Universität St. Gallen

Hochschule für Wirtschafts-, Rechts- und Sozialwissenschaften
sowie Internationale Beziehungen

Masterarbeit

Probleme der strafprozessualen Überwachung abgeleiteter Internetdienste wie Facebook, Skype oder Whatsapp

Lösungen im neuen BÜPF?

vorgelegt von

Laura Dusanek

Magnihalden 6

CH-9000 St. Gallen

laura.dusanek@student.unisg.ch

14-612-220

vorgelegt bei

Prof. Dr. Marc Forster

Universität St. Gallen

20. Mai 2019

Inhaltsverzeichnis

Abkürzungsverzeichnis

a.M.	anderer Meinung
AAKD	Anbieterin(nen) abgeleiteter Kommunikationsdienste
Abs.	Absatz, Absätze
aBÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 6. Oktober 2000 (Stand am 1. September 2017), aufgehoben am 1. März 2018, AS 2001 3096
aFMG	Fernmeldegesetz vom 21. Juni 1991, aufgehoben am 20. Oktober 1997, AS 1992 581
AJP	Aktuelle Juristische Praxis
Art.	Artikel
AS	Amtliche Sammlungen des Bundesrecht; bis 1987: Sammlungen der eidgenössischen Gesetze; bis 1948: Amtliche Sammlung der Bundesgesetze und Verordnungen (Eidgenössische Gesetzessammlung)
Aufl.	Auflage
aVÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 31. Oktober 2001 (Stand am 1. September 2017), aufgehoben am 1. März 2018, SR 780.11, AS 2001 3111, 2018 147
BAKOM	Bundesamt für Kommunikation
BBl	Bundesblatt
BGE	Bundesgerichtsentscheid(e)
BGer	Bundesgericht
BJ	Bundesamt für Justiz
BS	Bereinigte Sammlung der Bundesgesetze und Verordnungen 1848–1947
BSK	Basler Kommentar
bspw.	beispielsweise
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (Stand am 1. März 2018), SR 780.1

BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (Stand am 23. September 2018), SR 101
bzgl.	bezüglich
bzw.	beziehungsweise
CCC	Übereinkommen über die Cyberkriminalität vom 23. November 2001, in Kraft getreten für die Schweiz am 1. Januar 2012 (Stand am 14. Februar 2019), SR 0.311.43
Ders.	Derselbe
Diss.	Dissertation
dt.	deutsch
EDV	Elektronische Datenverarbeitung
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 4. November 1950, in Kraft getreten für die Schweiz am 28. November 1974 (Stand am 23. Februar 2012), SR 0.101
engl.	englisch
etc.	et cetera
EU	Europäische Union
EÜR	Europäisches Übereinkommen über die Rechtshilfe in Strafsachen vom 20. April 1959, in Kraft getreten für die Schweiz am 20. März 1967 (Stand am 16. Januar 2013), SR 0.351.1
f., ff.	folgende, fortfolgende
FDV	Verordnung über Fernmeldedienste vom 9. März 2007 (Stand am 1. März 2018), SR 784.101.1
FMG	Fernmeldegesetz vom 30. April 1997 (Stand am 1. März 2018), SR 784.10
Fn.	Fussnote(n)
ggf.	gegebenenfalls
gl.M.	gleicher Meinung
GovWare	Government Ware

GwÜ	Übereinkommen über Geldwäscherei sowie Ermittlung, Beschlagnahme und Einziehung von Erträgen aus Straftaten vom 8. November 1990, in Kraft getreten für die Schweiz am 1. September 1993 (Stand am 1. September 2015), SR 0.311.53
h.L.	herrschende Lehre
Hrsg.	HerausgeberInnen
i.B.a.	in Bezug auf
i.S., i.S.v.	im Sinne, im Sinne von
i.V.m.	in Verbindung mit
IMSI	International Mobile Subscriber Identity (engl.), Internationale Mobilfunk-Teilnehmerkennung (dt.)
inkl.	inklusive
insb.	insbesondere
IP	Internet Protocol (engl.), Internetprotokoll (dt.)
IPBPR	Internationaler Pakt über bürgerliche und politische Rechte vom 16. Dezember 1966, in Kraft getreten für die Schweiz am 18. September 1992 (Stand am 27. März 2017), SR 0.103.2
IRI	Intercept Related Informations (engl.)
IRSG	Bundesgesetz über die internationale Rechtshilfe in Strafsachen vom 20. März 1981 (Stand am 1. März 2019), SR 351.1
IRST	Internationale Rechtshilfe in Strafsachen
IT	Informationstechnik
Kap.	Kapitel
Komm	Kommentar
lit.	litera
m.E.	meines Erachtens
m.w.H.	mit weiteren Hinweisen
Mio.	Millionen

N	Note(n), Randnote(n)
No.	number (engl.)
Nr.	Nummer(n)
OTT	Over-the-top
P2P	Peer-to-Peer (engl.), Rechner-Rechner-Verbindung (dt.)
PG	Postgesetz vom 17. Dezember 2010 (Stand am 1. Januar 2012), SR 783.0
Rspr.	Rechtsprechung
RVUS	Staatsvertrag zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen vom 25. Mai 1973, in Kraft getreten für die Schweiz am 23. Januar 1977 (Stand am 23. Januar 1977), SR 0.351.933.6
Rz.	Randziffer(n)
SJZ	Schweizerische Juristen-Zeitung
SMS	Short Messages Service (engl.), Kurznachrichtendienst (dt.)
sog.	sogenannt, sogenannte(r)
SR	Systematische Sammlung des Bundesrechts
SRF	Schweizer Radio und Fernsehen
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (Stand am 1. März 2019), SR 311.0
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (Stand am 1. März 2019), SR 312.0
T-CY	Cybercrime Convention Committee (engl.)
TVG	Bundesgesetz über den Telegraphen- und Telephonverkehr (Telegraphen- und Telephonverkehrsgesetz) vom 14. Oktober 1922, aufgehoben am 1. April 1992, BS 7 867, AS 39 13
u.a.	unter anderem, anderen
u.U.	unter Umständen
ÜPF	Überwachung Post- und Fernmeldeverkehr

usw.	und so weiter
v.a.	vor allem
VD	Kanton Waadt
vgl.	vergleiche
VÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 15. November 2017 (Stand am 9. April 2019), SR 780.11
VÜPF 1997	Verordnung über den Dienst für die Überwachung des Post- und Fernmeldeverkehrs vom 1. Dezember 1997, aufgehoben am 1. Januar 2002, AS 1997 3022, 2001 3111
z.B.	zum Beispiel
z.T.	zum Teil
ZBJV	Zeitschrift des bernischen Juristenvereins
Ziff.	Ziffer(n)
zit.	zitiert
ZStrR	Schweizerische Zeitschrift für Strafrecht

Literaturverzeichnis

AEPLI MICHAEL, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Unter Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich, Diss. Zürich 2003 (zit.: AEPLI)

BANGERTER SIMON, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht – unter vergleichender Berücksichtigung der StPO, Diss. Zürich 2014 (zit.: BANGERTER)

BERTSCHMANN SIMON, Randdatenerhebung im Fernmeldeverkehr gemäss Art. 273 StPO, in: AJP 2019, 358–363 (zit.: BERTSCHMANN)

BRODOWSKI DOMINIK, Verdeckte technische Überwachungsmassnahmen im Polizei- und Strafverfahrensrecht, Zur rechtsstaatlichen und rechtspraktischen Notwendigkeit eines einheitlichen operativen Ermittlungsrechts, Tübingen 2016 (zit.: BRODOWSKI)

BSK IRST, NIGGLI MARCEL A./HEIMGARTNER STEFAN (Hrsg.), Basler Kommentar, Internationales Strafrecht (IRSG, GwÜ), 1. Aufl., Basel 2015 (zit.: BSK IRST-BEARBEITERIN)

BSK StPO, NIGGLI MARCEL A./HEER MARIANNE/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung/Jugendstrafprozessordnung, 2. Aufl., Basel 2014 (zit.: BSK StPO-BEARBEITERIN)

BUNDESAMT FÜR KOMMUNIKATION BAKOM, Leitfaden zum „Meldeformular für das Erbringen von Fernmeldediensten“, Ausgabe 7 (zit.: BAKOM, Leitfaden)

BURGERMEISTER DANIEL, Beweiserhebung in der Cloud, Masterarbeit St. Gallen 2015 (zit.: BURGERMEISTER)

DIENST ÜBERWACHUNG POST- UND FERNMELDEVERKEHR ÜPF, Merkblatt „FDA - AAKD“, Abgrenzung zwischen Fernmeldedienstanbieterinnen (FDA) und Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD), Stand am 26. Juli 2018 (zit.: DIENST ÜPF, Merkblatt „FDA – AAKD“)

DOMBROWSKI NADINE, Extraterritoriale Strafrechtsanwendung im Internet, Berlin 2014 (zit.: DOMBROWSKI)

DONATSCH ANDREAS/HANSJAKOB THOMAS/LIEBER VIKTOR (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung (StPO), 2. Aufl., Zürich/Basel/Genf 2014 (zit.: Komm StPO-BEARBEITERIN)

FLACH BEAT, Entspricht die Praxis des Dienstes ÜPF hinsichtlich Pflichten der Anbieterinnen abgeleiteter Kommunikationsdienste dem Gesetz?, Interpellation Nr. 19.3267, eingereicht von FLACH BEAT im Nationalrat am 21. März 2019 (zit.: Interpellation FLACH)

FORSTER MARC, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs, in: GSCHWEND LUKAS/HETTICH PETER/MÜLLER-CHEN MARKUS/SCHINDLER BENJAMIN /WILDHABER ISABELLE (Hrsg.), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, 615–635 (zit.: FORSTER)

GRAF DAMIAN K., Strafbewehrter Geheimnisvorrat im grenzüberschreitenden Kontext, in: SJZ 112/2016, 193–200 (zit.: GRAF, SJZ)

GRAF DAMIAN K., Strafverfolgung 2.0: Direkter Zugriff der Strafbehörden auf im Ausland gespeicherte Daten?, Jusletter IT vom 21. September 2017 (zit.: GRAF, Jusletter IT)

HANSJAKOB THOMAS, Das neue BÜPF, Nötig oder Zwängerei?, in: ZStrR 134/2016, 429–444 (zit.: HANSJAKOB, ZStrR)

HANSJAKOB THOMAS, Der Einsatz von GovWare in der Schweiz, Zum geplanten Art. 269ter StPO, in: Jusletter IT vom 15. Mai 2014 (zit.: HANSJAKOB, Jusletter IT)

HANSJAKOB THOMAS, Die Erhebung von Daten des Internetverkehrs – Bemerkungen zu BGer 6B_656/2015 vom 16.12.2016, in: forumpoenale 4/2017, 252–257 (zit.: HANSJAKOB, Erhebung von Daten)

HANSJAKOB THOMAS, Einsatz von GovWare in der Strafverfolgung, Zu Notwendigkeit und Anwendungsbereich von Art. 269ter StPO, in: GSCHWEND LUKAS/HETTICH PETER/MÜLLER-CHEN MARKUS/SCHINDLER BENJAMIN/WILDHABER ISABELLE (Hrsg.), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, 637–651 (zit.: HANSJAKOB, GovWare)

HANSJAKOB THOMAS, Einsatz von GovWare – zulässig oder nicht?, Zum Einsatz von Computerprogrammen bei der Überwachung von Internet-Telefonie, in: Jusletter vom 5. Dezember 2011 (zit.: HANSJAKOB, Jusletter)

HANSJAKOB THOMAS, Überwachungsrecht der Schweiz, Kommentar zu Art. 269 ff. StPO und zum BÜPF, Zürich/Basel/Genf 2017 (zit.: HANSJAKOB, Überwachungsrecht)

HANSJAKOB THOMAS, Wichtig Entwicklungen der Bundesgerichtspraxis zu Überwachungen des Post- und Fernmeldeverkehrs, Bemerkungen zu den Bundesgerichtsentscheiden 138 IV 232 vom 16.11.2012 und 1B_481/2012 vom 22.1.2013, in: forumpoenale 3/2013, 173–177 (zit.: HANSJAKOB, Wichtige Entwicklungen)

HEIMGARTNER STEFAN, Die internationale Dimension von Internetstraffällen – Strafhoheit und internationale Rechtshilfe in Strafsachen, in: SCHWARZENEGGER CHRISTIAN/ARTER OLIVER/JÖRG

FLORIAN S. (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, 117–150 (zit.: HEIMGARTNER, Internetstraffälle)

HEIMGARTNER STEFAN, Strafprozessuale Beschlagnahme, Wesen, Arten und Wirkungen unter Berücksichtigung der Beweismittel-, Einziehungs-, Rückgabe- und Ersatzforderungsbeschlagnahme, Diss. Zürich 2011 (zit.: HEIMGARTNER, Beschlagnahme)

JEAN-RICHARD-DIT-BRESSEL MARC, Die Mailbox – Ziel oder Weg? Zur Abgrenzung von Beschlagnahme und Überwachung im Strafverfahren, in: ZStrR 125/2007, 157–179 (zit.: JEAN-RICHARD-DIT-BRESSEL)

KLAUS SAMUEL/MATHYS ROLAND, „The Best of BÜPF" – Was ändert sich mit der Revision?, in: Jusletter IT vom 22. September 2016 (zit.: KLAUS/MATHYS)

MORSCHER LUKAS, Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, in: ZBJV 147/2011, 177–221 (zit.: MORSCHER)

ROTH SIMON, Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess, Direkter Zugriff oder Rechtshilfe?, in: Jusletter vom 17. August 2015 (zit.: ROTH)

RYSER DOMINIC, „Computer Forensics", eine neue Herausforderung für das Strafprozessrecht, Strafprozessrechtliche Beweissicherung, Beweisführung mit Sachverständigengutachten und Beweiswürdigung in IT-Fällen, in: SCHWARZENEGGER CHRISTIAN/ARTER OLIVER/JÖRG FLORIAN S. (Hrsg.), Internet-Recht und Strafrecht, Bern 2005, 553–594 (zit.: RYSER)

SCHLAURI SIMON, Definition des Fernmeldedienstes gemäss FMG und BÜPF, Rechtswidrige Uminterpretation des Begriffs des Fernmeldedienstes, Digitale Gesellschaft vom 9. Oktober 2018, abgerufen am 20. März 2019 von <https://www.digitale-gesellschaft.ch/2018/10/09/rechtswidrige-uminterpretation-des-begriffs-der-fernmeldedienste-definition-des-fernmeldedienstes-gemaess-fmg-und-buepf/> (zit.: SCHLAURI, Definition des Fernmeldedienstes)

SCHLAURI SIMON, Überwachungsgesetz BÜPF, Überwachungsbehörde will Geltungsbereich ausweiten, in: Digitale Gesellschaft vom 22. Mai 2018, abgerufen am 21. März 2019 von <https://www.digitale-gesellschaft.ch/2018/05/22/ueberwachungsbehoerde-will-geltungsbereich-ausweiten-ueberwachungsgesetz-buepf/> (zit.: SCHLAURI, Überwachungsgesetz BÜPF)

SCHMID NIKLAUS, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im allgemeinen, in: ZStrR 111/1993, 81–109 (zit.: SCHMID)

SCHMID NIKLAUS/JOSITSCH DANIEL, Schweizerische Strafprozessordnung, Praxiskommentar, 3. Aufl., Zürich/St. Gallen 2018 (zit.: SCHMID/JOSITSCH, 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, 179–192 (zit.: SCHNEIDER)

SCHWEINGRUBER SANDRA, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, in: Jusletter vom 10. November 2014 (zit.: SCHWEINGRUBER)

„IMSI-Catcher“, in: Wikipedia, Die freie Enzyklopädie, Bearbeitungsstand am 22. Februar 2019, abgerufen am 5. März 2019 von <https://de.wikipedia.org/w/index.php?title=IMSI-Catcher&oldid=185934191>

„Internetdienstanbieter“, in: Wikipedia, Die freie Enzyklopädie, Bearbeitungsstand am 6. Mai 2018, abgerufen am 7. März 2019 von <https://de.wikipedia.org/w/index.php?title=Internetdienstanbieter&oldid=177196290>

SEITZ NICOLAI, Strafverfolgungsmassnahmen im Internet, Köln 2004 (zit.: SEITZ)

SRF, Facebook Schweiz soll Daten herausrücken, Der Internet-Riese soll den Strafverfolgungsbehörden in Zukunft besser unter die Arme greifen, in: SRF News vom 16. Februar 2017, abgerufen am 10. April 2019 von <https://www.srf.ch/news/schweiz/facebook-schweiz-soll-daten-herausruecken> (zit.: SRF, Facebook Schweiz soll Daten herausrücken)

Materialienverzeichnis

Hinweis: *Die aufgeführten Materialien werden in den Fussnoten abgekürzt zitiert. Die Zitierweise ist jeweils kursiv vorangestellt.*

BBl 1889 III 879, Bundesgesetz betreffend die Erstellung Telegraphen- und Telephon-Linien vom 26. Juni 1889

BBl 1921 III 280, Botschaft vom 6. Juni 1921 betreffend die Revision des Bundesgesetzte vom 22. Juni 1877 über den telegraphischen Verkehr im Inneren der Schweiz und vom 27. Juni 1889 betreffend das Telephonwesen nebst Änderungen vom 7. Dezember 1894, 23. Dezember 1914 und 23. Januar 1920

BBl 1968 I 585, Botschaft vom 21. Februar 1968 über die Verstärkung des strafrechtlichen Schutzes des persönlichen Geheimbereichs

BBl 1979 I 574, Bundesgesetz über den Schutz der persönlichen Geheimsphäre (Änderungen von Bundesgesetzen) vom 23. März 1979

BBl 1976 I 529, Bericht der Kommission des Nationalrates vom 32. Oktober 1975 betreffend Parlamentarische Initiative über den Schutz der persönlichen Geheimsphäre

BBl 1988 I 1311, Botschaft vom 7. Dezember 1987 zum Fernmeldegesetz (FMG)

BBl 2010 4697, Botschaft vom 18. Juni 2010 über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität

BBl 2013 2683, Botschaft vom 27. Februar 2013 zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

BBl 2017 6559, Botschaft vom 6. September 2017 zur Revision des Fernmeldegesetzes

Explanatory Report No. 185, Council of Europe (Europarat), Explanatory Report of 23 November 2001 to the Convention on Cybercrime

Final Report T-CY, Cybercrime Convention Committee (T-CY) Cloud Evidence Group, Final report of 16 September 2016, Criminal justice access to electric evidence in the cloud: Recommendations for consideration by the T-CY

Erläuternder Bericht Totalrevision VÜPF, Erläuternder Bericht zur Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)

Vorentwurf BÜPF, Vorentwurf vom 30. April 2010 zum Bundesgesetz betreffend Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Judikaturverzeichnis

Hinweis: *Die aufgeführte Rechtsprechung wird in den Fussnoten abgekürzt zitiert. Die Zitierweise ist jeweils kursiv vorangestellt.*

Amtlich publizierte Entscheide des Bundesgerichts:

BGE 111 Ib 50, Auszug aus dem Urteil vom 8. Juli 1985

BGE 130 II 193, Auszug aus dem Urteil 1A_153/2003 vom 11. Februar 2004

BGE 137 IV 340, Auszug aus dem Urteil 1B_376/2011 vom 3. November 2011

BGE 139 IV 98, Auszug aus dem Urteil 1B_481/2012 vom 22. Januar 2013

BGE 139 IV 195, Auszug aus dem Urteil 1B_128/2013 vom 8. Mai 2013

BGE 140 IV 86, Auszug aus dem Urteil 1B_377/2013 vom 27. März 2014

BGE 140 IV 181, Auszug aus dem Urteil 1B_19/2014 vom 28. Mai 2014

BGE 141 IV 108, Auszug aus dem Urteil 1B_344/2014 vom 14. Januar 2015

BGE 143 IV 21, Auszug aus dem Urteil 1B_185/2016 vom 16. November 2016

BGE 143 IV 270, Auszug aus dem Urteil 1B_29/2017 vom 24. Mai 2017

Nicht amtlich publizierte Entscheide des Bundesgerichts:

BGer 1B_425/2010, Urteil vom 22. Juni 2011

BGer 1B_131/2015, Urteil vom 30. Juli 2015

BGer 1B_52/2015, Urteil vom 24. August 2015

BGer 1B_347/2015, Urteil vom 29. März 2016

BGer 1B_142/2016, Urteil vom 16. November 2016

BGer 6B_656/2015, Urteil vom 16. Dezember 2016

Entscheide kantonaler Gerichte:

Chambre des recours pénal VD 2014/540, Urteil vom 18. Juni 2014, Entscheid-Nr. 416

Abbildungsverzeichnis

I. Einleitung

Der technische Fortschritt im Bereich der Telekommunikation über das Internet bzw. über abgeleitete Internetdienste wie Whatsapp, Facebook, Skype und Instagram stellt die Strafverfolgungsbehörden vor neue Herausforderungen. Klassische Kommunikationsmittel werden zunehmend durch Internetkommunikationsmöglichkeiten ersetzt. So steht den Benutzenden[1] heutzutage eine Vielzahl an Kommunikationsmitteln über das Internet zur Verfügung. Dies hat jedoch auch zur Folge, dass die neuen Kommunikationstechnologien (wie bereits die klassischen) für die Begehung von Straftaten missbraucht werden.

