Durchsuchung, Beschlagnahme, Telekommunikationsüberwachung und Online-Durchsuchung im Strafverfahren und im Bereich der Gefahrenabwehr

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Seminar „Open Source Intelligence (OSINT)“

Bund Deutscher Kriminalbeamter – KRIPO-Akademie

Dienstag, 11. August 2015

Prof. Dr. iur. Frank Czerner

Historisch-kriminalistische Bedeutung dieses Tagungsortes: Am Galgenberg

http://www.google.de/imgres?imgurl=http%3A%2F%2Fwww.chlab.net%2Fontour%2Fmittweida%2Fmw%2F41_P7247351.jpg&imgrefurl=http%3A%2F%2Fwww.chlab.net%2Fontour%2Fmittweida%2Fmw%2F41_P7247351.html&h=525&w=700&tbnid=muxxaerzVLtUzM%3A&zoom=1&docid=lw7jXF4_wSLqTM&itg=1&ei=8PiMU7fzOYPe7AaQnoDoDA&tbm=isch&client=firefox-a&ved=0CFkQrQMwAQ

Polizei erlangt Informationen: Strafverfolgung oder Gefahrenabwehr?

- Liegt überhaupt eine **strafbare Handlung** vor / ggf. schon strafbares Vorbereitungs- bzw. Versuchsstadium?
- Sind Ermittlungsmaß-nahmen nach der StPO zulässig oder geht es primär um **geplante Straftaten**?

http://media1.faz.net/ppmedia/aktuell/sport/3886100968/1.563463/default/fans-im-fanblock-unter-ganz-genauer-beobachtung-der-polizei.jpg

Legalitätsprinzip: §§ 152 II, 160 I, 163 StPO

§ 152 StPO:

(1) Zur Erhebung der öffentlichen Klage ist die Staatsanwaltschaft berufen.

(2) *Sie* ist, soweit nicht gesetzlich ein anderes bestimmt ist, verpflichtet, wegen aller verfolgbaren Straftaten einzuschreiten, sofern ***zureichende tatsächliche Anhaltspunkte*** vorliegen.

§ 160 StPO: Pflicht zur Sachverhaltsaufklärung

(1) Sobald die Staatsanwaltschaft durch eine Anzeige oder auf anderem Wege von dem Verdacht einer Straftat Kenntnis erhält, hat sie zu ihrer Entschließung darüber, ob die öffentliche Klage zu erheben ist, den Sachverhalt zu erforschen.

(2) Die Staatsanwaltschaft hat nicht nur die zur Belastung, sondern *auch die zur Entlastung* dienenden Umstände zu ermitteln und für die *Erhebung der Beweise Sorge zu tragen*, deren Verlust zu besorgen ist.

§ 163 Aufgaben der Polizei im Ermittlungsverfahren

(1) Die Behörden und Beamten des Polizeidienstes haben Straftaten zu erforschen und alle keinen Aufschub gestattenden Anordnungen zu treffen, um die Verdunkelung der Sache zu verhüten. […].

Im Anfang …

...war ein Verdacht

Anfangsverdacht

„zureichende tatsächliche Anhaltspunkte“

= Möglichkeit der Tatbegehung

> Genügt für Beschlagnahme (eines Rechners, Festplatte etc.), § 94 StPO

und für Zulässigkeit einer TKÜ, § 100a StPO – *mit„qualifiziertem* Anfangsverdacht“ (II)

Hinreichender Tatverdacht

= Verurteilungswahrscheinlichkeit

Dringender Tatverdacht

= Sehr hohe Wahrscheinlichkeit der Tatbegehung

Strafverfolgung: Legalitätsprinzip, §§ 152 II, 160 I, 163 StPO

Politisch ausgehöhlter Verfolgungszwang durch gezielte Einflussnahme in laufendes Ermittlungsverfahren durch Justizminister Heiko Maas gegenüber Generalbundesanwalt Harald Range (04.08.2015)?

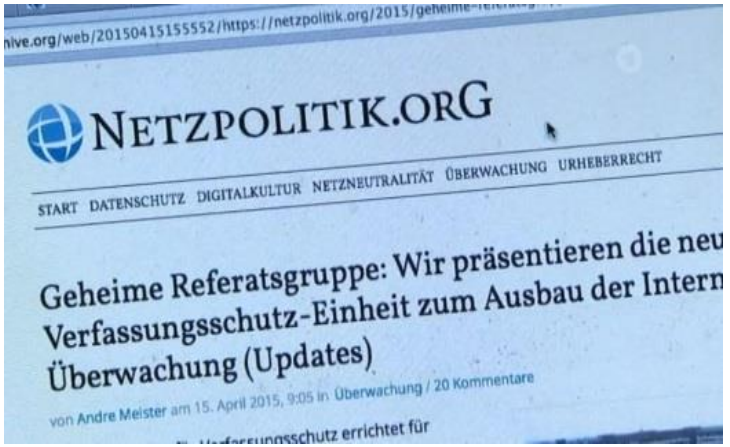
http://www.thueringer-allgemeine.de/startseite/detail/-/specific/Weimarer-Rechtsanwalt-ueber-Streits-zwischen-Range-und-Maas-1951248295; http://www.tagesspiegel.de/politik/netzpolitik-affaere-harald-range-musste-gehen-jetzt-mit-hans-georg-maassen/12142926.html

Legalitätsprinzip und Staatsschutz

Der „Fall“:

Berichte des Blogs Netzpolitik.org über Einrichtung einer Referatsgruppe 3C „Erweiterte Fachunterstützung Internet und über Pläne des Verfassungsschutzes, Online-Netzwerke stärker zu überwachen. Dazu stellten die Journalisten am 15.04. 2015 vertrauliche Unterlagen ins Netz. Der Verfassungsschutz erstattete daraufhin Anzeige. GenBA Range leitete ein Ermittlungsverfahren wegen Landesverrats gegen Netzpolitik.org ein, was u.a. eine Debatte über Pressefreiheit entfachte.

