Master of Advanced Studies in Forensics (MAS Forensics)

# Beweiserhebung in der Cloud ☁

Eingereicht von

MLaw Daniel Burgermeister, RA
am 12. August 2015

betreut von

lic.iur. Adrian Schulthess, Fürsprecher

# Inhaltsverzeichnis

## Literaturverzeichnis

AEPLI MICHAEL, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten – Unter besonderer Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich, Zürich 2004.

BANGERTER SIMON, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht – unter vergleichender Berücksichtigung der StPO, Zürich 2014.

BIAGGINI GIOVANNI, Bundesverfassung der Schweizerischen Eidgenossenschaft, Zürich 2007 (zit. BIAGGINI Kommentar BV, Art. 13 N 1).

BOMMER FELIX, Löschung als Einziehung von Daten, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 171 ff.

BUNDESAMT FÜR JUSTIZ, Leitfaden zur Beweiserhebung in Verbindung mit Internet-accounts bei Dienstanbietern (Providern) mit Sitz in den USA, 14.05.2014 (zit. Leitfaden BJ Beweiserhebung US-Provider).

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI), Cloud Computing Grunlagen, https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html (zuletzt besucht am 20.07.2015).

BURGERMEISTER DANIEL, Ermittlungen im Internet / ICT-Bereich, Leitfaden der Staatsanwaltschaft St. Gallen, St. Gallen, 08.11.2013 bzw. 08.05.2015.

DOMBROWSKI NADINE, Extraterritoriale Strafrechtsanwendung im Internet, Berlin 2014.

DONATSCH ANDREAS/HANSJAKOB THOMAS/LIEBER VIKTOR (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung (StPO), 2. Aufl., Zürich 2014 (zit. BEARBEITER, StPO-Kommentar, Art. 1 N 1).

DONATSCH ANDREAS/SCHMID ALBERT, Der Zugriff auf E-Mails im Strafverfahren – Überwachung (BÜPF) oder Beschlagnahme?, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 151 ff.

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITBEAUFTRAGTER (EDÖB), Erläuterungen zu Cloud Computing, 2014, http://www.edoeb.admin.ch/datenschutz/00626/00876/01203/index.html?lang=de (zuletzt besucht am 20.07.2015).

FRAUNHOFER INSTITUT, Cloud-Computing für die öffentliche Verwaltung – ISPRAT-Studie, November 2010, http://www.cloud.fraunhofer.de/de/publikationen/isprat_cloud.html (zuletzt besucht am 20.07.2015).

GERCKE MARCO/BRUNST PHILIPP W., Praxishandbuch Internetstrafrecht, München 2009.

GLESS SABINE, Strafverfolgung im Internet, in: ZStrR 130, 2012.

GOLDSCHMID PETER/MAURER THOMAS/SOLLBERGER JÜRG (Hrsg.), Kommentierte Textausgabe zur Schweizerischen Strafprozessordnung, Bern 2008 (zit. BEARBEITER, kommentierte Textausgabe StPO, Art. 1 N 1).

HANSJAKOB THOMAS, BÜPF / VÜPF – Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, 2. Aufl., St. Gallen 2006 (zit. Hansjakob, BÜPF-Kommentar, Art. 1 BÜPF N 1).

HEIMGARTNER STEFAN, Die internationale Dimension von Internetstraffällen, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 117 ff. (zit. HEIMGARTNER, Internationale Dimension).

HEIMGARTNER STEFAN, Strafprozessuale Beschlagnahme – Wesen, Arten und Wirkungen, Zürich 2011 (zit. HEIMGARTNER, Strafprozessuale Beschlagnahme).

HILBER MARC (Hrsg.), Handbuch Cloud Computing, Köln 2014 (zit. BEARBEITER, Handbuch Cloud Computing, S. 1).

INTERNATIONAL COMPETITION NETWORK, Anti-Cartel Enforcement Manual, Cartel Working Group, Subgroup 2: Enforcement Techniques, Chapter 3: Digital Evidence Gathering, März 2010, http://www.internationalcompetitionnetwort.org/uploads/library/doc627.pdf (zuletzt besucht am 02.08.2015; zit. ICN).

JEAN-RICHARD-DIT-BRESSEL MARC TH., Zur Abgrenzung von Beschlagnahme und Überwachung im Strafverfahren, in: ZStrR 125, 2007, S. 157 ff.

JOSITSCH DANIEL, Durchsuchung und Siegelung elektronischer Daten, Handout Lehrveranstaltung Strafprozessrecht II, Frühjahrsemester 2015, http://www.rwi.uzh.ch/lehreforschung/alphabetisch/jositsch/lehrveranstaltung/handout12.pdf (zuletzt besucht am 20.07.2015).

KURZIDIM MICHAEL, Die besten Cloud Anbieter der Schweiz, in: Computerworld, 10.07.2014, http://www.computerworld.ch/news/software/artikel/marktueberblick-die-besten-cloud-anbieter-der-schweiz-66054 (zuletzt besucht am 14.07.2015).

MÜLLER THOMAS/GÄUMANN STEFAN, Siegelung nach Schweizerischer StPO, in: Anwaltsrevue 6-7/2012, S. 290 ff.

NIGGLI MARCEL ALEXANDER/HEER MARIANNE/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar Schweizerische Strafprozessordnung, 2. Aufl., Basel 2014 (zit. BEARBEITER, BSK StPO, Art. 1 StPO N 1).

OODRIVE, Trusted Cloud Solutions, IaaS – PaaS – SaaS – Was sind die Unterschiede, 03.02.2014, http://de.oodrive.com/de/content/iaas-paas-saas-was-sind-die-unterschiede (zuletzt besucht am 20.07.2015).

RYSER DOMINIC, „Computer Forensics", eine neue Herausforderung für das Strafprozessrecht, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, S. 553 ff.

SCHMID NIKAUS, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im allgemeinen, in: ZStrR 111, 1993, S. 81 ff. (zit. SCHMID, strafprozessuale Fragen, ZStrR).

SCHMID NIKLAUS, Handbuch des schweizerischen Strafprozessrechts, 2. Aufl., Zürich/St. Gallen 2013 (zit. SCHMID, Handbuch StPO).

SCHMID NIKLAUS, Schweizerische Strafprozessordnung Praxiskommentar, 2. Aufl., Zürich/St. Gallen 2013 (zit. SCHMID, Praxiskommentar StPO).

SCHNEIDER JÜRG, Internet Service Provider im Spannungsfeld zwischen Fernmeldegeheimnis und Mitwirkungspflichten bei der Überwachung des E-Mail-Verkehrs über das Internet, in: AJP 2005, S. 179 ff.

SCHULZ HAJO, Island – Insel der grünen Rechenzentren, 17.06.2012, http://www.heise.de/newsticker/meldung/Island-Insel-der-gruenen-Rechenzentren-169591.html (zuletzt besucht am 15.07.2015).

SCHWARZENEGGER CHRISTIAN, Sperrverfügungen gegen Access-Provider, in: Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Electronic Commerce Law, Bern 2003, S. 249 ff.

SCHWEINGRUBER SANDRA, Cybercrime – Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, in: Jusletter 10.11.2014.

SCHWERHA JOSEPH J., Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from „Cloud Computing Providers“, 15.01.2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2079_reps_IF10_reps_joeschwerha1a.pdf (zuletzt besucht am 31.07.2015).

SÖBBING THOMAS, Cloud Computing, die Zukunftsvision von Amazon, Google und Microsoft rechtlich betrachtet, in: Jusletter 10.08.2009.

SPOENLE JAN, Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?, 31.12.2010, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/international cooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf (zuletzt besucht a 31.07.2015).

SWISSCOM, Die Cloud für die Schweiz, 2013, http://www.swisscom.ch/ist/dam/documents/factsheets/2013-die-cloud-fuer-die-schweiz.pdf, zuletzt besucht am 20.07.2015 (zit. Swisscom, Factsheet).

US-DEPARTEMENT OF JUSTICE, Investigative Guide for Obtaining Electronic Evidence from the United States, 25.05.2012 (zit. Guidance Electronic Evidence).

WALDER STEPHAN, Rechtshilfe bei Internetkriminalität, Referat Fachtagung Staatsanwaltschaft St. Gallen, 19.11.2014 (Folien).

## Materialienverzeichnis

Botschaft zu den Bundesgesetzen betreffend die Überwachung des Post- und Fernmeldeverkehrs und über die verdeckte Ermittlung vom 01.07.1998, BBl 1998 4241.

Botschaft zur Vereinheitlichung des Strafprozessrechts vom 21.12.2005, BBl 2006 1085.

Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18.06.2010, BBl 2010 4697.

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27.02.2013, BBl 2013 2683.

Council of Europe (Europarat), Explanatory Report to the Convention on Cybercrime, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

## Abkürzungsverzeichnis

| | |
|---|---|
| a | alt |
| Abs. | Absatz |
| AGB | Allgemeine Geschäftsbedingungen |
| AJP | Allgemeine Juristische Praxis |
| a.M. | anderer Meinung |
| Art. | Artikel |
| Aufl. | Auflage |
| BBl | Bundesblatt |
| BGE | Entscheidungen des Schweizerischen Bundesgerichts (amtliche Sammlung) |
| BGer | Bundesgericht |
| BJ | Bundesamt für Justiz |
| BSI | Bundesamt für Sicherheit in der Informationstechnik (Deutschland) |
| bspw. | beispielsweise |
| BStGer | Bundesstrafgericht |
| BStP | Bundesgesetz vom 15.06.1934 über die Bundesstrafrechtspflege (ausser Kraft; SR 312.0) |
| BÜPF | Bundesgesetz vom 06.10.2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (SR 780.1) |
| BV | Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18.04.1999 (SR 101) |
| bzw. | beziehungsweise |
| CCC | Convention on Cybercrime (Übereinkommen über die Cyberkriminalität) des Europarates vom 23.11.2001 (SR 0.311.43) |
| CRM | Customer Relationship Management |
| CSP | Cloud Service Provider |
| d.h. | das heisst |

| | |
|---|---|
| E. | Erwägung |
| EDÖB | Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter |
| engl. | englisch |
| etc. | et cetera |
| EU | Europäische Union |
| EuGH | Gerichtshof der Europäischen Union |
| f./ff. | folgende/fortfolgende |
| fedpol | Bundesamt für Polizei |
| FMG | Fernmeldegesetz vom 30.04.1997 (SR 784.10) |
| frz. | französisch |
| FZR | Freiburger Zeitschrift für Rechtsprechung |
| Hrsg. | Herausgeber |
| IaaS | Infrastracture as a Service |
| ICN | International Competition Network |
| ICT | Information and Communication Technology |
| insb. | insbesondere |
| IRSG | Bundesgesetz über die internationale Rechtshilfe in Strafsachen vom 20.03.1981 (SR 351.1) |
| i.S. | im Sinne |
| ISP | Internet Service Provider |
| IT | Informationstechnik |
| i.V.m. | in Verbindung mit |
| lit. | litera |
| m.E. | meines Erachtens |
| N | Note |
| NIST | National Institute of Standards and Technology |
| PaaS | Platform as a Service |

| | |
|---|---|
| Rz. | Randziffer |
| S. | Seite |
| SaaS | Software as a Service |
| StGB | Schweizerisches Strafgesetzbuch vom 21.12.1937 (SR 311.0) |
| StPO | Schweizerische Strafprozessordnung vom 05.10.2007 (SR 312.0) |
| TPF | Amtliche Sammlung der Entscheide des Schweizerischen Bundesstrafgerichts |
| u.a. | unter anderem |
| vgl. | vergleiche |
| VPN | Virtual Private Network |
| vs. | versus |
| VStrR | Bundesgesetz vom 22.03.1974 über das Verwaltungsstrafrecht (SR 313.0) |
| VÜPF | Verordnung vom 31.10.2001 über die Überwachung des Post- und Fernmeldeverkehrs (SR 780.11) |
| z.B. | zum Beispiel |
| zit. | zitiert |
| ZStrR | Schweizerische Zeitschrift für Strafrecht |

## Kurzfassung

Cloud Computing stellt die Strafverfolgungsbehörden auf der ganzen Welt vor neue Herausforderungen bei der Beweismittelerhebung. Dennoch kann festgestellt werden, dass die schweizerische Strafprozessordnung den Strafverfolgungsbehörden u.a. mit Durchsuchung, Edition und Überwachungsmassnahmen ausreichende Möglichkeiten bietet, um Daten einer Cloud als Beweismittel zu erheben, solange sich die Daten bzw. die Cloud Service Provider in der Schweiz befinden. Wenn sich die zu erhebenden Daten im Ausland befinden bzw. durch ausländische Cloud Service Provider gehostet werden, ist die Beweiserhebung erschwert, aber nicht unmöglich. Gerade mit der Convention on Cybercrime des Europarats wurde ein gutes Instrument geschaffen, um an Daten in Vertragsstaaten der Konvention zu gelangen. Erwähnenswert ist Art. 29 der Konvention, der es ermöglicht, dass strafverfahrensrelevante Daten durch den ersuchten Staat umgehend gesichert werden können, damit diese für ein folgendes Rechtshilfeverfahren nicht verloren gehen. Auch Art. 32 lit. b der Konvention erleichtert den Strafverfolgungsbehörden die Beweiserhebung im Ausland, wenn mit Zustimmung einer berechtigten Person vom Inland aus direkt auf die relevanten Daten einer Cloud zugegriffen werden darf. Trotz Cybercrime-Konvention kann es aber leider immer noch zu langwierigen Rechtshilfeverfahren kommen, wenn Daten im Ausland erhältlich gemacht werden sollen. Insbesondere sind Rechtshilfeersuchen an Staaten, welche die Convention on Cybercrime nicht unterzeichnet und ratifiziert haben, erfahrungsgemäss nicht immer erfolgsversprechend. Es wird daher dafür plädiert, dass einerseits weitere Staaten der Konvention beitreten oder weitere bi- oder multilaterale Verträge in diesem Bereich geschaffen werden und andererseits die Convention on Cybercrime im Bereich der zwangsweisen grenzüberschreitenden Beweiserhebung ausgebaut wird. In diesem Zusammenhang muss das traditionelle Territorialitätsprinzip einem moderneren, pragmatischeren Prinzip weichen, damit in Zukunft erfolgreich Strafverfolgung im Bereich von Cloud Computing betrieben werden kann. Als gutes Beispiel für eine Überdenkung des Territorialitätsprinzips darf das Zugriffsprinzip (engl. Access Approach) angeführt werden.

# 1. Einleitung

In einem Factsheet der Swisscom aus dem Jahre 2013 heisst es: *„Swisscom baut die Cloud für die Schweiz."*[1] Die Idee der Swisscom ist es, alle möglichen Daten, wie beispielsweise Lohnabrechnungen, Quittungen, Verträge, Steuerunterlagen usw. in ihrer Cloud zu speichern[2], und in Zukunft sollen auch sensiblere Daten wie Patientendaten in einer Cloud sicher abgelegt werden können.[3] Diese „360-Grad-Cloud" soll das digitale Schliessfach der Schweiz werden.

Wenn wir dieser Vision der Swisscom folgen, werden wir uns in Zukunft als Strafverfolger aber auch als Bürger vermehrt mit dem Thema Cloud Computing beschäftigen müssen, ob wir wollen oder nicht.

## 1.1. Was heisst Cloud Computing?

Es konnte sich bislang keine allgemeingültige Definition des Begriffs Cloud Computing durchsetzen.[4] Sehr vereinfacht habe ich den Begriff Cloud im Leitfaden der Staatsanwaltschaft St. Gallen zu Ermittlungen im Internet / ICT-Bereich umschrieben: *„In sogenannten Clouds werden Daten nicht mehr direkt vor Ort auf einem Speichermedium (Festplatte, DVD, USB-Stick etc.) gespeichert, sondern im Internet (auf Servern im In- und Ausland, häufig sogar verteilt auf verschiedene Server). Vorteil dieses Dienstes ist der orts- und geräteunabhängige Datenzugriff. Das geht so weit, dass sogar ganze Programme (z.B. auch Microsoft Office Anwendungen[5]) nicht mehr auf einem Gerät installiert sind, sondern über eine Internetverbindung genutzt werden. Nachteil für uns Strafverfolger ist der erschwerte Zugriff auf diese Daten."*[6]

Auf der Webseite des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) wird Cloud Computing folgendermassen beschrieben: *„Cloud Computing (deutsch: rechnen in der Wolke) ist ein Begriff aus der Informationstechnik (IT). Er bedeutet, vereinfacht gesagt, dass Software, Speicherkapazitäten oder Rechnerleistung über ein Netzwerk, zum Beispiel das Internet, oder innerhalb eines Virtual Private Network (VPN)*

[1] SWISSCOM, Factsheet, S. 6.
[2] SWISSCOM, Factsheet, S. 20.
[3] SWISSCOM, Factsheet, S. 34.
[4] BSI – Cloud Computing Grundlagen.
[5] Microsoft Office 365: https://office.live.com/start/default.aspx (zuletzt besucht am 14.07.2015).
[6] BURGERMEISTER, S. 5.

*bedarfsorientiert bezogen, d.h. gemietet werden. Die IT-Landschaft (z.B. Rechenzentrum, Datenspeicher, Mail- oder Kollaborationssoftware, Entwicklungsumgebungen oder Spezialsoftware wie Customer Relationship Management (CRM)) steht nicht mehr im Eigentum des Unternehmens oder der Behörde und wird nicht mehr von diesen selbst betrieben, sondern von einem oder mehreren Cloud-Service-Anbietern als Dienstleistung (Service) gemietet."*[7]

### 1.1.1. Arten von Clouds

Es werden vom NIST (National Institute of Standards and Technology; US-amerikanische Standardisierungsstelle) die sogenannten Bereitstellungsmodelle (Deployment Models) Private Clouds, Public Clouds, Hybrid Clouds und Community Clouds unterschieden:[8]

Von einer Private Cloud wird gesprochen, wenn die Cloud-Infrastruktur nur einer Institution betrieben wird. Sie kann von der Institution selbst oder einem Dritten organisiert und geführt werden und dabei im Rechenzentrum der eigenen Institution oder einer fremden Institution stehen.

