern und auszuleiten.

Die Maßnahme wird dem Anschlussinhaber derzeit wegen einer Gefährdung des Untersuchungszwecks nicht mitgeteilt (§ 101 Abs. 5 Satz 1 StPO).

Die Durchsicht der vom Provider übermittelten Nachrichten wird gem. § 100 Abs. 3 S. 2 StPO der Staatsanwaltschaft übertragen.

Gründe: …

Eine vorherige Anhörung des Beschuldigten unterbleibt, da sie den Ermittlungszweck gefährden würde, § 33 Abs. 4 S. 1 Strafprozessordnung.

Anlage 7
Muster für staatsanwaltschaftliche oder polizeiliche Anordnung nach § 100h StPO

In dem Ermittlungsverfahren

gegen Unbekannt
wegen des Verdachts

wird gemäß § 100h Abs. 1 Ziff. 2 StPO der Einsatz technischer Mittel zu Observationszwecken bezüglich der nichtidentifizierten Nutzer der E-Mail-Adressen / Nicknames

[…]

die über Torchat oder E-Mail kommunizieren, angeordnet.

Mit der Durchführung der Maßnahme wird [*Polizeidienstelle/IT-Dienststelle*] beauftragt.

Gründe:

Die noch nicht identifizierten Beschuldigten sind verdächtig, […].

Hierbei handelt es sich um Straftaten von auch im Einzelfall erheblicher Bedeutung gemäß §§ […] StGB.

Der geschilderte Tatverdacht ergibt sich aus den Ermittlungen der/des […].

Der Einsatz von verdeckten Empfangsbestätigungsdiensten als technische Mittel zur Täterermittlung ist auf Grundlage des § 100h Abs. 1 Nr. 2 StPO zulässig (vgl. Meyer-Goßner, StPO, 54. Aufl. 2011, § 100h Rdnr. 2 m.w.N.).

Ohne die getroffene Anordnung wäre die weitere Erforschung des Sachverhalts und die Identifizierung der noch nicht identifizierten Täter, die äußerst konspirativ agieren und sich nur unter Pseudonymen sowie unter Verwendung von Anonymisierungsdiensten zur Verschleierung ihrer IP-Adressen austauschen, aussichtslos bzw. wesentlich erschwert.

[…]
Name, Amtsbezeichnung

Anlage 8
Muster für Skype-Tracking gem. § 100g StPO

Beschluss

In dem Ermittlungsverfahren gegen
wegen des Verdachts

wird auf Antrag der Staatsanwaltschaft gemäß § 100g StPO angeordnet, dass TK-Verkehrsdaten in Echtzeit und unter Einsatz technischer Mittel für folgende

1. Kennung:
2. Kennung:
3. Kennung:

[…]

im Zeitraum von ____ bis ____ erhoben werden.

Die Maßnahme(n) werden dem/den Anschlussinhaber(n) und -nutzer(n) derzeit wegen einer Gefährdung des Untersuchungszwecks nicht mitgeteilt (§ 101 Abs. 5 Satz 1 StPO).

Gründe:
Die bisher nicht ermittelten Nutzer mit den Kennungen […] stehen im Verdacht […] begangen zu haben.

Es besteht daher der Verdacht einer Straftat gemäß § […] StGB.
Sie waren jeweils Nutzer der o.g. Skype-Accounts.
Diese Maßnahme ist unerlässlich, weil die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Die Zuständigkeit des Amtsgerichts […] ergibt sich aus § 162 Abs. 1 S. 2 StPO.
Eine vorherige Anhörung des Beschuldigten unterbleibt, da sie den Ermittlungszweck gefährden würde, § 33 Abs.4 S. 1 Strafprozessordnung.