Die ARD berichtete bereits in 06/14 über die Pläne des Verfassungsschutzes und erwähnte einzelne Tätigkeiten (Internet- und Telefonüberwachung).
> Verfahrenseinstellung durch Generalbundesanwaltschaft (stellv. Generalbundesanwalt) am 10.08.2015 mangels „Staatsgeheimnisses“



Zur Klärung der Frage, ob die Veröffentlichung durch netzpolitik.org die Bekanntgabe von Staatsgeheimnissen darstellt, gab Range ein externes Gutachten (= Beweismittel in einem Strafverfahren) in Auftrag, dessen Fertigstellung vom BMJ gestoppt und der Gutachter zu entlassen sei – so Range.

http://www.thueringer-allgemeine.de/startseite/detail/-/specific/Weimarer-Rechtsanwalt-ueber-Streits-zwischen-Range-und-Maas-1951248295http://www.spiegel.de/politik/deutschland/heiko-maas-entlaesst-harald-range-a-1046724.htm;; http://www.daserste.de/information/politik-weltgeschehen/mittagsmagazin/videos/netzpolitik-org-102~_v-varxl_dbfa4c.jpg

Strafverfolgung: Legalitätsprinzip – politisch einschränkbar?

- **Offenbaren v. Staatsgeheimnissen, § 95 StGB:** Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, an einen Unbefugten gelangen läßt oder öffentlich bekanntmacht und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft, wenn die Tat nicht in § 94 mit Strafe bedroht ist.
- **Begriff des Staatsgeheimnisses, § 93 StGB:** (1) Staatsgeheimnisse sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheim gehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden.

- **Landesverrat, § 94 StGB**:

(1) Wer ein Staatsgeheimnis
1. einer fremden Macht oder einem ihrer Mittelsmänner mitteilt oder

2.sonst an einen Unbefugten gelangen läßt oder öffentlich bekanntmacht, *um* die Bundesrepublik Deutschland *zu benachteiligen* oder eine *fremde Macht zu begünstigen*,

und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland *herbeiführt*, wird mit Freiheitsstrafe nicht unter einem Jahr bestraft.

Ermittlungsmaßnahmen (StPO)

z.B.: - Vernehmungen

- Durchsuchung < > Beschlagnahme
- Überwachung der Telekommunikation
- Haftbefehl…

Zwar grds.: „Ermittlungs-Generalklausel“ für Polizei/ Staatsanwaltschaft für *allgemeine, unspezifische* Maßnahmen, aber:

> Grundsätzliches Problem bei diesen Maß-nahmen: **Grundrechtseingriffe**! > hierzu spezialgesetzliche Rechtsgrundlage erforderlich

Beschlagnahme von „Gegenständen“

http://www.pipeline.de/pipeline/showpics.php?id=10203464_l&rid=1
http://www.superbiene.de/wp-content/uploads/2014/09/Pa

http://www.fronline.de/image/view/3319378,1586676,dm
FlashTeaserRes,K%25C3%25BCchenmesser+%2
528media_654738%2529.jpg ; http://www.zdf.de/ZDF/zd
fportal/blob/28720494/2/data.jpg

Problem: Wo liegt der **Schwerpunkt** der polizeilichen Tätigkeit?

> ***Strafverfolgung*** / Repression > StPO, oder

> ***Gefahrenabwehr*** / Prävention > PolG/Länder

oder ggf. ***Doppelfunktionelle*** Maßnahmen??

StPO oder PolG??

§ 94 StPO: Beschlagnahme

[Sicherstellung und **Beschlagnahme** von Gegenständen zu **Beweiszwecken**]

(1) **Gegenstände**, die als Beweismittel für die Untersuchung von Bedeutung sein *können*, sind in Verwahrung zu nehmen oder in anderer Weise *sicherzustellen*. [≠ § 26 PolG-Sachsen]

(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der **Beschlagnahme**.

PolG-Sachsen: § 27, Beschlagnahme

(1) Die Polizei kann eine **Sache** beschlagnahmen, wenn dies erforderlich ist

1. zum Schutz eines Einzelnen oder des Gemeinwesens gegen eine unmittelbar bevorstehende Störung der öffentlichen Sicherheit oder Ordnung oder zur Beseitigung einer bereits eingetretenen Störung,

2. zur Verhinderung einer missbräuchlichen Verwendung durch eine Person, die nach diesem Gesetz oder nach anderen Rechtsvorschriften festgehalten oder in Gewahrsam genommen worden ist.

Ermittlungsmaßnahmen

§ 94 StPO: Beschlagnahme

[Sicherstellung und **Beschlagnahme** von Gegenständen zu **Beweis-zwecken**] – *Anfangsverdacht genügt*

(1) **Gegenstände**, die als Beweismittel für die Untersuchung von Bedeutung sein *können*, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.

(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der **Beschlagnahme**.

http://www.luna-park.de/wp-content/uploads/2015/04/Fotolia_64663828_XS.jpg

Beschlagnahmefähige „**Gegenstände**“ iSv § 94 StPO: Computer, Festplatten, CDs, DVDs, USB-Stick, Speicherkarten, Disketten, Smartphone (als Datenträger), sonstige „verkörperte Informationsspeicher“ - *auch **Daten** als solche??? (ustr.)*

… auch historisch …

Bayerisches Ausführungsgesetz

zur

Reichs-Strafprozeßordnung

vom

18. August 1879.

Mit Sachregister.

Augsburg, 1879.