In einer Public Cloud werden die Dienste von der Allgemeinheit oder einer grossen Gruppe genutzt, zum Beispiel einer ganzen Branche, und die Dienste werden von einem Anbieter zur Verfügung gestellt.

Bei einer Community Cloud wird die Infrastruktur von mehreren Institutionen geteilt, die ähnliche Interessen haben (z.B. Universitäten, Bibliotheken etc.). Eine solche Cloud kann von einer dieser Institutionen oder einem Dritten betrieben werden.

Werden eine Public Cloud und eine Private Cloud gleichzeitig und parallel genutzt, spricht man von einer Hybrid Cloud.[9]

[7] EDÖB , Erläuterungen zu Cloud Computing.
[8] BSI, Cloud Computing Grundlagen.
[9] EDÖB, Erläuterungen zu Cloud Computing.

### 1.1.2. Servicemodelle

Die Cloud-Dienste können in die folgenden drei Servicemodelle eingeteilt werden.[10]

#### *1.1.2.1 Infrastracture as a Service (IaaS)[11] – Auslagerung der materiellen Infrastruktur*

Der Cloud-Anbieter stellt in der Cloud einen Server zur Verfügung, auf dem die Cloud-Nutzer ihre Daten oder Anwendungen abspeichern können. Der Cloud-Anbieter ist nur für das Funktionieren des Netzes, dessen Zugang, der Hardware etc. verantwortlich. Der Nutzer hat die volle Kontrolle über das IT-System vom Betriebssystem aufwärts, da alles innerhalb seines Verantwortungsbereichs betrieben wird. Führender Anbieter von IaaS in der Schweiz ist gemäss einer Studie von Experton aus dem Jahre 2014 die Swisscom.[12]

#### *1.1.2.2 Platform as a Service (PaaS)[13] – Auslagerung der materiellen Infrastruktur, der Anwendungen und Daten*

Der Cloud-Anbieter stellt eine komplette Infrastruktur bereit und bietet dem Nutzer auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. Die Bewirtschaftung der Daten erfolgt durch den Nutzer. Der Kunde hat nur noch die Kontrolle über seine Anwendungen, die auf der Plattform laufen, und keinen Zugriff auf die darunterliegenden Schichten (Hardware, Betriebssystem). Ein bekannter Anbieter von PaaS ist beispielsweise die Google Cloud Platform, bei welcher bausteinmässig Entwicklerdienste angeboten werden.[14] Aber auch in der Schweiz gibt es Anbieter von PaaS, bspw. die Abraxas Informatik AG.[15]

#### *1.1.2.3 Software as a Service (SaaS)[16] – das „Alles-in-Einem-Angebot":*

Der Kunde ist nur noch Konsument in der Cloud. Er bewirtschaftet nichts mehr selber. Er übergibt praktisch die ganze Kontrolle an den CSP (Cloud Service Provider) und kann die Daten auf der Cloud nur noch mit der vom Anbieter zur Verfügung gestellten Funktionali-

[10] http://de.oodrive.com/de/content/iaas-paas-saas-was-sind-die-unterschiede; EDÖB, Erläuterungen zu Cloud Computing; BSI, Cloud Computing Grundlagen; vgl. auch WEISS, Handbuch Cloud Computing, S. 5 Rz. 5 ff.; SCHORER, Handbuch Cloud Computing, S. 63 Rz. 22 ff.; SWISSCOM, Factsheet, S. 12.
[11] Vgl. auch WEISS, Handbuch Cloud Computing, S. 5 Rz. 10.
[12] Vgl. KURZIDIM.
[13] Vgl. auch WEISS, Handbuch Cloud Computing, S. 5 Rz. 11.
[14] https://cloud.google.com (zuletzt besucht am 14.07.2015); vgl. auch SCHORER, Handbuch Cloud Computing, S. 64 Rz. 23.
[15] Vgl. https://www.abraxas.ch/de/angebot/themen/cloud-computing (zuletzt besucht am 14.07.2015).
[16] Vgl. auch WEISS, Handbuch Cloud Computing, S. 5 Rz. 12.

tät bearbeiten. SaaS ist wohl der meist verbreitete und meistgenutzte Service des Standardusers.[17] Bekannte Beispiele dazu sind iCloud, Dropbox, OneDrive, Google Drive etc. oder auch reine E-Mail-Anbieter wie GMX etc.[18]

Beispielsweise bietet Apple mit der iCloud u.a. die Möglichkeit, neben Mails, Kontakten und Kalendereinträgen, Fotos, Dokumente und Einstellungen automatisch in die Cloud zu laden und mit allen Geräten des Besitzers zu synchronisieren.[19] Google Drive beinhaltet neben einem gewöhnlichen Online-Speicherplatz für Dateien aller Art eine Office-Lösung mit Google Docs, Sheets, Slides und Forms, mit welcher Dokumente gemeinsam online bearbeitet werden können.[20] Auch das Geschäftssoftwareunternehmen SAP verfügt über eine Cloud-Lösung, mit welcher Anwendungen für Finanzen, Personalwesen, Vertrieb etc. online betrieben werden.[21]

Der Ausdruck „as a Service" wird noch für weitere Cloud-Angebote benutzt. Dazu gehören Database as a Service (DBaaS), Desktop as a Service (DaaS), Storage as a Service etc. Aus diesem Grund wird auch von XaaS, also irgendetwas als Dienstleistung gesprochen, obwohl sich die meisten Angebot den beschriebenen Kategorien zuordnen lassen.[22]

## 1.2. Welche Probleme stellen sich durch Clouds im Strafverfahren?

Das erste Problem ist die Unkenntnis der Strafverfolgungsbehörde darüber, dass die beschuldigte Person überhaupt einen Cloud-Dienst nutzt. Nehmen wir den klassischen Fall einer KOBIK-Meldung[23] wegen Herunterladens von Kinderpornografie über ein Peer-to-Peer-Netzwerk[24]: Der Staatsanwalt stellt nach Eingang einer solchen Meldung einen Durchsuchungsbefehl für die Örtlichkeit des betreffenden Internetanschlusses aus. Die Polizei führt die Hausdurchsuchung durch und stellt diverse Datenträger (PCs, externe Festplatten, USB-Sticks etc.) sicher. Diese Datenträger werden anschliessend digitalforensisch auf kinderpornografische Daten ausgewertet. Nun kann es durchaus sein, dass

[17] SCHORER, Handbuch Cloud Computing, S. 65 Rz. 25.
[18] SCHORER, Handbuch Cloud Computing, S. 65 Rz. 25/26.
[19] https://www.apple.com/chde/icloud/ (zuletzt besucht am 14.07.2015).
[20] https://www.google.com/drive/ (zuletzt besucht am 14.07.2015).
[21] Cloud-Suite auf http://www.sap.com/germany/pc/tech/cloud/software/cloud-applications/entreprise-suite.html (zuletzt besucht am 14.07.2015); vgl. auch Fraunhofer Institut, Cloud-Computing für die öffentliche Verwaltung, S. 17.
[22] BSI, Cloud Computing Grundlagen; vgl. auch SCHORER, Handbuch Cloud Computing, S. 65 Rz. 24 und S. 66 Rz. 27.
[23] KOBIK: Koordinationsstelle zur Bekämpfung der Internetkriminalität.
[24] Peer-to-Peer-Netzwerke („P2P") sind Rechnernetzwerke, bei denen alle Rechner gleichberechtigt im Netz zusammenarbeiten. Üblicherweise werden in solchen Netzwerken Daten ausgetauscht.

sich auf den lokal sichergestellten Datenträgern keine entsprechenden Daten finden lassen, da die tatverdächtige Person die strafrelevanten Dateien in einer Cloud gespeichert hat. Wenn nun die beschuldigte Person in einer Einvernahme nicht aussagt, einen Cloud-Dienst zu nutzen, und es auf den sichergestellten Datenträgern auch keine Hinweise (z.B. Browserverlauf) dafür gibt, wird die ermittelnde oder untersuchende Behörde nie erfahren, dass die beschuldigte Person einen Cloud-Dienst benutzt.

Ein zweites Problem stellt sich bei folgender Konstellation: Der Beschuldigte, ein mutmasslicher Betrüger, führt ein belegloses Büro, d.h. er nutzt Online-Anwendungen für seine Arbeit und sämtliche damit erstellten Dokumente sind in einer Cloud abgespeichert. Es ist der ermittelnden Behörde bekannt, welche Anbieterin er benutzt. Der Beschuldigte rückt aber das Passwort für seinen Zugang nicht heraus. Die Cloud-Anbieterin hat ihren Sitz in der Schweiz. Wo die Datenserver liegen, ist aber nicht bekannt.

Die dritte Konstellation stellt sich gleich dar wie die zweite, jedoch befindet sich die Cloud-Anbieterin im Ausland. Wie gelangt nun die Strafverfolgungsbehörde an die Daten, wenn die beschuldigte Person nicht kooperiert?

Weitere Fragen stellen sich bei der Sicherstellung von Daten in Clouds von Unternehmen: Was für einen Cloud-Dienst nutzt die Unternehmung? Handelt es sich dabei um eine Private Cloud, auf die nur die fragliche Unternehmung Zugriff hat?

Wo können die Daten erhältlich gemacht werden? Am Ort des Sitzes der Cloud-Anbieterin? Am Serverstandort? Hat die Cloud-Anbieterin überhaupt Zugriff auf die Daten oder stellt sie nur die Infrastruktur für den Kunden zur Verfügung (IaaS oder PaaS). Wer ist zuständig für diese Datenerhebung? Welche rechtlichen Grundlagen gibt es? Muss internationale Rechtshilfe beansprucht werden?

Diese Masterarbeit soll Wege aufzeigen, wie die Strafverfolgungsbehörden nach geltendem Recht an verfahrensrelevante Daten im In- und Ausland gelangen können, mit und ohne Kooperation der beschuldigten Person. Zudem soll sie Anregungen geben, in welchem Bereich das Recht weiterentwickelt werden soll. Kein Thema dieser Arbeit ist der Umgang mit sichergestellten verschlüsselten Daten.

# 2. Überblick über strafprozessuale Zwangsmassnahmen betreffend Datenerhebungen

## 2.1. Allgemeines

Zwangsmassnahmen sind Verfahrenshandlungen der Strafbehörden, die in Grundrechte der Betroffenen eingreifen und die u.a. dazu dienen Beweise zu sichern (Art. 196 StPO). Sie können nur ergriffen werden, wenn dafür eine gesetzliche Grundlage besteht (Art. 197 Abs. 1 lit. a StPO), ein hinreichender Tatverdacht vorliegt (Art. 197 Abs. 1 lit. b StPO), keine milderen Mittel den gleichen Zweck ermöglichen (Art. 197 Abs. 1 lit. c StPO; Subsidiarität[25]) und die Bedeutung der Straftat die Zwangsmassnahme rechtfertigt (Art. 197 Abs. 1 lit. d StPO; Proportionalität[26]). Nach Abs. 2 von Art. 197 StPO sind Zwangsmassnahmen auch gegen nicht beschuldigte Personen möglich. Jedoch sollten diese mit besonderer Zurückhaltung angeordnet werden.[27]

Die StPO sieht keine Normen vor, die sich explizit auf die Beweissammlung im Internet beziehen. Es gibt jedoch einige Regelungen in der StPO, die Anknüpfungspunkte bieten, um im Internet – und damit in einer Cloud – an Beweise zu gelangen.[28] Im Folgenden werden diese Normen näher erläutert.

## 2.2. Durchsuchung von Aufzeichnungen

Art. 246 StPO ermöglicht die Durchsuchung von Aufzeichnungen, wenn zu vermuten ist, dass darin Informationen zu finden sind, die der Beschlagnahme unterliegen. Als Beweisgegenstände im Sinne von Art. 246 StPO bzw. Art. 192 StPO werden nicht nur Urkunden nach Art. 110 Abs. 4 StGB erfasst, sondern jedes Schriftstück mit einem entsprechenden Informationsgehalt. Darunter fallen auch elektronische Datenaufzeichnungen.[29] Grundsätzlich verlangt Art. 192 Abs. 1 StPO, dass die Strafbehörde die Beweisgegenstände vollständig und im Original zu den Akten nimmt. In Anwendung des Verhältnismässigkeitsgrund-

[25] HUG/SCHEIDEGGER, StPO-Kommentar, Art. 197 N 17.
[26] HUG/SCHEIDEGGER, StPO-Kommentar, Art. 197 N 20.
[27] HUG/SCHEIDEGGER, StPO-Kommentar, Art. 197 N 22 f.; RIGHETTI, Kommentierte Textausgabe StPO, S. 189.
[28] GLESS, ZStrR 130 (2012), Strafverfolgung im Internet, S. 6.
[29] BBl 2006 1085, S. 1214; vgl. auch SCHMID, Handbuch StPO, N 958 und N 1073; DONATSCH, StPO-Kommentar, Art. 192 N 5; KELLER, StPO-Kommentar, Art. 246 N 6; THORMANN/BRECHBÜHL, BSK StPO, Art. 246 StPO N 3; BGE 137 IV 189 E. 4 S. 194.

satzes dürfen auch Kopien erstellt werden, wenn dies für die Zwecke des Verfahrens genügt (Art. 192 Abs. 2 StPO und Art. 247 Abs. 3 StPO).[30] In Bezug auf die Durchsuchung und Sicherung einer Cloud ist die Möglichkeit der Kopie (Spiegelung) im Sinne der Verhältnismässigkeit von grosser Bedeutung. Gerade bei einer Public Cloud kann nicht die ganze Infrastruktur im Original „zu den Akten genommen" werden, da auf einer solchen Cloud auch Daten von Unbeteiligten gespeichert sind, welche weiterhin auf den Cloud-Dienst Zugriff haben sollten.[31] Jedoch kann es der Beschlagnahmezweck (Art. 263 StPO) verlangen, dass die Originaldaten erhoben werden müssen. Dies ist der Fall, wenn es nicht nur um die Erhebung von Beweismitteln geht, sondern auch die spätere Einziehung der Daten gesichert werden soll. Zu denken ist dabei z.B. an kinderpornografische Dateien.[32]

Die Bestimmung von Art. 246 StPO ist Grundlage dafür, dass bei einer Hausdurchsuchung[33] sichergestellte Datenträger auf straf- und verfahrensrelevante Daten ausgewertet werden dürfen. Gemäss Art. 241 StPO muss eine Durchsuchung von Aufzeichnungen wie alle weiteren Durchsuchungen oder Untersuchungen in einem schriftlichen Befehl angeordnet werden. Nur in dringenden Fällen kann die Anordnung mündlich erfolgen, muss aber nachträglich schriftlich bestätigt werden.

## 2.3. Exkurs: Online-Durchsuchung nach Art. 246 StPO

Art. 246 StPO begründet nach herrschender Meinung keine gesetzliche Grundlage für eine Online-Durchsuchung von Aufzeichnungen, da es sich bei einer Massnahme nach Art. 246 StPO um eine offene Zwangsmassnahme handelt, die für den Betroffenen erkennbar ist und entsprechend Art. 241 StPO diesem grundsätzlich mit schriftlichem Befehl mitzuteilen ist.[34] Die Online-Durchsuchung eines einzelnen Gerätes hätte mit der Revision des BÜPF und Schaffung einer gesetzlichen Grundlage für den Einsatz von GovWare[35] eingeführt

[30] Vgl. RFJ/FZR 2008 86; SCHMID, Handbuch StPO, N 1075; DONATSCH, StPO-Kommentar, Art. 192 N 15 f.; THORMANN/BRECHBÜHL, BSK StPO, Art. 246 StPO N 27 und N 30; BBl 2006 1085, S. 1239.
[31] Vgl. THORMANN/BRECHBÜHL, BSK StPO, Art. 246 StPO N 27.
[32] Vgl. THORMANN/BRECHBÜHL, BSK StPO, Art. 247 StPO N 31.
[33] Gemäss Art. 244 StPO Abs. 2 lit. b ist eine Hausdurchsuchung ohne Einwilligung der berechtigten Person u.a. möglich, wenn zu vermuten ist, dass im zu durchsuchenden Raum zu beschlagnahmende Gegenstände vorhanden sind.
[34] THORMANN/BRECHBÜHL, BSK StPO, Art. 246 StPO N 5; SCHMID, Handbuch StPO, N 1061, Fn 256; KELLER, StPO-Kommentar, Art. 246 N 8; AEPLI, S. 132; HEIMGARTNER, Strafprozessuale Beschlagnahme, S. 41.
[35] Gemäss Wikipedia (https://de.wikipedia.org/wiki/Govware; zuletzt abgerufen am 13.07.2015) werden Computerprogramme als Govware (Kofferwort aus engl. governmental, „behördlich" und Software) bezeichnet, die von einem Staat oder einem für den Staat arbeitenden Privatunternehmen entwickelt wurden, um vom Benutzer unerwünschte und ggf. schädliche Funktionen auszuführen. In der Schweiz sollen in Zukunft die Kommunikationsinhalte und Randdaten insbesondere von Smartphones und Computer (Voice

werden können[36], wurde aber explizit im neu zu schaffenden Art. 269ter StPO ausgenommen.[37] Folglich wird es vorläufig in der Schweiz wegen der fehlenden gesetzlichen Grundlage keine Möglichkeit einer Online-Durchsuchung eines einzelnen Gerätes geben.[38] Dagegen könnte aber die Online-Durchsuchung einer Cloud unter den Bestimmungen von Art. 269 f. StPO im Sinne einer geheimen Überwachung möglich sein.