Die neuen Technologien erschweren die technische Durchführung einer Überwachung des Fernmeldeverkehrs, weshalb der Gesetzgeber mit der Herausforderung konfrontiert ist, eine effiziente und wirksame Strafverfolgung in diesem hoch komplexen Bereich zu garantieren. Der Gesetzgeber hat dieses Problem bereits im Jahre 2013 erkannt und eine Totalrevision des Bundesgesetzes über den Post- und Fernmeldeverkehr (BÜPF) vorgelegt. Vor der Revision war eine Überwachung von abgeleiteten Internetdiensten rechtlich problematisch bzw. unzulässig, weil sie durch die gesetzliche Grundlage nicht gedeckt war. Die Rechtspraxis war auch mit weiteren Problemen konfrontiert: Anbieterinnen von abgeleiteten Internetdiensten bzw. reine Service Provider konnten denn auch nicht zur Speicherung von Randdaten verpflichtet werden und die Überwachung von (heute weit verbreiteter) verschlüsselter Kommunikation, welche regelmässig nur durch den Einsatz besonderer Informatikprogramme (sog. GovWare) brauchbare Ergebnisse lieferte, war rechtlich äusserst umstritten. Mit der Totalrevision des BÜPF wurden diese Überwachungshindernisse insoweit behoben, als dass der Kreis der Mitwirkungspflichten erweitert wurde und neu auch die Anbieterinnen abgeleiteter Kommunikationsdiente erfasst. Des Weiteren wurde mit Art. 269ter StPO eine rechtliche Grundlage für den Einsatz besonderer Informatikprogramme wie der GovWare geschaffen. Im Kapitel II. (*II. Rechtslage der Schweiz zur Post- und Fernmeldeüberwachung*) der gegenständlichen Arbeit wird vertieft auf die alt- und neurechtlichen Probleme der Überwachung abgeleiteter Kommunikationsdienste eingegangen, wobei die für die Telekommunikation grundlegende (alte) h.L. und Rechtsprechung, welche neu auch auf die Anbieterinnen abgeleiteter Internetdienste Anwendung findet, fundiert besprochen wird.

Zwar hat der Gesetzgeber eine Überwachung der abgeleiteten Internetdienste mittlerweile rechtlich verankert, doch besteht das bereits unter altem Recht grosse Problem der transnationalen Delinquenz weiter. Die Anwendung des schweizerischen Rechts wird durch den Grundsatz der Territorialität be-

[1] Die vorliegende Arbeit verfolgt eine geschlechtergerechte Schreibweise: Um diese zu gewährleisten wird regelmässig zwischen weiblichen und männlichen Personenbezeichnungen abgewechselt, wobei für die „Anbieterin“ stets die weibliche und für den „Gesetzgeber“ oder den „Bundesrat“ stets die männliche Form verwendet wird. Des Weiteren werden geschlechtsneutrale Bezeichnungen („die/der Benutzende“) verwendet. Die jeweils gewählte weibliche oder männliche Form schliesst eine männliche bzw. weibliche Form gleichberechtigt in die Bezeichnung ein.

grenzt, was eine effiziente Strafverfolgung in grenzüberschreitenden Fällen erheblich erschwert, sodass zumeist nur der formelle Rechtshilfeweg offensteht. Im Bereich der Kommunikation über abgeleitete Kommunikationsdienste ist jedoch eine effiziente transnationale Strafverfolgung besonders wichtig, weil viele grosse Anbieterinnen abgeleiteter Internetdienste ihren Sitz im Ausland (vorwiegenden den USA) haben und die Daten auch dort verwaltet und gespeichert werden.

Das Internationale Übereinkommen vom 23. November 2001 über die Cyberkriminalität (CCC) ist am 1. Januar 2012 für die Schweiz in Kraft getreten. Das CCC strebt eine wirksame Bekämpfung von Computerkriminalität und eine verstärkte, zügige und gut funktionierende internationale Zusammenarbeit in Strafsachen an. So sieht es Instrumente vor, die eine transnationale Datenerhebung unter bestimmten Voraussetzungen erleichtern. Nichtsdestotrotz stellt die virtuelle Globalisierung ein grundsätzliches Problem für eine wirksame Bekämpfung von Cybercrime und die Rechtsanwendung im Bereich des Internets dar, welches auch durch das revidierte BÜPF und die CCC nicht behoben wurde[2]. Folglich stellt sich die Frage, ob sich nicht eine Relativierung des Territorialitätsprinzips angesichts der transnationalen Cyberkriminalität förmlich aufdrängt? Oder bietet sich eine Möglichkeit, die in der Schweiz ansässigen Tochter- oder Partnergesellschaften (wie bspw. jene von Google und Facebook) von ausländischen Internetdienstanbieterinnen zur Mitwirkungen bei der Datenerhebung zu verpflichten? Das Problem der grenzüberschreitenden Datenerhebung wird in Kapitel III. (*III. Grenzüberschreitende Strafverfolgungsmassnahmen*) eingehend behandelt. Die Instrumente der CCC zur vereinfachten Verfolgung von Cybercrime werden vorgestellt und diskutiert. Es werden auch verschiedene Auslegungsvarianten des Territorialitätsprinzips aufgezeigt und diskutiert.

In Kapitel IV. (*IV. Bedeutung und Auswirkungen der Erkenntnisse auf die Praxis*) werden die Erkenntnisse des II. und III. Kapitels zusammengefasst und die Autorin stellt ihre eigene Meinung im Rahmen zweier Schemata vor. Das erste Schema zur Datenerhebung in der Schweiz bezieht sich auf das in Kapitel II. diskutierte Vorgehen. Das zweite Schema stellt das Vorgehen zur grenzüberschreitenden Datenerhebung dar und umfasst die Ergebnisse des III. Kapitels. Die beiden Schemata dienen den Strafverfolgungsbehörden und der Gerichtspraxis als Orientierung bei der Verfügung und Beurteilung von nationalen und transnationalen Strafverfolgungsmassnahmen. Das Ziel dieses Kapitels ist es, eine übersichtliche, gegliederte und von der Autorin empfohlene Vorgehensweise vorzustellen.

[2] BBl 2013 2683, 2689.

II. Rechtslage der Schweiz zur Post- und Fernmeldeüberwachung

1. Gesetzliche Entwicklungen

Die gesetzlichen Entwicklungen im Bereich des Post- und Fernmeldeverkehrs sind für das Verständnis der heutigen Regelungen nicht unbedeutend, weshalb sie in diesem Kapitel kurz dargestellt werden.

Im 20. Jahrhundert lag der Regelungsbereich zur Post- und Fernmeldeüberwachung im Kompetenzbereich der Kantone und des Bundes, wobei das Bundesrecht lediglich gewisse Rahmenbedingungen für die kantonale Rechtsetzung festlegte. Mit Erlass des BÜPF im Jahr 2002 wurden die Regelungen erstmals auf Bundesebene vereinheitlicht. 2011 wurden die materiellen Bestimmungen des BÜPF in die Schweizerische Strafprozessordnung überführt und schliesslich mit der Totalrevision des BÜPF auf März 2018 angepasst.[3]

Das Bundesgesetz über das Telephonwesen vom 27. Juni 1889[4] sah noch keine strafprozessualen Überwachungsmöglichkeiten des Telefonverkehrs vor. Anfang des 20. Jahrhunderts waren erstmals Überwachungsmöglichkeiten im Bundesgesetz über den Telegraphen- und Telephonverkehr vom 14. Oktober 1922[5] (TVG) vorgesehen. Einzelheiten waren jedoch dem kantonalen Prozessrecht vorbehalten. Nur wenige Kantone sahen detaillierte Regelungen vor. Der Gesetzgeber hielt zwar den Schutz der Benutzenden von Telefonanlagen vor unbefugter Abhörung und Aufzeichnung fest, erkannte aber gleichzeitig auch, dass die Strafverfolgungsbehörden die Möglichkeit haben müssen, zur Aufklärung von Straftaten das Fernmeldegeheimnis durchbrechen zu können.[6]

Im Rahmen eines Postulatsauftrages wurde am 20. Dezember 1968 das Schweizerische Strafgesetzbuch[7] durch Art. 179bis ff. StGB ergänzt, welche den strafrechtlichen Schutz des persönlichen Geheimbereichs verstärkten, indem das Abhören und Aufnehmen eines fremden, nicht öffentlichen Gesprächs und das Beobachten und Aufnehmen von Tatsachen aus dem Geheimbereich unter Strafe gestellt wurden[8]. So wurden mit der Revision des TVG 1968 die Überwachungsmöglichkeiten insoweit begrenzt, als dass nur noch zur Verfolgung von *Verbrechen* überwacht werden durfte (wobei vor der Revision eine Überwachung zur Verhinderung eines *Verbrechens* oder *Vergehens* zulässig war). Die Bestimmungen im TVG stellten jedoch weiterhin nur Rahmenbedingungen für die kantonale Gesetzgebung zur Zulässigkeit von Überwachungen dar.[9]

---

3 HANSJAKOB, Überwachungsrecht, Rz. 1–2.

4 Vgl. dazu BBl 1889 III 879.

5 Vgl. dazu BBl 1921 III 280.

6 HANSJAKOB, Überwachungsrecht, Rz. 3, 5–7.

7 Vgl. dazu BBl 1968 I 585.

8 BBl 1968 I 585, 590–591.

9 HANSJAKOB, Überwachungsrecht, Rz. 8–9.

1979 wurden ausführliche gesetzliche Regelungen zu den Zulässigkeitsvoraussetzungen einer Überwachung geschaffen: Das Bundesgesetz über den Schutz der persönlichen Geheimsphäre[10] wurde erlassen, wodurch auch weitere Bundesgesetzte, darunter das TVG und das StGB geändert wurden. Die Überwachung wurde auf Vergehen ausgedehnt, während zusätzliche Kriterien, insbesondere die Subsidiarität einer Überwachung, eingeführt wurden. Die Verfügung über eine Überwachungsmassnahme musste des Weiteren von einer richterlichen Aufsichtsbehörde genehmigt werden. Die Kantone mussten innert einer Übergangsfrist von drei Jahren die bundesgesetzlichen Grundzüge übernehmen und ihre Strafprozessordnungen dementsprechend anpassen. Dies führte dazu, dass die kantonalen Regelungen sehr ähnlich wurden.[11]

1991 trat ein Fernmeldegesetz[12] (aFMG) an die Stelle des mittlerweile überholten TVG. 1997 trat bereits ein neues Fernmeldegesetz (FMG) in Kraft, welches die Voraussetzungen der Fernmeldeüberwachung nicht wesentlich anders regelte als das aFMG von 1991. Rechtlich bedeutend waren vor allem zwei Änderungen: Zum einen berücksichtigte das FMG von 1997 die neusten technischen Entwicklungen. Insbesondere hatten die Anbieterinnen von Fernmeldediensten die Informationen in Echtzeit abzuliefern und die Informationspflicht konnte auch die Randdaten umfassen. Zum anderen wurde ihnen eine angemessene Entschädigung für die Überwachungsmassnahmen gesetzlich garantiert.[13]

Auf Anfang 1998 wurde mit der Verordnung vom 1. Dezember 1997 über den Dienst für die Überwachung des Post- und Fernmeldeverkehrs (VÜPF 1997) eine neue Dienststelle in Bern geschaffen. Der Dienst übernahm vor allem das Personal und die technischen Einrichtungen des Rechtsdienstes der Swisscom, welche sich bis anhin mit der Telefonüberwachung beschäftigt hatte. Der Dienst war eine Schaltstelle zwischen den Anbieterinnen von Post- und Fernmeldediensten auf der einen und den Strafverfolgungsbehörden auf der anderen Seite. Im Wesentlichen beschränkten sich die Aufgaben des Dienstes auf die Aufzeichnung des Fernmeldeverkehrs. Am 1. Januar 2002 wurde die Verordnung mit Art. 34 der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 31. Oktober 2001 (aVÜPF) aufgehoben.[14]

Schliesslich wurde 2002 das Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs vom 6. Oktober 2000 (aBÜPF) erlassen, welches den gesamten Bereich der Post- und Fernmeldeüberwachung auf Bundesebene abschliessend regelte. Die kantonalen Bestimmungen traten ausser Kraft. 2011 wurden die materiellen Bestimmungen des aBÜPF mit der Einführung der Schweizeri-

[10] Vgl. dazu BBl 1979 I 574; 1976 I 529.

[11] HANSJAKOB, Überwachungsrecht, Rz. 3.

[12] Vgl. dazu BBl 1988 I 1311.

[13] HANSJAKOB, Überwachungsrecht, Rz. 28–29.

[14] HANSJAKOB, Überwachungsrecht, Rz. 36–38.

schen Strafprozessordnung in jene überführt. Organisatorische Bestimmungen blieben im aBÜPF geregelt.[15]

Bereits 2010 legte der Bundesrat einen Entwurf zur Totalrevision des BÜPF vor[16]. Die Forderung zur Revision kam vor allem von den Strafverfolgungsbehörden und dem Dienst „Überwachung des Post- und Fernmeldeverkehrs“[17], wonach das Gesetz an die rasanten technischen Entwicklungen des Fernmeldeverkehrs anzupassen sei. Es war nur schwer oder gar unmöglich mittels des bis anhin geltenden Gesetzes die Überwachungsmassnahmen bei den Anbieterinnen durchsetzen zu können. Die Totalrevision des BÜPF trat am 18. März 2018 in Kraft. Es ging nicht darum, neue Überwachungsmassnahmen zu schaffen, sondern die gesetzlichen Bestimmungen und Überwachungsmöglichkeiten an den aktuellen technischen Fortschritt anzupassen.[18]

Um zu verstehen, weshalb sich eine Totalrevision förmlich aufgedrängt hatte, wird nachfolgend der technische Fortschritt ab der Jahrhundertwende kurz aufgezeigt: 1998 war es bereits möglich mit dem Mobiltelefon das Internet zu nutzen, doch taten dies nur rund 0,1% der 1,7 Mio. Handynutzenden in der Schweiz. Heute besitzen knapp 12 Mio. der Schweizer ein Mobiltelefon, wobei rund 90% davon das Internet auf dem Handy nutzen, also fast 7’000-mal mehr als noch im Jahr 1998.[19]

Die Kommunikationstechnologie zur SMS wurde bereits 1992 erfunden, so dass 1998 in der Schweiz 100’000 SMS pro Tag versendet wurden. Bis 2012 stieg die Zahl kontinuierlich auf 18 Millionen an und verzeichnete 2015 einen Rückgang auf 5,5 Millionen. Dies lag v.a. daran, dass immer mehr Menschen auf die (damals) billigere Kommunikation über Whatsapp umgestiegen sind. Bereits 2015 wurden 58 Mio. Messages über Whatsapp verschickt; Zuwachsrate immer noch steigend. Die Whatsapp-Kommunikation läuft nicht über das konventionelle Festnetz wie die SMS-Nachricht, sondern über das Internet und die Inhalte der Textnachrichten sind so verschlüsselt, dass sie seit 2016 nicht einmal Whatsapp selbst zu entschlüsseln vermag. Für die Strafverfolgungsbehörden bedeutet dies, dass der Whatsapp-Verkehr nicht mehr durch die herkömmlichen Überwachungstechnologien überwacht werden kann. Dies gilt auch für weitere Kommunikationskanäle via Internet, wie beispielsweise Facebook, Instagram usw. Nicht nur die Kommunikation mittels Textnachrichten hat sich im Vergleich zu 1998 deutlich verändert, sondern auch die Telefonkommunikation: So kann unter anderem mittels

---

15 HANSJAKOB, Überwachungsrecht, Rz. 3.

16 Vgl. dazu den Vorentwurf BÜPF. Am 27. Februar 2013 legte der Bundesrat die Botschaft zum BÜPF vor, vgl. dazu BBl 2013 268.

17 Der Dienst ÜPF ist heute an das EJPD angegliedert und dient als Bindeglied zwischen den Strafverfolgungsbehörden und den Anbieterinnen von Post- und Fernmeldediensten.

18 HANSJAKOB, ZStrR, 430–431; HANSJAKOB, Überwachungsrecht, Rz. 3, 80–81.

19 HANSJAKOB, ZStrR, 431.

Skype und auch Whatsapp, Instagram etc. über das Internet und mittlerweile auch verschlüsselt telefoniert werden.[20]

Des Weiteren bieten die modernen Smartphones Internetdienste an, die über das Telefonieren und Versenden von Textnachrichten hinausgehen: E-Mails können verschickt werden, es kann gesurft, eingekauft, Radio gehört, Fernsehen geschaut oder ein Kalender geführt werden, verschiedene Geräte können miteinander synchronisiert und es kann ein Datenspeicher für Fotos, Videos etc. eingerichtet werden. Es ist also einleuchtend und nachvollziehbar, dass die Überwachungstechnologien von 1998 nicht auf den enormen technischen Wandel eingestellt waren und sich deshalb eine Revision aufgedrängt hatte.[21]

Im Rahmen der BÜPF-Revision fand auch eine Anpassung der Art. 269 ff. StPO statt. So wurden u.a. gesetzliche Grundlagen zum Einsatz besonderer Überwachungstechniken wie Government Ware (sog. GovWare, auch „Staatstrojaner" genannt) oder IMSI-Catcher[22] geschaffen. Der technische Wandel drängte auch eine Totalrevision der VÜPF auf, welche per 1. März 2018 in Kraft trat.[23]

---

20 HANSJAKOB, ZStrR, 431–432.

21 HANSJAKOB, ZStrR, 432.

22 Die IMSI-Catcher werden in der gegenständlichen Arbeit nicht näher behandelt. Beim Einsatz von IMSI-Catcher handelt es sich um den Einsatz besonderer technischer Geräte zur Überwachung i.S.v. Art. 269bis StPO. Gemäss Wikipedia sind IMSI-Catcher „Geräte, mit denen die auf der Mobilfunkkarte eines Mobiltelefons gespeicherte International Mobile Subscriber Identity (IMSI) ausgelesen und der Standort eines Mobiltelefons innerhalb einer Funkzelle eingegrenzt werden kann." Mit dem Einsatz von IMSI-Catcher können Gespräche mitgehört, aufgenommen und eine Person, Sache (bspw. ein Mobiltelefon) oder deren Standort identifiziert werden, vgl. dazu HANSJAKOB, Überwachungsrecht, Rz. 550–554.

23 KLAUS/MATHYS, Rz. 7–8, 44; vgl. dazu Erläuternder Bericht Totalrevision VÜPF.

2. Strafprozessuale Zwangsmassnahmen zur Datenerhebung in der Schweiz

In diesem Kapitel werden die Zwangsmassnahmen der StPO, die der Beweiserhebung im Internet dienen, näher erläutert. Dabei handelt es sich insb. um die Durchsuchung (Art. 246–248 StPO), die Beschlagnahme (Art. 263–268 StPO), die Edition (Art. 265 StPO) und die geheime Überwachung (Art. 269–279 StPO). Zwangsmassnahmen sind in Art. 196 ff. StPO geregelt. Durch das Ergreifen einer Zwangsmassnahme wird in die grundrechtlich geschützten Güter der betroffenen Person eingegriffen.[24] Um den Grundrechtseingriff zu rechtfertigen, muss eine gesetzliche Grundlage für die Massnahme bestehen (Art. 197 Abs. 1 lit. a StPO), ein hinreichender Tatverdacht vorliegen (Abs. 1 lit. b) und das angestrebte Ziel darf nicht durch ein milderes Mittel erreicht werden (Abs. 1 lit. c).

Der einfachste Weg ist es, wenn die betroffene Person die Daten freiwillig und ohne Zwang herausgibt. Die beschuldigte Person kann bspw. im Rahmen einer Einvernahme die Benutzerdaten eines bestimmten Kontos oder Laptops mitteilen. Auch bei einer freiwilligen Datenherausgabe steht ihr das Recht auf Siegelung (Art. 248 StPO) zu.[25] Erfolgt die Herausgabe nicht freiwillig, ist eine entsprechende Zwangsmassnahme zu verfügen.