Richter/in am Amtsgericht

Anlage 9
Muster für Durchsuchungsbeschluss beim Beschuldigten gem. § 102 StPO

Urschriftlich mit Akten
dem Amtsgericht – Ermittlungsrichter/in –
in …
unter Hinweis insbesondere auf Bl. … d.A.

mit dem Antrag, einen Beschluss gem. § 102 StPO gem. anliegendem Entwurf zu erlassen:

Beschluss

In dem Ermittlungsverfahren

gegen

wegen

wird gemäß § 102 StPO die Durchsuchung der Wohnung mit allen Nebenräumen, eventuell vorhandener Geschäftsräume und des sonstigen umfriedeten Besitztums des Beschuldigten sowie seiner Person und der ihm gehörenden bzw. von ihm genutzten Sachen (einschließlich Kraftfahrzeugen) angeordnet, weil aufgrund von Tatsachen zu vermuten ist, dass die Durchsuchung zur Auffindung von Beweismitteln, nämlich insbesondere

☐ **Computer (Desktop, Laptop, Notebook, Tablet)**
☐ **nebst Monitor, Tastatur, Maus und Verkabelung sowie Modem und Router, welche zur Tatplanung und -durchführung verwendet wurden,**
☐ **internetfähige Mobiltelefone nebst Zubehör (Ladegerät, Dockingstation), welche zur Tatplanung und -durchführung verwendet wurden**
☐ **Speichermedien (Externe Festplatten, USB-Sticks, Speicherkarten, CD/DVD/Blu-ray)**
☐ **internetfähige Spielekonsolen (z.B. X-Box, Playstation, Nintendo Wii)**
☐ **internetfähige Multimediaplayer (z.B. TV oder Multimediabox mit Internetzugang)**
☐ **Kontounterlagen / UKash-/Paysafecard-Nummern**
☐ **Unterlagen/Notizzettel mit Passwörtern und Hinweisen auf externe Datenspeicher im Internet oder E-Mailpostfächer etc.**

führen wird.

Zusatz bei Nachtzeitdurchsuchung:
Die Durchsuchung ist zur Nachtzeit zulässig, § 104 StPO.

Gründe:

…

Verbrechen / Vergehen, strafbar gemäß

Der Tatverdacht beruht auf ...

Beispiel für mögliche Begründung einer Durchsuchung zur Nachtzeit:

Aus früheren Durchsuchungsmaßnahmen bei dem Beschuldigten in vorangegangenen Ermittlungsverfahren ist bekannt, dass er seine PCs und Datenträger vollständig verschlüsselt. Für eine erfolgreiche Auswertung der im Rahmen der Durchsuchung sicherzustellenden Beweismittel ist es daher ausschlaggebend, den Beschuldigten unmittelbar vor laufendem Rechner zu einem Zeitpunkt aufzugreifen, an dem die ansonsten verschlüsselten Datencontainer geöffnet sind und damit entschlüsselt vorliegen. Sollte der Rechner zum Zeitpunkt des Zugriffs außer Betrieb sein, besteht die Gefahr, dass die Rechner und Datenträger trotz moderner IT-Forensik aufgrund von nicht zu überwindender Verschlüsselungstechnik nicht ausgewertet werden können.
Gegenwärtig hat der Beschuldigte einen außerordentlich unsteten Tagesablauf. Er schläft morgens meist sehr lange und ist dafür nachts lange wach. Häufig geht er erst nach 21 Uhr an seinen PC, so dass sich im Rahmen der Umsetzung des Durchsuchungsbeschlusses die Notwendigkeit eines Zugriffs zur Nachtzeit ergeben kann. Bei einem längerfristigen bzw. wiederholten Aufstellen der polizeilichen Zugriffskräfte ist eine Entdeckung durch den Beschuldigten oder ihm nahestehende Personen zu befürchten. Somit wäre der Durchsuchungszweck gefährdet.

Eine vorherige Anhörung des Beschuldigten unterbleibt, da sie den Ermittlungszweck gefährden würde, § 33 Abs. 4 S. 1 StPO.

Anlage 10
Muster für Ersuchen Vollstreckung Durchsuchungsbeschluss

Vfg.

1. ☐ _____

2. WVl. _____

3. Urschriftlich mit ___ Bd. Akten ☐ und ___ Bd. Beiakten ☐ Anlagen:_____

   dem / der

   Regionalen Kriminalinspektion / Kriminalkommissariat

   in <Ort>

   übersandt mit dem Ersuchen, den Beschluß Bl. <Seitenzahl des DS-Beschlusses>zu vollstrecken.