## 2.4. Beschlagnahme

Nach Art. 263 Abs. 1 lit. a StPO können Gegenstände bei beschuldigten Personen wie auch bei einer Drittperson beschlagnahmt werden, die voraussichtlich als Beweismittel gebraucht werden. Es stellt sich die Frage, ob elektronische Daten als Gegenstände im Sinne von Art. 263 StPO zu verstehen sind oder nur der Datenträger beschlagnahmt werden kann. Es könnte im Fall von Daten, die auf einer Cloud liegen, zu Schwierigkeiten führen, wenn als Gegenstand nur beschlagnahmt werden kann, was bereits physisch existiert.[39] Nach SCHMID[40] kann auf eine rechtliche Grundlage der Beschlagnahme von Daten über den Grundsatz „a maiore minus“[41] geschlossen werden: Wenn theoretisch eine ganze Serverfarm beschlagnahmt werden dürfte, muss auch die Beschlagnahme von noch herzustellenden Kopien einzelner Daten als milderes Mittel möglich sein. Einen anderen Ansatz verfolgt HEIMGARTNER[42], indem er den Begriff „Gegenstand“ als Synonym für ein abgeschlossenes, reales oder ideales Objekt, das dem Betrachter gegenübersteht, verstanden sieht. Darunter seien auch Informationen in Form elektronischer Daten zu subsumieren. Auch BANGERTER argumentiert dafür, dass der Begriff „Gegenstand“ weit zu verstehen ist, so dass sowohl körperliche wie auch unkörperliche Objekte damit erfasst sind.[43] Das Bundesgericht entschied zudem mehrfach bei Entsiegelungsverfahren, wenn ein Datenträger Daten enthält, welche dem Anwaltsgeheimnis unterliegen, dass diese durch den Entsiege-

over IP) mittels GovWare überwacht werden können (vgl. Entwurf Art. 269ter StPO; HANSJAKOB, StPO-Kommentar, Art. 269ter N 1 ff.).

[36] Vgl. THORMANN/BRECHBÜHL, BSK StPO, Art. 246 StPO N 5.

[37] Vgl. Botschaft BÜPF vom 27.02.2013, S. 2702; S. 2772; S. 2774; S. 2776; S. 2778 und S. 2779; HANSJAKOB, StPO-Kommentar, Art. 269ter N 4.

[38] Vgl. auch BANGERTER, S. 10.

[39] BOMMER/GOLDSCHMID, BSK StPO, Art. 263 N 28; BGE 126 I 50 E. 4c S. 58 f. .

[40] SCHMID, Strafprozessuale Fragen ZStrR. S. 96.

[41] a maiore minus bzw. argumentum a maiore ad minus ist ein Grundsatz der juristischen Methodenlehre und bezeichnet den Schluss vom Grösseren auf das Kleinere, von einer weitergehenden Regelung auf einen weniger Voraussetzungen erfordernden Fall (EGON SCHNEIDER [Begründer], FRIEDRICH E. SCHNAPP: Logik für Juristen. Die Grundlage der Denklehre und der Rechtsanwendung. 6. Aufl., München 2006).

[42] HEIMGARTNER, Strafprozessuale Beschlagnahme, S. 89.

[43] BANGERTER, S. 248.

lungsrichter ausgeschieden werden müssen.[44] Können bzw. müssen einzelne Daten ausgeschieden werden und versiegelt bleiben, hat dies m.E. zur Folge, dass auch elektronische Daten unabhängig von einem Datenträger nach Art. 263 StPO beschlagnahmt werden können.

Eine andere Meinung vertritt u.a. AEPLI. Er kommt zum Schluss, dass elektronisch gespeicherte Daten keine Gegenstände sind und folglich nicht Objekt der Beweismittelbeschlagnahme sein können. Er stützt sich dabei v.a. auf die historische, systematische und teleologische Auslegung von § 96 Abs. 1 ZH-StPO (dieser Paragraph entspricht im Grossen und Ganzen dem heutigen Art. 263 StPO).[45]Auch RYSER ist der Meinung, dass Daten durch ihre „Unkörperlichkeit" nicht unter den Begriff „Gegenstände" zu subsumieren sind und daher nicht Objekte der Beweismittelbeschlagnahme sein können.[46] Diese Ansicht vertritt auch KELLER: *„Informationen sind etwas Immaterielles und können als solches nicht beschlagnahmt werden. Beschlagnahmt werden können nur körperliche Gegenstände, auf oder in denen Informationen irgendeiner Form aufgezeichnet sind."*[47] Nach den geschilderten Auffassungen ist die Beschlagnahme von Daten nur durch die Beschlagnahme des physischen Datenträgers möglich, auf dem die Daten gespeichert sind.[48]

## 2.5. Exkurs: Sperrverfügung

Wenn der Zweck der Beschlagnahme die spätere Einziehung ist (Art. 263 Abs. 1 lit. d StPO), kann als zumindest vorübergehende Massnahme die Sperrung eines Zuganges zu einem Cloud-Dienst diskutiert werden. Dies kann bspw. sinnvoll sein, wenn eine beschuldigte Person in einer Public Cloud strafrelevante Dateien gespeichert hat. In der Schweizerischen Strafprozessordnung wird eine solche Sperrverfügung nicht explizit erwähnt. Es stellt sich daher die Frage, ob eine solche unter dem Titel der Beschlagnahme verfügt werden kann.

Die Beschwerdekammer des Bundesstrafgerichts hatte zu beurteilen, ob Art. 46 VStrR (Beschlagnahme; entspricht mehr oder weniger Art. 263 StPO) eine ausreichende rechtliche Grundlage für die Sperrung einer Internetseite darstellt, zumal die Sperrung von Internetseiten als eigene Zwangsmassnahme im VStrR nicht aufgeführt ist. Grundsätzlich wäre

[44] Vgl. BGE 126 II 495, E. 5e/aa S. 501 f.; BGE 130 II 193 E. 2.1 S. 195; BGE 137 IV 189 E. 4 S. 194.
[45] AEPLI, S. 44 ff., insb. S. 59.
[46] RYSER, S. 561.
[47] KELLER, StPO-Kommentar, Art. 246 N 6.
[48] Vgl. BANGERTER, S. 246; zum Einziehungsobjekt vgl. BOMMER, Löschung als Einziehung von Daten, S. 178 f.

unter Anwendung von Art. 46 Abs. 1 lit. b VStrR im Sinne einer Sicherungsbeschlagnahme die Wegnahme der Hardware für den Zugang zu den fraglichen Internetseiten möglich gewesen. Die Sperre der Internetseite stellt eine mildere Massnahme als die Beschlagnahme von Gegenständen dar. Das Bundesstrafgericht kommt zum Schluss, dass die Bestimmung von Art 46 Abs. 1 lit. b VStrR im Sinne von „a maiore minus" als gesetzliche Grundlage für eine solche Sperre ausreicht.[49]

Zum gleichen Ergebnis kommt auch die Beschwerdekammer des Kantonsgerichts Waadt, die eine Beschwerde gegen eine verfügte Sperrung des Zugangs zu einem Blog zu beurteilen hatte, auf welchem ehrverletzende Äusserungen gepostet waren. Sie führt aus, dass bei einer Webseite mit einem Blog nicht eigentlich von einem körperlichem Objekt im Sinne von Art. 69 StGB gesprochen werden kann. Dennoch sei sie gleich zu behandeln. Eine solche Auslegung sei konform, wenn nicht nach dem Wortlaut, dann zumindest nach dem Sinn. Dem technischen Fortschritt sei bei der Auslegung der Norm Rechnung zu tragen (unter Hinweis auf BGE 131 IV 16, wo entschieden wurde, dass das Herunterladen von pornografischen Bildern als Herstellen von Pornografie i.S. Art. 197 Abs. 3 StGB gelte.). Art. 263 Abs. 1 lit. d StPO ist folglich eine hinreichende gesetzliche Grundlage für die vorläufige Sperrung des Zugangs zu einem Blog.[50]

Im Kanton Waadt war das Kantonsgericht jedoch nicht immer dieser Ansicht. Schwarzenegger schildert den Fall der Lausanner Sperrverfügungen vom 11. Dezember 2002: Eine Untersuchungsrichterin verfügte unter Androhung von Art. 292 StGB, dass 32 Access-Provider mit Sitz in diversen Kantonen der Schweiz den Zugang zu einer Webseite mit ehrverletzenden Inhalten zu sperren haben. Gegen diese Verfügung erhoben die Verfügungsadressaten Rekurs beim Kantonsgericht Waadt (Tribunal d'accusation du Canton de Vaud). Das angerufene Kantonsgericht entschied schliesslich, dass ein Internetzugang kein Gegenstand im Sinne von Art. 58 Abs. 1 aStGB sein kann, weshalb die strafprozessuale Zwangsmassnahme der Beschlagnahme unzulässig sei. Die Sperrverfügungen waren daher nach Auffassung des Kantonsgerichts Waadt nichtig.[51]

[49] Urteil BStGer BV.2004.26 vom 16.02.2005.
[50] Chambre des recours pénale canton de Vaud, 2014/540, Entscheid-Nr. 416, vom 18.06.2014, E. 4.
[51] SCHWARZENEGGER, Sperrverfügungen gegen Access-Provider, S. 257 f.

## 2.6. Edition

In Art. 265 Abs. 1 StPO wird eine Herausgabepflicht des Inhabers von zu beschlagnahmenden Gegenständen (und Vermögenswerten) statuiert. Ausgenommen von dieser Pflicht sind gemäss Art. 265 Abs. 2 StPO die beschuldigte Person (lit. a) und Unternehmen (lit. c) wegen des Verbots des Selbstbelastungszwangs und Personen, die ein Zeugnis- oder Aussageverweigerungsrecht haben (lit. b). Die herauszugebenden Gegenstände können mit einer Verfügung eingefordert werden (Editionsverfügung; Art. 265 Abs. 3 StPO)[52]. Da m.E. auch Daten als beschlagnahmefähige Gegenstände gelten (siehe oben), können solche grundsätzlich auch mittels Editionsverfügung eingeholt werden. Der Editionspflichtige hat die geforderten Daten, die ohne aufwändige Suche aufzufinden sind, auf Datenträger zu kopieren oder auszudrucken. Er kann aber nicht verpflichtet werden, nach deliktsrelevanten Objekten zu suchen.[53]

Häufig werden Editionen in einem Stadium des Verfahrens angeordnet, in welchem die beschuldigte Person noch nicht weiss, dass ein Strafverfahren gegen sie im Gange ist. Damit ein gewisser Überraschungseffekt bleibt bzw. die Ermittlungen durch die zu frühe Kenntnis der beschuldigten Person vom Strafverfahren nicht gefährdet werden, wird in vielen Fällen in der Editionsverfügung ein Mitteilungsverbot angeordnet, meist unter Androhung einer Strafe gemäss Art. 292 StGB. Es stellt sich die Frage, ob ein solches Mitteilungsverbot zulässig ist, zumal es sich bei der Edition grundsätzlich um eine offene und nicht um eine heimliche Massnahme handelt. BOMMER und GOLDSCHMID erörtern das Mitteilungsverbot anhand der (heimlichen) Kontosperre.[54] Sie diskutieren u.a., ob die Geheimhaltungspflicht nach Art. 73 Abs. 2 StPO oder die Zeugnispflicht nach Art. 163 Abs. 2 StPO bzw. das Schweigegebot für Zeugen (Art. 165 StPO) gesetzliche Grundlage bieten zur Anordnung eines Mitteilungsverbotes. Weil beide Bestimmungen die Geheimhaltungspflicht nicht generell regeln, sondern mit diesen nur spezifischen Geheimhaltungsbedürfnissen begegnet werden soll, stellen sie nach Ansicht von BOMMER und GOLDSCHMID keine geeignete Grundlage für das Mitteilungsverbot dar.[55] BOMMER und GOLDSCHMID kommen zum Schluss, dass keine gesetzliche Grundlage im Sinne von Art. 197 Abs. 1 lit. a StPO besteht, um ein eine heimliche Kontosperre zu erlassen. Sie verweisen aber darauf, dass das Bundesgericht eine befristete Informationssperre implizit als zulässig erachtet, da

[52] HEIMGARTNER, StPO-Kommentar, Art. 265 N 10.
[53] HEIMGARTNER, Strafprozessuale Beschlagnahme, S. 63.
[54] BOMMER/GOLDSCHMID, BSK StPO, Art. 266 StPO N 16 ff.
[55] BOMMER/GOLDSCHMID, BSK StPO, Art. 266 StPO N 20 und 21.

es sich nur um einen leichten Grundrechtseingriff handle, der sich auf die Generalklausel in Art. 101 Abs. 2 BStP[56] stützen lasse, und (nur) schwere Eingriffe einer ausreichenden formalgesetzlichen Grundlage bedürfen.[57] Aufgrund dieses Bundesgerichtsentscheides dürfte ein Mitteilungsverbot auch bei einer Datenedition möglich sein.

## 2.7. Geheime Überwachungsmassnahmen

### 2.7.1. Allgemeine Voraussetzungen

Art. 269 f. StPO erlaubt unter den folgenden Voraussetzungen die Überwachung des Post- und Fernmeldeverkehrs der beschuldigten Person und (eingeschränkt)[58] von Drittpersonen: Es muss ein dringender Tatverdacht auf eine Katalogtat[59] vorliegen, die Schwere der Straftat muss die Überwachung rechtfertigen und die bisherigen Untersuchungshandlungen sind erfolglos geblieben oder die Ermittlungen wären ohne die Überwachungsmassnahme aussichtlos oder würden unverhältnismässig erschwert (Art. 269 Abs 1 StPO). Die Überwachung des Post- und Fernmeldeverkehrs benötigt die Genehmigung durch das Zwangsmassnahmengericht (Art. 272 Abs. 1 StPO).

### 2.7.2. Daten des Fernmeldeverkehrs

Die Bestimmungen zur Überwachung des Fernmeldeverkehrs sind bei der Erhebung von Daten in einer Cloud von Bedeutung, wenn es sich dabei um Daten handelt, die dem Fernmeldegeheimnis unterliegen. Es stellt sich aber die Frage, ob Cloud-Service-Provider an das Fernmeldegeheimnis gebunden sind und folglich die Bestimmungen des BÜPF bzw. von Art. 269 ff. StPO zur Überwachung des Datenverkehrs mit einem Cloud-Service-Provider anwendbar sind. Das Fernmeldegeheimnis ergibt sich aus Art. 13 Abs. 1 BV und konkreter aus Art. 43 FMG.[60] Art. 2 FMG bezeichnet als Gegenstand des Fernmeldegesetzes die fernmeldetechnische Übertragung von Informationen, die nicht dem Bundesgesetz über Radio und Fernsehen unterstehen.[61] Informationen sind nach Art. 3 lit. a FMG für Menschen, andere Lebewesen oder Maschinen bestimmte Zeichen, Signale, Schriftzeichen, Bilder, Laute und Darstellungen jeder anderen Art. Die fernmeldetechnische Übertragung

[56] Art. 101 Abs. 2 BStP entspricht Art. 139 Abs. 1 StPO.
[57] BOMMER/GOLDSCHMID, BSK StPO, Art. 266 StPO N 23 mit Hinweis auf BGE 131 I 425.
[58] Art. 270 lit. b StPO.
[59] Katalogtaten sind unter Art. 269 Abs. 2 StPO abschliessend aufgeführt.
[60] Vgl. BIAGGINI, Kommentar BV, Art. 13 N 10.
[61] Vgl. HANSJAKOB, BÜPF-Kommentar, Art. 1 BÜPF N 23; AEPLI, S. 16.

wird in Art. 3 lit. c FMG definiert als elektrisches, magnetisches, optisches oder anderes, elektromagnetisches Senden oder Empfangen von Informationen über Leitungen oder Funk. Art. 4 Abs. 1 FMG sieht für Erbringerinnen von Fernmeldediensten eine Meldepflicht vor. Das Bundesamt für Kommunikation (BAKOM) führt ein Register der gemeldeten Anbieterinnen. Um herauszufinden, ob Anbieterinnen von Cloud-Diensten als Fernmeldediensterbringerinnen im Sinne des FMG gelten, könnte das Register des BAKOM auf Cloud-Dienstanbieterinnen durchsucht werden. Ich habe dieses Experiment mit einem kleinen Cloud-Service-Provider durchgeführt.[62] Die Liste des BAKOM kann nach Namen, nach Diensten (Telefondienst, Verbreitung Radio-/Fernsehprogramme, Internet Zugang etc.) und nach Arten (DVB-T, GSM, Satelliten, Richtfunk etc.) durchsucht werden.[63] Da der Dienst „Cloud" nicht aufgeführt war, habe ich zunächst die Liste der Anbieterinnen „Internet Zugang" durchgesehen. Der ausgewählte CSP fand sich nicht darunter (er ist aber auch kein Anbieter eines Internetzugangs). Danach habe ich nach dem Namen der Gesellschaft gesucht, was auch nicht erfolgreich war. Aus diesem Ergebnis müsste gefolgert werden, dass ein Cloud-Service-Provider kein Anbieter von Fernmeldediensten ist. Jedoch kann nach Art. 4 Abs. 2 FMG der Bundesrat insbesondere für Fernmeldedienste von geringer technischer und wirtschaftlicher Bedeutung Ausnahmen vorsehen. Da es sich beim Cloud-Service-Provider in meinem Experiment um eine kleine Unternehmung handelt, ist die Möglichkeit gross, dass dieser unter die Ausnahme von Art. 4 Abs. 2 FMG fällt. Das durchgeführte Experiment konnte also die Frage nicht beantworten, ob ein Cloud-Service-Provider Anbieter von Fernmeldediensten im Sinne des FMG ist. HANSJAKOB schreibt im BÜPF-Kommentar zur Ausnahmeregelung von Art. 4 Abs. 2 FMG, dass diese *„die fatale Folge hat, dass die nicht meldepflichtigen Anbieterinnen überhaupt nicht mehr unter den Anwendungsbereich des BÜPF fallen."*[64] Gemäss Art. 1 Abs. 2 BÜPF unterliegen dem Geltungsbereich des BÜPF alle staatlichen, konzessionierten oder meldepflichtigen Anbieterinnen von Post- und Fernmeldedienstleistungen sowie Internet-Anbieterinnen. Nach Hansjakob unterliegen jedoch nur reine Access-Provider (Internetzugang) der Meldepflicht nach Art. 4 Abs. 1 FMG, reine Service-Provider nicht. Wird also auf die Meldepflicht abgestellt, unterliegen reine Service-Provider nicht dem BÜPF.[65] Da viele Internet Service Provider (ISP; dazu gehören auch Cloud-Service-Provider) keine Access-Provider sind,