A. Durchsuchung von Aufzeichnungen (Art. 246–248 StPO)

Die Durchsuchung dient dazu, Aufzeichnungen auf ihre mögliche Beweiseignung hin zu prüfen. Art. 246 StPO gewährt der zuständigen Strafverfolgungsbehörde[26] die Möglichkeit, nach Informationen zu suchen, die der Beschlagnahme (Art. 263 ff. StPO) unterliegen. Unter den Begriff der Aufzeichnungen fallen alle Datenträger, insbesondere auch elektronische Datenverarbeitungs- oder Speicheranlagen (bspw. Festplatten, Mobiltelefone).[27] Die Art. 246–248 StPO regeln die Durchsuchung von Urkunden im weitesten Sinne. Die Bestimmungen erfassen u.a. Schrifturkunden, Fotos, gespeicherte Daten[28], Laptops und iPhones.[29] In den Anwendungsbereich der Durchsuchung und Beschlagnahme fallen demnach gespeicherte E-Mails und Randdaten, die auf Datenverarbeitungsanlagen von Absenderin oder Empfängerin gespeichert sind. Dasselbe gilt für abgerufene E-Mails, die in der Mailbox gespei-

---

[24] Komm StPO-HUG/SCHEIDEGGER, Art. 196 N 1.

[25] BURGERMEISTER, 19; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 246 N 1. BURGERMEISTER spricht sich gegen ein Recht auf Siegelung bei einer freiwilligen Datenherausgabe aus. Die Einwilligung zur Durchsuchung und Auswertung stelle eine Willenserklärung dar, welche einer Siegelung offensichtlich widerspreche.

[26] Die zuständige Strafverfolgungsbehörde ist im Regelfall die Staatsanwaltschaft oder das Gericht, ausnahmsweise bei Dringlichkeit die Polizei (Art. 198 Abs. 1 und Art. 241 Abs. 2 StPO). Dasselbe gilt auch für die Beschlagnahme (Art. 198 Abs. 1 und Art. 263 Abs. 3 StPO). Zum Erlass einer Editionsverfügung sind einzig die Staatsanwaltschaft und die Gerichte, nicht aber die Polizei, befugt. Die Polizei kann lediglich um Herausgabe ersuchen. Vgl. dazu BSK StPO-BOMMER/GOLDSCHMID, Art. 265 N 18, 21.

[27] Komm StPO-KELLER, Art. 246 N 1–6.

[28] In Kap. II./2./B. folgt eine kurze Diskussion darüber, ob elektronische Daten nach den Regeln der Beschlagnahme von körperlichen Gegenständen eingezogen werden können.

[29] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 246 N 1.

chert sind. Dabei können die E-Mails auch auf dem Server der Mailanbieterin[30] gespeichert sein und dort durchsucht werden.[31]

Nach herrschender Lehre stellt Art. 246 StPO keine gesetzliche Grundlage für eine der betroffenen Person *nicht* erkennbare Online-Durchsuchungen dar.[32] Art. 246–248 StPO gelten nur für *offene* Durchsuchungen, d.h. für die betroffene Person erkennbare Zwangsmassnahmen. Bis zur Revision des BÜPF war unklar, nach welchen Regeln eine Online-Durchsuchung stattzufinden hat. Mit Inkrafttreten des revidierten BÜPF wurde Art. 269ter StPO geschaffen, welcher den Einsatz GovWare zur Überwachung des Fernmeldeverkehrs regelt. Die GovWare wäre im Stande, Online-Durchsuchungen zu ermöglichen. Art. 269ter StPO verzichtet jedoch auf die Einführung einer gesetzlichen Grundlage für Online-Durchsuchungen[33].[34]

Vor einer Durchsuchung hat die zuständige Behörde der betroffenen Person die Möglichkeit zu geben, sich vorläufig dazu zu äussern (Art. 247 Abs. 1 StPO). Damit dieses Äusserungsrecht wirksam ausgeübt werden kann, ist die betroffene Person in knapper Form mittels Befehl über den Gegenstand und die gesuchten Aufzeichnungen zu informieren. Des Weiteren ist die Inhaberin der Aufzeichnungen in geeigneter Weise anzuhören und die Aussagen sind zu protokollieren. Ist eine vorgängige Anhörung nicht möglich (bspw. wegen Abwesenheit der Inhaberin) hat eine Siegelung stattzufinden. Das BGer hält eine Siegelung dann für geboten, „wenn die Beschlagnahme ohne Vorankündigung erfolgt und der Besitzer ausserstande ist, sich an Ort und Stelle darüber zu äussern, was für das Verfahren wesentlich sein könnte und was nicht“[35].[36]

Die betroffene Person kann sich mittels Siegelungsantrag gegen die Durchsuchung ihrer Aufzeichnungen zur Wehr setzen. Die Siegelung nach Art. 248 StPO ist ein Rechtsbehelf sui generis. Sie gewährleistet vorläufigen Rechtsschutz dahingehend, dass die Strafverfolgungsbehörde keine Kenntnis vom Inhalt der versiegelten Aufzeichnungen oder Gegenstände erhält. Im Anschluss an den Siegelungsantrag kann die Strafverfolgungsbehörde innert 20 Tagen ein Entsiegelungsgesuch stellen (Art. 248 Abs. 2 StPO). Im Vorverfahren entscheidet das Zwangsmassnahmengericht über die Zulässigkeit der

---

30 Eine Mailanbieterin in diesem Sinne ist eine Internet*zugangs*anbieterin, wobei Analoges auch für Fernmeldedienstanbieterinnen und Anbieterinnen abgeleiteter Kommunikationsdienste gilt, vgl. dazu ausführlich unten, Kap. II./2./D./c., II./3./B./b. und II./3./A./d.

31 Komm StPO-KELLER, Art. 246 N 8; vgl. auch AEPLI, 17–18, 23. Ausschlaggebend ist, dass sich die Daten *ausserhalb* des Kommunikationsverkehrs befinden. Befinden sich die Daten innerhalb des Kommunikationsverkehrs, ist das BÜPF anwendbar. Zur vertieften Behandlung dieser Thematik wird auf Kap. II./3./A./d. und II./3./B./b. verwiesen.

32 Komm StPO-KELLER, Art. 246 N 8; AEPLI, 132; HEIMGARTNER, Beschlagnahme, 41; BSK StPO-THORMANN/BRECHBÜHL, Art. 246 N 5.

33 BBl 2013 2683, 2702, 2772, 2774, 2776, 2778–2779.

34 Komm StPO-HANSJAKOB, Art. 269ter N 4; vgl. auch BSK StPO-THORMANN/BRECHBÜHL, Art. 246 N 5.

35 BGE 111 Ib 50, E. 3.b.

36 BSK StPO-THORMANN/BRECHBÜHL, Art. 247 N 1–8.

Durchsuchung (Art. 248 Abs. 3 lit. a StPO); in allen anderen Fällen das Gericht, bei dem die Sache hängig ist (Art. 248 Abs. 3 lit. b StPO).[37]

B. Beschlagnahme (Art. 263–268 StPO)

Nach Art. 263 Abs. 1 lit. a StPO sind die Strafverfolgungsbehörden befugt, Gegenstände oder Vermögenswerte der betroffenen Person zu beschlagnahmen, wenn sie voraussichtlich als Beweismittel taugen. Folglich handelt es sich bei der Beschlagnahme um eine provisorische strafprozessuale Massnahme zur Beweissicherung und Beweiserhaltung. Der Beschlagnahme unterliegen Gegenstände und Vermögenswerte (Art. 263 Abs. 1 StPO). Als Gegenstand beschlagnahmt werden kann nur, was bereits physisch existiert; namentlich körperliche Sachen, wozu auch elektronische Daten gehören.[38]

Dass elektronische Daten nach den Regeln der Beschlagnahme von körperlichen Gegenstände eingezogen werden können, ist in der Lehre nicht unumstritten. SCHMID argumentiert, dass es aufgrund des Grundsatzes a maiore ad minus auch möglich sein solle, immaterielle Informationen allein zu beschlagnahmen. Könne die ganze technische Speicherungseinrichtung beschlagnahmt werden, sollten auch die einzelnen darauf liegenden (immateriellen) Informationen ein zu edierendes Beweismittel darstellen.[39] Auch HEIMGARTNER und BANGERTER subsumieren Informationen in Form elektrischer Daten unter den Begriff des Gegenstandes i.S.v. Art. 263 Abs. 1 StPO.[40]

AEPLI hingegen vertritt die Meinung, Daten seien nicht körperlicher Natur und könnten somit nicht Objekt der Beschlagnahme bilden. Es könne nur das jeweilige Speichermedium, auf dem die Daten verkörpert seien, beschlagnahmt werden. Würden immaterielle Informationen unter den Begriff der Gegenstände subsumiert, bestünde eine zu weit gefasste Auslegung des Begriffs.[41] Auch RYSER spricht sich gegen eine weite Auslegung der Gegenstände aus und verneint eine Beschlagnahme von Daten.[42] M.E. ist der Ansicht von SCHMID zu folgen und elektronische Daten sollen unabhängig von einem Datenträger nach Art. 263 ff. StPO beschlagnahmt werden können. Das BGer vertritt in BGE 140 IV 181 dieselbe Ansicht[43].

Die Förmlichkeiten der Beschlagnahme werden in Art. 263 Abs. 2 StPO geregelt, wonach die anordnende Strafverfolgungsbehörde einen schriftlichen und kurz begründeten Beschlagnahmebefehl auszu-

---

37 BSK StPO-THORMANN/BRECHBÜHL, Art. 248 N 1, 18, 30.

38 BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 9, 24, 28.

39 SCHMID, 92, 96.

40 HEIMGARTNER, Beschlagnahme, 89; BANGERTER, 248.

41 AEPLI, 56, 59.

42 RYSER, 561.

43 Vgl. dazu BGE 140 IV 181, E. 2.6–2.7.

stellen hat. Der betroffenen Person ist eine Kopie des Beschlagnahmebefehls zuzustellen.[44] Gemäss Art. 264 Abs. 3 i.V.m. Art. 248 StPO erfolgt der Rechtsschutz auf dem Weg der Siegelung.[45]

C. Edition (Art. 265 StPO)

Nach Art. 265 Abs. 1 StPO wird der Inhaber der zu beschaffenden Gegenstände oder Vermögenswerte zur Herausgabe verpflichtet. Von der Pflicht befreit sind die beschuldigte Person, Personen, die ein Zeugnis- und Aussageverweigerungsrecht haben und Unternehmen (Art. 265 Abs. 2 lit. a–c StPO). Die Herausgabepflicht besteht nur für jene Gegenstände und Vermögenswerte, die beschlagnahmt werden sollen (i.V.m. Art. 263 Abs. 1 StPO).[46] Wie bereits oben[47] erklärt, sind Daten beschlagnahmefähige Gegenstände, weshalb sie grundsätzlich auch der Editionspflicht unterliegen. Die herausgabepflichtige Person hat die zu edierenden Daten auf einen Datenträger zu kopieren oder auszudrucken[48].

In Bezug auf das Verhältnismässigkeitsprinzip (Art. 197 Abs. 1 lit. c StPO) stellt die Edition eine der Beschlagnahme gegenüberstehende mildere Massnahme dar, wonach die Beschlagnahme nur als ultima ratio anzuordnen ist. Die Strafverfolgungsbehörden sind verpflichtet, mittels Erlass einer schriftlichen Editionsverfügung (Art. 265 Abs. 3 StPO) dem Verhältnismässigkeitsprinzip Rechnung zu tragen. Die Editionsverfügung ist ein Herausgabebefehl, mit dem die Adressatin zur Herausgabe bestimmter Gegenstände oder Vermögenswerte verpflichtet wird. Die betroffene Person hat auch bei der Edition die Möglichkeit, ein Nichtbestehen der Herausgabepflicht auf dem Weg der Siegelung (Art. 248 StPO) geltend zu machen (Art. 264 Abs. 3 StPO analog).[49]

D. Geheime Überwachung (Art. 269–279 StPO)

Charakteristisch für die Überwachung des Post- und Fernmeldeverkehrs nach Art. 269–279 StPO ist, dass sie *geheim* erfolgt. Die inhaltliche Überwachung nach Art. 269–272 StPO erfolgt *aktiv*, also in *Echtzeit*. Art. 273 StPO regelt die Randdatenerhebung und Teilnehmeridentifikation, welche in *Echtzeit* (Abs. 1) oder *rückwirkend* (Abs. 3) erfolgen können. Dieses Unterkapitel hat die Voraussetzungen und das Verfahren einer strafprozessualen Überwachung zum Gegenstand. Unter d. wird explizit auf die (rückwirkende) Randdatenerhebung und unter e. auf die Überwachung mittels GovWare eingegangen.

---

44 BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263–268 N 18; Art. 266 N 5.

45 BSK StPO-BOMMER/GOLDSCHMID, Art. 264 N 57–58.

46 BSK StPO-BOMMER/GOLDSCHMID, Art. 265 N 1, 4, 9–15.

47 Vgl. dazu oben, Kap. II./2./B.

48 HEIMGARTNER, Beschlagnahme, 63.

49 BSK StPO-BOMMER/GOLDSCHMID, Art. 265 N 1, 16, 29a.

a. Voraussetzungen und Verfahren

Art. 269 StPO regelt die Voraussetzungen für eine zulässige Überwachung des Post- und Fernmeldeverkehrs[50] der beschuldigten Person und u.U. einer Drittperson (Art. 270 lit. b StPO): Eine Überwachungsmassnahme darf nur zur Verfolgung einer Straftat i.S. des Straftatenkatalogs von Abs. 2 angeordnet werden. Es muss ein dringender Tatverdacht auf eine Katalogtat bestehen (Abs. 1 lit. a), die Schwere der Straftat muss die Zwangsmassnahme rechtfertigen und die bisherigen Untersuchungshandlungen müssen erfolglos geblieben sein oder die Ermittlungen wären ohne die Massnahme aussichtslos oder würden unverhältnismässig erschwert (Abs. 1 lit. b und c).[51]

Für eine Überwachung hat die Staatsanwaltschaft eine Anordnungsverfügung zu erlassen, welche sich an den Dienst ÜPF richtet. Innert 24 Stunden ist die Anordnung beim Zwangsmassnahmengericht einzureichen und bedarf einer Genehmigung desselben (Art. 274 Abs. 1 lit. a und Art. 272 Abs. 1 StPO)[52]. Neben der Anordnung ist eine Begründung, welche die Voraussetzungen von Art. 269 StPO und Besonderheiten nach Art. 270 f. StPO nennt, einzureichen (Art. 274 Abs. 1 lit. b StPO).[53] Naturgemäss ist es bei geheimen Überwachungsmassnahmen nicht möglich, der betroffenen Person rechtliches Gehör zu gewähren. Demzufolge bezweckt das Genehmigungsverfahren einen gewissen Ausgleich. Fehlt die Genehmigung, sind die Erkenntnisse aus der Überwachung absolut unverwertbar (Art. 277 i.V.m. Art. 141 Abs. 1 StPO). Wird die Überwachung verspätet genehmigt, bleiben die vor der Genehmigung gewonnenen Erkenntnisse unverwertbar.[54]

Der Dienst ÜPF erhebt die Überwachungsdaten bei der Anbieterin. Er betreibt die EDV-Anlage, welche die Daten von den Anbieterinnen entgegennimmt und den Polizeibehörden zur Verfügung stellt. Mit Einsatz von GovWare hat der Dienst nichts zu tun. Der mit GovWare abgefangener Fernmeldeverkehr wird direkt an die dafür zuständige Strafverfolgungsbehörde (hier die Polizei) weitergeleitet.[55]

---

[50] In der vorliegenden Arbeit wird ausschliesslich auf den Fernmeldeverkehr eingegangen, weshalb auf die parallele Nennung des „Post- und" Fernmeldeverkehr im weiteren Verlauf verzichtet wird. Auf detaillierte Ausführungen zum Postverkehr wird grundsätzlich verzichtet. Der Vollständigkeit halber wird der Postverkehr im Folgenden (Fn. 63) in einer Fussnote kurz umschrieben und in Kap. II./3./A./d. in Bezug auf eine Analogie diskutiert.

[51] BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 269 N 28–47.

[52] Keine Genehmigung ist erforderlich, wenn der Anschlussinhaber und die Zielperson (sofern nicht identisch) der Überwachungsmassnahme zustimmen. Dies ist v.a. bei einer rückwirkenden Randdatenerhebung praktikabel. Gleichwohl sind dem Zwangsmassnahmengericht entsprechende Anordnungen zu unterbreiten, damit es über die Notwendigkeit einer Genehmigung entscheiden kann. Vgl. dazu BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 272 N 6; HANSJAKOB, Überwachungsrecht, Rz. 343–347.

[53] BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 274 N 4–5; HANSJAKOB, Überwachungsrecht, Rz. 930, 933.

[54] BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 272 N 4–5.

[55] HANSJAKOB, Überwachungsrecht, Rz. 1402–1403.

b. Gegenstand und Anwendungsbereich

Charakteristisch für eine Beweiserhebung nach Art. 269 ff. StPO ist erstens, dass es um *geheime* Überwachungsmassnahmen geht, also um Zwangsmassnahmen, die ohne Wissen der beschuldigten Person durchgeführt werden. Die Heimlichkeit gilt als Wesensmerkmal der Echtzeitüberwachung[56]. Zweitens greifen die geheimen Überwachungen in das gesetzlich besonders geschützte *Fernmeldegeheimnis* ein. Ein Eingriff darf folglich nur unter bestimmten Voraussetzungen erfolgen.[57]

Nach herrschender Auffassung ist das *Fernmeldegeheimnis* wesentliches Schutzobjekt von Art. 269–279 StPO; in den Anwendungsbereich des BÜPF fällt also nur das, was auch unter das Fernmeldegeheimnis fällt.[58] Die Überwachung des Fernmeldeverkehrs stellt einen Eingriff in das Fernmeldegeheimnis i.S.v. Art. 43 FMG dar. Art. 13 Abs. 1 BV, Art. 8 Abs. 1 EMRK und Art. 17 Abs. 1 des Internationalen Pakts vom 16. Dezember 1966 über bürgerliche und politische Rechte (IPBPR) garantieren den Schutz des Fernmeldegeheimnisses. Namentlich umfasst das Fernmeldegeheimnis den „Schutz der Korrespondenz wie auch der Beziehung, die mittels [...] Fernmeldediensten aufgenommen werden“[59] und gilt als wesentlicher Inhalt des Schutzes der Privatsphäre. Der Fernmeldeverkehr, welcher den Internetverkehr miteinschliesst, geniesst den Schutz des eben beschriebenen Fernmeldegeheimnisses[60]. Ein Eingriff stellt eine schwere Grundrechtseinschränkung dar, weshalb diese auf einer formell gesetzlichen Grundlage beruhen, im öffentlichen Interesse liegen und verhältnismässig sein muss (vgl. Art. 36 BV und Art. 8 EMRK).[61] Die Art. 269 ff. StPO und das BÜPF schaffen eine gesetzliche Grundlage für die Aufhebung des Fernmeldegeheimnisses.[62]

Das Gesetz findet auf die Überwachung des *Post-*[63] *und Fernmeldeverkehrs* Anwendung. Als Fernmeldeverkehr gilt namentlich die in Art. 2 und 3 lit. c FMG geregelte fernmeldetechnische Übertragung, also das elektrische, magnetische, optische oder andere elektromagnetische Senden und Empfangen von Informationen über Leitungen oder Funk. Der Internetverkehr, welcher den E-Mail-Verkehr einschliesst, gilt als besondere Art des Fernmeldeverkehrs und unterstand bereits nach altem Recht dem BÜPF[64]. Der Fernmeldeverkehr wird in diesem Zusammenhang als *Kommunikationsvor-*

---

56 JEAN-RICHARD-DIT-BRESSEL, 166.

57 HANSJAKOB, Überwachungsrecht, Rz. 298.

58 BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 269 N 21.

59 BBl 2013 2683, 2787.

60 BBl 2013 2683, 2704.

61 BBl 2013 2683, 2787.

62 HANSJAKOB, Überwachungsrecht, Rz. 1327; vgl. auch DERS., Jusletter, Rz. 14.

63 Unter Postverkehr sind alle Tätigkeiten zu verstehen, die unter das Postgesetz (PG) subsumiert werden. Gemäss Art. 1 Abs. 1 lit. a PG sind dies alle gewerbsmässigen Postdienste, mit Ausnahme der Dienstleistungen zum Zahlungsverkehr durch die Schweizerische Post (Art. 1 Abs. 2 BÜPF und Art. 1 Abs. 1 lit. b PG).