   Sofern dem Durchsuchungszweck entsprechende Gegenstände aufgefunden werden, sind diese **vorläufig sicherzustellen** und nicht zu beschlagnahmen. Auch in dem Falle, dass der Beschuldigte Widerspruch gegen die vorläufige Sicherstellung erhebt, ist **keine Beschlagnahme** auszusprechen sondern die Akte hier vorzulegen, damit die richterliche Bestätigung der vorläufigen Sicherstellung beantragt werden kann
   Die Notwendigkeit dieser Vorgehensweise ergibt sich aus § 110 Abs. 3 StPO. Solange die in § 110 StPO angesprochenen „Papiere", zu denen auch Speichermedien gezählt werden, noch nicht beschlagnahmt wurden, dauert die Durchsuchung an. Solange dies der Fall ist, besteht nach § 110 Abs. 3 StPO die Möglichkeit, auf externe Datenspeicher (bspw. Email-Postfächer, aber auch anderer externer Speicherplatz) ohne die Einholung weiterer Beschlüsse oder die Zustimmung des Beschuldigten zuzugreifen.
   Diese Möglichkeit ist nach erklärter Beschlagnahme ausgeschlossen.

   ☐ Den Durchsuchungstermin bitte ich mit mir fernmündlich abzusprechen.

   ☐ Von der Wohnung sind Lichtbilder zu fertigen.

   ☐ Die erfolgte Durchsuchung bitte ich mir
   ☐ fernmündlich ☐ unter Aktenvorlage ☐ schriftlich
   zu melden.

   ☐ Eine Entscheidung, ob und wie die ggf. sichergestellten Beweismittel auszuwerten sind, wird von mir nach erfolgter Durchsuchung getroffen.

   ☐ Mit der Auswertung der ggf. sichergestellten Beweismittel soll anschließend ein externer Sachverständiger beauftragt werden.

   ☐ Mit der Auswertung der ggf. sichergestellten Beweismittel soll ein polizeilicher Sachverständiger beauftragt werden. Es wird um die namentliche Benennung des Sachverständigen gebeten. Hierzu ergeht ein gesonderter Auswertungsauftrag.

   ☐ Die Beweismittel sind zunächst auf der dortigen Dienststelle zu verwahren.

   ☐ Die ggf. sichergestellten Beweismittel sind mit den Akten nach hier zu übersenden.

☐ Besch. ist / sind verantwortlich zu vernehmen.

<Name>
<Dienstbezeichnung>

Anlage 11
Muster Nachweis über vorläufig sichergestellte Speichermedien

Polizeipräsidium
Kriminaldirektion

ZK50 Internet- und Computerkriminalität

VNr.

LÜ-Nummer (wird von der StA eingetragen)

Staatsanwaltschaft

Geschäftsnummer der Staatsanwaltschaft

Sachbearbeiter
Telefon
Fax

Nachweis über vorläufig sichergestellte Speichermedien

In der Strafsache
gegen
wegen Verdachts der/des
wurden am in bei
die nachstehend aufgeführten Speichermedien gem. § 110 StPO vorläufig sichergestellt

1. Verzeichnis (Fortsetzung auf weiterem Vordruck, wenn Platz nicht ausreicht)

Lfd. Nr.	Anzahl	Bezeichnung der Speichermedien	Mutmaßliche/r Eigentümer(in)/Fundort	Erledigungsvermerk

Ort, Datum, Name, Amtsbezeichnung, Dienststelle, Unterschrift(en) der amtshandelnden Person(en)

Nachweis erhalten:

Datum, Unterschrift (Betroffene / Zeugen)

2.

Eintragung in das Asservatenbuch vornehmen	Nr. des Asservatenbuches	Lfd.-Nr im Asservatenbuch	Handzeichen und Datum

Rechtsbehelfsbelehrung:
Die betroffene Person kann gegen eine vorläufige Sicherstellung, die gemäß § 102 i. V. m. § 110 StPO erfolgt ist, bei dem Amtsgericht in dessen Bezirk die vorläufige Sicherstellung stattgefunden hat, die richterliche Entscheidung entspr. § 98 II 2 StPO beantragen.