[62] Alpha Solutions AG, weil diese AG im Juli 2015 ein ansprechendes Werbeplakat in einer der Unterführungen am Bahnhof St. Gallen angeschlagen hatte.
[63] BAKOM, Suche unter Fernmeldedienstanbieter, https://www.eofcom.admin.ch/eofcom/public/searchCatalog.do (zuletzt besucht am 27.07.2015).
[64] HANSJAKOB, BÜPF-Kommentar, Art. 1 BÜPF N 23.
[65] HANSJAKOB, BÜPF-Kommentar, Art. 1 BÜPF N 24.

wären solche nach der geschilderten Auslegung wegen der fehlenden Meldepflicht nicht in Anwendung des BÜPF überwachbar. Aus der Botschaft zum BÜPF vom 1. Juli 1998 lässt sich aber ableiten, dass diese Auslegung nicht der Meinung des Gesetzgebers entspricht.[66] Sofern ein Internet-Service-Provider eine öffentliche Dienstleistung anbietet, gelangt das BÜPF zur Anwendung, auch wenn der Dienstleister nicht meldepflichtig ist. Wenn ein Dienstleister ausschliesslich innerhalb eines Unternehmens Informationen mittels der unternehmenseigenen Infrastruktur weiterleitet, betreibt er keinen Fernmeldedienst und unterliegt damit nicht dem Fernmeldegeheimnis.[67] Solche Daten sind mittels Durchsuchung und Beschlagnahme zu erheben.[68]

In Art. 1 Abs. 2 BÜPF wird von „Internet-Anbieterinnen" gesprochen, in Art. 1 Abs. 2 lit. e VÜPF von „Internetzugangsanbieterinnen". Internetzugangsanbieterin wird in Ziff. 1 des Anhangs zur VÜPF beschrieben als *„Fernmeldedienstanbieterin oder der Teil einer Fernmeldedienstanbieterin, die der Öffentlichkeit fernmeldetechnische Übertragungen von Informationen auf der Basis der IP-Technologien (Netzprotokolle im Internet [Internet Protocol]) unter Verwendung von IP-Adressen anbietet."*[69] Nach der Definition in der VÜPF müsste vom Wortlaut her davon ausgegangen werden, dass nur Internet-Access-Provider unter die Bestimmungen des VÜPF fallen, andere Internet-Service-Provider nicht.

### 2.7.3. Daten bei E-Mail-Providern

Es ist mittlerweile unbestritten, dass gerade Anbieter von E-Maildiensten, auch wenn diese keine Internetzugangsanbieter (Access-Provider) sind, unter das FMG und somit unter die Bestimmungen des BÜPF und unter die Anwendung von Art. 269 ff. StPO fallen. Nach herrschender Lehre und nach bundesgerichtlicher Rechtsprechung unterliegen aber nur solche Daten dem Fernmeldegeheimnis, die sich in einer Übermittlungsphase befinden. Vor und nach der Übertragung unterstehen die Daten nicht dem Fernmeldegeheimnis.[70] In analogiam wird die Überwachung des Postverkehrs zur Auslegung herangezogen, um zu klären, in welchem Zeitraum E-Mails dem Fernmeldegeheimnis unterliegen. Bei einem Brief liegt eine Überwachung vor, wenn ihn der Absender abgeschickt hat und die Strafverfolgungsbehörde darauf zugreift, bevor dieser beim Empfänger angekommen ist. Nach

[66] BBl 1998 4241, S. 4255; vgl. auch HANSJAKOB, BÜPF-Kommentar, Art. 1 BÜPF N 25.
[67] HANSJAKOB, BÜPF-Kommentar, Art. 1 BÜPF N 25; vgl. auch SCHNEIDER, AJP 2005, S. 184; AEPLI, S. 16.
[68] Vgl. BBl 1998 4241, S. 4255; AEPLI, S. 17.
[69] Vgl. SCHNEIDER, AJP 2005, S. 183.
[70] AEPLI, S. 17 und S. 18; JEAN-RICHARD-DIT-BRESSEL, ZStrR 125 (2007), S. 171; BGE 140 IV 181.

Ankunft des Briefes im Briefkasten befindet sich dieser im Herrschaftsbereichs des Empfängers und der Übermittlungsvorgang ist abgeschlossen. Der Brief kann nun beschlagnahmt werden.[71] Verfügt der Adressat über ein Postfach und wird der Brief dort zugestellt, liegt dieser bis zur Leerung durch den Empfänger im Herrschaftsbereich der Post. Sie kann den Brief wieder aus dem Postfach nehmen und der Strafverfolgungsbehörde übergeben.[72] JEAN-RICHARD-DIT-BRESSEL geht von einer geteilten Datenherrschaft aus, bei der im Falle eines Postfachs sowohl der Empfänger wie auch die Post Zugriff auf die Briefe haben. Der Empfänger kann den Brief aus dem Postfach nehmen und dann wieder hineinlegen. Auch kann die Post den Brief wieder herausnehmen.[73] Der Kommunikationsvorgang ist erst abgeschlossen, wenn der Empfänger die alleinige Datenherrschaft erlangt. Nach bundesgerichtlicher Auffassung erlangt der Empfänger die alleinige Datenherrschaft, wenn er das Postfach öffnet. Er bestimmt ab diesem Zeitpunkt, was mit dem Brief geschieht. Er kann den Brief öffnen oder nicht, mitnehmen oder fortwerfen, im Postfach belassen und dort aufbewahren. Wenn er ihn im Postfach belässt, kann der Brief beschlagnahmt werden. Gemäss Bundesgericht kann es keinen Unterschied machen, wo der Empfänger den Brief aufbewahrt. Sei es zuhause, im Postfach bei der Post oder bei einem Dritten. Das Zugreifen der Strafverfolgungsbehörde auf einen Brief, den der Empfänger aufbewahrt, ereignet sich folglich nach Abschluss des Kommunikationsvorgangs und nicht heimlich. Es handelt sich dabei also nicht um eine Überwachungsmassnahme.[74]

In Bezug auf E-Mails bedeutet die Analogie zur Briefpost folgendes: Wenn ein E-Mail auf dem Server des Empfängerproviders in das E-Mailkonto des Empfängers gelangt, dann entspricht dies dem Einlegen eines Briefes in das Postfach. Das Einloggen des E-Mail-Benutzers in sein E-Mailkonto entspricht dem Öffnen des Postfachs. Er erlangt damit Kenntnis vom Eingang der E-Mail und damit auch die Datenherrschaft. Er kann alleine bestimmen, was mit der E-Mail geschieht. Er kann sie löschen, herunterladen oder auf dem Server des Providers weiteraufbewahren. Ab diesem Zeitpunkt ist der Kommunikationsvorgang beendet und die E-Mail nicht mehr durch das Fernmeldegeheimnis geschützt.[75]

E-Mails, die auf einem Mailserver liegen, aber vom Benutzer noch nicht abgerufen wurden, unterliegen aber noch dem Fernmeldegeheimnis. Sie befinden sich bis zum Abruf durch den Kontoinhaber in der Übermittlungsphase und unterliegen damit dem Fernmelde-

[71] BGE 140 IV 181 E. 2.4 S. 184.
[72] BGE 140 IV 181 E. 2.5.2 S. 185.
[73] JEAN-RICHARD-DIT-BRESSEL, ZStrR 125 (2007), S. 172.
[74] BGE 140 IV 181 E. 2.5.3 S. 185.
[75] BGE 140 IV 181 E. 2.6 S. 186; JEAN-RICHARD-DIT-BRESSEL, ZStrR 125 (2007), S. 173 f.

geheimnis.[76] Folglich kommen bei einer derartigen Datenerhebung die Bestimmungen von Art. 269 ff. StPO zur Anwendung. Im Gegensatz dazu unterliegen E-Mails der Beschlagnahme, wenn der Kontoinhaber durch ein erfolgtes Einloggen in sein Konto von diesen E-Mails bereits Kenntnis hat.[77]

### 2.7.4. Daten bei Cloud-Service-Providern

Wie in der Einleitung kurz erwähnt, fallen Webmail-Provider unter die Cloud-Service-Provider im Sinne von Software as a Service (SaaS).[78] Es stellt sich die Frage, ob bei anderen Cloud-Diensten die gleiche Vorgehensweise wie bei den Webmail-Diensten zur Anwendung gelangt, also unterschieden werden muss, ob sich die zu erhebenden Daten in einer Übermittlungsphase befinden oder nicht. Während des Übermittlungsvorgangs unterstünden die Daten demnach dem Fernmeldegeheimnis und müssten nach den Bestimmungen von Art. 269 ff. StPO erhoben werden. Nach Abschluss des Übermittlungsvorgangs könnten die Daten via Edition herausverlangt werden und müssten allenfalls versiegelt werden. Diese Ansicht vertritt JEAN-RICHARD-DIT-BRESSEL im Basler Kommentar zur StPO, welcher im Grundsatz zuzustimmen ist.[79] Jedoch spielt es m.E. auch eine Rolle, um welche Art von Cloud-Dienst es sich im konkreten Fall handelt. In diesem Sinne liegt der Ansatz von HEIMGARTNER nahe, die Bestimmung der zu erhebenden Daten als Unterscheidungsmerkmal zu verwenden: Sind die Daten für Dritte bestimmt, unterstehen sie dem Fernmeldegeheimnis und müssen nach dem Verfahren von Art. 269 ff. StPO erhoben werden. Sind sie nicht für Dritte bestimmt, unterliegen sie der Beschlagnahme.[80] Daten, die sich bspw. im Sinne eines papierlosen Büros oder als Sicherungskopie auf einem Datenserver ausserhalb der lokalen IT-Infrastruktur befinden, unterliegen m.E. nicht dem Fernmeldegeheimnis, da keine fernmeldetechnische Übertragung von Informationen für Dritte im Sinne von Art. 3 lit. b FMG stattfindet.[81] In diesem Bereich kann die Unterscheidung von Private Cloud und Public Cloud von Bedeutung sein. Beim Vorliegen einer Private Cloud ist eher zu vermuten, dass die Daten nur für die firmeninterne Nutzung gedacht sind. Bei einer Public Cloud wird wohl eher von einer Zurverfügungstellung auch für Dritte ausgegangen. Jedoch kann dies nicht verallgemeinert werden. Bei der Abfassung dieser Arbeit habe ich einen Cloud-Dienst zur Herstellung einer Backup-Kopie benutzt. Bei dem

[76] AEPLI, S. 21 f.; HANSJAKOB, BÜPF-Kommentar, Vorbemerkungen BÜPF, N 20.
[77] BGE 140 IV 181 E. 2.6 S. 186; TPF 2008 42, S. 43.
[78] Vgl. Ausführungen auf S. 16.
[79] JEAN-RICHARD-DIT-BRESSEL, BSK StPO, Art. 269 StPO N 24.
[80] HEIMGARTNER, Strafprozessuale Beschlagnahme, S. 184 f.
[81] Vgl. DONATSCH/SCHMID, S. 156.

von mir benutzten Cloud-Dienst handelt es sich um eine Public Cloud. Die gespeicherten Daten sind aber nicht für Dritte bestimmt. Eine Erhebung dieser Daten müsste mittels Beschlagnahme und nicht mittels geheimer Überwachungsmassnahmen erfolgen.

Wie stellt sich aber die Situation dar, wenn mittels eines Tools mehrere Personen über einen Cloud-Dienst am gleichen Dokument arbeiten? Wenn es sich dabei um Personen handelt, die in der gleichen Unternehmung tätig sind und für ein Projekt am gleichen Dokument arbeiten, dann greifen meiner Ansicht nach die Bestimmungen zur Beschlagnahme, da das fragliche Dokument nicht für Dritte ausserhalb der Organisation bestimmt ist. Arbeiten daran aber auch Personen ausserhalb der Organisation, müsste wohl eine Überwachung nach Art. 269 ff. StPO stattfinden.

Ein weiterer Aspekt, der in einem konkreten Fall im Gegensatz zur Edition und Beschlagnahme für die Überwachung einer Cloud nach Art. 269 ff. StPO spricht, ist die Heimlichkeit der Massnahme. Sollen die Daten ohne Wissen der betroffenen Person erhoben werden, sind geheime Überwachungsmassnahmen anzuordnen.[82] Eine Alternative könnte die Edition mit Mitteilungsverbot sein, aber nur dann, wenn es sich nicht um Daten handelt, die dem Fernmeldegeheimnis unterliegen.

### 2.7.5. Rückwirkende Erhebung von Randdaten

Dem Fernmeldegeheimnis unterliegen auch die sogenannten Randdaten der Kommunikation wie Zeitpunkt, Länge und Teilnehmer, sofern diese Daten beim Fernmeldeanbieter gespeichert sind.[83] Dass auch solche Daten dem Fernmeldegeheimnis unterliegen, kann aus Art. 43 FMG i.V.m. Art. 24b VÜPF und Art. 273 StPO abgeleitet werden. Der Begriff Randdaten wird weder im BÜPF bzw. in der VÜPF noch in Art. 273 StPO verwendet. In diesen Bestimmungen wird von Verkehrs- und Rechnungsdaten gesprochen. „Randdaten" ist einfach ein anderer Ausdruck für Verkehrs- und Rechnungsdaten. Technisch korrekt müsste es Intercept Related Information heissen.[84]

Im Zusammenhang mit der Datenerhebung in Clouds kommt eine rückwirkende Erhebung von Randdaten im Sinne von Art. 273 StPO zur Anwendung, wenn beispielsweise Logfiles von Servern zu erheben sind. In solchen Logfiles wird protokolliert, wann welche IP-Adresse auf den Server zugegriffen hat. Im Gegensatz zur Echtzeitüberwachung bzw. zur

[82] Vgl. JEAN-RICHARD-DIT-BRESSEL, BSK StPO, Art. 269 StPO N 21.
[83] AEPLI, S. 23 ff.; vgl. auch Anhang VÜPF Ziff. 7 (Verkehrs- und Rechnungsdaten).
[84] HANSJAKOB, StPO-Kommentar, Art. 273 N 3; SCHMID, Praxiskommentar StPO, Art. 273 N 2.

Überwachung von Kommunikationsinhalten nach Art. 269 StPO muss lediglich ein dringender Tatverdacht auf ein Verbrechen oder Vergehen (oder eine Übertretung nach Art. 179septies StGB) vorliegen und keine Katalogtat nach Art. 269 Abs. 2 StPO (Art. 273 Abs. 1 StPO).

### 2.7.6. Online-Durchsuchung einer Cloud nach Art. 269 ff. StPO

Meines Erachtens kann unter dem Titel von Art. 269 ff. StPO keine Online-Durchsuchung einer Cloud durchgeführt werden, wenn die Daten auf der Cloud nicht unter den Geltungsbereich von Art. 1 Abs. 1 BÜPF fallen, es sich also nicht um Daten des Fernmeldeverkehrs handelt. Da auch die Durchsuchung von Aufzeichnungen nach Art. 246 StPO[85] keine gesetzliche Grundlage für eine *geheime* Online-Durchsuchung ermöglicht, kann eine solche Durchsuchung in der Schweiz nicht durchgeführt werden.

[85] Vgl. Ausführungen auf S. 7 f.

# 3. Vorgehensweise bei Daten bzw. CSP in der Schweiz

## 3.1. Freiwillige Datenherausgabe

Um an verfahrensrelevante Daten zu gelangen, ist es meist der einfachste Weg, die betroffene Person aufzufordern, die Daten freiwillig herauszugeben. In diesem Sinn kann die beschuldigte Person bspw. in einer Einvernahme nach den Benutzerdaten für die fragliche Cloud und nach der Einwilligung der Sichtung, Sicherung und Auswertung verfahrensrelevanter Daten gefragt werden.[86] Es stellt sich die Frage, ob in einer derartigen Konstellation der Betroffene die Möglichkeit der Siegelung hat oder diese mit der ursprünglichen Einwilligung in die Verfahrenshandlung verwirkt ist. Wenn die betroffene Person vor Durchführung die Einwilligung zur Durchsuchung und Auswertung gegeben hat, liegt eine Willensäusserung vor, die einer Siegelung offensichtlich entgegenspricht. Somit dürfte die nachträgliche Siegelung der erhobenen Daten nicht mehr möglich sein. Jedoch besteht auf Seiten der Untersuchungsbehörde das Risiko, dass die betroffene Person geltend macht, im Zeitpunkt der Einwilligung sich der Konsequenzen einer solchen Einwilligung nicht bewusst gewesen zu sein. Um eine solche Situation zu vermeiden, ist es empfehlenswert, nicht nur die Einwilligung zu protokollieren, sondern die betroffene Person über allfällige Folgen zu informieren und diese Information ebenfalls in einem Protokoll festzuhalten. Schliesslich sind Daten zu beschlagnahmen, die mit Einwilligung der betroffenen Person erhoben worden sind.