64 Auch die Botschaft zum BÜPF qualifiziert den Internetverkehr als (besonderen) Fernmeldeverkehr. So fällt auch die Internettelefonie wie die konventionelle Telefonie unter das Fernmeldegeheimnis. Vgl. dazu BBl

gang verstanden und geniesst nur während dieses Vorgangs den Schutz des Fernmeldegeheimnisses. Vor Beginn bzw. nach Abschluss des Kommunikationsvorgangs gilt das Fernmeldegeheimnis nicht (mehr). Der Beginn und das Ende beurteilen sich danach, wer die Datenherrschaft innehat.[65]

Da sich die Möglichkeiten der Fernmeldekommunikation mittlerweile vervielfacht haben, fallen grundsätzlich alle fernmeldetechnischen Übertragungen, die dem Fernmeldegeheimnis unterliegen, unter Art. 269 ff. StPO. Dies gilt insbesondere auch für die Internetkommunikation via E-Mail, Internettelefonie und Messenger (Skype, Whatsapp, Facebook Messenger, Google etc.). Sind die Kommunikation oder Postings beispielsweise auf Twitter oder Facebook öffentlich zugänglich, fällt die Überwachung dieser Inhalte aber nicht unter Art. 269 ff. StPO. Auf öffentlich zugängliche Posts dürfen die Strafverfolgungsbehörden direkt (auch mithilfe eines fingierten Profils) zugreifen.[66]

Es wird nicht die betroffene Person, sondern ihr Fernmeldeverkehr überwacht. Dazu wird die Überwachung eines *Anschlusses* verfügt (vgl. auch Art. 270 StPO). Gegenstand der Überwachung des Fernmeldeverkehrs sind sodann Informationen über den *Zeitpunkt*, die *Dauer* und den *Standort* der überwachten Person sowie über die *Anschlussdaten* und den *Standort des Gesprächspartners*. Art. 273 StPO spricht diesbezüglich von Teilnehmeridentifikation. Als gängige Bezeichnung für diese Daten haben sich die Begriffe Randdaten oder Verbindungsdaten etabliert[67]. Die zuständige Behörde besitzt auch ein Recht auf *Kenntnisnahme* und *Aufzeichnung des Inhalts* des Fernmeldeverkehrs.[68]

In örtlicher Hinsicht ist die Anwendung des Gesetzes auf die *Schweiz* beschränkt. Es müssen sich nicht beide Gesprächsteilnehmenden in der Schweiz befinden. Erforderlich ist lediglich, dass der Fernmeldeverkehr über die Schweiz abgewickelt wird und die Daten in der Schweiz anfallen und dort ediert werden können. Dies ist bspw. der Fall, wenn im ausländischen Netz mit Schweizer Mobilnummern oder mit ausländischen Mobilnummer in der Schweiz über das Schweizer Netz telefoniert wird.[69]

2013 2683, 2704; HANSJAKOB, Jusletter, Rz. 14; Komm StPO-HANSJAKOB, Art. 270 N 3; BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 269 N 15.

65 BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 269 N 22–23. Wer ab welchem Zeitpunkt die Datenherrschaft besitzt, wird unten in Kap. II./3./A./d. thematisiert.

66 HANSJAKOB, Überwachungsrecht, Rz. 233, 429–430; BBl 2013 2683, 2704.

67 Auf die verschiedenen Datenarten wird unten in Kap. II./3./A./a.–c. näher eingegangen.

68 Die bisherige Praxis zum Gegenstand der Überwachung wurde im Rahmen der BÜPF-Revision nicht weiter diskutiert und unausgesprochen übernommen, vgl. HANSJAKOB, Überwachungsrecht, Rz. 282–283, 287–293.

69 HANSJAKOB, Überwachungsrecht, Rz. 389–391, 397.

c. Persönlicher Geltungsbereich

aa. Ausweitung des persönlichen Geltungsbereichs mit dem neuen BÜPF

Der persönliche Geltungsbereich des BÜPF wird neu in Art. 2 BÜPF (Art. 1 Abs. 2 und Abs. 4 aBÜPF) geregelt. Alle Anbieterinnen, die dem BÜPF unterstellt sind, werden neu als *Mitwirkungspflichtige* bezeichnet.

Gemäss Art. 1 Abs. 2 aBÜPF fielen nach altem Recht alle konzessionierten und meldepflichtigen Anbieterinnen von Post- und Fernmeldedienstleistungen, Internetanbieterinnen und Betreiberinnen von internen Fernmeldenetzen und Hauszentralen in den Geltungsbereich des BÜPF. Gemäss Art. 4 Abs. 1 FMG galt die Meldepflicht nur für Anbieterinnen, die einen Fernmeldedienst erbrachten, wobei Ausnahmen für Fernmeldedienste von geringer technischer und wirtschaftlicher Bedeutung vorgesehen waren (Art. 4 Abs. 2 FMG). Dies hatte zur Folge, dass die nicht meldepflichtigen Anbieterinnen nicht vom Anwendungsbereich des BÜPF erfasst wurden[70].

Unter den Begriff der Internetanbieterinnen fielen nur Internet*zugangs*anbieterinnen[71] (sog. Access Provider) und nicht *reine* Internet*dienst*anbieterinnen (sog. Service Provider). Die Internetanbieterinnen allgemein betreiben keine eigenen Netze, sondern bieten nur Internetdienste an: Die Access Provider bieten ihrer Kundschaft Internetzugang an; die Service Provider hingegen bieten gewisse Dienstleistungen im Internet an. Die nicht meldepflichtigen Service Provider besassen jedoch auch Daten, welche für die Strafverfolgungsbehörden im Rahmen der Kriminalitätsbekämpfung von Interesse waren. Die meldepflichtigen Access Provider waren zwar zur Meldung verpflichtet, hatten aber keinen Zugriff auf Daten, welche im Zusammenhang mit Services von anderen Providern angeboten wurden. Es bestand also sowohl bezüglich der nicht meldepflichtigen Fernmeldedienstanbieterinnen als auch bezüglich der Überwachungspflicht von Service Providern eine gesetzliche Lücke.[72]

Der persönliche Geltungsbereich wurde im revidierten BÜPF erheblich erweitert. Die Erweiterung dient insbesondere zur Behebung der Problematik, dass sich Daten im Zusammenhang mit dem Fernmeldeverkehr regelmässig bei Personen oder Unternehmen befinden, die nach altem Recht nicht dem BÜPF unterstanden und damit nicht überwacht werden konnten. Die dem BÜPF unterstellten Anbieterinnen werden neu in sechs Kategorien von Mitwirkungspflichtigen geregelt (Art. 2 BÜPF): Anbieterinnen von Postdiensten nach dem PG (lit. a); Anbieterinnen von Fernmeldediensten (lit. b); Anbieterinnen von Diensten, die sich auf Fernmeldedienste stützen und eine Einweg- oder Mehrwegkommu-

---

70 HANSJAKOB, Überwachungsrecht, Rz. 1378.

71 Das aVÜPF definierte die Internetanbieterinnen (bzw. Internet*zugangs*anbieterinnen) als Fernmeldedienstanbieterinnen oder einen Teil davon, die in der Öffentlichkeit fernmeldetechnische Übertragungen von Informationen auf der Basis der IP-Technologien (Netzprotokolle im Internet) unter Verwendung von IP-Adressen anboten (Art. 1 Abs. 2 lit. e aVÜPF und Ziff. 1 im Anhang zum aVÜPF), vgl. dazu SCHNEIDER, 183–184. Abgeleitete Internetdienste (wie Facebook und Whatsapp) fielen nach altem Recht weder unter die Fernmeldedienst- noch unter die Internetzugangsanbieterinnen.

72 HANSJAKOB, Überwachungsrecht, Rz. 1377; vgl. auch BBl 2013 2683, 2705–2709.

nikation ermöglichen (Anbieterinnen abgeleiteter Kommunikationsdienste) (lit. c); Betreiberinnen von internen Fernmeldenetzen (lit. d); Personen, die ihren Zugang zu einem öffentlichen Fernmeldenetz Dritten zur Verfügung stellen (lit. e); sowie professionelle Wiederverkäuferinnen von Karten und ähnlichen Mitteln, die den Zugang zu einem öffentlichen Fernmeldenetz ermöglichen (lit. f). Der genaue Umfang der jeweiligen Mitwirkungspflicht ist für jede Kategorie gesondert geregelt.[73] Im weiteren Verlauf des Kapitels werden nur die für diese Arbeit relevanten Anbieterinnenkategorien von Art. 2 lit. b und c BÜPF genauer untersucht.

Neu müssen die Anbieterinnen von Fernmeldediensten nicht mehr konzessions- oder meldepflichtig sein (Art. 4 FMG). Es ist also möglich, dass eine Anbieterin von ihrer Pflicht nach Art. 4 Abs. 2 FMG befreit wird, aber dennoch anderen Pflichten im Bereich der Überwachung des Fernmeldeverkehrs (Art. 26 ff. BÜPF) untersteht. Somit ist bereits eine der oben angesprochenen Lücken des aBÜPF geschlossen worden.[74]

Das FMG definiert, was eine Fernmeldedienstanbieterin[75] i.S.v. Art. 2 lit. b BÜPF ist[76]. Nach der Fernmeldegesetzgebung verpflichten sich Anbieterinnen von Fernmeldediensten für die Öffentlichkeit, Informationen (i.S.v. Art. 3 lit. a FMG) fernmeldetechnisch (i.S.v. Art. 3 lit. c FMG) selber zu befördern oder zu übertragen. Internet*zugangs*anbieterinnen gelten als Fernmeldedienstanbieterinnen i.S. des FMG und folglich auch i.S. des BÜPF. Für andere Internetanbieterinnen, wie beispielsweise reine Dienstanbieterinnen, gilt dies gemäss bundesrätlicher Botschaft nicht[77]. Allenfalls würden diese unter Art. 2 lit. c BÜPF fallen.[78]

Unter die in Buchstabe c aufgeführten Anbieterinnen abgeleiteter Kommunikationsdienste fallen Dienstanbieterinnen, die weder Internetzugangs- noch Fernmeldedienstanbieterinnen sind, jedoch ebenfalls Dienste im Internetverkehr bereitstellen, die nur in Verbindung mit der Tätigkeit einer Fernmeldedienstanbieterin (v.a. einer Internetzugangsanbieterin) angeboten werden können. Ohne die Zusammenarbeit mit einer Anbieterin, die die Daten fernmeldetechnisch überträgt, können die Internetdienstanbieterinnen ihre Dienste im Internet nicht anbieten. Denn sie übertragen oder befördern keine

---

73 BBl 2013 2683, 2694.

74 BBl 2013 2683, 2706–2707.

75 Der im weiteren Verlauf der Arbeit verwendete Begriff der „Fernmeldedienstanbieterin" umfasst die klassischen Fernmeldedienstanbieterinnen (inkl. der bereits nach altem Recht dazugehörenden Internetzugangsanbieterinnen, wie z.B. Swisscom, Bluewin) und (reine) Internetdienstanbieterinnen/Anbieterinnen abgeleiteter Internetdienste, die als Fernmeldedienstanbieterinnen zu qualifizieren sind, vgl. dazu Kap. II./2./D./c./bb.–cc.

76 Vgl. dazu Art. 3 lit. a–c FMG und Art. 2 FDV. Das neue BÜPF übernimmt die bisherige Definition der Fernmeldedienstanbieterinnen aus dem FMG. Beim neuen Geltungsbereich des BÜPF entfällt lediglich die Bedingung der Meldepflicht gemäss FMG beim BAKOM.

77 Die fernmeldetechnische Übertragung von Informationen gemäss Definition im FMG dient als Abgrenzungskriterium zwischen den Fernmeldedienstanbieterinnen (lit. b) und den Anbieterinnen abgeleiteter Kommunikationsdienste (lit. c). Weiter unten, Kap. II./2./D./c./bb., wird jedoch zu sehen sein, dass reine Service Provider u.U. als Fernmeldedienstanbieterinnen qualifiziert werden.

78 BBl 2013 2683, 2707.

Daten selbst. Würden die Anbieterinnen abgeleiteter Kommunikationsdienste die fernmeldetechnische Übertragung von Informationen selbst übernehmen, wären sie wiederum als Fernmeldedienstanbieterinnen zu qualifizieren.[79]

Anbieterinnen abgeleiteter Kommunikationsdienste i.S.v. Art. 2 lit. c BÜPF erlauben eine Einweg- oder Mehrwegkommunikation. Die Einwegkommunikation gestattet das Hochladen von Dokumenten ins Internet (z.B. GoogleDocs, Microsoft Office Live). Die Mehrwegkommunikation erlaubt die Kommunikation zwischen Internetnutzenden (z.B. Facebook). Auch Anbieterinnen von Speicherplatz für E-Mails, verschiedene Arten von Hosting-Providern[80], Chat-Plattformen, Plattformen für den Dokumentenaustausch und Anbieterinnen von Internettelefonie (z.B. Skype) sind unter die gesetzliche Bestimmung zu subsumieren. Nicht erfasst sind Unternehmen, welche die Kommunikation nur erleichtern (bspw. durch reine Verschlüsselungsprogramme), aber selbst keine Kommunikation ermöglichen.[81]

bb. Mitwirkungspflichten von Anbieterinnen abgeleiteter Kommunikationsdienste

Anbieterinnen abgeleiteter Kommunikationsdienste haben gemäss Art. 27 Abs. 1 BÜPF eine Überwachung der Kommunikation, die über die von ihnen angebotenen Dienste erfolgt, durch den Dienst ÜPF oder durch die von diesem beauftragten Personen (namentlich die Polizei) zu *dulden*[82]. Sie müssen Zugang zu ihren Anlagen gewähren und die für die Überwachung notwendigen Auskünfte erteilen. Die Überwachung bezieht sich auf Daten, welche die überwachte Person über die Internetanbieterin versendet oder bei dieser speichert. Gemäss Art. 27 Abs. 2 BÜPF müssen die Anbieterinnen abgeleiteter Kommunikationsdienste die ihnen zur Verfügung stehenden Randdaten des Fernmeldeverkehrs liefern. Die Pflicht von Fernmeldedienstanbieterinnen, Randdaten aufzubewahren (Art. 26 Abs. 5 BÜPF), gilt für Anbieterinnen abgeleiteter Kommunikationsdienste nicht. Dies kann insb. zur Folge haben, dass für die Strafverfolgungsbehörden wichtige Informationen verloren gehen. Bei der Herausgabe von Randdaten durch eine Anbieterin i.S.v. Art. 2 lit. c BÜPF handelt es sich grundsätzlich um eine rückwirkende Überwachung und eine spezielle Form der strafprozessualen Beschlagnahme (Art. 263 ff. StPO). Bei diesem Spezialfall der Edition von der Beschlagnahme unterliegenden Daten ist das

79 BBl 2013 2683, 2707–2708.

80 Z.B. Hosting von Anwendungen oder E-Mail-Diensten (z.B. .gmx), Anbieten von Cloud-Services.

81 BBl 2013 2683, 2708.

82 Die Pflicht von Fernmeldedienstanbieterinnen, Überwachungsdaten in Echtzeit an die zuständige Behörde weiterzuleiten (Art. 26 Abs. 1 BÜPF), trifft die Anbieterinnen abgeleiteter Kommunikationsdienste nicht. Da der Anwendungsbereich von Art. 2 lit. c BÜPF jedoch sehr weit gehe und damit sämtliche Anbieterinnen jeglicher internetbasierter Dienste dem BÜPF unterstelle, erscheint es für einige Autoren sachgerecht, dass die jeweiligen Mitwirkungspflichten eingeschränkt werden, vgl. dazu KLAUS/MATHYS, Rz. 21–22.

Verfahren nach Art. 273 StPO zu beachten. Demnach bedarf es zwingend einer Genehmigung des Zwangsmassnahmengerichts (Art. 273 Abs. 2 StPO).[83]

Gemäss Art. 27 Abs. 3 BÜPF kann der Bundesrat gewisse Anbieterinnen abgeleiteter Kommunikationsdienste von grosser wirtschaftlicher Bedeutung oder einem grossen Benutzerkreis allen oder einem Teil der in Art. 26 BÜPF genannten Pflichten von Fernmeldedienstanbieterinnen unterstellen[84]. Art. 22 und 52 VÜPF legen bestimmte Grenzen fest, nach denen einer Anbieterin abgeleiteter Kommunikationsdienste weitergehende Auskunftspflichten (Art. 22 VÜPF) oder weitergehende Überwachungspflichten (Art. 52 VÜPF) auferlegt werden können. Solche Anbieterinnen müssen sich innert drei Monaten beim Dienst ÜPF melden, welcher dann über das Auferlegen von weitergehenden Pflichten entscheidet.[85]

Die Botschaft zum BÜPF betont die Zulässigkeit und Notwendigkeit einer solchen Delegationsvorschrift. Der Ansicht des Bundesrats und einer entsprechenden Delegationsnorm ist m.E. nichts entgegenzusetzen. Schliesslich betrifft die Vorschrift einen technischen Bereich, der sich rasant entwickelt. Deshalb muss sich das anwendbare Gesetz rasch an die neuen Bedürfnisse im Bereich der Überwachung anpassen können. Zulässig ist die Norm, weil sie einschränkende Kriterien enthält, die sich konkreter gestalten lassen. Schliesslich können nur die Pflichten derjenigen Anbieterinnen abgeleiteter Kommunikationsdienste ausgeweitet werden, die Dienstleistungen von grosser wirtschaftlicher Bedeutung oder für eine grosse Benutzerschaft anbieten. Es ist insb. vorgesehen, die Bestimmung auf Anbieterinnen von grossen E-Mail-Diensten anzuwenden.[86]

---

83 BBl 2013 2683, 2742–2744; HANSJAKOB, Überwachungsrecht, Rz. 1669, 1686–1688.

84 Art. 27 Abs. 3 BÜPF ist das Korrelat zu Art. 26 Abs. 6 BÜPF, welcher den Bundesrat ermächtigt, Fernmeldedienstanbieterinnen von bestimmten gesetzlichen Pflichten zu befreien, insb. wenn sie Dienstleistungen von geringer wirtschaftlicher Bedeutung oder im Forschung- und Bildungsbereich anbieten (Art. 51 VÜPF „FDA mit reduzierten Überwachungspflichten").

Fernmeldedienstanbieterinnen sind verpflichtet, dem Dienst den Inhalt und die Randdaten des Fernmeldeverkehrs der überwachten Person zu liefern (Art. 26 Abs. 1 lit. a und b BÜPF). Gemäss Abs. 2 lit. a BÜPF sind sie verpflichtet, die für die Durchführung der Überwachung notwendigen (technischen) Informationen zu liefern. Nach Abs. 2 lit. b BÜPF müssen sie die Überwachung dulden, wenn sie wegen ihrer geringen wirtschaftlichen Bedeutung (Art. 26 Abs. 6 BÜPF) die Überwachung nicht selbst durchführen müssen. Insb. haben sie Zugang zu ihren Anlagen zu gewähren. Des Weiteren müssen sie die von ihnen angebrachte Verschlüsselung entfernen (Abs. 2 lit. c BÜPF). Sie können nach Art. 26 Abs. 4 BÜPF zur Echtzeitüberwachung und rückwirkenden Überwachung verpflichtet werden. Sie sind auch verpflichtet, die Randdaten des Fernmeldeverkehrs während sechs Monaten aufzubewahren (Art. 26 Abs. 5 BÜPF). Diese Pflicht gilt auch für jene Fernmeldedienstanbieterinnen, die gemäss Art. 26 Abs. 6 BÜPF nicht verpflichtet sind, aktive Überwachungen selbst vorzunehmen. Auch nach Art. 26 Abs. 6 BÜPF befreite Anbieterinnen sind verpflichtet, den Pflichten nach Art. 26 Abs. 2 BÜPF nachzukommen. Sie sind auch nicht von der Pflicht befreit, die ihnen zur Verfügung stehenden Randdaten zu liefern. Vgl. dazu HANSJAKOB, Überwachungsrecht, Rz. 1669–1681.

85 BBl 2013 2683, 2744–2745; DIENST ÜPF, Merkblatt „FDA - AAKD", 2; HANSJAKOB, Überwachungsrecht, Rz. 1689–1691; KLAUS/MATHYS, Rz. 22.