Math. Rieger'sche Buchhandlung.

https://www.deutsche-digitale-bibliothek.de/binary/WTGZTTLROO7JEY5GBT4QDOMCCICTALMO/mvpr/1.jpg

Deutscher Bundestag **Drucksache 18/4621**

18. Wahlperiode 15.04.2015

Gesetzentwurf

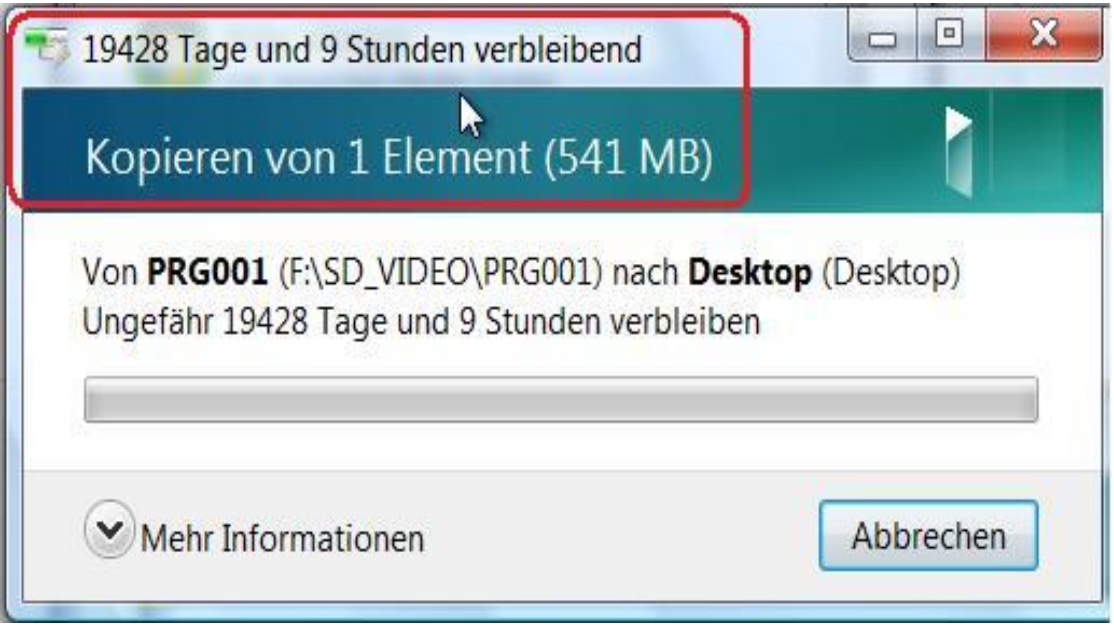
der Bundesregierung

Entwurf eines Gesetzes zur Stärkung der Opferrechte im Strafverfahren

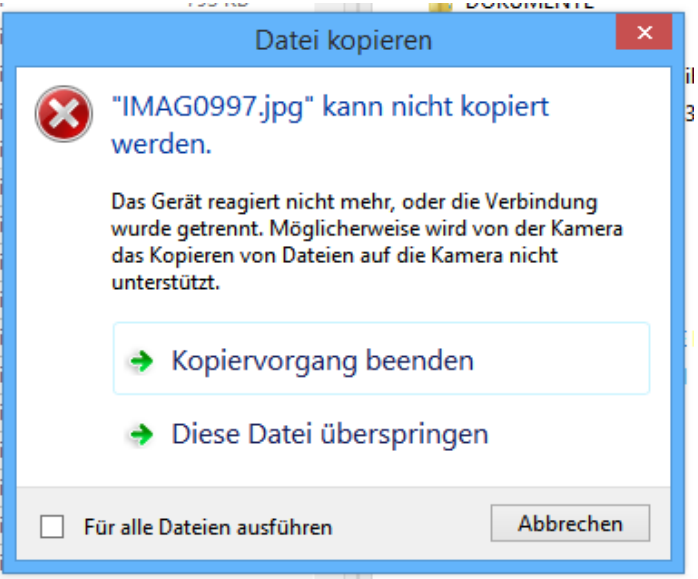
(3. Opferrechtsreformgesetz)

https://www.bundestag.de/blob/374650/c6ffdec80df8824d797a8d997d4fa5e0/gesetzentwurf-data.pdf

Kopieren von (allen??!) Daten??



http://www.drwindows.de/attachments/41633d1306344856-kopieren-der-daten-dauert-sehr-lange-kopieren.jpg;
http://www.android-hilfe.de/attachments/ashampoo_snap_2013-11-28_10h56m46s_001_datei-kopieren-png.263068/



Kopieren von Daten als *mildere* Maßnahme ggü. Beschlagnahme?

> Kopie ersetzt Beschlag-nahme (so Rspr.)

> wie erkennt man verfah-rensrelevante Daten?

> was ist überhaupt verfahrensrelevant?

> Problem des Verschlüs-selns, Verschleierns, Unsichtbarmachens oder Löschens verfahrens-relevanter Datenbestände

Suche nach Beweismaterial

http://polpix.sueddeutsche.com/bild/1.113481.1358229377/640x360/schweiz.jpg

Weiteres Problem, auch beim Kopieren:

- Beschränkung auf notwendigstes Material wegen Verhältnismäßigkeitsgrundsatz / Übermaßverbot
  > „Schutz des Kernbereichs der Persönlichkeit“ vor staatlichem Zugriff, auch über Menschenwürde abgesichert
- Verhältnismäßigkeit > Begrenzung auf verfahrensrelevantes Material,

> Begrenzung auf bestimmte Zeiträume, Personen, Suchbegriffe (– *aber welche??)* >> aus genannten Gründen problematisch
> andererseits: umfassende Ermittlungspflicht wegen § 244 StPO!!