Vermerk für den polizeilichen Sachbearbeiter:
Weder die Abwesenheit noch ein Widerspruch des Betroffenen macht eine Beschlagnahme der Speichermedien gem. § 98 II 1 StPO erforderlich.

Anlage 12
Muster für Antrag auf richterliche Bestätigung analog § 98 Abs. 2 Satz 2 StPO

Vfg.

1. WV

2. U.m.A. dem Amtsgericht
- Ermittlungsrichter -
in <Ort>

übersandt unter Hinweis auf Bl. <Seitenzahl Beschwerde> d. A. übersandt mit dem Antrag,

entsprechend § 98 Abs 2 S 2 StPO die vorläufige Sicherstellung <der/des> <Bezeichnung Asservat> richterlich zu bestätigen.

<Der / Die> Datenträger wurden vorläufig sichergestellt zum Zwecke der Durchsicht i.S.d. § 110 StPO. Als Papiere sind insoweit auch alle elektronischen Datenträger und Datenspeicher anzusehen (vgl. Meyer-Goßner, 54. Auflage § 110 Rn. 1 m.w.N.) Die vorläufige Sicherstellung stellt noch keine Beschlagnahme dar, sie dient vielmehr vorbereitend dazu, mögliche Beschlagnahmegegenstände aus dem bei der Durchsuchung vorgefundenen Material auszusondern (BVerfG 18.12.2002, 2 BvR 1910/02; BVerfG NJW 2003, 2669). Da die Durchsicht auf die Staatsanwaltschaft bzw. ihre Ermittlungspersonen übertragen ist, ist die entsprechende Anwendung des § 98 Abs. 2 S.2 StPO auf diese Maßnahme angebracht (BVerfG NStZ 2002, 377; NJW 2003, 2669; BGH CR 1999, 292; BGH NStZ 2003, 670; Fischer, § 110 Rn 10; K/K § 110 Rn 9). <Die / Der> vorläufig sichergestellte <Bezeichnung Asservat> wird nunmehr dahingehend ausgewertet, ob <er / sie> Beweismittel in hiesigem Verfahren <ist/sind>.

<Name>
<Dienstbezeichnung>

Anlage 13
Muster für ein staatsanwaltschaftliches Herausgabeverlangen nach § 95 StPO

Ermittlungsverfahren

gegen

wegen

Sehr geehrte Damen und Herren,

in dem vorbezeichneten Ermittlungsverfahren ist die Herausgabe von Beweismitteln durch Ihr Unternehmen erforderlich.

Gemäß § 95 Abs. 1 StPO verpflichte ich Sie zur Auslieferung folgender Gegenstände:

Datenträger (Festplatten) mit sämtlichen Daten zu den Servern mit der

IP-Adresse XXX (Root Server XXX / http:// XXX)

Die Datenträger kommen als Beweismittel für die Untersuchung in Betracht (§ 94 StPO).

Sie haben die Datenträger an die dieses Ersuchen überbringenden Kriminalbeamten der/des <*Einsetzen zust. Kripo-Dienststelle*> zu übergeben bzw. die Spiegelung der Datenträger (1:1-Backup) durch die Beamten zu ermöglichen.

Die Erfüllung des o. g. Herausgabeverlangens dient der Abwendung von Durchsuchungs- bzw. Beschlagnahmemaßnahmen. Nur höchst vorsorglich weise ich darauf hin, dass Zeugen gesetzlich verpflichtet sind, auf Ladung vor der Staatsanwaltschaft zu erscheinen und zur Sache auszusagen (§ 161a Absatz 1 StPO). Wer einen als Beweismittel in Betracht kommenden Gegenstand in seinem Gewahrsam hat, ist verpflichtet, ihn auf Erfordern vorzulegen und auszuliefern (§ 95 Absatz 1 StPO).