86 BBl 2013 2683, 2744.

cc. Abgrenzung zwischen Fernmeldedienstanbieterinnen und Anbieterinnen abgeleiteter Kommunikationsdienste

Der Dienst ÜPF hat Ende April 2018 ein Merkblatt veröffentlicht, welches die Unklarheiten bzgl. der Abgrenzung zwischen Fernmeldedienstanbieterinnen und Anbieterinnen abgeleiteter Kommunikationsdienste beseitigen soll. Im Folgenden wird die Praxis des Dienstes ÜPF vorgestellt.

Gemäss Art. 3 lit. b FMG ist (wie bereits oben in Kap. II./2./D./c./aa. erwähnt) unter einem Fernmeldedienst die *fernmeldetechnische Übertragung von Informationen für Dritte* zu verstehen. Der Begriff wurde lange mit den Fernmeldenetzen und den Netzbetreiberinnen in Verbindung gebracht. Auch die Botschaft 2013 orientierte sich noch an dieser Ansicht[87]. Gemäss dem Dienst ist dies inzwischen überholt. Mittlerweile hat sich eine Vielzahl von Internetdiensten (sog. Over-the-top Dienste bzw. OTT-Dienste[88]) etabliert, welche mit den klassischen Fernmeldediensten konkurrieren. OTT-Dienste werden zwar unabhängig von den Betreiberinnen von Fernmeldenetzten (bzw. Zugangsanbieterinnen) erbracht, sind jedoch mit den klassischen von der Netzbetreiberin erbrachten Fernmeldediensten funktional gleichzusetzen. So können auch reine Service Provider ohne ein eigenes Netz zu den Fernmeldedienstanbieterinnen gehören. Gemäss dem Merkblatt des Dienstes gehören bspw. Kommunikationsdienste für die Übertragung von Sprache, Text, Bild, Ton, Video, E-Mail, Messaging und Kommunikationsdienste in Social Media zu den OTT-Diensten, die als Fernmeldedienste zu qualifizieren sind. Dies gilt unabhängig davon, ob der Zugang zu den Diensten über eine App, eine Internetseite oder ein Fest- bzw. Mobilfunknetz erfolgt.[89]

Welche Dienste als Anbieterinnen abgeleiteter Kommunikationsdienste (Art. 2 lit. c BÜPF) zu qualifizieren sind, wird folgendermassen konkretisiert: Online-Speicherdienste (Cloud Storage, File Hosting, Share Hoster, Online Storage, File Sharing), Dienste zum Hochladen und Teilen von Inhalten (z.B. Videos), Cloud Computing, Online-Marktplätze (wobei die Kommunikationsdienste innerhalb der Online-Marktplätze als Fernmeldedienste gelten), Social Media (auch hier gelten die Kommunikationsdienste innerhalb der Social Media als Fernmeldedienste) und Lokalisierungsdienste.[90]

Gemäss Merkblatt wird bspw. Facebook als Social Media zu den Anbieterinnen abgeleiteter Kommunikationsdienste gehören; der in Facebook integrierte Messanger jedoch zu den Fernmeldediensten. Facebook ist eine Anbieterin, die sowohl Fernmeldedienste als auch abgeleitete Kommunikations-

87 Vgl. dazu ausführlich BBl 2013 2683, 2707.

88 Dazu gehören bspw. Facebook und Whatsapp.

89 DIENST ÜPF, Merkblatt „FDA - AAKD“, 3–4; vgl. auch BAKOM, Leitfaden, 4. Auch die Botschaft vom 6. September 2017 zur Revision des FMG betrachtet die OTT-Dienste als Fernmeldedienste i.S.v. Art. 3 lit. b FMG, vgl. BBl 2017 6559, 6660.

90 DIENST ÜPF, Merkblatt „FDA - AAKD“, 5.

dienste erbringt[91]. Die entsprechende Kategorisierung im Einzelfall wird durch den Dienst ÜPF vorgenommen[92]. Massgebend für die Zuordnung ist insbesondere die wirtschaftliche Bedeutung der Anbieterin und der beiden von ihr erbrachten Dienste. In der Regel wird eine Anbieterin, die sowohl abgeleitete Kommunikations- als auch zu einem wesentlichen Teil Fernmeldedienste erbringt, als Fernmeldedienstanbieterin (Art. 2 lit. b BÜPF) qualifiziert.[93] Facebook als OTT-Dienst wäre wohl vollumfänglich als Fernmeldedienstanbieterin zu qualifizieren.

Die durch den Dienst ÜPF vorgenommene Kategorisierung der Fernmeldedienste und der abgeleiteten Kommunikationsdienste stösst im gesellschaftlichen Diskurs auf Kritik. SCHLAURI spricht von einer „rechtswidrigen Uminterpretation des Begriffs der Fernmeldedienste". Die Neuinterpretation widerspreche deutlich den Absichten des Gesetzgebers beim Erlass des neuen BÜPF. Das Gesetz weise die Kompetenz, Anbieterinnen abgeleiteter Kommunikationsdienste den Überwachungspflichten einer Fernmeldedienstanbieterin zu unterstellen, klar dem Bundesrat zu (vgl. dazu Art. 27 Abs. 3 BÜPF), wofür strenge Kriterien (nämlich jene der grossen wirtschaftlichen Bedeutung und der grossen Anzahl an Nutzenden) gelten würden. Würde der Begriff der Fernmeldedienstanbieterinnen nun soweit ausgeweitet, dass die OTT-Dienste (wie es der Dienst ÜPF beschreibt) darunterfallen würden, stelle dies eine Untergrabung der Kompetenzordnung des BÜPF dar.[94] Dem wird entgegengehalten, dass jene Anbieterinnen abgeleiteter Kommunikationsdienste, welche den Überwachungspflichten einer Fernmeldedienstanbieterin unterstellt werden, nicht als Fernmeldedienstanbieterin, sondern als „AAKD mit weitergehenden Überwachungspflichten" (i.S.v. Art. 52 VÜPF) zu qualifizieren sind. Also sind sie immer noch Anbieterinnen abgeleiteter Kommunikationsdienste nach Art. 2 lit. c BÜPF. Hier greift der Dienst ÜPF nicht vor und der Bundesrat kann die Aufgabe der Unterstellung nach Art. 27 Abs. 3 BÜPF weiterhin ausüben. Bei den als Fernmeldedienst geltenden OTT-Diensten handelt es sich folglich um eine andere, nicht die Delegationsnorm tangierende Praxis.

Meines Erachtens ist das Vorgehen des Dienstes ÜPF rechtmässig und sachgerecht. Es erscheint sinnvoll, jene OTT-Dienste, welche den klassischen Fernmeldediensten gleichgestellt sind, auch als solche zu behandeln. Wie der Dienst ÜPF in seinem Merkblatt zu Recht erklärt, stellen die weit verbreiteten internetbasierten Dienste eine erhebliche Konkurrenz für die klassischen Fernmeldedienste dar[95]. Des

---

91 Agiert eine Unternehmung gleichzeitig als Zugangs- und reine Dienstanbieterin, ist sie sowohl als Anbieterin i.S.v. Art. 2 lit. b als auch als Anbieterin i.S.v. Art. 2 lit. c BÜPF zu qualifizieren. Folglich treffen die Unternehmung je nach Tätigkeit unterschiedliche Überwachungspflichten. Vgl. dazu BBl 2013 2683, 2708.

92 DIENST ÜPF, Merkblatt „FDA - AAKD", 7.

93 DIENST ÜPF, Merkblatt „FDA - AAKD", 7.

94 SCHLAURI, Definition des Fernmeldedienstes; vgl. auch SCHLAURI, Überwachungsgesetz BÜPF. Auch FLACH äussert im Rahmen einer Interpellation kritische Fragen bzgl. der vom Dienst ÜPF aufgestellten Abgrenzung zwischen den Anbieterinnen. Unter anderem fragt er sich, ob die Praxis des Dienstes ÜPF mit jener in der Botschaft zum BÜPF vereinbar sei und ob der Bundesrat das Vorgehen des Dienstes für rechtmässig halte. Vgl. dazu die Interpellation FLACH.

95 DIENST ÜPF, Merkblatt „FDA - AAKD", 3. Der Dienst orientiert sich bei seinem Vorgehen an der Praxis des BAKOM, vgl. dazu BAKOM, Leitfaden.

Weiteren ist zu erwähnen, dass nicht alle OTT-Dienste als Fernmeldedienste zu qualifizieren sind. Es scheint auch, als habe der Bundesrat der Praxis des Dienstes (und des BAKOM) zugestimmt, indem die Botschaft zur Revision des FMG die OTT-Dienste definitionsgemäss unter die Fernmeldedienste subsumiert[96]. Meiner Ansicht nach ist es also durchaus geboten, bestimmte internetbasierte Dienste den Fernmeldediensten gleichzusetzen, zumal ihre Bedeutungen im Bereich des Kommunikationsaustauschs weitestgehend deckungsgleich sind.

d. Randdatenerhebung (Art. 273 StPO)

Art. 273 StPO gibt der Strafverfolgungsbehörde die Möglichkeit, Randdaten bei der Anbieterin zu erheben. Die Randdaten können *aktiv* (Abs. 1) oder sechs Monate[97] *rückwirkend*[98] erhoben werden (Abs. 3). Durch den Verweis auf Art. 8 lit. b und Art. 19 Abs. 1 lit. b BÜPF wird geregelt, worum es sich bei den Randdaten im Sinne dieses Artikels handelt. Demnach handelt es sich um „Daten, aus denen hervorgeht, mit wem, wann, wie lange und von wo aus die überwachte Person Verbindung hat oder gehabt hat, sowie die technischen Merkmale der entsprechenden Verbindung".

Bei Randdaten des Internetverkehrs handelt es sich v.a. um Informationen darüber, wann und an wen von einer bestimmten E-Mail-Adresse E-Mails verschickt bzw. wann und von wem E-Mails erhalten und ob und wann diese zugestellt wurden. Diese Randdaten sind regelmässig beim Provider[99] vorhanden und können auch von diesem verlangt werden.[100]

Bei der Randdatenerhebung dürfen nur Randdaten und *nicht* auch Kommunikations*inhalte* erhoben werden. Dies gilt insb. auch für die rückwirkende Erhebung nach Art. 273 Abs. 3 StPO. Kommunikationsinhalte dürften auch dann nicht rückwirkend ediert werden, wenn sie bei der Fernmeldedienstan-

---

96 Vgl. dazu die Ausführungen in BBl 2017 6559, insb. 6659–6660.

97 Der Bundesrat wollte mittels Revision des BÜPF die Frist von sechs auf zwölf Monate verlängern. Der Gesetzgeber hat sich nun aber entschieden, die Frist bei sechs Monaten zu belassen. Es hat sich bereits unter altem Recht die Frage gestellt, ob es allenfalls zulässig gewesen sei, die sechsmonatige Frist zu verlängern. In BGE 139 IV 98 hat das BGer festgestellt, dass eine Überwachung für einen längeren Zeitraum zulässig sei, wenn „besondere Gründe" dies rechtfertigen würden. Im kurz darauffolgenden BGE 139 IV 195 sprach sich das BGer aber dafür aus, dass die sechsmonatige Frist strikte einzuhalten sei. Gemäss HANSJAKOB ist das BGer nun trotzdem frei (insb. aufgrund des Umstandes, dass die Frist nicht auf zwölf Monate verlängert wurde), die Frist mittels Auslegung und unter bestimmten Voraussetzungen zu verlängern, vgl. dazu HANSJAKOB, Überwachungsrecht, Rz. 917.

98 Auf die qualifizierte rückwirkende Randdatenerhebung („Antennensuchlauf"), welche im Gesetz nicht explizit geregelt ist, wird in der vorliegenden Arbeit nicht eingegangen.

99 Unter dem Begriff „Provider" sind jegliche Internetdienstanbieterinnen wie Access und Service Provider zu verstehen, vgl. dazu auch die Definition einer „Internetdienstanbieterin" auf Wikipedia. Dem gesetzlichen Terminus folgend werden in der gegenständlichen Arbeit unter den Begriff „Provider" neben Internetzugangs- insb. auch reine Internetdienstanbieterinnen subsumiert, unabhängig davon, ob sie Fernmeldedienstanbieterinnen (Art. 2 lit. b BÜPF) oder Anbieterinnen abgeleiteter Kommunikationsdienste (Art. 2 lit. c BÜPF) sind.

100 HANSJAKOB, Überwachungsrecht, Rz. 860.

bieterin vorhanden bzw. gespeichert sind[101]. Die Betreffzeile (einer E-Mail) gehört allerdings zu den Randdaten, auch wenn sie Hinweise auf den Inhalt liefern kann.[102] Art. 273 StPO ist nur anwendbar, soweit sich die Daten ausschliesslich über die Anbieterin erheben lassen. Sind die Daten bspw. auf einem Mobiltelefon gespeichert, sind die Vorschriften über die Edition/Beschlagnahme anwendbar.[103]

Eine Randdatenerhebung ist dann zulässig, wenn sie zur Aufklärung eines Verbrechens oder Vergehens oder des Missbrauchs einer Fernmeldeanlage (Art. 179^{septies} StGB) erforderlich ist; ein Verdacht auf eine Katalogtat wird nicht vorausgesetzt. Die gesetzlichen Anforderungen an die Randdatenerhebung sind deshalb tiefer als an die Überwachung von Inhalten, weil sie einen weitaus geringeren Eingriff in das Fernmeldegeheimnis darstellt[104]. Nichtsdestotrotz wird eine Genehmigung durch das Zwangsmassnahmengericht vorausgesetzt (Art. 273 Abs. 2 StPO).

Nach Art. 273 Abs. 3 StPO können die Randdaten der letzten sechs Monate rückwirkend ediert werden (rückwirkende Überwachung). Deshalb statuiert Art. 26 Abs. 5 BÜPF die Pflicht der Fernmeldedienstanbieterinnen, Daten zur Teilnehmeridentifikation und Verkehrs- und Rechnungsdaten während sechs Monaten aufzubewahren. Diese Pflicht gilt (wie bereits erwähnt[105]) nicht für Anbieterinnen abgeleiteter Kommunikationsdienste nach Art. 2 lit. c BÜPF. Diese müssen lediglich die bei ihnen vorhandenen Angaben liefern.[106] Unter Berücksichtigung der aktuellen Praxis des Dienstes ÜPF und des BAKOM müssten jene Anbieterinnen abgeleiteter Internetdienste, welche als Fernmeldedienste klassifiziert werden, der Pflicht von Art. 26 Abs. 5 BÜPF nachkommen und die Randdaten und Daten zur Teilnehmeridentifikation der letzten sechs Monate abspeichern.

e. Einsatz von GovWare (Art. 269ter StPO)

Damit die für eine Überwachung benötigten Daten erhoben und eingesehen werden können, wird vorausgesetzt, dass die Anbieterin über unverschlüsselte Daten des Fernmeldeverkehrs verfügt. Bei einer Kommunikation mit End-zu-End-Verschlüsselung werden die Text- und Sprachmitteilungen auf dem Gerät der Absenderin jedoch verschlüsselt und erst auf dem Gerät des Empfängers wieder entschlüs-

[101] Komm StPO-HANSJAKOB, Art. 273 N 9; FORSTER, 49; BERTSCHMANN, 358–359. Der bereits *abgerufene* Inhalt der Kommunikation kann nach Art. 263 ff. StPO ediert werden. Dabei handelt es sich weder um eine (aktive) Echtzeitüberwachung noch um eine rückwirkende Inhaltsüberwachung. Der Inhalt des Kommunikationsverkehrs wird von den Anbieterinnen nicht im Sinne einer Vorratsdatenspeicherung aufgezeichnet, weshalb eine rückwirkende Inhaltüberwachung mangels entsprechender Daten nicht in Betracht fällt. Vgl. dazu BERTSCHMANN, 358. Diese Problematik wird weiter unten in Kap. II./3./B./b. vertieft behandelt.

[102] HANSJAKOB, Überwachungsrecht, Rz. 858.

[103] Vgl. u.a. auch AEPLI, 23; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 273 N 7.

[104] BGE 137 IV 340, E. 6.4–6.5, 6.7.

[105] Vgl. Kap. II./2./D./c./bb.

[106] HANSJAKOB, Überwachungsrecht, Rz. 912–917.

selt[107]. Dies hat zur Konsequenz, dass weder die Anbieterin, welche selbst keine Datennetze betreibt, noch der Provider des Kunden den Gesprächsverkehr unverschlüsselt an die Strafverfolgungsbehörden liefern kann. Werden also verschlüsselte Informationen geliefert, läuft eine konventionelle Überwachung ins Leere. Hierzu wird eine der Strafverfolgungsbehörde bekannte Verschlüsselung angebracht. Der auf diese Weise verschlüsselte Verkehr wird an die Strafverfolgungsbehörden weitergeleitet, wo er dann entschlüsselt werden kann. Die Strafverfolgungsbehörden müssen den Gesprächsverkehr direkt auf dem Computer bzw. Mobiltelefon der überwachten Person abgreifen, und zwar noch *bevor* er verschlüsselt wird. Die Revision des BÜPF setzte sich zum Ziel, mit dem Art. 269ter StPO eine saubere gesetzliche Grundlage für den Einsatz solcher Technologien zu schaffen. Zuständig für die Installation der GovWare auf dem überwachten Gerät ist nicht der Dienst ÜPF, sondern die Polizei. Die zuständige Polizeibehörde nimmt dann auch den ausgeleiteten Gesprächsverkehr entgegen und zeichnet ihn auf.[108]

Eine Alternative zum Einsatz von GovWare ist die Verpflichtung der Anbieterinnen verschlüsselter Leistungen, den Schlüssel zur Entschlüsselung der Daten zu liefern (Art. 26 Abs. 2 lit. c BÜPF). Die Durchsetzung einer solchen Verpflichtung scheitert jedoch oftmals daran, dass viele der auf dem Markt tätigen Anbieterinnen ihren Sitz im Ausland haben.[109] Hinzu kommt, dass das Informatikprogramm ausserordentlich aufwendig und mit extrem hohen Kosten verbunden ist, was den Anwendungsbereich der GovWare zusätzlich einschränkt[110].

Durch den Einsatz von GovWare dürfen nur der Inhalt der Kommunikation und die Randdaten des Fernmeldeverkehrs abgefangen werden. Art. 26 BÜPF definiert, um welche Daten es sich dabei konkret handelt. Dazu gehören der normale Telefonverkehr über Internet, der E-Mail-Verkehr, Kommunikationsverkehr über SMS und andere Messaging-Dienste. Die GovWare-Technologie wäre auch in der Lage, auf private Informationen, wie bspw. Fotos oder Videos zuzugreifen oder Online-Durchsuchungen durchzuführen. Art. 269ter StPO schliesst jedoch diese beiden Möglichkeiten aus. Es

---

[107] Das Aufkommen der Internettelefonie über *Skype* war grundlegend für den Bedarf eines solchen Informatikprogramms. Mittlerweile ist die verschlüsselte Kommunikation insb. auch bei *Whatsapp* und *Viber* verbreitet. Eine Anbieterin von solchen Programmen liefert nur die Software, welche es den Benutzenden ermöglicht, mit anderen Personen, welche die gleiche Software nutzen, über Internet zu telefonieren. Die Programmanbieterin verfügt allerdings nicht über den Gesprächsverkehr ihrer Kunden, weil sie nur das Programm und nicht auch die Infrastruktur zur Gesprächsübertragung zu Verfügung stellt. Um der Datensicherheit Gewähr zu leisten, benutzen solche Programme eine End-zu-End-Verschlüsselung. Des Weiteren laufen solche Programme über Peer-to-Peer-Systeme (P2P-System), wobei die Informationen aufgeteilt und in kleineren Datenpaketen verschickt werden. Die Daten werden erst bei der Empfängerin wieder zusammengesetzt. Weder der Provider des Absenders noch jener der Empfängerin ist diesbezüglich in der Lage, die einzelnen Datenpakete zu identifizieren und zusammenzusetzen. Vgl. ausführlich HANSJAKOB, Jusletter, Rz. 6–7; DERS., GovWare, 642.

[108] HANSJAKOB, Überwachungsrecht, Rz. 574–576, 587; DERS., Jusletter, Rz. 8–9; DERS., GovWare, 648.

[109] BBl 2013 2683, 2777; HANSJAKOB, GovWare, 643.