## 3.2. Vorgehensweise bei einer Hausdurchsuchung

Wird bei einer Hausdurchsuchung ein Computer angetroffen, der gerade mit einer Cloud verbunden ist, auf welcher verfahrensrelevante Daten vermutet werden, dann soll eine Sicherung dieser Daten auf ein externes Speichermedium der Polizei erfolgen. Die Daten liegen im Herrschaftsbereich des Betroffenen und die Sicherstellung dieser Daten ist mit dem Durchsuchungsbefehl abgedeckt. Die mit dem Computer vor Ort verbundene Cloud ist wie eine externe Festplatte zu behandeln. Dabei wird vom sogenannten Zugriffsprinzip gesprochen.[87]

[86] So auch AEPLI, S. 127.
[87] JOSITSCH, S. 3.

Dem Betroffenen bleibt die Möglichkeit der Siegelung gemäss Art. 248 StPO. Macht der Betroffene keinen Gebrauch von der Siegelung oder wurde der Datenträger vom Zwangsmassnahmengericht entsiegelt, müssen die verfahrensrelevanten Daten beschlagnahmt werden. Gegen die Beschlagnahme bleibt dem Betroffenen das Rechtsmittel der Beschwerde nach Art. 393 f. StPO, um sich gegen diese Zwangsmassnahme zu wehren. Mit dem Rechtsbehelf[88] der Siegelung und dem Rechtsmittel der Beschwerde ist der Betroffene ausreichend geschützt gegen den staatlichen Grundrechtseingriff.

## 3.3. Exkurs: Territorialitätsprinzip vs. Zugriffsprinzip

In der Schweiz gilt das Territorialitätsprinzip, das in Art. 3 StGB verankert ist. Es ist *„die primäre Grundlage des sogenannten internationalen Strafrechts."*[89] Es schützt die Souveränität des Staates und besagt, dass grundsätzlich kein Staat berechtigt ist, auf fremdes Territorium einzuwirken.[90] In der Schweiz ist das Handeln für einen fremden Staat auf schweizerischem Gebiet ohne Bewilligung im Strafgesetzbuch unter Strafe gestellt (Art. 271 StGB). Auch kann bestraft werden, wer die Gebietshoheit eines fremden Staats verletzt, insbesondere durch unerlaubte Vornahme von Amtshandlungen auf dem fremden Staatsgebiet (Art. 299 StGB). Unter diesem Aspekt fragt es sich, ob Handlungen einer schweizerischen Strafverfolgungsbehörde mit Auswirkungen auf einen fremden Staat erlaubt oder eben verboten sind. Darf wie im oben geschilderten Fall während einer Hausdurchsuchung mit dem vor Ort befindlichen Computer, der aktiv mit einer Cloud im Ausland verbunden ist, auf diese Cloud zugegriffen und die entsprechenden Daten vor Ort gesichert werden?

DOMBROWSKI unterscheidet zwischen Hoheitsakten auf fremden Staatsgebiet und extraterritorialen Hoheitsakten.[91] Hoheitsakte, die ohne Einwilligung durch staatliche oder staatlich gelenkte Organe vorgenommen werden, die sich physisch auf dem fremden Staatsgebiet befinden, sind völkerrechtlich generell unzulässig.[92] Hoheitsakte sind gemäss DOMBROWSKI auch mit Verweis auf das Bundesgericht nicht auf Zwangsmassnahmen beschränkt.[93] Im Gegensatz zu Hoheitsakten auf fremdem Staatsgebiet können extraterritoria-

[88] SCHMID, Handbuch StPO, N 1076 mit Verweis auf Botschaft StPO, S. 1239.
[89] BGE 108 IV 145 E. 3 S. 146.
[90] DOMBROWSKI, S. 5.
[91] DOMBROWSKI, S. 11.
[92] DOMBROWSKI, S. 12.
[93] DOMBROWSKI, S. 10 f. mit Verweis auf BGE 65 I 39 E. 2 S. 44.

le Hoheitsakte erlaubt sein.[94] Als extraterritorialer Hoheitsakt wird hoheitliches Handeln auf dem eigenen Staatsgebiet durch eigene staatliche Organe bezeichnet, das in ein fremdes Staatsgebiet hineinwirkt.[95] Als Beispiel für einen solchen extraterritorialen Hoheitsakt führt DOMBROWSKI u.a. den Zugriff auf Computersysteme im Ausland auf.[96] Ein extraterritorialer Hoheitsakt verletzt insbesondere dann Völkerrecht, wenn er die Gebietshoheit des fremden Staats unmittelbar verletzt, wenn er in seinen Wirkungen einem Hoheitsakt auf fremden Staatsgebiet gleichkommt oder die Ordnung und Sicherheit des fremden Staates beeinträchtigt.[97] Es besteht bei einem Teil der Lehre die Ansicht, dass bereits der Zugriff durch Ermittler auf frei verfügbare Daten im Ausland einen Eingriff in die Gebietshoheit des betreffenden Staats darstelle. Ein solcher könne auch nicht durch das Einverständnis von Privatpersonen und juristischen Personen gerechtfertigt sein, da diese nicht über die Dispositionsbefugnis über die staatlichen Hoheitsrechte verfügen.[98] Ein Zugriff auf frei verfügbare Daten sei nur unter dem Aspekt von Art. 32 lit. a CCC gerechtfertigt. Voraussetzung ist folglich, dass der Zielstaat die Konvention unterzeichnet und ratifiziert hat. Jedoch kann die Rechtfertigung eines solchen Zugriffs auch aus international anerkanntem Gewohnheitsrecht abgeleitet werden, da vor Verabschiedung der Convention on Cybercrime die Mehrheit der Staaten eine solche Vorgehensweise zumindest geduldet haben.[99] Art. 32 lit. a CCC wird also nur deklaratorischen Charakter haben.[100] Wenn der Zugriff auf frei verfügbare Daten bereits Anlass zu Diskussionen gibt, dann erst recht der Zugriff auf Daten, die einer Zugangsbeschränkung unterliegen. Nach einem grossen Teil der Lehre ist der Abruf im Ausland gespeicherter, zugangsbeschränkter Daten durch Strafverfolgungsbehörden ohne entsprechende Ermächtigung völkerrechtswidrig. Daten, die auf diese Weise erhoben worden sind, unterliegen nach dieser Ansicht einem Verwertungsverbot.[101] SCHWERHA tönt an, dass allenfalls eine Ausnahme vom Territorialitätsprinzip bei Gefahr in Verzug *(engl.: exigent circumstances)* gemacht werden könnte.[102] Ob im Anschluss an eine derartige Handlung bei Gefahr in Verzug noch der formelle Weg eingeschlagen werden müsste, beantwortet SCHWERHA leider nicht. Meines Erachtens müsste nach geltendem Recht ein formelles Rechtshilfeersuchen gestellt werden.

[94] DOMBROWSKI, S. 13 und S. 133.
[95] DOMBROWSKI, S. 12.
[96] DOMBROWSKI, S. 12.
[97] DOMBROWSKI, S. 13 f.
[98] DOMBROSWI, S. 154; HEIMGARTNER, Strafprozessuale Beschlagnahme, S. 93.
[99] DOMBROWSKI, S. 155 f.
[100] DOMBROSWKI, S. 158.
[101] DOMBROWSKI, S. 159; RYSER, S. 575 ff.; vgl. AEPLI, S. 130 f.; HEIMGARTNER, Strafprozessuale Beschlagnahme, S. 266; HEIMGARTNER, Internationale Dimension, S. 136.
[102] SCHWERHA, S. 18; vgl. auch DOMBROWSKI, S. 167.

In der Schweiz wird in der Lehre das Zugriffsprinzip diskutiert. Beim Zugriffsprinzip ist nicht der Standort des Datenträgers entscheidend, sondern wer von wo aus Zugriff auf die verfahrensrelevanten Daten hat.[103] Dies ist die Folge der Unkörperlichkeit von elektronischen Daten. Die Herrschaft über die Daten liegt bei der Person, welche die Zugriffsberechtigung hat, und nicht bei der, die im physischen Besitz des Datenträgers ist. Der Inhaber der Daten weiss oftmals selbst nicht, an welchem geografischen Ort seine Daten abgespeichert sind. Jedoch darf gemäss BANGERTER ein Zugriff auf diese Daten nur innerhalb von Räumlichkeiten erfolgen, die vom Hausdurchsuchungsbefehl abgedeckt sind. Der Hausdurchsuchungsbefehl darf seine Begrenzungsfunktion nicht verlieren und es darf keine heimliche Online-Durchsuchung stattfinden.[104] Gemäss diesen Ausführungen darf folglich ein Zugriff vor Ort auf die mit dem Computer verbundene Cloud erfolgen. Jedoch stellt sich immer noch die Frage, ob ein solcher Zugriff auf Daten im Ausland eine Souveränitätsverletzung darstellt.

SCHMID sah die heutige Problematik bereits im Jahr 1993, als das Internet noch kaum verbreitet war.[105] Seines Erachtens hat der folgende *„Standpunkt einiges für sich“*: *„Werden internationale Datenübertragungs- und Verarbeitungsnetze mit direkten Zugriffsmöglichkeiten betrieben, so wird von der jeweils betroffenen nationalen Gesetzgebung toleriert, dass die Informationen nicht nur am Orte, an dem sie primär gespeichert sind, sondern auch jederzeit in andern Ländern abgerufen werden können. Daraus könnte gefolgert werden, dass keine Verletzung der nationalen Souveränität vorliegt, wenn nun nicht die Datenberechtigten selbst, sondern Strafverfolgungsbehörden von dieser grenzüberschreitenden, ubiquitären Verfügbarkeit der Daten Gebrauch machen.“*[106]

BANGERTER seinerseits verweist darauf, dass verschiedene Wettbewerbsbehörden, darunter auch die EU-Kommission, bei ihren Durchsuchungen und Beschlagnahmen den „Access Approach“ anwenden und darin keine Souveränitätsverletzung sehen.[107] Das Anti-Cartel Enforcement Manual des International Competition Network, auf das sich BANGERTER bezieht, umschreibt den „Access Approach“ so: *„Some agencies look at the fact whether the company searched, raided or inspected has access, uses and controls the information stored at the other business premises of the company. If the company has access, uses and*

[103] JOSITSCH, S. 3.
[104] BANGERTER, S. 280 ff.; JOSITSCH, S. 4.
[105] *„Es wird geschätzt, dass das Internet im Jahr 1993 lediglich 1% der Informationsflüsse der weltweiten Telekommunikation ausmachte“*, https://de.wikipedia.org/wiki/Geschichte_des_Internets (zuletzt besucht am 02.08.2015).
[106] SCHMID, Strafprozessuale Fragen, S. 109.
[107] BANGERTER, S. 281.

*controls the digital information, the digital information is regarded as being at the searched, raided or inspected premises and access is permitted and copying done. The location where the digital information is stored is no issue."*[108] Das Territorialitätsprinzip muss so verstanden werden, *„dass es darauf ankommt, in welchem Territorium der Zugriff auf die Daten und somit ein Eingriff in die Freiheitsrecht des Betroffenen stattfindet"*[109] und nicht wo der Speicherort ist.[110] Folglich dürfte die beschriebene Vorgehensweise, also der Zugriff auf eine Cloud während einer Hausdurchsuchung, erlaubt sein.

Dieser Ansicht kann jedoch entgegengehalten werden, dass gewisse Nutzer ihre Daten bewusst auf Clouds aufbewahren, die in Ländern betrieben werden, wo der Zugriff für Dritte (und damit auch für staatliche Behörden) erschwert oder gar unmöglich ist. Doch dem Durchschnittsnutzer wird die Örtlichkeit des Cloud-Dienstes egal sein, solange die Funktionen einfach zu bedienen sind. Sonst würden Cloud-Dienste von Grosskonzernen wie Google (Google Drive)[111], Microsoft (OneDrive)[112], Apple (iCloud)[113] usw. nicht sehr erfolgreich sein, da jederzeit damit gerechnet werden muss, dass die eigenen Daten durch US-amerikanische Geheimdienste überwacht werden.[114] Um weiterhin erfolgreich Strafverfolgung betreiben zu können, muss folglich das Zugriffsprinzip zur Anwendung gelangen.[115]

## 3.4. „Zwangsweise" Datenerhebung

Fehlt die Einwilligung der beschuldigten Person in die Datenerhebung oder sollen die Daten vorerst ohne Wissen der beschuldigten Person erhoben werden, ist zunächst zu unterscheiden, ob die zu erhebenden Daten dem Fernmeldegeheimnis unterstehen oder nicht. Muss davon ausgegangen werden, dass die zu erhebenden Daten dem Fernmeldegeheimnis[116] unterliegen, ist eine Überwachungsmassnahme nach Art. 269 ff. StPO anzuordnen. Da es wohl in den meisten Fällen um Erhebung von Inhaltsdaten (und nicht von Randda-

[108] ICN, S. 23.
[109] JOSITSCH, S. 4.
[110] BANGERTER, S. 281; JOSITSCH, S. 4.
[111] https://www.google.com/drive (zuletzt besucht am 14.07.2015).
[112] https://onedrive.live.com (zuletzt besucht am 14.07.2015).
[113] https://www.icloud.com (zuletzt besucht am 14.07.2015).
[114] Siehe NSA-Affäre: https://de.wikipedia.org/wiki/Globale_Überwachungs-_und_Spionageaffäre (zuletzt besucht am 14.07.2015).
[115] Vgl. BANGERTER, S. 281 f.
[116] Vgl. hierzu Ausführungen auf S. 12 ff.

ten) geht, kann nur eine Echtzeitüberwachung im Sinne von Art. 269 StPO zur Anwendung gelangen. Die Voraussetzungen zur Echtzeitüberwachung wurden bereits kurz erörtert.[117]

Handelt es sich nicht um Daten, die durch das Fernmeldegeheimnis geschützt sind, können die Daten mittels Editionsverfügung beim Cloud Service Provider eingefordert werden.[118] Soll sichergestellt werden, dass die beschuldigte Person vorläufig keine Kenntnis der Datenerhebung erhält, kann die Editionsverfügung mit einem Mitteilungsverbot versehen werden.[119] Vor Verwendung der Daten im Strafverfahren muss aber die an den Daten berechtigte Person, meistens wohl die beschuldigte Person, auf das Siegelungsrecht aufmerksam gemacht werden.[120] Wurde auf eine Siegelung verzichtet oder die Daten entsiegelt, sind die erhobenen Daten zu beschlagnahmen.[121]

## 3.5. Siegelung

Gemäss Art. 248 Abs. 1 StPO müssen Aufzeichnungen und Gegenstände versiegelt werden, die nach Angaben der Inhaberin oder des Inhabers wegen eines Aussage- oder Zeugnisverweigerungsrechts oder aus anderen Gründen nicht durchsucht oder beschlagnahmt werden dürfen. Diese dürfen von den Strafbehörden weder eingesehen noch verwendet werden. Im Zusammenhang mit der Erhebung von Daten einer Cloud darf folglich der Inhaber die Siegelung der Daten verlangen. Dabei stellen sich in erster Linie die zwei folgende Fragen: Wer ist Inhaber der Daten und damit legitimiert, die Siegelung zu verlangen, und wie soll eine Siegelung von Daten einer Cloud vorgenommen werden?