Die §§ 94 ff. StPO erlauben die Sicherstellung und Beschlagnahme von Datenträgern und den hierauf gespeicherten Daten als Beweisgegenstände im Strafverfahren. Die einschlägigen Eingriffsbefugnisse sind zwar ursprünglich auf körperliche Gegenstände zugeschnitten. Der historische Gesetzgeber, der die überkommenen Normen über die Beschlagnahme geschaffen hat, konnte noch nicht mit der Möglichkeit rechnen, dass elektronische Daten als nichtkörperliche Informationen für die Beweisführung im Strafverfahren Bedeutung erlangen könnten. §§ 94 ff. StPO erlauben auch die Sicherstellung von Daten auf behördeneigenen Datenträgern. Der Wortsinn gestattet es, als "Gegenstand" des Zugriffs auch nichtkörperliche Gegenstände zu verstehen. Der Wortlaut wird durch die Annahme, auch unkörperliche Gegenstände seien von §§ 94 ff. StPO erfasst, schon im Hinblick auf die Unterscheidung gegenüber dem engeren Begriff der (körperlichen) Sache nicht überschritten (vgl. BVerfG NJW 2005, 1917-1923).

Die Auslegung von § 95 Abs. 1 StPO i.V.m. § 94 Abs. 1 StPO, wonach sich das Herausgabeverlangen auch auf einen Beweisgegenstand beziehen kann, der nicht bereits vorhanden ist, sondern erst aufgrund des Herausgabeverlangens geschaffen werden muss (hier: durch Zusammenstellung von Einzeldaten nach konkreten Kriterien aus einem Gesamtdatenbestand), überschreitet nicht die Wortlautgrenze des § 95 StPO. Sie ist auch nicht willkürlich, da sie gegenüber der Beschlagnahme des Gesamtdatenbestandes das mildere Mittel darstellt (vgl. BVerfG NStZ-RR 2003, 176-177).

Beide Verpflichtungen können mit Zwangsmitteln durchgesetzt werden und sind nicht von einem entsprechenden Gerichtsbeschluss abhängig.

Insbesondere ist kein Gerichtsbeschluss nach § 100g StPO erforderlich, da Ihr Unternehmen kein Telekommunikationsdienstleister nach dem TKG ist und die Daten keine zukünftigen Telekommunikationsvorgänge betreffen (§ 100g Abs. 3 StPO).

Für den Fall der Verweigerung der Herausgabe der Beweismittel drohe ich vorsorglich bereits jetzt die Verhängung eines Zwangsgeldes in Höhe von bis zu 1.000,- Euro an.

Für Ihre Aufwendungen werden Sie gemäß § 23 Abs. 2 JVEG entschädigt.

Von der Benachrichtigung Ihrer Kundschaft über das vorliegende Verlangen oder allgemein über die Existenz eines Ermittlungsverfahrens ist abzusehen, da dies ein strafrechtlich relevantes Verhalten (z.B. Strafvereitelung, Begünstigung oder Beihilfe zu einer Straftat) darstellen kann.

Mit freundlichen Grüßen

Name, Amtsbezeichnung

Anlage 14
Muster für staatsanwaltschaftliche Zustimmung zum VE-Einsatz bei nicht bestimmten Beschuldigten und nicht Betreten von Wohnungen gem. § 110b I StPO

In dem Ermittlungsverfahren gegen wegen

wird entsprechend dem gemeinsamen Runderlass des Hessischen Ministeriums für Inneres und für Sport und des Hessischen Ministeriums der Justiz, für Integration und Europa vom 30.12.2009

dem Einsatz eines Verdeckten Ermittlers gem.
☐ **§§ 110a Abs. 1, S. 1 ☐ Nr. 1, ☐ Nr. 2, ☐ Nr. 3, ☐ Nr. 4, 110b Abs. 1 StPO**
☐ **§§ 110a Abs. 1, S. 2, 110b Abs. 1 StPO**
☐ **§§ 110a Abs. 1, S. 4, 110b Abs. 1 StPO**
für einen Zeitraum von Monaten zugestimmt.