[110] Vgl. dazu HANSJAKOB, Überwachungsrecht, Rz. 584–585; DERS., Jusletter IT, Rz. 10.

dürfen also ausschliesslich Daten geliefert werden, welche auch durch eine normale Echtzeitüberwachung erhältlich sind.[111]

Der Einsatz von GovWare ist an die Voraussetzungen von Art. 269 Abs. 1 und 3 StPO geknüpft (Art. 269ter Abs. 1 lit. a StPO): Es muss ein dringender Tatverdacht vorliegen, die Massnahme muss verhältnismässig sein und das Subsidiaritätsprinzip muss eingehalten werden. Die Hürden an die Verhältnismässigkeit sind etwas höher als bei normalen Überwachungen, weil einerseits in das Computersystem der überwachten Person eingedrungen und andererseits ein Eindringen in nicht öffentliche Räume allenfalls notwendig wird, um das Programm in das Zielsystem einschleusen zu können. Bei der verfolgten Straftat muss es sich auch um eine Katalogtat nach Art. 286 Abs. 2 StPO handeln (Art. 269ter Abs. 1 lit. b StPO). Zudem bedarf es einer doppelten Subsidiarität (Art. 269ter Abs. 1 lit. c StPO), wonach GovWare nur dann eingesetzt werden darf, wenn die bisherigen Überwachungsmassnahmen erfolglos geblieben sind.[112]

[111] BBl 2013 2683, 2772; HANSJAKOB, Überwachungsrecht, Rz. 591, 622.

[112] HANSJAKOB, GovWare, 646–648; DERS., Überwachungsrecht, Rz. 629–630, 634.

3. Zur Abgrenzung zwischen Überwachung und Edition bzw. Beschlagnahme

A. Unterscheidung zwischen Bestandes- und Verbindungsdaten

a. Bestandesdaten

Die Bestandesdatenauskunft ist in Art. 21 BÜPF (Art. 14 aBÜPF) geregelt und gibt Auskunft über registrierte Fernmeldeanschlüsse. Die Bestandesdaten umfassen Daten über den Inhalt einer Vertragsbeziehung des Kunden mit einer Fernmeldedienstanbieterin, wer Abonnent eines bestimmten Anschlusses oder Postfachs ist oder wer eine bestimmte Internetadresse benutzt.[113] Die Auskünfte nach Art. 21 BÜPF unterliegen nicht dem Fernmeldegeheimnis.[114] Bei der Auskunft über Bestandesdaten haben die Strafverfolgungsbehörden bereits Kenntnis über die (Internet-)Anschlüsse. Ihnen wird lediglich die Inhaberschaft dieses Anschlusses, bzw. wer bei der Anbieterin unter diesem Anschluss registriert ist, mitgeteilt.[115] Bestandesdaten sind nach den Regeln der Edition/Beschlagnahme (Art. 263 ff. StPO) zu edieren. Die Bestandesdaten sind zum Teil über den Dienst erhältlich und können vorerst ohne Wissen der betroffenen Person erhoben werden. Eine Bewilligung des Zwangsmassnahmengerichts ist nicht erforderlich.[116]

Wird eine Straftat über das Internet begangen, findet Art. 22 BÜPF (Art. 14 Abs. 4a BÜPF) Anwendung. Die Internetanbieterinnen sind verpflichtet, alle (auch rückwirkende) Angaben zu machen, die die Identifikation des Urhebers ermöglichen. Dabei geht es nicht um die Edition von Randdaten (wer wann mit wem kommuniziert hat[117]), sondern um die Frage, wer einen *bestimmten Anschluss benutzt* hat (bzw. die Edition von Bestandesdaten). Es sollen die Regelungen über die Edition von Bestandesdaten gelten. Entsprechende Bestandesdaten müssen zehn Jahre rückwirkend ediert werden.[118]

Das Ziel von Art. 22 BÜPF ist, dass Personen, die über das Internet kommunizieren, gleichermassen identifizierbar sein sollen wie diejenigen, die es über das Telefon tun. Zur Identifizierung beim Telefonverkehr genügt ein Blick in die Abonnementdaten, weil der Benutzer in der Regel über längere Zeit mit demselben Gerät und der gleichen Telefonnummer telefoniert. Ein bestimmter Internetverkehr kann, auf die gleiche Weise wie ein bestimmter Telefonanruf einer Rufnummer, einer bestimmten IP-Adresse zugeordnet werden. Anders als die Telefonnummer wird die IP-Adresse allerdings von der Anbieterin *dynamisch* an die Kunden zugeteilt, weil sie regelmässig nicht über genügend IP-Adressen für jeden einzelnen Internetverkehr verfügt. Das heisst, dass jedem Kunden bei jedem Internetverkehr

---

[113] HANSJAKOB, Überwachungsrecht, Rz. 300.

[114] BBl 2013 2683, 2733.

[115] FORSTER, 620.

[116] Komm StPO-HANSJAKOB, Art. 273 N 7.

[117] Vgl. die Erläuterungen zu den Randdaten, Kap. II./3./A./b.

[118] Komm StPO-HANSJAKOB, Art. 273 N 8.; HANSJAKOB, Überwachungsrecht, Rz. 1637–1638; FORSTER, 621; BGE 141 IV 108, E. 6.2.

eine neue IP-Adresse zugeteilt wird. Die Anbieterinnen müssen deshalb über eine Datenbank verfügen, die Informationen darüber enthält, wer zu welchem Zeitpunkt welche IP-Adresse genutzt hat.[119]

b. Verbindungs- bzw. Randdaten

Die Erhebung von sog. Verbindungsdaten[120] dient der Teilnehmeridentifikation i.S.v. Art. 273 Abs. 1 StPO. Teilnehmende einer bestimmten Fernmeldeverbindung werden über eine gewisse Zeit hinweg identifiziert. Dies erfolgt dadurch, dass Verkehrsdaten (und keine Kommunikationsinhalte) erhoben werden und gestützt auf diese eine Identifikation der Teilnehmenden und Anschlüsse stattfindet[121]. Bei der Erhebung von Randdaten geht es insbesondere darum, *wer wann mit wem* kommuniziert hat[122]. Dabei sind den Strafverfolgungsbehörden bloss strafbare Kommunikationsaktivitäten (und keine bestimmten Fernmelde- oder Internetanschlüsse) bekannt.[123]

Welche Informationen konkret unter den Begriff der Randdaten fallen, wird in den Art. 54 ff. VÜPF definiert. Beim E-Mail-Verkehr sind dies beispielsweise das Datum, die Uhrzeit, die Art des Ereignisses, die Teilnehmeridentifikatoren, die Sender- und Empfängeradressen, das verwendete Protokoll, die IP-Adressen des Servers und des Clients sowie die IP-Adressen und Namen der sendenden und empfangenden E-Mail-Server (Art. 62 VÜPF).[124]

c. Inhaltsdaten

Inhaltsdaten umfassen den eigentlichen Inhalt einer Kommunikation (z.B. Text einer SMS- oder E-Mail-Nachricht, Chat in Whatsapp, Postings auf Social Media-Plattformen). Eine aktive (geheime) Überwachung von Kommunikationsinhalten erfolgt immer in Echtzeit, also noch während des Kommunikationsvorgangs.[125] Für eine Echtzeitüberwachung müssen die Voraussetzungen von Art. 269 Abs. 1 lit. a–c StPO vorliegen: Bei der verfolgten Straftat muss es sich um eine Katalogtat i.S.v. Art. 269 Abs. 2 lit. a StPO handeln und die Überwachung muss vom Zwangsmassnahmengericht bewilligt werden. Inhaltsdaten dürfen nicht rückwirkend (mittels Art. 273 Abs. 3 StPO) erhoben werden. Bereits

---

[119] HANSJAKOB, Überwachungsrecht, Rz. 1637–1638; DERS., Wichtige Entwicklungen, 175–176; BGE 141 IV 108, E. 5.1.

[120] Auch Verkehrs- oder Randdaten genannt. Technisch korrekt als „Intercept Related Informations“ (IRI, mit dem Verkehr verbundene Informationen) zu bezeichnen, vgl. dazu Komm StPO-HANSJAKOB, Art. 273 N 3. Im Verlauf der Arbeit werden die Begriffe „Verbindungs-“ und „Randdaten“ synonym verwendet.

[121] FORSTER, 620.

[122] Art. 273 StPO spricht explizit von Randdaten, wobei auf Art. 8 lit. b BÜPF verwiesen wird. Danach handelt es sich um Daten, aus denen hervorgeht, mit wem, wann, wie lange und von wo aus die überwachter Person Verbindung hat oder gehabt hat, sowie die technischen Merkmale der entsprechenden Verbindung.

[123] Komm StPO-HANSJAKOB, Art. 273 N 1–8; FORSTER, 620–621. Zur vertieften Theorie bzgl. Randdatenerhebungen wird auf die Ausführungen oben in Kap. II./2./D./d. verwiesen.

[124] Vgl. mit weiteren Beispielen BERTSCHMANN, 359–360.

[125] FORSTER, 623–624, Fn. 49.

abgerufene Kommunikationsinhalte können jedoch im Rahmen einer Edition/Beschlagnahme von einem physischen Gerät oder beim Provider erhoben werden. Diesbezüglich sind die Regelungen von Art. 263 ff. StPO zu beachten und es findet kein besonderes Verfahren nach Art. 269 ff. StGB statt. Eine solche Datenerhebung darf nicht heimlich erfolgen und der betroffenen Person müssen die üblichen Rechtsmittel gegen Beweiserhebungen offenstehen. Eine Bewilligung des Zwangsmassnahmengerichts ist nicht erforderlich. Der Rechtsschutz erfolgt auf dem Weg der Siegelung.[126]

d. E-Mail-Verkehr

Die Praxis zum Postverkehr ist für den E-Mail-Verkehr massgebend, weshalb im Folgenden kurz auf den Postverkehr eingegangen wird: Postsendungen können nach Art. 246 f. StPO von der zuständigen Behörde sichergestellt und, falls erforderlich, nach Art. 263 ff. StPO beschlagnahmt werden. Der Inhaber der sichergestellten Sendungen hat das Recht, sich vorgängig dazu zu äussern und die Siegelung i.S.v. Art. 248 StPO zu verlangen. Werden Beweismittel mit Wissen des Inhabers beschlagnahmt, liegt keine geheime Überwachung vor. Befinden sich Daten im Einflussbereich der Absenderin oder des Empfängers, besitzen sie die Datenherrschaft und die Informationen unterliegen nicht (mehr) dem Fernmeldegeheimnis. Dabei ist es unerheblich, ob der Empfänger die Informationen bereits zur Kenntnis genommen hat.[127]

Gemäss Bundesgericht liegt ein Brief im alleinigen Herrschaftsbereich des Empfängers, wenn er sich in dessen Briefkasten befindet.[128] Legt die Post den Brief in ein Postfach des Empfängers, besteht vorerst eine geteilte Herrschaft von Post und Briefempfänger. Der Kommunikationsvorgang gilt erst dann als abgeschlossen, wenn der Empfänger die alleinige Herrschaft erlangt hat, also ab dem Zeitpunkt, in dem er das Postfach öffnet.[129] Ist eine Postsendung noch nicht beim Empfänger eingetroffen, ist eine Überwachung nach Art. 269 ff. StPO zu verfügen, weil in dieser Konstellation die Informationen noch dem Fernmeldegeheimnis unterliegen. Treffen bspw. nach einer Verhaftung weitere für die Strafverfolgungsbehörde interessante Postsendungen bei der beschuldigten Person ein, können diese nur mit Zustimmung der betroffenen Person beschlagnahmt werden. Fehlt eine Zustimmung, ist eine Überwachung anzuordnen.[130]

Das Bundesgericht hat in analogiam zum Postverkehr folgenden Grundsatz für den E-Mail-Verkehr formuliert: Eine E-Mail gelangt auf den Server der Fernmeldedienstanbieterin des Empfängers in dessen E-Mail-Konto. Ab dem Zeitpunkt, indem der Empfänger sein Mailkonto öffnet und sieht (bzw.

---

[126] HANSJAKOB, Überwachungsrecht, Rz. 326–327, 441.

[127] HANSJAKOB, Überwachungsrecht, Rz. 302–304; BGE 140 IV 181, E. 2.4–2.6.

[128] BGE 140 IV 181, E. 2.5.2.

[129] BGE 140 IV 181, E. 2.5.3.

[130] HANSJAKOB, Überwachungsrecht, Rz. 305.

sehen kann), dass die E-Mail eingegangen ist[131], kann er über sie verfügen. Ob die E-Mail gelesen bzw. zur Kenntnis genommen wurde, ist nicht entscheidend. Die Herausgabe von Nachrichten ab diesem Zeitpunkt stellt eine Edition nach Art. 265 StPO dar; vor diesem Zeitpunkt liegt eine Echtzeitüberwachung nach Art. 269 ff. StPO vor. Soweit sich die E-Mail-Nachricht noch auf dem Server des Providers befindet, kann sie dort beschlagnahmt werden. Bei einer (geheimen) Echtzeitüberwachung wird die Nachricht, noch bevor sie vom Empfänger auf dessen Nachrichtenkonto abgerufen wird, *abgefangen*. Sinngemäss dürften diese Überlegungen auch für den SMS-Verkehr und andere Formen der Internetkommunikation gelten.[132]

Werden Smartphones und andere digitale Kommunikationsgeräte *physisch* beschlagnahmt oder sichergestellt und will die Staatsanwaltschaft die darauf gespeicherten Daten (Randdaten, Kontaktnummer, abgerufener Kommunikationsinhalte) auswerten, liegt nach der Praxis des Bundesgerichts grundsätzlich keine Überwachung (Art. 269 ff. StPO) und auch keine (rückwirkende) Randdatenerhebung (Art. 273 (Abs. 3) StPO), sondern eine Edition/Beschlagnahme (Art. 263 ff. StPO) vor. Die betroffene Person kann die Siegelung (Art. 248 Abs. 1 StPO) des sichergestellten Geräts verlangen.[133]

Zusammenfassend kann festgehalten werden, dass eine Unterscheidung zwischen der Edition von gespeicherten Informationen und der geheimen Überwachung des Informationsverkehrs vorzunehmen ist. Die Edition/Beschlagnahme von gespeicherten Nachrichten erfolgt nach Art. 263 ff. StPO. Eine geheime inhaltliche Überwachung erfolgt immer in Echtzeit nach den Regeln von Art. 269 ff. StPO. Eine rückwirkende Überwachung ist bloss im Rahmen einer Teilnehmeridentifikation und einer Randdatenerhebung nach Art. 273 StPO (und nicht bzgl. Kommunikationsinhalten) zulässig.[134]

e. Messenger-Verkehr

Die Kommunikation über Messaging-Dienste (bspw. Whatsapp, Facebook- oder Instagram-Messenger) ist in der Praxis besonders wichtig, weil der Nachrichtenverkehr über besonders lange Zeit auf dem benutzten Gerät gespeichert bleibt. Eine strafprozessuale Überwachung solcher Messaging-Dienste scheitert vor allem daran, dass sich die Betreiberinnen meistens im Ausland befinden und der Nachrichtenverkehr solcher Dienste verschlüsselt ist. Die Anbieterinnen sind selbst oft nicht in der Lage, den Nachrichtenverkehr zu entschlüsseln. Deshalb ist es umso wichtiger, die Nachrichten unverschlüsselt aus den beschlagnahmten Geräten auslesen zu können.[135]

---

[131] Sog. „Abrufen" der Nachricht, was dringend vom Anklicken und Lesen der Nachricht zu unterscheiden ist.

[132] FORSTER, 623–625, Fn. 39, 41–42, 46–49; BGE 140 IV 181, E. 2.6–2.7; HANSJAKOB, Überwachungsrecht, Rz. 313, 316; JEAN-RICHARD-DIT-BRESSEL, 174.

[133] BGE 140 IV 181, E. 2.4, 2.10; 143 IV 270, E. 4.6; BGer 1B_347/2015, E. 1.1; 1B_52/2015, E. 1.2; 1B_131/2015, E. 1.2; FORSTER, 623–624.

[134] Vgl. dazu FORSTER, Fn. 49.

[135] HANSJAKOB, Überwachungsrecht, Rz. 325–327.

Auf weitere Ausführungen wird verzichtet und oben auf Kap. II./3./A./d. zum E-Mail-Verkehr verwiesen. Die beschriebene Praxis zum E-Mail-Verkehr dürfte wohl analog auch für den Messenger-Verkehr gelten[136].

B. Abgrenzungsschwierigkeiten bei Daten des Internetverkehrs

a. „IP-History"

HANSJAKOB spricht von einer klaren gesetzlichen Regelung bezüglich einer Datenerhebung des Internetverkehrs (wonach die Regelungen über Bestandesdaten Anwendung finden sollen[137]).[138] Die Umsetzung in der Praxis gestaltet sich jedoch vor allem bei *untypischen Fällen* von Bestandesdatenerhebungen (bzw. wenn der (Internet-)Anschluss den Strafverfolgungsbehörden nicht bereits bekannt ist[139]) eher schwierig. So hat das Bundesgericht in mehreren Urteilen Abgrenzungsschwierigkeiten zwischen Bestandes- und Randdatenerhebungen festgestellt[140]. Schliesslich hat es eine Unterscheidung zwischen der Erhebung von Rand- und Bestandesdaten betreffend einer sog. „IP-History"[141] getroffen: Bei der Erhebung einer „IP-History" handle es sich in jenen Fällen um eine Randdatenerhebung (Art. 273 StPO), in denen der Strafverfolgungsbehörde lediglich strafbare Internetkommunikationsaktivitäten bekannt geworden seien und über die Verbindungs-Randdaten der betreffenden Internetkommunikation die zugewiesenen IP-Adressen und (in einem zweiten Schritt) die registrierten Kunden erst eruiert werden müssten. Hierzu müssten die Teilnehmenden an konkreten Fernmeldeverbindungen über einen gewissen Zeitraum hinweg identifiziert werden. Dies stelle eine Verkehrsdatenerhebung dar und sei als Randdatenerhebung nach Art. 273 StPO zu qualifizieren. Erst gestützt auf diese (Randdaten-)Erhebung könnten schliesslich die Registrierungsdaten als Bestandesdaten ediert werden. Sei den zuständigen Behörden bereits eine E-Mail-Adresse oder ein Internetanschluss bekannt, dann stelle die Erhebung der Registrierungsdaten grundsätzlich eine Bestandesdatenerhebung i.S.v. Art. 22 BÜPF dar. Um eine blosse Registrierungsdatenerhebung handle es sich insb. auch dann, wenn eine bereits bekannte statische IP-Adresse betroffen sei[142].[143]

---

[136] FORSTER, Fn. 49.

[137] Dazu wird insb. oben auf Kap. II./3./A./a., verwiesen.

[138] HANSJAKOB, Wichtige Entwicklungen, 176.

[139] In BGE 139 IV 98 war der Staatsanwaltschaft bereits ein Internetanschluss mit einer *statischen* IP-Adresse bekannt. In diesem Fall hat das BGer Art. 14 Abs. 4 aBÜPF (neu Art. 22 BÜPF) für anwendbar erklärt. Dies hatte zur Folge, dass die sechsmonatige Frist für eine rückwirkende Teilnehmeridentifikation im Rahmen einer Randdatenerhebung i.S.v. Art. 273 Abs. 3 StPO nicht zur Anwendung kam.

[140] BGE 139 IV 98; 141 IV 108.

[141] Liste der IP-Adressen, von denen aus auf ein bestimmtes Mailkonto zugegriffen wird.

[142] Ein solcher Sachverhalt lag BGE 139 IV 89 zugrunde, vgl. Fn. 139. Beim mobilen verschlüsselten Internetverkehr und insb. bei der Kommunikation über Social Media sind statische IP-Adressen allerdings untypisch.

[143] BGE 141 IV 108, E. 5.1, 6.2; vgl. auch BGer 6B_656/2015, E. 1.3.1–1.3.2 m.w.H; gl.M. auch FORSTER, 623; BERTSCHMANN, 360–361; SCHWEINGRUBER, Rz. 29; a.M. HANSJAKOB, Wichtige Entwicklungen, 177.