Telekommunikationsüberwachung - TKÜ

http://www.telekommunikation.und-kosten.de/images/telekommunikation-kosten-003.jpg

§ 3 Nr. 22 TKG: "Telekommunikation" der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen;

§ 3 Nr. 23 TKG: "Telekommunikationsanlagen" technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können;…

Phasen des Datentransfers

- **Absenden der Mail / SMS** > Beginn eines dynamischen TKÜ-Prozesses gem. § 100a StPO, der auch bei >
- **Zwischenspeicherung** beim Provider andauert

> Bei offenem Zugriff auf Daten: § 94 StPO: Beschlagnahme der Daten, die ggü Mail-Provider angeordnet werden könne / nicht § 100a StPO, weil TKÜ-Prozess jetzt abgeschlossen ist [ustr.] und Durchsicht gem. § 110 StPO

> Bei verdecktem/heimlichem Zugriff auf Daten: „*fingierte*“ TKÜ-Maßnahme (obwohl TKÜ eigentlich hier [-]) ergebnisorientiert wg. erhöhtem Schutzbedarf (massiverer Grundrechtseingriff) oder über § 110 III StPO

> *Mindermeinung*: keine Eingriffsgrundlage und unzulässig/ keine Kumulierung von §§ 94, 100a StPO >> *massive Beeinträchtigung der Strafverfolgung*

- wenn Mail / SMS vom Empfänger **abgerufen / gelesen / gespeichert** wird, endet zwar TKÜ-Vorgang, aber: Vorgehen auch hier ustr.:
  > § 100a StPO greift noch immer wg. Schutzbedürfnis d. Betroffenen (h.M.)
  > nur § 94 StPO greife ein (bei dem schon ein Anfangsverdacht (!) genügt, da TKÜ beendet sei – Risiko der Umgehung der strengen TKÜ-Regularien durch gezieltes Abwarten und späteres Zugreifen

§ 100a StPO: [Telekommunikationsüberwachung]

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. *bestimmte Tatsachen* den *Verdacht* begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete *schwere Straftat* begangen, in Fällen, in denen der *Versuch strafbar* ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,

2. die Tat *auch im Einzelfall schwer wiegt* **und**

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten *auf andere Weise wesentlich erschwert oder aussichtslos* wäre. [>>>]

§ 100a StPO: [Telekommunikationsüberwachung]

(2) **Schwere Straftaten im Sinne des § 100 a Absatz 1 Nr. 1 StPO sind**: (= *numerus clausus!!!)*

1. aus dem Strafgesetzbuch:

a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80 bis 82 […]

e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, […]

f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b, 177 Abs. 2 Nr. 2 [….]

g) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften nach § 184b Abs. 1 bis 3 […]

h) Mord und Totschlag nach den §§ 211 und 212,

i) Straftaten gegen die persönliche Freiheit nach den §§ 232 bis 233a, 234, 234a, 239a und 239b,

j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244a,

k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,

l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,

m) Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 und 4,

n) Betrug und Computerbetrug […]

s) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 […], des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316c […]

2. aus der Abgabenordnung [= Steuerhinterziehung]

3. aus dem Arzneimittelgesetz […]; 4. aus dem Asylverfahrensgesetz […] 7. aus dem Betäubungsmittelgesetz […]

9. aus dem Kriegswaffenkontrollgesetz […]; 11. aus dem Waffengesetz […]

10. aus dem Völkerstrafgesetzbuch (Völkermord, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen)

§ 100a StPO: [Telekommunikationsüberwachung]

Im Katalog des § 100a II StPO fehlen z.B. die §§ 184, 184a, d-h, 224 – 227, 221 III StGB

> Dieses Defizit ist nicht kompensierbar, auch nicht durch Heranziehung des allgemeinen Rechtferti-gungsgrundes des § 34 StGB (numerus clausus!)

http://p5.focus.de/img/fotos/origs3410790/0935372226-w300-h168-o-q75-p5/jugendkriminalitaet.jpg
http://www.google.de/imgres?imgurl=http%3A%2F%2Festb.msn.com%2Fi%2F94%2F28D35
6CEEF34E9E8F825A53C8259F.jpg&imgrefurl=http%3A%2F%2Fwww.hqboard.net%2Fshow
thread.php%2F16201-Das-OWNED-Bilderspiel%2Fpage257&h=300&w=500&tbnid=U9dHy2
CH5qaTPM%3A&docid=cnjKo2hC2OcJfM&ei=GPG1VaDKOcG-sAGQ3q6wCw&tbm=isch&i
act=rc&uact=3&dur=565&page=1&start=0&ndsp=8&ved=0CD8QrQMwA2oVChMIoLbrs
Pf6xgIVQR8sCh0Qrwu2

Verbindungs- bzw. Verkehrsdaten

Ebenfalls von § 100a StPO im Rahmen der TKÜ mit umfasst:

§ 3 Nr. 30 TKG:

„**Verkehrsdaten**“: Daten, die bei der Erbringung eines Telekommunikations-dienstes erhoben, verarbeitet oder genutzt werden;

> = Informationen zu bestimmten Kommunikationsvorgängen mit beteiligten Rufnummern, Datum, Uhrzeit (von – bis), bei Mobilfunk der Standort (= Funkzelle), Gerätekennung, bei Internetnutzung auch die jeweilige Teilnehmeridentifikationsnummer (**IP-Adresse**) *(> s.u., Folie 30)*

- Verkehrsdaten auf Endgeräten unterfallen mangels TK nicht mehr § 100a StPO und können nach § 94 II StPO beschlagnahmt werden
- Speicherung von Verkehrsdaten für einen eventuellen späteren Abruf durch Ermittlungsbehörden?? **§ 100g StPO) ist vom BVerfG für nichtig erklärt worden** (NJW 2010, 833, Urt. v. 02.03.2010), *> s.u.*