Nach dem Wortlaut von Art. 248 Abs. 1 StPO steht dem Inhaber der Aufzeichnungen und Gegenständen das Siegelungsrecht zu. Nach der früheren Rechtsprechung war nur der Gewahrsamsinhaber antragsberechtigt, selbst wenn er die Aufzeichnungen nur fiduziarisch hält.[122] Bei elektronisch gespeicherten Daten ist Inhaber der Gewahrsamsträger der Datenverarbeitungsanlange bzw. des elektronischen Speichermediums.[123] In Bezug auf Daten in einer Cloud dürfte damit dem Cloud Service Provider diese Eigenschaft zukommen. Jedoch hat das Bundesgericht seine Rechtsprechung geändert und erweitert den Kreis der

[117] Vgl. hierzu Ausführungen auf S. 12.
[118] Vgl. hierzu Ausführungen auf S. 10 ff.
[119] Vgl. hierzu Ausführungen auf S. 11 f.
[120] Vgl. hierzu Ausführungen auf S. 25.
[121] Vgl. hierzu Ausführungen auf S. 8 ff.
[122] THORMANN/BRECHBÜHL, BSK StPO, Art. 248 StPO N 6; KELLER, StPO-Kommentar, Art. 248 N 5; vgl. auch MÜLLER/GÄUMANN, S. 291; SCHMID, Handbuch StPO N 1077; SCHMID, Praxiskommentar, Art. 248 N 3.
[123] AEPLI, S. 92; KELLER, StPO-Kommentar, Art. 248 N 5; BGE 140 IV 28 E. 4.3.2 S. 34.

siegelungslegitimierten Personen. Es beruft sich dabei u.a. auf den französischen Gesetzestext, in dem nicht wie im deutschen und italienischen Wortlaut der Begriff „Inhaber" bzw. „detentore" verwendet wird (frz. „détenteur"), sondern der Begriff „interéssé" (Interessierter)[124]. Auch wird bei der bundesgerichtlichen Auslegung die Botschaft zur StPO herangezogen, in welcher nebst dem eigentlichen Gewahrsamsinhaber auch die an den Aufzeichnungen rechtlich berechtigte Person als Inhaberin im Sinne von Art. 248 Abs. 1 StPO verstanden wird.[125] In Anwendung dieser Rechtsprechung auf Daten einer Cloud ist folglich der Kunde des Cloud Service Providers, der seine Daten in der betreffenden Cloud gespeichert hat, berechtigt, die Siegelung zu beantragen. Als Konsequenz davon kann auch die beschuldigte Person antragsberechtigt sein. Als weitere Folge der Ausweitung dieser Legitimation müssen die Strafverfolgungsbehörde vor Durchsuchung allfällige Berechtigte von Amtes wegen darauf aufmerksam machen, dass sie eine Siegelung verlangen können, sofern die Geheimwahrungsrechte offensichtlich oder aufgrund der Umstände von der Behörde erkennbar sind.[126]

Die siegelungslegitimierte Person kann nach dem Wortlaut von Art. 248 Abs. 1 StPO die Angabe machen, dass die Daten wegen eines Aussage- oder Zeugnisverweigerungsrechts oder aus anderen Gründen die Daten nicht durchsucht oder beschlagnahmt werden dürfen. Das bedeutet, dass die blosse Behauptung, ein schutzwürdiges Geheimnis bestehe, ausreicht, damit die Strafverfolgungsbehörde Daten versiegeln muss.[127] Die beschuldigte Person hat gemäss Art. 158 Abs. 1 lit. b StPO ein generelles Aussageverweigerungsrecht. Es könnte folglich angenommen werden, dass die beschuldigte Person mit Berufung auf das Aussageverweigerungsrecht immer die Siegelung beantragen kann. Dies kann selbstverständlich nicht sein. Es wird daher Art. 264 Abs. 1 StPO herangezogen, in welchem die Einschränkungen für die Beschlagnahme festgehalten sind (Unterlagen aus dem Verkehr der beschuldigten Person mit ihrer Verteidigung, persönliche Aufzeichnungen und Korrespondenz der beschuldigten Person und Gegenstände aus dem Verkehr zwischen der beschuldigten Person und Personen, denen nach Art. 170 bis 173 StPO ein Zeugnisverweigerungsrecht zusteht).[128] Diese sind entsprechend auf die Siegelungsgründe anzuwenden.[129]

[124] BGE 140 IV 28 E. 4.3.2 S. 34.
[125] BGE 140 IV 28 E. 4.3.3 S. 35; BBl 2006 1085, S. 1239; vgl. auch KELLER, StPO-Kommentar, Art. 248 N 6; MÜLLER/GÄUMANN, S. 291 f.
[126] MÜLLER/GÄUMANN, S. 292; KELLER, StPO-Kommentar, Art. 248 N 7; BGE 140 IV 28 E. 4.3.5 S. 37.
[127] KELLER, StPO-Kommentar, Art. 248 N 8; *Siegelungsgrund plausibel machen:* SCHMID, Praxiskommentar, Art. 248 N 4; SCHMID, Handbuch StPO N 1076; so auch THORMANN/BRECHBÜHL, BSK StPO, Art. 248 StPO N 10; BBl 2006 1085, S. 1239.
[128] MÜLLER/GÄUMANN, S. 291.

Nebst dem Aussage- und Zeugnisverweigerungsrecht sind in Art. 248 Abs. 1 StPO auch „andere Gründe“ als Siegelungsgrund aufgeführt. Gemäss Botschaft fallen darunter beispielsweise Gegenstände, die Geheimnisse ohne Relevanz für das Verfahren enthalten.[130] Gemäss Lehre können etwa Fabrikations- und Geschäftsgeheimnisse sowie schützenswerte Privatgeheimnisse unter den Titel „andere Gründe“ fallen.[131] Das Bundesgericht setzte sich in einem Entscheid vom 26. März 2012 mit der Frage auseinander, was unter „andere Gründe“ zu subsumieren sei. Es folgert, *„dass das Zwangsmassnahmengericht im Entsiegelungsentscheid prüfen muss, ob die allgemeinen Voraussetzungen für eine Durchsuchung gegeben sind [...], namentlich ob ein konkreter Tatverdacht vorliegt [...].“*[132] Dabei muss das Zwangsmassnahmengericht auch die Untersuchungsrelevanz der zur Beweissicherung beschlagnahmten und versiegelten Dokumente und Dateien prüfen. Die Berechtigten dürfen im Entsiegelungsverfahren auch entsprechende Einwände geltend machen. Nach Ansicht des Bundesgerichts scheint es *„aus prozessökonomischen Gründen und zur Vermeidung von Doppelspurigkeiten und Abgrenzungsproblemen“* daher sinnvoll, *„den Anwendungsbereich des Siegelungsverfahrens weit zu fassen und sämtliche Einwände gegen die Durchsuchung im Entsiegelungsverfahren zu prüfen, sofern es dem Berechtigten im Ergebnis darum geht, die Einsichtnahme der Staatsanwaltschaft in die sichergestellten Unterlagen und deren Verwertung zu verhindern.“*[133]

Wie bereits angetönt, ist nicht klar, wie Daten einer Cloud versiegelt werden sollen. Die Datenverarbeitungsanlagen und Datenträger sollen in *„computergerechter Weise“* versiegelt werden.[134] Da die Daten nicht mittels amtlichen Siegels gekennzeichnet werden können, muss darauf geachtet werden, dass beispielsweise Passwörter und Verschlüsselungen nur der Untersuchungsbehörde bekannt sind.[135] Daten einer Cloud werden entweder bei einer Hausdurchsuchung vor Ort durch die Polizei auf einen externen Datenträger gespeichert, durch Edition beim Cloud Service Provider wohl auch in Form eines externen Datenträgers erhältlich gemacht oder mit Einwilligung der betroffenen Person auf einen externen Datenträger gespeichert. Faktisch wird also eine Kopie erstellt.[136] Da der Strafverfolgungsbehörde nun ein oder mehrere Datenträger vorliegen, können diese versiegelt

[129] KELLER, StPO-Kommentar, Art. 248 N 15 ff.; THORMANN/BRECHBÜHL, BSK StPO, Art. 248 N 45 ff.; MÜLLER/GÄUMANN, S. 291.
[130] BBl 2006 1085, S. 1239.
[131] MÜLLER/GÄUMANN, S. 291; KELLER, StPO-Kommentar, Art. 248 N 23 f.
[132] Urteil BGer 1B_117/2012 vom 26.03.2012 E.3.3.
[133] Urteil BGer 1B_117/2012 vom 26.03.2012 E.3.3; vgl. auch MÜLLER/GÄUMANN, S. 291 und S. 293.
[134] JOSITSCH, S. 4; SCHMID, strafprozessuale Fragen, S. 94 f.; AEPLI, S. 138.
[135] JOSITSCH, S. 4.
[136] Vgl. dazu THORMANN/BRECHBÜHL, BSK StPO, Art. 248 StPO N 14.

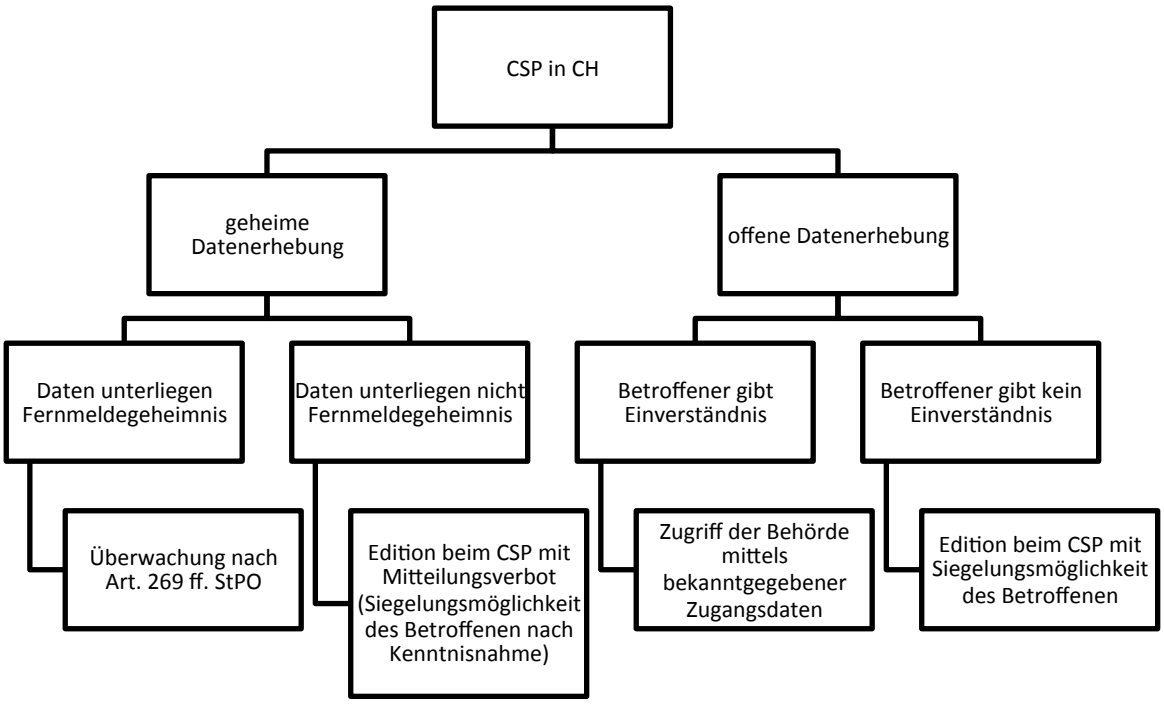
werden, indem sie zum Beispiel mit einem Passwort geschützt werden oder ganz banal in ein Behältnis gelegt werden, das mit einem amtlichen Siegel verschlossen wird und so dem Entsiegelungsgericht übergeben wird.

Wenn die betreffenden Daten versiegelt sind, unterliegen sie einem suspensiv bedingten Verwertungsverbot, bis das Entsiegelungsgericht über die Entsiegelung der Daten entschieden hat.[137] Der Entsiegelungsrichter hat eine Triage vorzunehmen, bei welcher er prüfen muss, welche Daten für eine Verwendung im Strafverfahren in Frage kommen und welche auszuscheiden sind.[138] Dazu kann er Sachkundige (z.B. der digitalen Forensik) beiziehen. Betroffene, die eine Versiegelung beantragt haben, *„haben die prozessuale Obliegenheit, den Entsiegelungsrichter bei der Sichtung und Klassifizierung von Dokumenten zu unterstützen; auch haben sie jene Dateien zu benennen, die ihrer Ansicht nach der Geheimhaltung unterliegen.“*[139] Die Triage von Daten kann z.B. mit Hilfe von Suchbegriffen stattfinden. Problematisch dabei ist aber, dass allfällige Zufallsfunde nicht entdeckt werden. Eine andere Variante ist die Sichtung und Ausscheidung anhand der Ordnerstruktur.[140]

Gemäss Bundesgericht müssen Kopien von Daten bei negativem Entsiegelungsentscheid vernichtet werden.[141] Die der Durchsuchung zugänglichen Daten sind auf einem neuen Datenträger zu speichern.[142] Im Hinblick darauf, dass eine Entwicklung im Strafverfahren die erneute Durchsuchung nötig macht (z.B. Erkenntnisse zu einem neuem Tatverdacht), schlagen THORMANN und BRECHBÜHL aber vor, eine Kopie des ursprünglichen (versiegelten) Datenträgers auf begründeten Antrag hin beim Entsiegelungsrichter bis zum rechtskräftigen Urteil zu hinterlegen.[143] Aus meiner Sicht macht der Vorschlag von THORMANN und BRECHBÜHL durchaus Sinn.

[137] Urteil Präsident Strafkammer Kantonsgericht Freiburg vom 13.07.2007, FZR 2008 S. 86 E. 1c S.88; JOSITSCH, S. 5.
[138] BGE 132 IV 63 E. 4, S. 65 ff.
[139] BGE 137 IV 189 E. 4.2. S. 195.
[140] Vgl. JOSITSCH, S. 4 f.
[141] Urteil BGer 1B_274/2008 vom 27.01.2009 E. 8.
[142] Urteil BGer 1B_104/2008 vom 16.09.2008 E. 3.
[143] THORMANN/BRECHBÜHL, BSK StPO, Art. 248 StPO N 58; JOSITSCH, S. 5; a.M. MÜLLER/GÄUMANN, S. 296.

## 3.6. Zusammenfassung in Form eines Schemas



# 4. Vorgehensweise bei Daten bzw. CSP im Ausland

## 4.1. Serverstandort vs. Standort des Cloud Service Providers

Zunächst muss die Frage geklärt werden, wo die verfahrensrelevanten Daten überhaupt erhältlich gemacht werden können. Müssen die Daten am Standort des Servers erhoben werden? Oder können sie auch am Sitz des Cloud Service Providers eingefordert werden, welcher die fragliche Cloud betreibt? Nach Ansicht von GLESS ist die Rechnerwolke selbst auf einem *„örtlich lokalisierten Server"* gespeichert, auf welchen *„die jeweils vor Ort zuständige Strafverfolgungsbehörde zugreifen könne."*[144] In der Realität aber muss angenommen werden, dass viele Cloud Service Provider die Daten auf verschiedenen Servern an verschiedenen Standorten abgespeichert haben. So kann der Kunde beim Anbieter Amazon für das Produkt Elastic Compute Cloud (EC2) nur wählen, aus welcher der Regionen (USA, Europa, Asien oder Südamerika) der Service erbracht wird, jedoch nicht aus welchem Land der Region. Zudem gibt Amazon aus Sicherheitsgründen auch nicht bekannt, wo die Unternehmung Rechenzentren betreibt.[145] Es kann durchaus sein, dass einzelne Daten sogar aufgeteilt sind und sich an unterschiedlichen Standorten befinden. Diese Serverstandorte müssen auch nicht unbedingt im gleichen Staat sein wie der Sitz des Cloud-Providers. Da Serverfarmen zur Kühlung ihrer Einrichtung einen gewissen Stromverbrauch haben, können Daten auf andere Serverfarmen verschoben werden, wenn an jenem Standort gerade Nacht ist und der Strompreis damit tiefer.[146] Zudem werden die Daten häufig doppelt, also an einem weiteren Serverstandort abgespeichert, damit bei einem allfälligen Ausfall des primären Standorts die Daten weiterhin verfügbar sind.[147] Folglich kann meistens nicht nachvollzogen werden, wo sich die Daten effektiv befinden. Dies verunmöglicht praktisch die Datenerhebung am Serverstandort. Damit bleibt die Lösung, dass die Daten am Sitz des Cloud-Providers erhoben werden.[148]

[144] GLESS, ZStrR 130 (2012), S. 7.
[145] SCHORER, Handbuch Cloud Computing, S. 73 Rz. 50.
[146] Vgl. SCHULZ, Island – Insel der grünen Rechenzentren; SPOENLE, S. 5; SCHWERHA, S. 9 f.; SÖBBING, Rz. 36.
[147] Vgl. Microsoft Online Services, Where is my data: https://www.microsoft.com/online/legal/v2/?docid=25 (zuletzt besucht am 15.07.2015).
[148] Vgl. WALDER, Folie Nr.16-18.

## 4.2. Freiwillige Datenherausgabe

### 4.2.1. Durch die beschuldigte Person

Betreffend die freiwillige Datenherausgabe durch die beschuldigte Person durch Bekanntgabe der Zugangsdaten (Benutzername und Passwort) kann auf die Ausführungen im Zusammenhang mit der freiwilligen Datenherausgabe bei Daten in der Schweiz verwiesen werden[149], da es m.E. keine Rolle spielt, ob sich die Daten in der Schweiz oder im Ausland befinden, wenn das Zugriffsprinzip angewendet wird.

### 4.2.2. Durch den Provider

In einem Fall der Staatsanwaltschaft St. Gallen wollte die zuständige Staatsanwältin beim deutschen Web-Mail-Provider GMX in Erfahrung bringen, welche Benutzerdaten für das fragliche Konto bei GMX hinterlegt sind und von welchen IP-Adressen aus auf das Web-Mail-Konto zugegriffen worden war. Sie schrieb GMX bzw. der 1&1 Internet AG in Montabaur (Deutschland), welche GMX betreibt, und forderte sie auf, die erwähnten Daten herauszugeben. Die 1&1 Internet AG kam dieser Aufforderung nach und übermittelte die gewünschten Daten. In der Folge stellt sich die Frage, ob ein solches Vorgehen zulässig und die so erhobenen Beweise verwertbar sind.