In BGer 6B_656/2015 gab eine (ausländische) Kommunikationsdienstanbieterin den (Schweizer) Untersuchungsbehörden Auskünfte darüber, wann die betroffenen (der Untersuchungsbehörde bereits bekannten) E-Mail-Adressen und Nachrichten erstellt und über welche IP-Adressen und Provider die Adressen generiert und die E-Mails verschickt wurden. Die Strafverfolgungsbehörde konnte mithilfe dieser Informationen ermitteln, wann und von wo aus die E-Mails versendet wurden. Informationen über die Identität der Inhaberin der inkriminierten E-Mail-Adressen konnten nicht ermittelt werden. Das Bundesgericht erwog, dass es sich im zitierten Entscheid um Daten gehandelt habe, welche die Kommunikation beträfen und somit Verbindungs-Randdaten dargestellt hätten. Daran habe nichts geändert, dass die E-Mail-Adressen bereits bekannt gewesen seien. Insbesondere seien nicht die Daten zur Inhaberin eines bestimmten Anschlusses (Bestandesdaten) erfragt worden. Über die erlangten IP-Adressen habe vielmehr der bis dahin unbekannte Anschluss und dessen Standort ermittelt werden können.[144]

HANSJAKOB kritisiert[145] die Beurteilung des Bundesgerichts insoweit, als dass er die Qualifikation der „IP-History" in BGer 6B_656/2015 als Bestandesdaten i.S.v. Art. 22 BÜPF für sachgerechter hält. Die „IP-History" habe im zitierten Entscheid nur Angaben darüber enthalten, wann und von wo aus die verdächtige Person auf ihr Mailkonto zugegriffen habe. Erst in Verbindung mit dem bereits bekannten Zeitpunkt der Mails habe ermittelt werden können, von wo aus die Mails verschickt worden seien. Gemäss HANSJAKOB hätte aber vor allem geklärt werden müssen, zu welcher Kategorie die Daten darüber gehören, *wer wann* auf sein Mailkonto zugegriffen hat.[146] Bei der „IP-History" könne „nicht von *Kommunikationsdaten* gesprochen werden, sondern eben nur von Daten, die den Benutzer eines bestimmten Mailkontos identifizieren würden. Deshalb handle es sich richtigerweise um Auskünfte i.S.v. Art. 22 BÜPF.[147] Die häufigsten Anwendungsfälle von Art. 22 BÜPF seien genau solche Fragen im Zusammenhang damit, wer eine bestimmte inkriminierte E-Mail verschickt oder wer in Social Media eine bestimmte Mitteilung verfasst habe.[148]

Meines Erachtens sind sowohl die Ausführungen des Bundesgerichts als auch diejenigen von HANSJAKOB nicht klar verständlich. Die Erwägungen des Bundesgerichts sind zwar nicht leicht zu durchschauen, machen jedoch in ihrer Gesamtheit Sinn. Die im zitierten Entscheid erhobenen Daten können in theoretischer Hinsicht und überspitzt gesagt weder den Verbindungs- noch den Bestandesdaten zugeordnet werden[149]. Es handelt sich weder um klassische Bestandesdaten nach Art. 22 BÜPF, weil

144 BGer 6B_656/2015, E. 1.4.1–1.4.2.

145 Vgl. dazu die Bemerkungen von HANSJAKOB zu BGer 6B_656/2015 in: HANSJAKOB, Erhebung von Daten.

146 HANSJAKOB, Erhebung von Daten, 255–256.

147 HANSJAKOB, Erhebung von Daten, 255; vgl. dazu auch DERS., Überwachungsrecht, Rz. 1640.

148 HANSJAKOB, Wichtige Entwicklungen, 176.

149 Anders verhielt es sich in BGE 139 IV 98 (vgl. schon oben, Fn. 139 und 142), wo der Internetanschluss mit einer statischen IP-Adresse der Staatsanwaltschaft bereits bekannt war. Es ging um die Identifikation eines bestimmten Benutzers, also eindeutig um Registrierungsdaten und demzufolge um eine Bestandesdatenerhe-

keine der Teilnehmeridentifikation dienenden Registrierungsdaten erhoben wurden, noch um klassische Verbindungs-Randdaten, weil nicht geklärt wurde, wer wann mit wem eine Verbindung gehabt hat. M.E. ist der Meinung des BGer, die „IP-History" in diesem Fall als Verbindungs-Randdaten zu qualifizieren, zuzustimmen, da schliesslich ein unbekannter Anschluss und dessen Standort anhand der IP-Adressen ermittelt werden konnte, weshalb es sinnvoll erscheint, von Daten auszugehen, welche die Kommunikation betreffen.

Die gesetzliche Trennung von Datenarten bedient sich teilweise einer verwirrlichen Terminologie, was auch Grund dafür ist, dass sich das BGer selbst mit einer klaren Kategorisierung schwertut. Zusammenfassend ist festzuhalten, dass die Abgrenzung gesetzlich alles andere als sauber ist. Es bleiben Unklarheiten offen, die letztlich von der Lehre und nicht vom Bundesgericht zu klären sind[150].

b. E-Mail-Nachrichten

Die vom Bundesgericht in BGE 140 IV 181 aufgestellte Regel zum E-Mail-Verkehr[151] gibt gemäss HANSJAKOB Anlass zu Bedenken. Handelt es sich bei der Datenerhebung um eine Edition nach Art. 265 StPO (und nicht um eine Überwachung), kann die Edition gemäss BGer einerseits durch Beschlagnahme des Geräts oder durch eine Anordnung zur Herausgabe der betreffenden E-Mail-Nachrichten an den Provider erfolgen. Letzteres bedeutet für HANSJAKOB insbesondere, dass in diesem Fall auch Kommunikationsinhalte rückwirkend ediert werden können, ohne dass sie vom Empfänger *gelesen*[152] wurden. Dies gehe in zweierlei Hinsicht ausserordentlich weit: Erstens werde der Provider gezwungen, neben Rand- auch Inhaltsdaten rückwirkend herauszugeben, während die Regelung von Art. 273 StPO nicht auf eine rückwirkende Edition von Inhaltsdaten zugeschnitten sei. Zweitens schaffe der bundesgerichtliche Entscheid die Möglichkeit, direkt von den Providern Maildaten edieren zu lassen, ohne dabei den Weg über den Dienst zu gehen. Problematisch sei auch, dass Inhaltsdaten beim Provider ediert würden, der an sich an das Fernmeldegeheimnis gebunden sei.[153]

M.E. ist der Betrachtungsweise von HANSJAKOB nicht zuzustimmen. HANSJAKOB deutet darauf hin, dass im zitierten Entscheid die Art. 296 ff. StPO hätten anwendbar sein müssen. Eine Begründung dafür ist nicht klar ersichtlich. Es lässt aber vermuten, dass das Fernmeldegeheimnis ausschlaggebend ist. Gemäss HANSJAKOB war der Provider im vorliegenden Fall noch an das Fernmeldegeheimnis gebunden, weswegen Art. 273 Abs. 3 StPO hätte gelten sollen und nur Rand- aber keine Inhaltsdaten

---

bung nach Art. 14 Abs. 4 aBÜPF (neu Art. 22 BÜPF). Auch in diesem Entscheid ist die Argumentation des BGer m.E. nicht leicht durchschaubar. Es darf aber nicht ausser Acht gelassen werden, dass das Gericht sich hauptsächlich mit der Frage der Sechsmonatsfrist von Art. 273 Abs. 3 StPO befasst hat.

[150] Vgl. zu dieser Meinung auch FORSTER, Fn. 38.

[151] Vgl. dazu oben, Kap. II./3./A./d.

[152] Die Nachricht muss jedoch vom Empfänger auf seinem Nachrichtenkonto *abgerufen* worden sein.

[153] HANSJAKOB, Überwachungsrecht, Rz. 316–318.

hätten ediert werden dürfen. Dieser Ansicht ist meines Erachtens zu widersprechen. Der Argumentation von HANSJAKOB wird entgegengehalten, dass der Provider nicht mehr an das Fernmeldegeheimnis gebunden war. Die E-Mail wurde vom Empfänger bereits abgerufen, womit er zugleich die alleinige Datenherrschaft erlangt hat. In Analogie zum Postfach[154] kann argumentiert werden, dass es keine Rolle spielen darf, ob der Empfänger die abgerufene Mail auf dem Server seines Providers oder auf seiner lokalen Datenverarbeitungsanlage aufbewahrt[155]. Gemäss der hier vertretenen Ansicht besteht also kein ersichtlicher Grund dafür, die auf dem Server des Providers belassenen, abgerufenen Mails besser zu schützen als jene, die sich auf dem lokalen Datenträger des Empfängers befinden. Dementsprechend geniesst der Empfänger in Bezug auf jene Rand- und Inhaltsdaten keinen Schutz des Fernmeldegeheimnisses (mehr) und einer Edition/Beschlagnahme beim Provider steht nichts entgegen. Die Beschlagnahme muss allerdings rechtmässig erfolgen und der betroffenen Person ist Rechtsschutz auf dem Weg der Siegelung zu gewähren.

c. Zugangsdaten

Eine weitere aktuelle Diskussion beschäftigt sich mit der Überwachung des Datenverkehrs unter Verwendung von *Zugangsdaten*[156]. Bei den Zugangsdaten handelt es sich um Login-Daten, mittels welcher man sich von verschiedenen Geräten aus auf ein bestimmtes Mail- oder Facebook-Konto einloggen kann. Auf diese Weise kann eine Kopie des Kommunikationsverkehrs der betroffenen Person auf eine Datenspeicherungsanlage der Strafverfolgungsbehörde heruntergeladen werden. Solche Möglichkeiten sind für die zuständigen Behörden äusserst interessant, weil sie mit niedrigem Aufwand verbunden sind und (im Falle von Kommunikationen mit End-zu-End-Verschlüsselung) unverschlüsselte Kommunikationsdaten liefern.[157]

In BGE 143 IV 270 kam die Strafverfolgungsbehörde an die Zugangsdaten für das Facebook-Konto eines Untersuchungshäftlings ran. Auf Auftrag der Staatsanwaltschaft sichtete die Polizei unter Verwendung der ermittelten Zugangsdaten das Facebook-Konto und stellte diverse Chat-Nachrichten sicher. Das Bundesgericht führte zunächst aus, dass Facebook als Anbieterin abgeleiteter Internetdienste nicht dem aBÜPF (Art. 1 Abs. 1 und Abs. 2 aBÜPF i.V.m. Art. 1 Abs. 2 lit. e aVÜPF) unterstanden habe[158], weshalb eine Überwachung nach Art. 269 ff. StPO gar nicht in Frage gekommen

---

[154] Vgl. dazu oben Kap. II./3./A./d.

[155] Vgl. dazu auch die Argumentation in BGE 140 IV 181, E. 2.6.

[156] Die Frage, ob der Zugriff der Strafverfolgungsbehörden mittels Zugangsdaten grenzüberschreitend geschieht (bzw. das Territorialitätsprinzip tangiert) wird in diesem Kapitel nicht berücksichtigt. Im zitierten BGE 143 IV 270 erfolgte der Zugriff grenzüberschreitend, was nicht ganz unproblematisch ist, aber in einem anderen Kapitel (Kap. III.) ausführlich behandelt wird. Die in diesem Kapitel aufgezeigte Lehre und Rechtsprechung ist im Rahmen einer innerstaatlichen Hoheitsausübung zu verstehen.

[157] HANSJAKOB, Überwachungsrecht, Rz. 439.

[158] Das BGer bestätigte in BGE 143 IV 270, E. 7.1 die Rspr. aus BGE 141 IV 108, E. 5.13; 143 IV 21, E. 3.1 und BGer 1B_142/2016, E. 3.1. Vgl. auch ROTH, Rz. 20–26, insb. Rz. 23.

sei.[159] Nach neuem Recht würde sich die Situation anders gestalten: Art. 2 lit. c BÜPF erfasst nun auch Anbieterinnen abgeleiteter Kommunikationsdienste[160]. Gemäss BGer durfte die Polizei im vorliegenden Fall den Facebook-Verkehr des Häftlings vorläufig nach den Regeln der Durchsuchung von Datenträgern sichern, weil Gefahr in Verzug bestand (Art. 263 Abs. 3 und Art. 265 Abs. 4 StPO). Es war auch zulässig, dem Beschuldigten einige Stichproben-Nachrichten vorzulegen, ohne ihm vorgängig die Möglichkeit zu geben, eine Siegelung zu verlangen.[161]

Zugangsdaten können bspw. im Rahmen einer Hausdurchsuchung sichergestellt werden. Voraussetzung für die Verwendung ist, dass sie rechtmässig erhoben wurden. Eine laufende Überwachung mittels Zugangsdaten richtet sich nach Art. 269 ff. StPO. Diesbezüglich ist eine Genehmigung des Zwangsmassnahmengerichts erforderlich. In der Regel wird eine solche Überwachung nicht über den Dienst ÜPF abgewickelt, weil die Anbieterinnen daran gar nicht beteiligt sind. Die Polizei kann die Daten direkt beim Provider abrufen. Art. 17 lit. c BÜPF bildet die Rechtsgrundlage dazu und erlaubt einen Direktzugang der Polizei zu den Überwachungsergebnissen. Auf diesem Weg dürfen jedoch keine Inhaltsdaten rückwirkend ediert werden (Art. 273 StPO).[162]

Mit dem vorliegenden Entscheid lässt das Bundesgericht die allgemeinen Regeln zur Sicherstellung und Durchsuchung (Art. 246 StPO) von Datenträgern auf jene Fälle anwenden, in denen die Strafverfolgungsbehörden einen direkten Zugriff auf das Konto der beschuldigten Person bei (ausländischen) Anbieterinnen abgeleiteter Internetdienste erhalten haben. Das BGer argumentiert wie folgt: Komme die Staatsanwaltschaft rechtmässig in den Besitz von Zugangsdaten zu einem bestimmten Benutzerkonto und beschaffe sich dadurch Beweisunterlagen, namentlich Chat-Nachrichten, geschehe dies über Internet und nicht auf dem Wege einer Überwachung des Fernmeldeverkehrs. Dieses Vorgehen entspreche auch der Rechtslage bei der Erhebung von passwortgeschützter Fernmeldekommunikation. Würden die Strafverfolgungsbehörden bspw. das Passwort zur Entsperrung eines sichergestellten Smartphones erfahren, seien sie ebenfalls berechtigt, die darauf gespeicherte abgeschlossene Fernmeldekommunikation (insb. vom Empfänger bereits abgerufene E-Mails oder SMS) zu sichten. Der Rechtsschutz erfolge über die Siegelung. Eine genehmigungsbedürftige Überwachung nach Art. 269 ff. StPO sei nur bei aktiver bzw. vom Empfänger noch nicht abgerufener Fernmeldekommunikation erforderlich. Da für Anbieterinnen abgeleiteter Internetdienste die Art. 296–279 StPO sowieso nicht gelten würden, könnten auch keine strengeren Zugriffsanforderungen gelten als bei der Fernmeldekommunikation i.e.S. Folglich sei eine Erhebung der (abgerufenen) Kommunikationsdaten mittels

[159] BGE 143 IV 270, E. 7.1.

[160] HANSJAKOB, Überwachungsrecht, Rz. 328. Allenfalls wäre Facebook auch als Fernmeldedienstanbieterin i.S.v. Art. 2 lit. b BÜPF zu qualifizieren, vgl. dazu die Ausführungen in Kap. II./2./D./d./cc.

[161] BGE 143 IV 270, E. 7.2–7.6.

[162] HANSJAKOB, Überwachungsrecht, Rz. 440–442.

Zugangsdaten insoweit zulässig, als dass die Zugangsdaten rechtmässig erhoben würden und die Durchsuchungsvoraussetzungen[163] erfüllt seien.[164]

HANSJAKOB findet das Vorgehen des Bundesgerichts insoweit heikel, als dass es die Regeln über die Sicherstellung und Durchsuchung von Datenträgern auf den im zitierten Entscheid dargelegten Sachverhalt anwenden lässt. Richtigerweise seien die Regeln über die Überwachung nach Art. 269 ff. StPO anwendbar gewesen, denn die Polizei sei im vorliegenden Fall mittels *fernmeldetechnischem Zugriff* auf Speichermedien an die Daten gekommen. Zudem sei die Kommunikation über Messenger-Verkehr vom Fernmeldegeheimnis geschützt. Private Chat-Nachrichten (also Inhaltsdaten der Kommunikation) seien nach den Regeln der Durchsuchung bei der beschuldigten Person, aber nicht auf dem Weg der Fernmeldekommunikation verfügbar, jedenfalls nicht gegen den Willen der beschuldigten Person. Die Erhebung der Chat-Nachrichten habe im zitierten Entscheid eine unzulässige, rückwirkende Inhaltsdatenerhebung dargestellt.[165]

HANSJAKOB hält folgende Lösung für sachgerechter: „Man hätte dem Häftling entweder eröffnen müssen, dass man seine Zugangsdaten zum Facebook-Konto besitzt, und wenn er dem Zugriff zugestimmt hätte, dann wären alle Daten abrufbar gewesen, auch die Kommunikationsinhalte der Vergangenheit. Hätte er nicht zugestimmt, dann wäre das Siegelungsverfahren durchzuführen gewesen, und man hätte dann auf die öffentlich einsehbaren Daten in Facebook zugreifen können, die nicht im Siegelungsverfahren hätten ausgesondert werden müssen, denn für diese Daten gilt das Fernmeldegeheimnis nicht. Private Kommunikation der Vergangenheit wäre auf diese Weise nicht erhältlich gewesen, weil man sie nur über einen Kommunikationsvorgang (eben Zugang über Internet zum Konto) und nicht durch Beschlagnahme eines Datenträgers hätte erheben können. Man hätte aber auch ohne Wissen des Beschuldigten eine aktive Überwachung des Facebook-Kontos nach Art. 269 StPO verfügen können. Damit wären aber nur die laufenden Kommunikationen [...] überwachbar gewesen, nicht dagegen die noch auf dem Server vorhandenen vergangenen Kommunikationen.“[166]

M.E. ist dem Vorgehen des Bundesgerichts bezüglich der Qualifikation der Zwangsmassnahme als Sicherstellung und Durchsuchung Recht zu geben. Hätte man die Edition des Chat-Verkehrs des Beschuldigten als Überwachung i.S.v. Art. 269 ff. StPO qualifiziert, wäre eine Anordnung der Überwachung im vorliegenden Fall gar nicht realisierbar gewesen, da, wie bereits das BGer zu Recht ausgeführt hat, Facebook als Anbieterin von abgeleiteten Internetdiensten zum damaligen Zeitpunkt nicht dem persönlichen Geltungsbereich des BÜPF unterstand. Zwar wäre dies unter neuem Recht anders,

[163] Durchsuchungsbefehl oder Gefahr in Verzug (Art. 241 StPO), hinreichender Tatverdacht (Art. 197 Abs. 1 lit. b StPO), Verhältnismässigkeit (Art. 197 Abs. 1 lit. c und d StPO) und Vermutung, dass es sich um Informationen handelt, die der Beschlagnahme unterliegen (Art. 246 StPO).

[164] BGE 143 IV 270, E. 7.1, 7.7.

[165] HANSJAKOB, Überwachungsrecht, Rz. 330, 442.

[166] HANSJAKOB, Überwachungsrecht, Rz. 332–333.

doch wäre eine rückwirkende Erhebung der Chat-Kommunikation mittels Art. 273 Abs. 3 StPO unzulässig. M.E. kann hier allerdings wiederum eine Analogie zum Postverkehr (und E-Mail-Verkehr) geschlossen werden[167]: Sobald der Empfänger die Nachrichten *abgerufen* hat, können sie mittels Durchsuchung und Beschlagnahme ediert werden[168].

Der Zugang über Internet zum Konto des Betroffenen und somit zu seinen Kommunikationsinhalten mittels seiner Zugangsdaten ist m.E. nicht als fernmeldetechnisch bzw. als Kommunikationsvorgang zu verstehen[169]. Der auf den eigentlichen Messenger-Verkehr bezogene Kommunikationsvorgang gilt ab dem Zeitpunkt, indem die Nachrichten abgerufen wurden, als abgeschlossen. Das Fernmeldegeheimnis gilt nicht (mehr). M.E. ist es nicht nötig, dass die Strafverfolgungsbehörden physisch ein Gerät beschlagnahmen müssen, um an eben jene Daten zu gelangen. Ein Zugriff mittels Zugangsdaten ist ressourcen- und zeitsparend und stellt eine massive Erleichterung der Strafverfolgung dar. Es kann denn auch die Verschlüsselung auf einfachstem Weg übergangen werden. Dabei wird dem Geheimhaltungsinteresse der betroffenen Person m.E. nicht weniger Rechnung getragen als bei einer klassischen Beschlagnahme. Schliesslich besteht auch hier das Recht auf Siegelung (Art. 248 StPO).

[167] Gl.M. ist auch FORSTER, Fn. 49, der die analoge Rspr. vom Post- zum E-Mail-Verkehr auch für *andere* Formen der Internetkommunikation als zulässig erachtet.

[168] Vgl. dazu oben, Kap. II./2./A.–C und II./3./A./d.

[169] Vgl. dazu BGE 143 IV 270, E. 7.1.