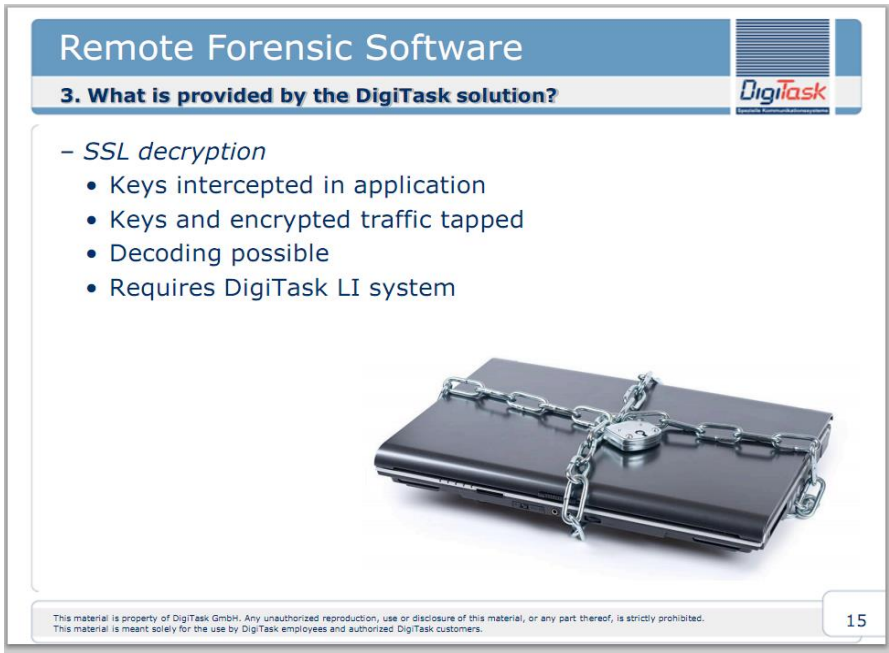
§ 42 PolG-Sachsen: Erhebung von Telekommunikationsdaten

(1) Zur Abwehr einer im Einzelfall vorliegenden Gefahr für die öffentliche Sicherheit oder Ordnung darf der Polizeivollzugsdienst von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt (Diensteanbieter), Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes (TKG) […], erhobenen Daten verlangen (§ 113 Abs. 1 Satz 1 TKG). Bezieht sich das Auskunftsverlangen nach Satz 1 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 TKG), darf die Auskunft nur verlangt werden, wenn die Endgeräte oder Speichereinrichtungen der Beschlagnahme unterliegen und tatsächliche Anhaltspunkte dafür sprechen, dass ohne den Zugriff auf gespeicherte Daten die Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates, das Leben, die Gesundheit oder die Freiheit einer Person sowie wesentliche Vermögenswerte aussichtslos oder wesentlich erschwert wäre.

Quellen-TKÜ

- von TKÜ zu unterscheiden:
- ein Programm wird auf den zu überwachenden Computer installiert (Remote Forensic Software [RFS]) und die Sprache bei Internettelephonie (Skype) wird abgefangen, noch bevor sie für den „Transport“ codiert wird (nach Codierung kaum Entschlüsselung möglich)
- = Überwachung von Telefonaten, die nicht über das klassische Telefonnetz geführt werden („Voice-over-IP-Kommunikation“)
- ustr., ob Quellen-TKÜ auch auf § 100a StPO gestützt werden kann (Komm.-Lit. (+), Rspr. (-))

http://tncdn.vikitech.netdna-cdn.com/assets/Recording-Skype-Calls-1.jpg;
http://cdn.arstechnica.net/12-01-2011/spyfile1.png



Durchsuchung: repressiv und präventiv

§ 110 III StPO

(3) 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; […]

§ 23 PolG-Sachsen: Durchsuchung von Personen

(1) Die Polizei kann eine Person durchsuchen, wenn […] 2.Tatsachen die Annahme rechtfertigen, dass sie Sachen mit sich führt, die sichergestellt oder beschlagnahmt werden dürfen […]

§ 24 PolG-Sachsen: Durchsuchung von Sachen

Die Polizei kann eine Sache durchsuchen, wenn

1. sie von einer Person mitgeführt wird, die nach § 23 Abs. 1 oder 2 durchsucht werden darf,

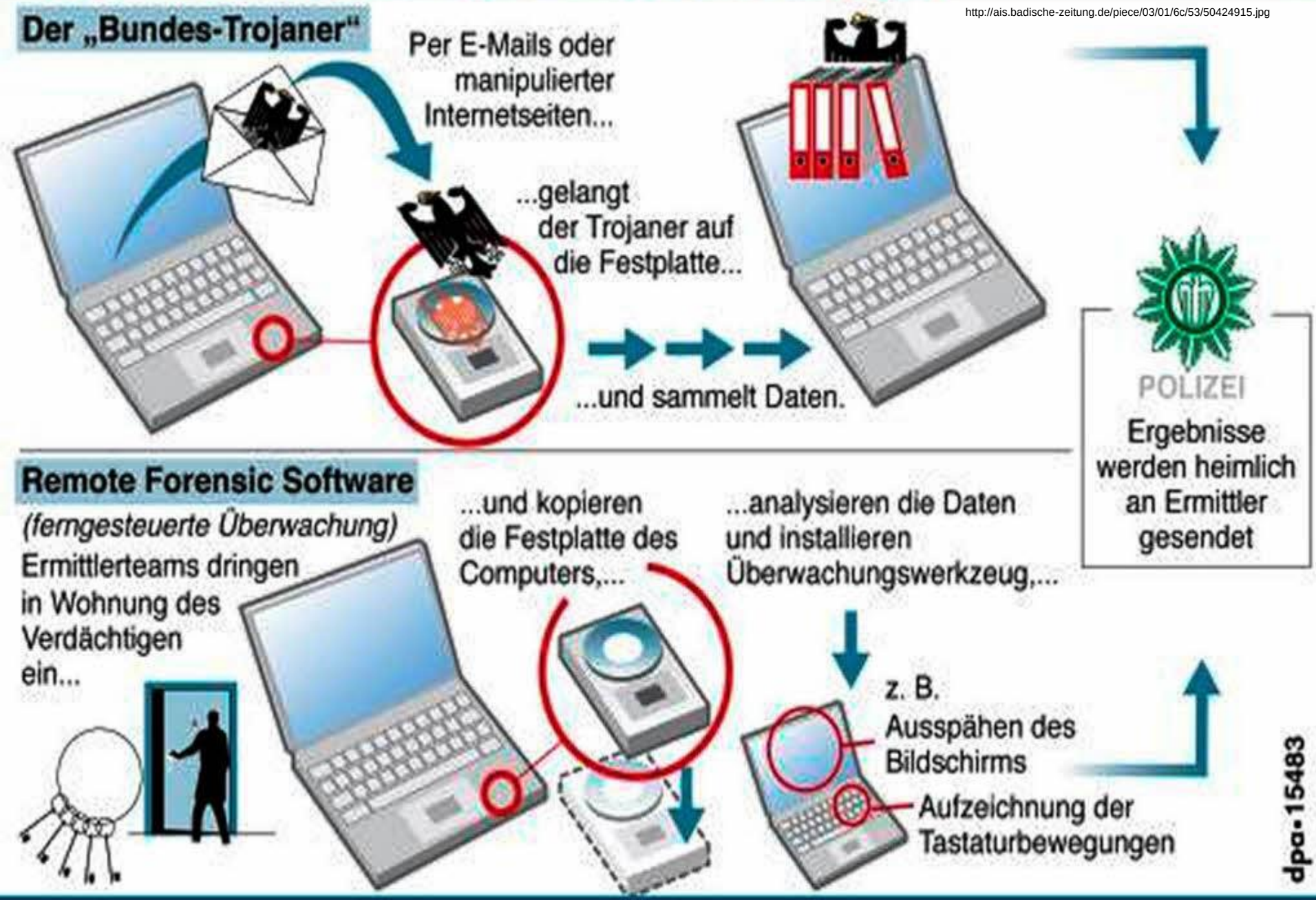
3. Tatsachen die Annahme rechtfertigen, dass sich in ihr *eine andere Sache* befindet, die sichergestellt oder beschlagnahmt werden darf …