### 4.2.3. Die Bestimmung von Art. 32 lit. b CCC

Gemäss Art. 32 lit. b CCC darf eine Vertragspartei ohne Genehmigung einer anderen Vertragspartei 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. Ist nun die 1&1 Internet AG als Betreiberin von GMX zur Zustimmung i.S. von Art. 32 lit. b CCC berechtigte Person? In den AGB von GMX sind u.a. die Datenschutzhinweise von GMX implementiert. In diesen Datenschutzhinweisen berechtigt sich GMX, Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfol-

[149] Vgl. Ausführungen auf S. 19.

gung zu erteilen.[150] Laut dieser Bestimmung in den AGB ist GMX bzw. die 1&1 Internet AG berechtigte Person i.S. von Art. 32 lit. b CCC.[151]

Nach der bundesrätlichen Botschaft über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität vom 18. Juni 2010[152] ist aber Art 32 lit. b CCC eng auszulegen, um der Gefahr des Missbrauchs unter Umgehung der Rechtshilfe oder in Verletzung der Privatsphäre Dritter entgegenzuwirken. So soll Art. 32 lit. b CCC nur zur Anwendung gelangen, *„wenn sie [die Vertragspartei] über die rechtmässige und freiwillige Zustimmung einer Person im Inland verfügt, die rechtmässig befugt ist, die Daten an eine inländische Strafverfolgungsbehörde weiterzuleiten. Handelt es sich um vertrauliches Datenmaterial einer Drittperson, zu deren Offenlegung diese keine Zustimmung erteilt hat, liegt keine Befugnis im Sinne von Artikel 32 der Konvention vor.“*[153]

SCHWEINGRUBER legt in ihrem Artikel im Jusletter vom 10. November 2014 dar, dass nicht ersichtlich sei, *„wieso diese Zustimmung nur von einer Person im Inland gegeben werden kann. Weder in der englischen Version des Übereinkommens noch in der deutschen Übersetzung ist dieses Kriterium vorhanden. [...] Es ist auch nicht nachvollziehbar, weshalb die Bedeutung von Art. 32 des Übereinkommens, der den grösstmöglichen Konsens zwischen den Vertragsparteien abbildet, noch weiter eingeschränkt werden soll, wenn das langfristige Ziel die Ausweitung des grenzüberschreitenden Datenzugriffs sein muss.“*[154] So plädiert SCHWEINGRUBER für eine wörtliche Auslegung von Art. 32 lit. b CCC, bei welcher es nicht darauf ankommt, ob sich die zur Zustimmung befugte Person im In- oder Ausland befindet.[155]

Die I. öffentlich-rechtliche Abteilung des Bundesgerichts äussert sich in einem Urteil vom 14. Januar 2015 u.a. zur Auslegung von Art. 32 lit. b CCC.[156] Sie sagt, dass der Formulierung in der bundesrätlichen Botschaft, es sei die Zustimmung „einer Person im Inland“ einzuholen, nicht gefolgt werden kann. Diese Formulierung finde weder im Wortlaut noch in den einschlägigen Materialien des Übereinkommens noch in der Fachliteratur eine Stütze. Das Bundesgericht hebt in seinen Ausführungen die Ziele des Übereinkommens hervor.

[150] GMX-AGB: https://service.gmx.net/de/cgi/g.fcgi/products/mail/agb (zuletzt besucht am 15.07.2015).
[151] Vgl. SCHWEINGRUBER, Jusletter, Rz 16.
[152] BBl 2010 4697, S. 4738.
[153] BBl 2010 4697, S. 4738.
[154] SCHWEINGRUBER, Jusletter, Rz 14; vgl. auch Explanatory Report CCC, N 293 und 294.
[155] Vgl. aber SPOENLE, S. 7: er geht davon aus, dass sich die zustimmende Person im Staat der untersuchenden Behörde befinden muss.
[156] BGer 1B_344/2014 vom 14.01.2015 E. 5.9. ff.

Zu diesen gehören die Verbesserung der Bekämpfung der grenzüberschreitenden Cyberkriminalität, die Erleichterung der Rechtshilfe und damit eine teilweise Lockerung des Erfordernisses des förmlichen Rechtshilfeweges. Wenn nun zusätzlich die Zustimmung einer Person im Inland verlangt würde, würde der Zweck des Übereinkommens unterlaufen.[157] Der direkte Zugriff auf ausländische Konten, wie er in Art. 32 lit. b CCC vorgesehen ist, wäre praktisch nicht möglich, da nur in den wenigsten Fällen eine zustimmungsberechtigte inländische Person ermittelbar sein dürfte, die auch noch der Datenerhebung zustimmen müsste.[158] Das Bundesgericht kommt zum Schluss, dass auch ausländische Personen und Gesellschaften als Zustimmungsberechtigte i.S. von Art. 32 lit. b CCC in Frage kommen. Zustimmungs- und weiterleitungsberechtigt sind somit auch ausländische Provider, die in ihren AGB und Datenverwendungsrichtlinien ein solches Weiterleitungsrecht an in- und ausländische Strafverfolgungsbehörden ausbedungen haben. Es muss aber zusätzlich geprüft werden, ob die anfragende Strafverfolgungsbehörde eine rechtswirksame freiwillige Zustimmung gegenüber dem ausländischen Provider eingeholt hat. Von einer konkludenten Zustimmung kann ausgegangen werden, wenn der angefragte Provider die Daten ohne Weiteres herausgibt.[159] Die von GMX erhaltenen Daten sind folglich im schweizerischen Strafverfahren verwertbar.[160]

## 4.3. „Zwangsweise“ Erhebung von Daten im Ausland

Wenn Daten im Ausland zwangsweise erhoben werden müssen, ist grundsätzlich der Rechtshilfeweg zu beschreiten. Zu unterscheiden ist dabei, ob die Datenerhebung in einem Staat durchzuführen ist, der die Convention on Cybercrime unterzeichnet und ratifiziert hat, oder in einem Staat, bei dem die Convention on Cybercrime nicht zur Anwendung gelangen kann.

### 4.3.1. Erhebung von Daten in einem CCC-Staat

Wenn Daten nicht direkt beim ausländischen Cloud Service Provider auf freiwilliger Basis erhältlich gemacht werden können (Art. 32 lit. b CCC)[161], muss eine zwangsweise Erhebung stattfinden. Um zu verhindern, dass die zu erhebenden Daten während der Dauer des

[157] BGer 1B_344/2014 vom 14.01.2015 E. 5.9.; vgl. auch Präambel CCC und Explanatory Report CCC, N 293 und 294.
[158] BGer 1B_344/2014 vom 14.01.2015 E. 5.9.
[159] BGer 1B_344/2014 vom 14.01.2015 E. 5.10; vgl. auch Schweingruber, Jusletter, Rz. 20.
[160] Vgl. aber SCHWERHA, S. 11 f., der auf die Problematik des Widerrufs der Zustimmung (zu den AGB) hinweist.
[161] Vgl. Ausführungen S. 30 ff.

beabsichtigten Rechtshilfeverfahrens gelöscht werden, kennt die Cybercrime-Konvention die sogenannte „Quick-Freeze-Procedure“[162]. In Art. 16 Abs. 1 CCC werden die Vertragsparteien verpflichtet, die erforderlichen gesetzgeberischen und anderen Massnahmen vorzusehen, damit ihre Behörden die umgehende Sicherung bestimmter Computerdaten, einschliesslich Verkehrsdaten, bewirken können.[163] Die Daten sollen längstens 90 Tage gesichert und erhalten werden, wobei eine Vertragspartei auch eine Verlängerung dieser Aufbewahrungsfrist vorsehen kann (Art. 16 Abs. 2 CCC). Die ersuchende Behörde kann dann in Anwendung von Art. 29 Abs. 1 CCC bei der zuständigen Behörde des betreffenden Staats um Anordnung der umgehenden Sicherung der gewünschten Daten ersuchen. Die Sicherung erfolgt zunächst für längstens 60 Tage, in welchem die ersuchende Behörde ein formelles Rechtshilfeersuchen an den ersuchten Staat auf Herausgabe stellen soll. Die Daten bleiben nach Eingang eines Ersuchens weiterhin gesichert, bis über das Ersuchen entschieden worden ist (Art. 29 Abs. 7 CCC).[164] Einen Spezialfall stellen Verkehrsdaten dar: Wenn von der ersuchten ausländischen Behörde bei der Bearbeitung des Ersuchens festgestellt wird, dass ein Provider eines Drittstaats an der Übermittlung beteiligt war, dann muss sie der ersuchenden Behörde umgehend Verkehrsdaten in ausreichender Menge liefern, damit diese den Ursprung der Übermittlung ermitteln kann (Art. 30 Abs. 1 CCC).[165] In der Schweiz hatte diese Bestimmung zur Folge, dass das Bundesgesetz über internationale Rechtshilfe in Strafsachen (IRSG) mit einem Art. 18b ergänzt werden musste.[166] Um eine sofortige Datensicherung im Sinne von Art. 29 CCC zu veranlassen, ist die Einsatzzentrale von fedpol zu kontaktieren, welche das Ersuchen umgehend an die Kontaktstelle des entsprechenden Staates weiterleitet. Wie bereits angetönt, ist im Anschluss an die umgehende Sicherung der Daten ein Rechtshilfeersuchen an den entsprechenden Staat zu stellen (Art. 31 Abs. 1 CCC).

### 4.3.2. Exkurs: Überblick über die Convention on Cybercrime (CCC)

Einzelne Artikel der Convention on Cybercrime wurden bereits erörtert.[167] Die Convention on Cybercrime umfasst insgesamt vier Kapitel. Kapitel I enthält Begriffsbestimmungen (Art. 1 CCC), Kapitel II Regelungen betreffend innerstaatlich zu treffende Massnahmen

[162] GERCKE/BRUNST, N 44; Explanatory Report CCC, N 159.
[163] Vgl. AEPLI, S. 145.
[164] Explanatory Report CCC, N 283 ff.
[165] Explanatory Report CCC, N 290.
[166] Vgl. BBl 2010 4697, S. 4733 f.
[167] Vgl. Ausführungen zu Art. 32 lit. a CCC, S. 21 ff., zu Art. 32 lit. b CCC, S. 30 ff., zu Art. 16 CCC, S. 33, zu Art. 29 CCC, S. 33; zu Art. 30 CCC, S. 33 und zu Art. 31 CCC, S. 33.

(Art. 2 bis Art. 22 CCC), Kapitel III Bestimmungen zur internationalen Zusammenarbeit (Art. 23 bis Art. 35 CCC) und Kapitel IV die Schlussbestimmungen (Art 36 bis Art. 44 CCC). Kapitel I ist selbsterklärend. In Kapitel II Abschnitt 1 sind Bestimmungen zum materiellen Strafrecht aufgeführt. Darunter fallen nebst verschiedene Tatbestände (Art. 2 bis Art. 10 CCC), welche im innerstaatlichen Recht unter Strafe gestellt werden müssen, auch Bestimmungen zu Versuch und Teilnahme (Art. 11 CCC), Verantwortlichkeit juristischer Personen (Art. 12 CCC) und Sanktionen und Massnahmen (Art. 13 CCC). Der zweite Abschnitt von Kapitel II enthält Normen zum Verfahrensrecht (Art. 14 bis Art. 22 CCC), dabei z.B. auch zu Zwangsmassahmen wie Durchsuchung und Beschlagnahme (Art. 19 CCC), die im innerstaatlichen Recht vorgesehen sein müssen. Das Kapitel III umfasst Regelungen zur internationalen Rechtshilfe (und sogar zur Auslieferung, Art. 24 CCC). Im Gegensatz zu Kapitel II, in welchem die Vertragsparteien dazu verpflichtet werden, bestimmte Normen im innerstaatlichen Recht einzuführen (falls nicht bereits vorhanden), enthält Kapitel III sogenannte self-executing Bestimmungen. Das bedeutet, dass einzelne Bestimmungen des Kapitels III direkt anwendbar sind. Für die Praxis eine wichtige Norm (neben bereits erwähnten) ist Art. 35 CCC (24/7-Netzwerk): Jede Vertragspartei hat eine Kontaktstelle zu bestimmen, welche während sieben Wochentagen 24 Stunden täglich für die Kontaktstellen anderer Vertragsstaaten erreichbar sein muss, um u.a. die umgehende Datensicherung nach Art. 29 und 30 CCC zu veranlassen.[168]

### 4.3.3. Erhebung von Daten in einem Nicht-CCC-Staat

Müssen Daten in einem Staat erhoben werden, der die Cybercrime-Konvention nicht unterzeichnet hat, bleibt lediglich der formelle Rechtshilfeweg. Dabei ist es hilfreich, den Rechtshilfeführer des Bundesamts für Justiz zu konsultieren, um in Erfahrung zu bringen, auf welche bi- oder multilaterale Verträge sich das Rechtshilfeersuchen stützen kann (sofern überhaupt Verträge mit dem betreffenden Staat bestehen), in welcher Sprache das Ersuchen verfasst sein muss, auf welchem Weg (direkte Zustellung oder über das Bundesamt für Justiz) und an welche Stelle im betreffenden Staat das Rechtshilfe gerichtet sein muss.[169] Im Gegensatz zum Vorgehen bei einem CCC-Staat gibt es keine Möglichkeit die Daten im Voraus sichern zu lassen, damit diese während der meistens langen Dauer eines formellen Rechtshilfeverfahrens nicht gelöscht werden. Folglich erscheinen rechtshilfewei-

[168] Eine Liste mit den Kontaktstellen der einzelnen Vertragsstaaten ist unter http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=&CL=ENG&VL=1 abrufbar (zuletzt besucht am 04.08.2015).

[169] Rechtshilfeführer: http://www.rhf.admin.ch/rhf/de/home/rhf.html (zuletzt besucht am 04.08.2015).

se Datenerhebungen in Nicht-CCC-Staaten wenig erfolgsversprechend. Dennoch sollte gerade in schwerwiegenden Fällen nicht darauf verzichtet, sondern ein Rechtshilfeersuchen gestellt werden.

### 4.3.4. Spezialfall Datenerhebung in den USA

Die USA sind Unterzeichnerstaat der Convention on Cybercrime. Dennoch gibt es eine Vorgehensweise, die in gewissen Bereichen von der Vorgehensweise bei anderen CCC-Staaten abweicht. Sollen Daten bei einem US-amerikanischen Provider erhoben werden, muss unterschieden werden, ob Content Data oder Non Content Data erhoben werden sollen. Entsprechend muss eine andere Vorgehensweise gewählt werden. Content Data sind Inhaltsdaten wie z.B. der Inhalt eines E-Mails. Von Non Content Data wird bei Benutzerinformationsdaten und IP-Adressen der Verbindungsprotokolle gesprochen.[170] Das US-Departement of Justice (DOJ) unterscheidet drei Typen von gespeicherten Informationen im Zusammenhang mit Beweiserhebungen bei US-amerikanischen Providern.

Suscriber Information beinhaltet den Konto- oder Benutzernamen des Kunden; die Namen und die Adresse des Kunden; die Telefonnummern des Kunden; die E-Mailadresse des Kunden; die IP-Adressen, welche der Kunde benutzte, um das Konto zu registrieren oder den Service zu beginnen; alle IP-Adressen, mit welcher sich der Kunde in sein Konto eingeloggt hat; die Uhrzeiten, Daten und Dauer der Sessionen sowie weitere Informationen, mit welchen der Kunde identifiziert werden kann (z.B. auch Kreditkartenangaben).[171]

Transactional Information enthält Aufzeichnungen darüber, mit wem der Kunde kommuniziert hat, welche Webseiten er besucht hat und weitere Informationen über die Online-Aktivitäten des Kunden. Bei E-Mails und Webhosting-Konten sind das Informationen über Ziel oder Quelle der Verbindung; Verbindungszeit mit Zeitzone und Datum einer Verbindung; Zeit mit Zeitzone und Datum des Verbindungsendes; Art der Verbindung (z.B. telnet, ftp, http etc.); Grösse des Datentransfers; Headerinformationen; Informationen über Bilder oder andere Dokumente, die auf das betreffende Konto heraufgeladen wurden (Datum, Zeit, Grösse der Datei etc.) sowie identifizierende Informationen über Personen, die auf eine spezifische Datei oder Webseite zugriffen haben.[172]

[170] Leitfaden BJ Beweiserhebung US-Provider, S. 2 f.
[171] Guidance Electronic Evidence, S. 5 f.
[172] Guidance Electronic Evidence, S. 6 f.

Bei Subscriber und Transactional Information handelt es sich um Non Content Data. Als dritten Typen kategorisiert das DOJ schliesslich Content Data wie Inhalte von E-Mails (inkl. Anhänge wie Bilder oder andere Dokumente) oder private Nachrichten auf einem Social Media Konto.[173]

Das DOJ hat genehmigt, dass US-amerikanische Provider direkt angeschrieben werden dürfen, damit diese auf freiwilliger Basis direkt Auskunft erteilen können. Dies betrifft aber nur Auskünfte über Non Content Data.[174] Es kann jedoch nicht darauf vertraut werden, dass sämtliche Provider von diesem Recht auch Gebrauch machen und freiwillig Auskunft erteilen. Aus eigener Erfahrung benötigt es bspw. bei Yahoo! immer ein formelles Rechtshilfeersuchen, auch wenn Non Content Data erhoben werden sollen.

Auch Facebook macht es einem nicht einfach: Auf Editionsbegehren der Staatsanwaltschaft St. Gallen über das Law Enforcement Online Request Portal von Facebook[175] reagierte Facebook mit folgendem Antwortschreiben: *„Dear Officer, We are in receipt of your request and have opened this as our case #000000. Unfortunately, we are unable to provide any data in response to your request as the user is located outside your jurisdiction. For future requests, please note that as you may be able to appreciate, we are bound by applicable law and our terms of service in responding to your request for user information. In this case, we have been advised by Swiss counsel that a request pursuant to Article 273 of the Criminal Procedure Code is required to compel disclosure of non-content subscriber records. Thank you, Facebook Law Enforcement Response Team."* Obwohl die Auskunft des „Swiss Counsel" von Facebook fragwürdig ist, wurde bei der Staatsanwaltschaft St. Gallen, um von Facebook Daten zu erhalten, so fortgefahren, dass beim kantonalen Zwangsmassnahmengericht ein Gesuch um Genehmigung der Erhebung von rückwirkenden Randdaten i.S. von Art. 273 StPO eingereicht wurde. Das kantonale Zwangsmassnahmengericht genehmigte bislang diese Gesuche. Der Entscheid des Zwangsmassnahmenrichters wurde dann auf Englisch übersetzt und über das erwähnte Portal von Facebook eingereicht. Daraufhin lieferte Facebook die gewünschten Daten.