Nach den bisherigen Erkenntnissen <Sachverhaltsschilderung>.
Bspw.: Nach den bisherigen Erkenntnissen gründete der Beschuldigte Anfang März 2012 zum Zweck des Austauschs kinderpornographischer Dateien ein Pädophilen-Board und administriert dieses seither. Es besteht weiter der Verdacht, dass der Beschuldigte innerhalb dieses Boards eine Dating-Seite installiert hat, die dem ausdrücklichen Ziel dient, Realtrefferi der Beteiligten zwecks Austauschs kinderpornographischer Dateien aber auch zum Zweck der Durchführung von sexuellen Handlungen an Kindern zu verabreden und durchzuführen.

Diese Handlungen sind mit Strafe bedroht gemäß §§ <Strafvorschriften>.

Der Tatverdacht beruht auf <Beweismittel>.

☐ Es handelt sich um Straftaten von auch im Einzelfall erheblicher Bedeutung
☐ auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung.
☐ auf dem Gebiet des Staatsschutzes (§§ 74a, 120 des Gerichtsverfassungsgesetzes).
☐ die gewerbs- oder gewohnheitsmäßig begangen worden ist.
☐ die von einem Bandenmitglied oder in anderer Weise organisiert begangen worden ist.

☐ Es handelt sich um ein Verbrechen, bei dem aufgrund bestimmter Tatsachen die Gefahr der Wiederholung besteht und die Aufklärung auf andere Weise aussichtslos oder wesentlich erschwert wäre.

☐ Es handelt sich um ein Verbrechen, bei dem der Einsatz eines Verdeckten Ermittlers aufgrund der besonderen Bedeutung der Tat geboten ist und andere Maßnahmen aussichtslos wären.

☐ Aufgrund der bestehenden Hinweise darauf, dass <Ausführungen zur Erforderlichkeit>, ist der zeitlich befristete Einsatz eines Verdeckten Ermittlers zur umfassenden Sachverhaltsaufklärung erforderlich.

< Tatsächliche Ausführungen dazu, warum vorgenannte Voraussetzungen gegeben sind.>
Bspw.:
Das Board und die Dating-Seite liegen im TOR-Netzwerk, sodass keine Real-IP-Adressen gewonnen werden können. Die individuelle Kommunikation zwischen den Mitgliedern erfolgt durch Nutzung von TOR-Chats, von TOR-Private-Messages oder über E-mail-Adressen bei TORMAIL.NET, sodass auch insoweit erfolgversprechende Ermittlungsansätze nicht vorhanden

sind. Es besteht die Gefahr der Fortsetzung des schweren sexuellen Missbrauchs, da die Nutzer durch das Board animiert werden, sich zur Durchführung sexuellen Missbrauchs zu treffen.

Name
Dienstbezeichnung

Anlage 15
Muster für gerichtlichen Beschluss für einen VE-Einsatz bei einem bestimmten Beschuldigten oder Betreten von Wohnungen gem. § 110b II StPO

Urschriftlich mit Akten
dem Amtsgericht – Ermittlungsrichter/in –
in …
unter Hinweis insbesondere auf Bl. … d.A.

mit dem Antrag, einen Beschluss gem. anliegendem Entwurf zu erlassen

Beschluss

In dem Ermittlungsverfahren

gegen

wegen

wird dem Einsatz eines verdeckten Ermittlers gemäß
☐ §§ 110a Abs. 1, S. 1 ☐ Nr. 1, ☐ Nr. 2, ☐ Nr. 3, ☐ Nr. 4, 110b Abs. 1, Abs. 2 ☐ Nr. 1, ☐ Nr. 2 StPO
☐ §§ 110a Abs. 1, S. 2, 110b Abs. 1, Abs. 2 ☐ Nr. 1, ☐ Nr. 2 StPO
☐ §§ 110a Abs. 1, S. 4, 110b Abs. 1, Abs. 2 ☐ Nr. 1, ☐ Nr. 2 StPO

zugestimmt.

Die Maßnahme wird bis zum <Datum> befristet.

Gründe:

Der Beschuldigte ist verdächtig, <Tatverdacht>.

Diese Handlungen sind mit Strafe bedroht gemäß §§ <Strafvorschriften>.