Online-Durchsuchung

- Heimliches Installieren einer Entschlüsselungs-Software /Kopierprogramm/Backdoor-Programm („Trojaner“) über das Internet
- Nutzerdaten können ausspioniert werden
- Surfverhalten im Internet kann beobachtet werden (einmalig und auf längere Dauer) – nur wenn Rechner **online** ist
- Ermittler können von außen auf den Rechner zugreifen und Daten auslesen und auch manipulieren oder auch schädigen
- Wegen Heimlichkeit der Maßnahme besteht idR keine Verdunkelungsgefahr bzgl. des Betroffenen
- Betroffenem kann die Menge der übertragenen Daten auffallen und er kann ggf. selbst den Trojaner entfernen/weiterversenden und gezielt unverdächtiges Datenmaterial versenden, um Ermittler zu täuschen
- Beweiswert der durch eine Online-Durchsuchung wird wegen der Manipulationsgefahren als nicht sehr hoch eingestuft
- **im Strafverfahrensrecht unzulässig**

Möglichkeiten der Online-Durchsuchung

http://ais.badische-zeitung.de/piece/03/01/6c/53/50424915.jpg



Agent provocateur im Internet?

Der sog. Lockspitzel (**agent provocateur**) beabsichtigt nicht die Vollendung der Haupttat – deshalb kein doppelter Anstifter-Vorsatz gem. § 26 StGB, sondern lediglich, dem Täter eine Falle zu stellen, in welche jener tritt (= polizeilich initiierte Tatprovokation)

> Nur bei schweren Straftaten zulässig (vgl. § 160 StPO: ->Anfangsverdacht („XXL“)

http://www.google.de/imgres?imgurl=http%3A%2F%2Fi.auto-bild.de%2Fir_img%2F5%2F8%2F0%2F8%2F7%2F0%2Fa9eb63dbde19e9a8.jpeg&imgrefurl=http%3A%2F%2Fwww.autobild.de%2Fbilder%2Flageberich t-kfz-diebstahl-bka-2009-950516.html&h=768&w=1152&tbnid=1e7qAeP4Sp-XiM%3A&docid=399oSE0fW1eg3M&ei=-anJVfOzO8T4aPvitAC&tbm=isch&iact=rc&uact=3&dur=1574&page=6&start=56&ndsp=12&ved=0CNoBEK0DMDxqFQoTCLOUiq_GoMcCFUQ8Ggode7ECKg
http://www.google.de/imgres?imgurl=http%3A%2F%2Fi.auto-bild.de%2Fir_img%2F5%2F8%2F0%2F8%2F7%2F0%2Fa9eb63dbde19e9a8.jpeg&imgrefurl=http%3A%2F%2Fwww.autobild.de%2Fbilder%2Flageberich t-kfz-diebstahl-bka-2009-950516.html&h=768&w=1152&tbnid=1e7qAeP4Sp-XiM%3A&docid=399oSE0fW1eg3M&ei=-anJVfOzO8T4aPvitAC&tbm=isch&iact=rc&uact=3&dur=1574&page=6&start=56&ndsp=12&ved=0CNoBEK0DMDxqFQoTCLOUiq_GoMcCFUQ8Ggode7ECKg

„Honeypot und agent provocateur“

http://www.google.de/imgres?imgurl=http%3A%2F%2Fwww.tiggerman.com%2Fgallery%2Fvar%2Falbums%2Ffood%2Ftigger-honeypot-02.gif%253Fm%253D1303186452&imgrefurl=http%3A%2F%2Fwww.tiggerman.com%2Fgallery%2Findex.php%2Ffood%2Ftigger-honeypot-02&h=935&w=680&tbnid=pAny0g1N3vqEbM%3A&docid=cDecSDvCwvcUSM&ei=qcLHVaWLMsvxUun7p8AB&tbm=isch&iact=rc&uact=3&dur=160&page=2&start=15&ndsp=15&ved=0CGsQrQMwF2oVChMI5YPP0PWcxwIVy7gUCh3p_QkY