In einem ähnlichen Fall der Staatsanwaltschaft II des Kantons Zürich gelangte diese auf ein vergleichbares Schreiben von Facebook an ihr Zwangsmassnahmengericht und ersuchte um Genehmigung der Erhebung von rückwirkenden Randdaten i.S. von Art. 273 StPO. Das zürcherische Zwangsmassnahmengericht wies das Gesuch ab, da es sich nicht als zu-

[173] Guidance Electronic Evidence, S. 8 f.
[174] Leitfaden BJ Beweiserhebung US-Provider, S. 2.
[175] https://www.facebook.com/records/ (zuletzt besucht am16.07.2015).

ständig erachtete. Gegen diesen Entscheid erhob die Oberstaatsanwaltschaft des Kantons Zürich Beschwerde ans Bundesgericht. Das Bundesgericht wies die Beschwerde ab, da *„für die von der Staatsanwaltschaft beabsichtigten Datenerhebungen (bzw. rückwirkenden Überwachungen) in den USA der Weg der internationalen Rechtshilfe in Strafsachen zu beschreiten ist. Das Zwangsmassnahmengericht hat das Gesuch um Genehmigung einer direkten grenzüberschreitenden Erhebung von Randdaten des Internetverkehrs (gestützt auf Art. 32 CCC i.V.m. Art. 273 StPO) zu Recht abgewiesen. Für eine „Genehmigung" der rechtshilfeweisen Herausgabe von Bestandesdaten war es gar nicht zuständig gewesen."*[176] Die Vorgehensweise der Staatsanwaltschaft St. Gallen war demnach nicht korrekt.

Um von US-amerikanischen Providern Auskünfte zu erhalten, kann auch versucht werden, Ableger dieser Unternehmungen in der Schweiz auf Grundlage der StPO anzuhalten, entsprechende Daten zu liefern. In der Schweiz befinden sich Ableger u.a. von Amazon (Amazon International Services GmbH in Schaffhausen), Apple (Apple Switzerland AG in Zürich), Facebook (Facebook Switzerland Sàrl in Vernier), Google (Google Switzerland GmbH in Zürich), Microsoft (Microsoft Schweiz GmbH in Wallisellen), Yahoo! (Yahoo! Switzerland Server Services Sàrl in Genf).[177] Dass eine solche Vorgehensweise erfolgreich sein kann, zeigt der Entscheid der Beschwerdekammer des Kantonsgerichts Waadt vom 18. Juni 2014.[178] Die Staatsanwaltschaft Waadt (Ministère public central, division entraide, criminalité économique et informatique) verfügte die Sperrung des Zugangs zu einem Blog, der auf einer Google-Seite gehostet war. Diese Verfügung[179] richtete der zuständige Staatsanwalt an die Google Switzerland GmbH in Zürich. Die Google Switzerland GmbH wehrte sich mit Beschwerde gegen diese Verfügung, indem sie geltend machte, gar nicht passivlegitimiert zu sein. Die Passivlegitimation läge bei der Google Inc. in Kalifornien. Die Beschwerdekammer des Kantonsgerichts Waadt entschied, dass die Google Switzerland GmbH in der zu beurteilenden Angelegenheit passivlegitimiert ist. Sie stützt sich in ihrer Argumentation einerseits auf ein Urteil des Gerichtshofs der Europäischen Union vom 13. Mai 2014.[180] In jenem Entscheid ging es darum, ob die Google Spain SL Verfügungsadressat sein kann betreffend die Löschung von indizierten Links mit personenbezogenen Informationen auf der Google-Suchseite. Der EuGH stellt fest, dass Google Spain eine Tochtergesellschaft mit eigener Rechtspersönlichkeit des Google-Konzerns ist.[181] Sie

[176] Urteil BGer 1B_344/2014 vom 14.01.2015, insb. E. 7.
[177] Vgl. WALDER, Folie Nr. 20.
[178] Chambre des recours pénale canton de Vaud, 2014/540, Entscheid-Nr. 416 vom 18.06.2014.
[179] Beschlagnahmebefehl nach Art. 263 Abs. 1 lit. d StPO.
[180] Urteil EuGH C-131/12 vom 13.05.2014.
[181] Urteil EuGH C-131/12 vom 13.05.2014 Ziff. 43.

sei eine „Niederlassung“ von Google Inc. im Sinne von Art. 4 Abs. 1 lit. a der EU-Richtlinie 95/46.[182] Das Gleiche gelte nach Auffassung des Kantonsgerichts Waadt auch für die Google Switzerland GmbH.[183] Andererseits stützt sich das Kantonsgericht Waadt auf einen Bundesgerichtsentscheid vom 31. Mai 2012.[184] Das Bundesgericht hatte u.a. zu entscheiden, ob neben Google Inc. auch die Google Switzerland GmbH in Bezug auf die Umsetzung einer Empfehlung des EDÖB betreffend die Bearbeitung von Personendaten passivlegitimiert sei. Das Bundesgericht bestätigte die Beurteilung des Bundesverwaltungsgerichts, dass die Google Switzerland GmbH bezüglich die Empfehlung des EDÖB passiv legitimiert sei.[185] Jedoch stellte sich die Situation so dar, dass die Google Switzerland GmbH für die Google Inc. gewisse Arbeiten im Bereich der Personendatenbearbeitung durchführte. Gemäss Beurteilung des Bundesverwaltungsgerichts war die Google Switzerland GmbH nicht bloss Stellvertreterin der Google Inc., obwohl die Google Switzerland GmbH während dem Verfahren vor Bundesverwaltungsgericht in ihren Worten als Vertreterin von Google Inc. auftrat und für Google Inc. handelte.[186]

### 4.3.5. Vorabklärungen über polizeiliche Kanäle (Interpol)

Zur Vorbereitung eines Rechtshilfeersuchen sind Vorabklärungen bspw. über Interpol hilfreich. So können auf dem polizeilichen Weg Daten, wie zum Beispiel die Identität von Inhabern von IP-Adressen und von technischen Randdaten abgeklärt werden, die ohne justiziellen Zwang zugänglich sind.[187] In einer von mir geführten Strafuntersuchung konnte auf diese Weise der Inhaber einer niederländischen IP-Adresse in den Niederlanden ermittelt werden, mit welcher über einen Trojaner auf einen Computer in St. Gallen zugegriffen worden war, um Login-Daten zu einem Geldtransferinstitut auszuspionieren.

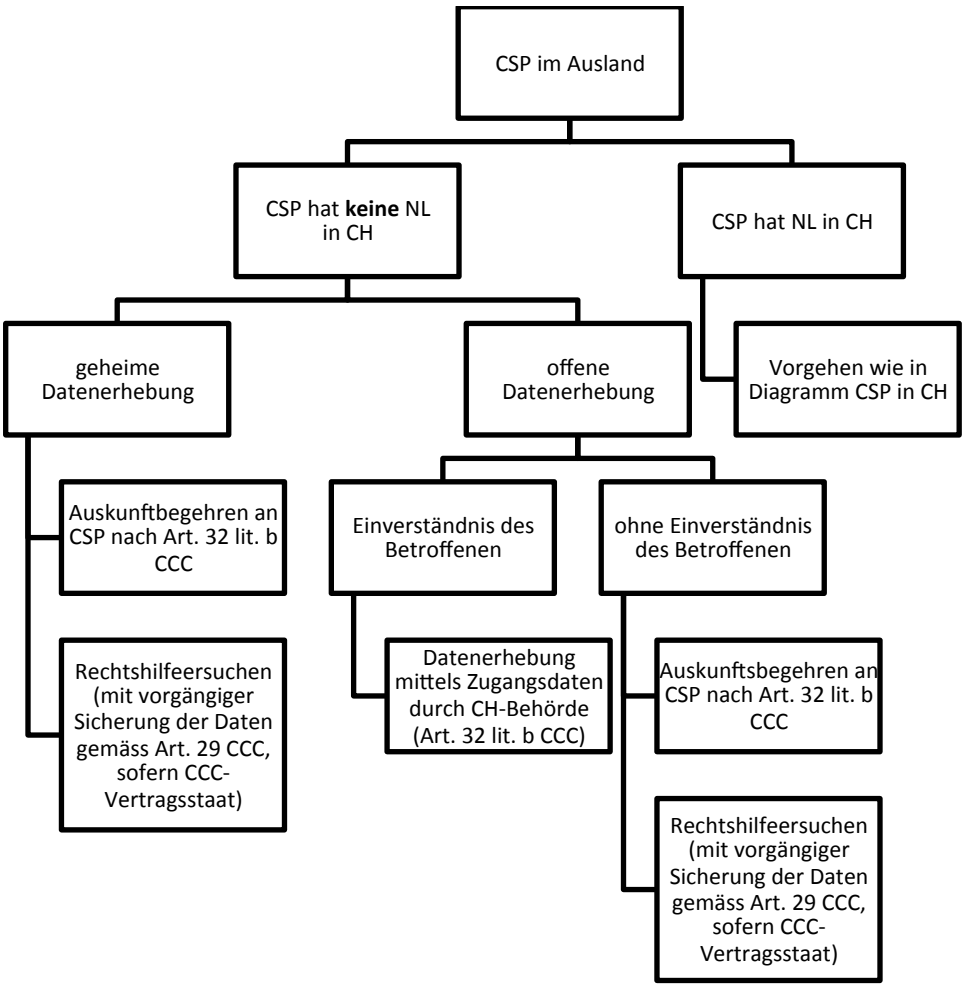
### 4.3.6. Siegelung

Damit Daten, die im Ausland nach den geschilderten Methoden erhoben worden sind, im schweizerischen Strafverfahren verwendet werden dürfen, muss die an den Daten berech-

[182] Urteil EuGH C-131/12 vom 13.05.2014 Ziff. 49 und 59.
[183] Chambre des recours pénale canton de Vaud, 2014/540, Entscheid-Nr. 416, vom 18.06.2014, E. 3b/dd.
[184] Urteil BGer 1C_230/2011 vom 31.05.2012.
[185] Urteil BGer 1C_230/2011 vom 31.05.2012 E. 4.
[186] Urteil BVGer A-7040/2009 vom 30.03.2011 E. 4.3.4 und 4.3.6.
[187] Vgl. Bundesamt für Justiz/Bundesamt für Polizei fedpol, Aufgabenabgrenzung vom 1. Februar 2010 im Bereich der internationalen Strafrechtshilfe (BJ) und der Polizeikoordination (fedpol), Stand 01.01.2012, S. 3.

tigte Person, meist die beschuldigte Person, auf das Recht der Siegelung aufmerksam gemacht werden. Es wird auf die vorgehenden Ausführungen zur Siegelung verwiesen.[188]

### 4.3.7. Zusammenfassung in Form eines Schemas




[188] Vgl. Ausführungen S. 24 ff.

# 5. Fazit

Strafrechtliche Beweiserhebungen in einer Cloud sind nicht unmöglich, auch wenn das Konstrukt des Cloud Computing auf den ersten Blick den einen oder anderen Strafverfolger vielleicht abschreckt. Wenn sich die zu erhebenden Daten bzw. der zuständige Cloud-Provider in der Schweiz befindet, sind den Strafverfolgungsbehörden in der schweizerischen Strafprozessordnung genügend Möglichkeiten gegeben, an die verfahrensrelevanten Daten zu gelangen. Schwieriger gestaltet es sich, wenn der Cloud-Provider seinen Sitz hat im Ausland.[189] Sofern eine „freiwillige" Datenherausgabe angestrebt werden kann, scheint mit dem in dieser Arbeit beschriebenen Art. 32 lit. b CCC die rechtliche Grundlage gegeben zu sein, Daten auf diese Weise zu erheben, sodass sie im schweizerischen Strafverfahren als Beweise verwertbar sind.[190] Fraglich bleibt, ob die Vorgehensweise nach Art. 32 lit. b CCC auch bei einem US-amerikanischen Provider zum Erfolg führt, wenn Inhaltsdaten (Content Data) erhoben werden sollen. Es müsste bei einem passenden Fall ausprobiert werden.

Einen spannenden Ansatz verfolgte die Staatsanwaltschaft des Kantons Waadt, indem sie einer Tochtergesellschaft eines amerikanischen Providers in der Schweiz nach schweizerischer Strafprozessordnung eine Verfügung zustellte. Dieses Vorgehen wurde zumindest durch die Beschwerdekammer des Kantonsgerichts Waadt geschützt.[191] Aus meiner Sicht müssen sich die Schweizer Strafverfolgungsbehörden auch in Zukunft getrauen, auf diese Weise an die grossen Internetkonzerne zu gelangen, um Auskünfte zu erhalten, sofern die fraglichen Konzerne eine Tochterfirma in der Schweiz betreiben.

Während des Abfassens dieser Masterarbeit habe ich mir Gedanken dazu gemacht, ob auf nationaler Ebene Regelungen eingeführt werden müssen, die es den Strafverfolgungsbehörden erleichtern, Daten bei Cloud-Service-Providern zu erheben. Wie bereits erwähnt, bin ich zum Schluss gelangt, dass die schweizerische Strafprozessordnung genügende Rechtsgrundlagen zur Datenerhebung bietet, wenn die Daten bei Cloud Service Providern in der Schweiz erhoben werden müssen. Im Hinblick auf Daten, welche bei Cloud Service Providern im Ausland eingefordert werden müssen, vertritt Belgien (i.c. betreffend einen ISP) einen interessanten Ansatz, den SCHWEINGRUBER in ihrem Artikel im Jusletter schil-

[189] Sehr passend der Titel des Artikels von Juana Vasella im plädoyer 1/15 vom 02.02.2015, S. 72: *Strafverfolger: An der Grenze ist oft Schluss.*
[190] Vgl. Ausführungen S. 30 ff.
[191] Vgl. Ausführungen S. 37 ff.

dert.[192] Nach Art. 46$^{bis}$ der belgischen Strafprozessordnung kann ein Staatsanwalt den Betreiber eines elektronischen Kommunikationsnetzes *(„l'opérateur d'une réseau de communication électronique")* oder eines elektronischen Kommunikationsdienstes *(„un fournisseur d'un service de communication électronique")* verpflichten, Auskunft zu geben über Daten, welche die Identifikation des Nutzers ermöglichen.[193] Nach Ansicht der belgischen Staatsanwaltschaft und des belgischen Kassationsgericht *(„Cour de cassation"/„Hof van cassatie")* beschränkt sich diese Bestimmung nicht nur auf Internet Service Provider in Belgien, sondern ist auf sämtliche Provider anwendbar, die ihre Dienste in Belgien (auch vom Ausland aus) anbieten.[194] In diesem Sinne könnte auch in der schweizerischen StPO oder im BÜPF eine Norm eingeführt werden, die auch ausländische Anbieter von Kommunikationsdienstleistungen verpflichtet, entsprechende Auskünfte zu erteilen, sofern sie in der Schweiz ihre Dienstleistungen erbringen.

Es ist m.E. unerlässlich, dass vom Territorialitätsprinzip abgewichen werden muss, wenn wir in Zukunft Strafverfolgung im Bereich des Internets und damit des Cloud Computing betreiben wollen. Das Zugriffsprinzip scheint dafür ein gutes Mittel zu sein, um zumindest von der Schweiz aus auf Daten im Ausland zugreifen zu können. Jedoch funktioniert dieses Prinzip nur, wenn es keinen staatlichen Zwang braucht, um an die gewünschten Daten zu gelangen. Datenerhebungen mittels hoheitlichem Zwang sind aufgrund der aktuellen rechtlichen Situation nur durch ein Rechtshilfeersuchen möglich. Trotz Convention on Cybercrime, welche zumindest die umgehende Sicherung von relevanten Daten ermöglicht, kann ein solches Verfahren seine Zeit dauern. Daher wird dafür plädiert, dass die Convention on Cybercrime im Bereich der „zwangsweisen" Datenerhebung ausgebaut wird.[195] Dies hätte für die Schweiz zur Folge, dass das IRSG entsprechend angepasst werden müsste. Dass dies nicht unmöglich ist, zeigt die Einführung von Art. 18b IRSG.

Beweiserhebung in der Cloud ist möglich. Im transnationalen Bereich müssten die rechtlichen Möglichkeiten aber noch ausgebaut werden.

[192] SCHWEINGRUBER, Rz. 33 ff.
[193] Code d'instruction criminelle abrufbar über www.droitbelge.be (zuletzt besucht am 07.08.2015).
[194] Vgl. NICOLAS ROLAND, Court of Appeals of Antwerp confirms Yahoo!'s obligation to cooperate with law enforcement agencies, Brüssel, 15.07.2014, http://www.stibbe.com/en/news/2014/july/benelux-ict-law-newsletter-49-court-of-appeal-of-antwerp-confirms-yahoo-obligation (zuletzt besucht am 07.08.2015).
[195] Vgl. SCHWERHA, S. 19.

## Selbständigkeitserklärung

Ich bestätige mit meiner Unterschrift, dass ich die vorliegende Arbeit selbständig ohne Mithilfe Dritter verfasst habe und in der Arbeit alle verwendeten Quellen angegeben habe. Ich nehme zur Kenntnis, dass im Falle von Plagiaten auf Note 1 erkannt werden kann.

St. Gallen, 12. August 2015

Daniel Burgermeister