Der Tatverdacht beruht auf <Beweismittel>.

☐ Es handelt sich um Straftaten von auch im Einzelfall erheblicher Bedeutung
☐ auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung.
☐ auf dem Gebiet des Staatsschutzes (§§ 74a, 120 des Gerichtsverfassungsgesetzes).
☐ die gewerbs- oder gewohnheitsmäßig begangen worden ist.
☐ die von einem Bandenmitglied oder in anderer Weise organisiert begangen worden ist.

☐ Es handelt sich um ein Verbrechen, bei dem aufgrund bestimmter Tatsachen die Gefahr der Wiederholung besteht und die Aufklärung auf andere Weise aussichtslos oder wesentlich erschwert wäre.

☐ Es handelt sich um ein Verbrechen, bei dem der Einsatz eines Verdeckten Ermittlers aufgrund der besonderen Bedeutung der Tat geboten ist und andere Maßnahmen aussichtslos wären.

☐ Aufgrund der bestehenden Hinweise darauf, dass <Ausführungen zur Erforderlichkeit>,

ist der zeitlich befristete Einsatz eines Verdeckten Ermittlers zur umfassenden Sachverhaltsaufklärung erforderlich.

Eine vorherige Anhörung des Beschuldigten unterbleibt, da sie den Ermittlungszweck gefährden würde, § 33 Abs. 4 S. 1 StPO.

Richter/in am Amtsgericht

Anlage 16
Muster für englischsprachiges Auskunftsersuchen in die USA

Anschrift Telemediendienst

Official request concerning sections <14,15 Telemedia Act oder section 113 Telecommunications Act>, section 161 / 163 German Code of Criminal Procedure

Dear Sir or Madam,

The XXX (Ort) Police Office is currently investigating on behalf of the Public Prosecutor´s office (file number <Az.>) in (Ort), concerning a case of <Straftatbez. auf englisch, z.B. fraud, ransom etc.>.

According to sections **<14,15 Telemedia Act oder 113 Telecommunications Act>**, section 161 / 163 German Code of Criminal Procedure, I am kindly asking for submission of subscriber data and IP-history that are related to the <Anzahl Accounts> following email-accounts which are used by the perpetrator:

- **<Email-Adresse>**
- **<Email-Adresse>**
- **<Email-Adresse>**
- **<Email-Adresse>**

Please send any information regarding this request to the following email-address:

<Email-Adresse>

of the competent department of the XXX (Ort) Police Office

If you do have any additional questions, do not hesitate to contact the case officers (<Email-Adresse(n) polizeil. Sachbearbeiter>)

Please do not contact the user.

Thank you for your cooperation in advance.
Kind regards

[…]
Name
Public Prosecutor/detective
at the Public Prosecutor's Office XXX/ XXX police office

Anlage 17
Muster für englischsprachiges Auskunftsersuchen an Facebook

Facebook
Attn: Security Department / Custodian of Records
18 Hacker Way
Menlo Park, CA 94025

records@facebook.com

Suppression of international cybercrime
here: Request concerning sections 14, 15 Telemedia Act , section 95 Code of Criminal Procedure (StPO)

Dear Sir or Madam,

The local police in xxx / Germany is currently investigating concerning xxx (Straftatbez. auf englisch)

(Within this context…./evtl. Näheres zu den gewünschten Informationen)

Within the ongoing investigation the facebook-account, holding the user ID

1234567890

using the name

XXX (http://www.facebook.com/xxx)

appeared.

According to section 15, section 14 Telemedia Act (TMG), section 95 Code of Criminal Procedure (StPO) we are kindly asking for submission of the

basic subscriber data including IP-history of the last 90 days regarding the a/m account.

Please do not contact the user.

(Hier noch mitteilen, ob der Account gesperrt werden darf oder ob dieses Vorgehen die Ermittlungen gefährden würde)

If you do have any additional questions do not hesitate to give us a call or write an email to xxx. Please send any information regarding this request to xxx

Thank you very much for your co-operations.

Kind Regards

“Name”
“Amtsbez. auf englisch”