- Durch Informationsstreuung in Web-Foren /Blogs sollen einzelne Adressaten (Tatverdächtige (!)) unter Vorspiegelung vermeintlich „interessanter“ Seiten animiert werden, bestimmte rechtswidrige Inhalte aufzurufen und herunter zu laden
- Tatsächlich gelangen die Nutzer beim Anklicken der betreffenden Links nicht auf den von ihnen erhofften Seiten (= untauglicher Versuch), sondern deren IP-Adresse wird durch Strafverfolgungsbehörde gespeichert
- Ustr., ob ein Sich-Verschaffen bestimmter rechtswidriger Schriften/Materialien bereits durch bloßes Aufrufen der betreffenden Seiten erfolgt, oder ob erst das Herunterladen/Speichern einzelner Inhalte zur Tatbestandserfüllung führt (vgl. *Birkenstock*, S. 130 ff.)

Verdeckte Ermittler und V-Personen als agent provocateur am Honeypot

- **<u>Verdeckte Ermittler</u>**:
  > § 110a ff. StPO
  > Rechtmäßigkeit über Art. 13 III - VII GG i.V.m. § 110c StPO (ustr., ob § 110c StPO eine EGL zum Betreten der Wohnung beinhaltet)
  > Präparieren frei zugänglicher PCs in der Wohnung durch VE: § 110c StPO
- **<u>V-Person</u>**, <u>Anlage D I Nr. 2.2 RiStBV</u>:
  > fehlende Dienstaufsicht („Wer kontrolliert die Kontrolleure“?)
  > §§ 110a ff. StPO für V-Personen nicht anwendbar
  > genügt Generalklausel der §§ 161, 163 StPO? ((+), *Meyer-Goßner/Schmitt, StPO, § 110a Rdz. 4a, § 163 Rdz. 34a*), notfalls über § 34 StGB

http://www.lto.de/fileadmin/_migrated/tx_ltoartikel/online-ermittler_473.jpg

Problem bei V-Person: Mitwirkung der V-Person kann weder erzwungen, noch hinreichend überprüft werden
> V-Person entscheidet letztlich selbst, ob/welche Informationen an die Polizei weitergegeben werden
> keine Durchführung einer online-Durchsuchung durch eine V-Person (vor dem 2. März 2010)

„Honeypot und agent provocateur“

bm=isch&iact=rc&uact=3&dur=160&page=2&start=15&ndsp=15&ved=0CGsQrQMwF2oVChMI5YPP0PWcxwIVy7gUCh3p_QkY

Abgrenzungsproblem bzgl. zwar tatgeneigter, aber (noch)nicht fest entschlossenem Betroffenen: Kann ein „Semi-omnimodo-facturus“ noch *angestiftet* werden?

- Nach BGH im Einklang mit Grundsatz des fair trial nur dann rechtmäßig, wenn sich die Maßnahme gegen eine Person richtet, gegen die *mehr* als nur ein *Anfangsverdacht* hinsichtlich einer schwerwiegenden Straftat besteht (z.B. § 100a II StPO, (Lit.))
- Es darf dabei aber nicht derartig nachhaltig auf die Person eingewirkt werden, dass sie erst dadurch verleitet wird, bestimmte Seiten aufzurufen
- Also: Zunächst unverdächtige, nicht tatgeneigte Person darf nicht zur Tatbegehung verleitet werden, um sie einem Strafverfahren zu unterziehen

> Meyer-Goßner/Schmitt, StPO, § 163 Rdz. 34a; Karlsruher Kommentar-Griesbaum, StPO, § 163, Rdz. 18

- Problematisch: Speicherung der IP-Adressen der Honeypot-Besucher: **§ 100g StPO**: Diese Norm ist vom BVerfG am 2. März 2010, soweit Verkehrsdaten erhoben werden, für verfassungswidrig und nichtig erklärt worden >> keine Rechtsgrundlage zur mehrmonatigen Speicherung der IP-Adresse
  >> erneute Gesetzesentwürfe zur Vorratsdatenspeicherung derzeit in der Diskussion

Vorbeugende Durchsuchungen?

§ 20k BKAG: Verdeckter Eingriff in informationstechnische Systeme

(1) Das Bundeskriminalamt darf ohne Wissen des Betroffenen mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben, wenn *bestimmte Tatsachen* die Annahme rechtfertigen, dass eine Gefahr vorliegt für

1. Leib, Leben oder Freiheit einer Person oder

2. solche Güter der Allgemeinheit, deren Bedrohung die *Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen* berührt. Eine Maßnahme nach Satz 1 ist auch zulässig, wenn sich noch nicht mit *hinreichender Wahrscheinlichkeit* feststellen lässt, dass ohne Durchführung der Maßnahme in näherer Zukunft ein Schaden eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinweisen. Die Maßnahme darf nur durchgeführt werden, wenn sie […] erforderlich ist und diese ansonsten aussichtslos oder wesentlich erschwert wäre.

§ 3 ATDG zur Gefahrenabwehr

(1) In der Antiterrordatei werden, soweit vorhanden, folgende Datenarten gespeichert:

Nr. 1a) der Familienname, die Vornamen, frühere Namen, andere Namen, Aliaspersonalien, abweichende Namensschreibweisen, das Geschlecht, das Geburtsdatum, der Geburtsort, der Geburtsstaat, aktuelle und frühere Staatsangehörigkeiten, gegenwärtige und frühere Anschriften, besondere körperliche Merkmale, Sprachen, Dialekte, Lichtbilder, die Bezeichnung der Fallgruppe nach § 2 und, soweit keine anderen gesetzlichen Bestimmungen entgegenstehen und dies zur Identifizierung einer Person erforderlich ist, Angaben zu Identitätspapieren (Grunddaten),

b) folgende weitere Datenarten (erweiterte Grunddaten):

aa) eigene oder von ihnen genutzte Telekommunikationsanschlüsse und Telekommunikationsendgeräte,

bb) Adressen für elektronische Post, cc) Bankverbindungen, dd) Schließfächer,

ee) auf die Person zugelassene oder von ihr genutzte Fahrzeuge, ff) Familienstand, gg) Volkszugehörigkeit,

hh) Angaben zur Religionszugehörigkeit, soweit diese im Einzelfall zur Aufklärung oder Bekämpfung des internationalen Terrorismus erforderlich sind,

ii) besondere Fähigkeiten, die nach den auf bestimmten Tatsachen beruhenden Erkenntnissen der beteiligten Behörden der Vorbereitung und Durchführung terroristischer Straftaten nach § 129a Abs. 1 und 2 des Strafgesetzbuchs dienen können, insbesondere besondere Kenntnisse und Fertigkeiten in der Herstellung oder im Umgang mit Sprengstoffen oder Waffen,

jj) Angaben zum Schulabschluss, zur berufsqualifizierenden Ausbildung und zum ausgeübten Beruf,

kk) Angaben zu einer gegenwärtigen oder früheren Tätigkeit in einer lebenswichtigen Einrichtung im Sinne des § 1 Abs. 5 des Sicherheitsüberprüfungsgesetzes oder einer Verkehrs- oder Versorgungsanlage oder -einrichtung, einem öffentlichen Verkehrsmittel oder Amtsgebäude,

ll) Angaben zur Gefährlichkeit, insbesondere Waffenbesitz oder zur Gewaltbereitschaft der Person,

mm) Fahr- und Flugerlaubnisse,

nn) besuchte Orte oder Gebiete, an oder in denen sich in § 2 Satz 1 Nr. 1 und 2 genannte Personen treffen,

oo) Kontaktpersonen zu den jeweiligen Personen nach § 2 Satz 1 Nr. 1 Buchstabe a oder Nr. 2, […]

Cloud Computing, § 110 III StPO

Speicherung der Daten nicht auf eigener Festplatte oder USB-Stick, sondern irgendwo im Internet und werden bei Bedarf geladen:

- Straftatrelevante Daten können ausgelagert/verteilt und dadurch dem Zugriff der Strafverfolgungsbehörden entzogen werden
- Gem. § 110 III StPO ist es zulässig, elektronische Datenträger auch auf räumlich getrennte Speichereinheiten (in der cloud) auszudehnen, sofern vom Rechner des Betroffenen hierauf zugegriffen werden kann
- § 110 III StPO soll keine heimliche Online-Durchsuchung gestatten

>> *völkerrechtliche Probleme*

http://blog.orangescape.com/files/2013/01/cloud_paas.jpg

Völkerrechtliche Probleme

http://cdn2.hubspot.net/hub/146766/file-17854747-png/images/cloud_computing.png

Bei Servern im Ausland:

- Ermittlungsbefugnisse sind auf das nationale Hoheitsgebiet begrenzt
- § 110 III StPO hat nur **intra**natio-nale, keine internationale Geltung
- Ermittlungen außerhalb nationaler Grenzen setzen Zustimmung des betroffenen Staates voraus
- Rechtshilfeersuchen an betreffen-den Staat: § 94 IRG: Ersuchen um Sicherstellung, Beschlagnahme und Durchsuchung
- Art. 19 Cybercrime-Konvention des Europarates vom 23.11.2001
  >> u.a. § 110 III StPO

Vorbeugende Durchsuchungen?

Artikel 19 – der Cybercrime-Konvention des Europarates

Durchsuchung und Beschlagnahme gespeicherter Computerdaten

1 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen,

a ein Computersystem oder einen Teil davon sowie die darin gespeicherten Computerdaten und

b einen Computerdatenträger, auf dem Computerdaten gespeichert sein können,

in ihrem Hoheitsgebiet zu durchsuchen oder in ähnlicher Weise darauf Zugriff zu nehmen.

2 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um sicherzustellen, dass ihre Behörden, wenn sie ein bestimmtes Computersystem oder einen Teil davon nach Absatz 1 Buchstabe a durchsuchen oder in ähnlicher Weise darauf Zugriff nehmen und Grund zu der Annahme haben, dass die gesuchten Daten in einem anderen Computersystem oder einem Teil davon im Hoheitsgebiet der betreffenden Vertragspartei gespeichert sind, und diese Daten von dem ersten System aus rechtmäßig zugänglich oder verfügbar sind, die Durchsuchung oder den ähnlichen Zugriff rasch auf das andere System ausdehnen können.

3 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihre zuständigen Behörden zu ermächtigen, Computerdaten, auf die nach Absatz 1 oder 2 Zugriff genommen wurde, zu beschlagnahmen oder in ähnlicher Weise sicherzustellen. Diese Maßnahmen umfassen die Befugnis,

a ein Computersystem oder einen Teil davon oder einen Computerdatenträger zu beschlagnahmen oder in ähnlicher Weise sicherzustellen;

b eine Kopie dieser Computerdaten anzufertigen und zurückzubehalten;

c die Unversehrtheit der einschlägigen gespeicherten Computerdaten zu erhalten;

d diese Computerdaten in dem Computersystem, auf das Zugriff genommen wurde, unzugänglich zu machen oder sie daraus zu entfernen.

4 Jede Vertragspartei trifft die erforderlichen gesetzgeberischen u.a. Maßnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen, dass jede Person, die Kenntnisse über die Funktionsweise des Computersystems oder über Maßnahmen zum Schutz der darin enthaltenen Daten hat, in vernünftigem Maß die notwendigen Auskünfte zu erteilen hat, um die Durchführung der in Abs.1, 2 genannten Maßnahmen zu ermöglichen.

http://www.seilers-werbeblog.ch/wp-content/uploads/2014/10/STAPO_hinten_polizeibeschriftung_VOG_2767_4c.jpg