III. Grenzüberschreitende Zwangsmassnahmen zur Datenerhebung

In diesem Kapitel wird die grenzüberschreitende Strafverfolgung von Cybercrime bzw. Computer- und Internetkriminalität näher beleuchtet. Dafür wird in einem ersten und zweiten Teil die Theorie zum Territorialitätsprinzip, zur internationalen Rechtshilfe in Strafsachen und zu ausgewählten Strafverfolgungsinstrumente[170] der Convention on Cybercrime[171] erläutert. In einem dritten Teil wird der Konflikt zwischen dem Territorialitätsprinzip und einer effizienten grenzüberschreitenden Strafverfolgung von Cybercrime diskutiert. Es werden Argumente für und gegen eine weite bzw. enge Auslegung des Territorialitätsprinzips aufgezeigt. In der Diskussion werden insb. die im zweiten Teil beschriebenen Instrumente der CCC und ausgewählte Bundesgerichtsentscheide besprochen.

1. Strafhoheit und internationale Rechtshilfe in Strafsachen

A. Territorialitätsprinzip

Das Territorialitätsprinzip (Art. 3 StGB) stellt eine Schranke staatlichen Handelns dar. Es begrenzt zum einen die Anwendbarkeit innerstaatlichen Strafrechts auf ausländische Sachverhalte und zum anderen das staatliche Handeln auf das eigene Hoheitsgebiet.[172] Übt der Staat Zwangs- oder Eingriffshandlungen auf fremdem Hoheitsgebiet aus, verletzt er u.U. die staatliche Souveränität des anderen Staates und verhält sich folglich völkerrechtswidrig. Derartige Handlungen können mittels internationalen (Rechtshilfe-)Abkommen, bilateralen Verträgen oder ad hoc-Genehmigungen zwischen den Staaten aber als zulässig eingestuft werden. Als unzulässig gelten aber Handlungen der Strafverfolgungsbehörden im Ausland zur Beweiserhebung, sofern sie nicht durch internationale Rechtshilfeabkommen, bilaterale Verträge oder ad hoc-Genehmigungen erlaubt sind. Das Schweizerische Strafrecht kennt eine Strafbestimmung, die das Handeln für einen fremden Staat auf schweizerischem Staatsgebiet ohne Bewilligung unter Strafe stellt (Art. 271 StGB). Auch bestraft werden kann, wer die Gebietshoheit eines fremden Staates verletzt, insb. durch unerlaubte Vornahme von Amtshandlungen auf fremdem Staatsgebiet (Art. 299 Abs. 1 StGB). Demnach ist unbestritten, dass die Strafverfolgungsbehörden nicht physisch im Ausland Beweise erheben dürfen, ohne dass es die internationale Rechtshilfe

---

[170] Die Art. 2–10 CCC erfassen u.a. Straftaten wie Hacking, unrechtsmässiges Abfangen von nicht öffentlich übertragenen Computerdaten, Datenbeschädigung, Computerbetrug und Kinderpornografie.

[171] Zu den 62 Mitgliedsstaaten des Übereinkommens zählen u.a. 26 EU-Staaten (mit Ausnahme von Irland und Schweden, die das Übereinkommen unterzeichnet, aber noch nicht ratifiziert haben), die Vereinigten Staaten, Kanada, Japan und Australien.

In einem ersten Teil (Art. 1–13 CCC) enthält die Konvention materielle Strafbestimmungen, welche die Harmonisierung des Strafrechts unter den Vertragsstaaten zum Ziel haben. In einem zweiten Teil befinden sich Regelungen für das Strafverfahren. Dabei geht es insb. um die Frage der Beweiserhebungen und -sicherungen i.B.a. elektronische Daten in der Strafuntersuchung (Art. 16–21 CCC). Gegenstand des dritten und letzten Teils sind Bestimmungen zur zwischenstaatlichen internationalen Zusammenarbeit in Strafsachen wie Rechtshilfe, Auslieferung und vorläufige Massnahmen (Art. 23–25 CCC).

[172] BGE 140 IV 86, E. 2.4.

oder ein Abkommen explizit erlauben würde. Eigenmächtige Sicherstellungen und Durchsuchungen von elektronischen Geräten oder Hausdurchsuchungen auf fremdem Staatsgebiet sind daher untersagt.[173] Unter diesem Aspekt stellt sich die Frage, ob Handlungen einer in der Schweiz handelnden schweizerischen Strafverfolgungsbehörde mit Auswirkungen auf ein fremdes Staatsgebiet im Hinblick auf das Territorialitätsprinzip erlaubt oder eben verboten sind[174]. Die Diskussion und Beantwortung dieser Frage stellte den Gegenstand von Kapitel. III./3. dar.

B. Internationale Rechtshilfe in Strafsachen

Die Rechtshilfe basiert auf der Tatsache, dass ein Staat nur innerhalb seines Territoriums tätig werden darf, weshalb es zwingend einer zwischenstaatlichen Kooperation bedarf. Der Begriff der Rechtshilfe bezeichnet diese materielle Unterstützung des ersuchten Staates an den ersuchenden Staat.[175] Befinden sich für die Strafverfolgungsbehörden interessante Daten im Ausland und will die Behörde zwangsweise an diese Daten gelangen, ist der Rechtshilfeweg massgebend. Soll auf öffentliche Websites und Downloads und die dazugehörenden Randdaten (z.B. die dem Domain-Namen zugehörige IP-Adresse) zugegriffen werden, ist ein direkter Zugriff (bzw. ohne Anordnung einer Zwangsmassnahme) zulässig. Sind die Daten jedoch nicht öffentlich zugänglich, ist der Rechtshilfeweg zu bestreiten. Der Rechtshilfe kommt also bei der Bekämpfung von Internetdelinquenz eine grosse Bedeutung zu.[176]

Rechtsgrundlagen für die Rechtshilfe finden sich einerseits im Bundesgesetz über internationale Rechtshilfe in Strafsachen (IRSG) und andererseits in zahlreichen bi- oder multilateralen Verträgen (z.B. EÜR, RVUS). Die Gewährung von Rechtshilfe hinsichtlich einer Zwangsmassnahme setzt eine beidseitige Strafbarkeit der im Ersuchen geschilderte Tat voraus (Art. 64 Abs. 1 IRSG[177]). Art. 64 Abs. 2 IRSG sieht Ausnahmen von der beidseitigen Strafbarkeit zur Entlastung der verfolgten Person und für die Verfolgung von sexuellen Handlungen mit Unmündigen vor. Die doppelte Strafbarkeit kann insb. im Bereich der Internetdelikte ein Hindernis für die Rechtshilfe darstellen. Dies ist namentlich der Fall, wenn einer der beiden Staaten ein (technisch neues) Internetdelikt noch nicht unter Strafe gestellt hat.[178]

---

[173] GRAF, Jusletter IT, Rz. 21–23.

[174] Wird durch die schweizerische Untersuchungshandlung das Territorialitätsprinzip verletzt und damit die Rechtshilfe in Strafsachen untergraben, hat dies den Beweisverlust wegen Unverwertbarkeit zufolge, vgl. dazu GRAF, Jusletter IT, Rz. 42; DOMBROWSKI, 159; RYSER, 575–577; HEIMGARTNER, Beschlagnahme, 266; DERS., Internetstraffälle, 136.

[175] BSK ISTR-HEIMGARTNER/NIGGLI, Einführung N 11, 19.

[176] HEIMGARTNER, Internetstraffälle, 134–136. Die Rechtshilfe in Strafsachen stellt neben der polizeilichen Zusammenarbeit und Amtshilfe ein wichtiges Element für die internationale Zusammenarbeit bei der Bekämpfung von Internetdelinquenz dar.

[177] Vgl. auch Art. 5 lit. a EÜR und Art. 4 RVUS.

[178] HEIMGARTNER, Internetstraffälle, 137–138.

Wird eine Überwachung im Ausland durchgeführt und ist somit der Rechtshilfeweg zu beschreiten, muss das Rechtshilfeersuchen die Rahmenbedingungen nach Art. 269 ff. StPO und dem BÜPF umschreiben. Dies dient der Verwertbarkeit der Daten in der Schweiz, welche nur gewährleistet ist, wenn die Vorschriften nach Art. 269 ff. StPO eingehalten werden. Unklar ist jedoch, ob vor der Übermittlung des Rechtshilfeersuchens ins Ausland eine richterliche Genehmigung nach Art. 274 StPO einzuholen ist, damit die Daten später ins schweizerische Verfahren eingeführt werden können. Diese Grundsatzfrage hat auch das Bundesgericht noch nicht eindeutig beantwortet. Es sind folgende vier Lösungen denkbar:[179]

Erstens: BGer 1B_142/2016 deutet darauf hin, dass für eine Datenerhebung im Ausland das Recht am Ort der Rechtshilfe massgeblich ist. Die im Ausland erhobenen Daten können dann in der Schweiz verwertet werden, wenn ihre Erhebung im Ausland zulässig ist.[180]

Zweitens: Ist eine Datenerhebung in der Schweiz genehmigungspflichtig, müssen die Daten zuerst im Ausland nach dortigem Recht erhoben werden. Über die Verwertbarkeit der Daten in der Schweiz entscheidet dann die in der Schweiz zuständige Genehmigungsbehörde. Gemäss einer nicht ganz eindeutigen Bundesgerichtspraxis[181] kann der Sachrichter Rügen über die Zulässigkeit einer Überwachung, die im Beschwerdeverfahren geltend gemacht werden, nicht mehr überprüfen. Deshalb vertritt HANSJAKOB die Ansicht, dass die Kompetenz zum Entscheid über die Zulässigkeit der Verwertung beim Genehmigungsrichter liegen solle.[182]

Drittens: Auch hier müssen die Daten zuerst im Ausland nach dortigem Recht erhoben werden. Anders als oben bei zweitens entscheidet hier jedoch anschliessend der Sachrichter über die Zulässigkeit der Verwertung der Daten. Dies der Regel folgend, dass der Sachrichter über die Zulässigkeit von Beweisen entscheiden kann.[183]

Viertens: Sind Daten im Ausland zu erheben, die in der Schweiz genehmigungspflichtig sind, muss die Staatsanwaltschaft vorgängig in der Schweiz eine Genehmigung in dem Sinne einholen, dass das Zwangsmassnahmengericht entscheidet, ob die Erhebung in der Schweiz zulässig sei. In Folge stellt die Staatsanwaltschaft mit diesem Entscheid ein Rechtshilfeersuchen[184].[185] Das BGer erachtet diesen Weg jedoch als unzulässig, weil der Grundsatz der Territorialität es verbiete, eigene Strafverfolgungsmassnahmen auf dem Hoheitsgebiet eines anderen Staates vorzunehmen; deshalb sei der

[179] HANSJAKOB, Überwachungsrecht, Rz. 397–398; vgl. dazu auch DERS., Erhebung von Daten, 256.

[180] HANSJAKOB, Überwachungsrecht Rz. 399; DERS., Erhebung von Daten, 256.

[181] Vgl. hierzu insb. BGer 1B_425/2010.

[182] HANSJAKOB, Überwachungsrecht, Rz. 400; DERS., Erhebung von Daten, 257.

[183] HANSJAKOB, Überwachungsrecht, Rz. 401; DERS., Erhebung von Daten, 257.

[184] Dies gilt als herrschende Praxis in Deutschland, wonach das Ersuchen Deutschlands an einen anderen Staat die (deutsche) Rechtsgrundlage, die Eingriffsvoraussetzungen und die richterliche Anordnung für die entsprechende Überwachungsmassnahme beinhalten muss, vgl. dazu BRODOWSKI, 389–390.

[185] HANSJAKOB, Überwachungsrecht, Rz. 402; DERS., Erhebung von Daten, 257.

Rechtshilfeweg massgeblich. Das Vorgehen des vierten Lösungsvorschlags lag dem Sachverhalt von BGE 141 IV 108 zugrunde: Die Staatsanwaltschaft wollte die Daten gestützt auf Art. 32 lit. b CCC direkt (d.h. ohne den Rechtshilfeweg zu beschreiten) einholen. Facebook USA behauptete jedoch, dass es sich bei der Datenerhebung nach Schweizer Recht um eine Randdatenerhebung i.S.v. Art. 273 StPO gehandelt habe, sodass eine Genehmigung des Zwangsmassnahmengerichts hätte vorgelegt werden müssen, wenn die Daten in den USA hätten erhoben werden sollen.[186] Sollen die Daten also innert nützlicher Frist erhältlich gemacht werden, bleibt gemäss HANSJAKOB nichts anderes übrig, als eine Bestätigung vom Schweizer Zwangsmassnahmengericht einzuholen, dass die Datenerhebungsmassnahme in der Schweiz genehmigungsfähig ist. Folglich spricht für HANSJAKOB auch nichts dagegen, dass das Zwangsmassnahmengericht eine solche Bestätigung ausstellen darf. Umgekehrt ist es auch so, dass bspw. den Rechtshilfeersuchen aus Deutschland eine entsprechende Bestätigung des zuständigen Zwangsrichters zur Durchführung der in der Schweiz beantragten Massnahme beigelegt wird.[187]

[186] BGE 141 IV 108, insb. E. 3, 5.3.

[187] HANSJAKOB, Überwachungsrecht, Rz. 402; DERS., Erhebung von Daten, 257. M.E. ist das Vorgehen von HANSJAKOB zu begrüssen, weshalb einer vorläufigen Bestätigung des Schweizer Zwangsmassnahmengerichts nichts entgegenstehen sollte.

2. Übereinkommen zur Bekämpfung von Cybercrime

Ein Rechtshilfeverfahren gestaltet sich regelmässig aufwändig, kompliziert und langwierig, wobei einige Staaten keine oder nur eine relativ kurze Frist für die Vorratsdatenspeicherung hinsichtlich der rückwirkenden Randdatenerhebung kennen. Demnach besteht das Risiko, dass die gesetzliche Überwachungsfrist abläuft, noch bevor über ein hängiges Rechtshilfegesuch entschieden werden konnte.[188] Abhilfe diesbezüglich schafft das CCC indem es spezifische Instrumente vorsieht, darunter die vorsorgliche umgehende Sicherung gespeicherter Computer- und Verkehrsdaten (Art. 29 CCC) sowie einen direkten grenzüberschreitenden Zugriff in jenen Fällen erlaubt, in denen die berechtigte Person dem Zugriff zustimmt (Art. 32 lit. b CCC).[189] Zweck des Übereinkommens ist die wirksame Bekämpfung von Computerkriminalität. Um den Zweck des Übereinkommens bestmöglich zu erfüllen, werden die zwischen den Mitgliedsstaaten bestehenden bi- oder multilateralen Verträge (wie bspw. das EÜR, RVUS) insoweit ergänzt, als dass eine gut funktionierende und zügige internationale Zusammenarbeit in Strafsachen gewährleistet werden soll.[190]

A. Grenzüberschreitender Zugriff auf Computerdaten (Art. 32 CCC)

Gemäss Art. 32 CCC darf die Strafverfolgungsbehörde eines Staates ohne die Genehmigung eines anderen Staates auf öffentlich zugängliche gespeicherte Computerdaten[191] (offene Quellen) zugreifen, unabhängig davon, wo sich die Daten geografisch befinden (lit. a); oder auf gespeicherte Computerdaten, die sich im Hoheitsgebiet eines anderen Staates 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 (lit. b).

Lit. a von Art. 3 CCC bezieht sich auf öffentlich zugängliche Daten wie beispielsweise öffentliche Facebook-Profile, Postings auf Facebook, Twitter oder auf Websites. Lit. b hingegen bezieht sich auf nicht öffentliche (insb. passwortgeschützte) Daten (z.B. Daten eines E-Mail- oder nicht öffentlichen Facebook-Kontos). Nicht öffentliche Daten können mit freiwilliger Zustimmung der Person, die rechtmässig zur Herausgabe befugt ist, mittels Online-Zugriff oder Empfang (E-Mail etc.) beschafft werden.[192] Eine konkludente freiwillige Zustimmung liegt dann vor, wenn die angefragte (berechtigte)

---

[188] FORSTER, 617; SEITZ, 355–357; BGE 141 IV 108, E. 5.5.

[189] FORSTER, 617–618.

[190] FORSTER, 615–616.

[191] „Computerdaten“ i.S. des Übereinkommens umfassen „jede Darstellung von Tatsachen, Informationen oder Konzepten in einer für die Verarbeitung in einem Computersystem geeigneten Form einschliesslich eines Programms, das die Ausführung einer Funktion durch ein Computersystem auslösen kann“, vgl. Art. 1 lit. b CCC.

[192] HEIMGARTNER, Internetstraffälle, 146; SCHWEINGRUBER, Rz. 10–12.

Person die Daten ohne Weiteres herausgibt. Wer als zustimmungsberechtigt i.S.v. Art. 32 lit. b CCC gilt, ergibt sich aus den tatsächlichen Umständen der Person selbst und aus dem anwendbaren Recht des Handlungsortes[193]. Gemäss der Botschaft des Bundesrats über die Genehmigung und Umsetzung des Übereinkommens ist Art. 32 lit. b CCC wegen der Gefahr von Missbräuchen unter Umgehung der Rechtshilfe und zum Schutz der Privatsphäre Dritter eng auszulegen, wonach es für die Anwendbarkeit von lit. b die freiwillige Zustimmung einer Person *im Inland* braucht.[194]

Im Grundsatzurteil BGE 141 IV 108 widerspricht das Bundesgericht der Meinung des Bundesrates, wonach es *keiner* Zustimmung einer rechtmässig zur Herausgabe befugten Person *im Inland* bedarf. Würde die Zustimmung einer Person im Inland verlangt, würden die Hauptziele des Übereinkommens (Verbesserung der Bekämpfung der grenzüberschreitenden Cyberkriminalität, Erleichterung der Rechtshilfe bzw. partielle Lockerung des Erfordernisses des förmlichen Rechtshilfewegs) unterlaufen werden. Regelmässig ist auch eine zustimmungsberechtigte inländische Person gar nicht auffindbar, was zur Konsequenz hätte, dass ein Zugriff mittels Art. 32 lit. b CCC auf ausländische E-Mail- oder Social-Media-Konten praktisch unmöglich wäre. Gemäss BGer kommen also auch ausländische Personen und Gesellschaften als Zustimmungsberechtigte i.S.v. lit. b in Frage.[195]

Ob eine konkrete Person rechtmässig über bestimmte Daten verfügen und sie herausgeben darf, beurteilt sich nach dem nationalen Recht des Staates, in welchen die betroffene Person handelt. Namentlich sind ausländische Internetprovider bzw. Anbieterinnen von sozialen Netzwerken (Service Provider), welche sich in ihren Allgemeinen Nutzungsbedingungen bzw. Datenverwendungsrichtlinien ein Weiterleitungsrecht von Daten an in- und ausländische Strafverfolgungsbehörden gegenüber ihren Kunden ausbedungen haben, herausgabeberechtigt[196].[197] Gemäss FORSTER, HEIMGARTNER und SEITZ können auch die inländischen Inhaberinnen von E-Mail-Konten und inländische Kundinnen von sozialen Netzwerken direkt ihre Zustimmung zur Datenherausgabe geben. Eine zusätzliche Zustimmung der ausländischen Providerfirma ist nicht notwendig. Internetnutzende sind sich denn oft gar nicht bewusst, in welchem Land ihre Daten gespeichert werden. Regelmässig werden die Daten des Internetverkehrs im Ausland (oft in den USA) gespeichert. Im Übrigen können sich mittels Art. 32 lit. b CCC auch im Inland agierende Tochter- oder Partnergesellschaften von ausländischen Providern einverstanden erklären, Daten herauszugeben, die im Ausland (bei der Muttergesellschaft) gespeichert sind. Speichern die Schweizer Töchter oder Partner die Daten jedoch in der Schweiz (sog. „Server Farms"), kommt das schweizerische Landesrecht (StPO/BÜPF) zur Anwendung.[198]

---

[193] Explanatory Report No. 185, Ziff. 294.

[194] BBl 2010 4697, 4737–4738.

[195] BGE 141 IV 108, E. 5.9–5.10; FORSTER, 619.

[196] Vgl. dazu Explanatory Report No. 185, Ziff. 294.

[197] BGE 141 IV 108, E. 5.9–5.10; vgl. dazu auch FORSTER, 619.

[198] FORSTER, Fn. 14; HEIMGARTNER, Internetstraffälle, 146; SEITZ, 370–371; MORSCHER, 214–215.

Die m.E. zu begrüssende Argumentation des Bundesgerichts und der Autoren verdeutlicht, dass nicht lediglich auf eine Zustimmung einer sich im Inland befindlichen Person abgestellt werden darf. Würde der Ansicht des Bundesrates gefolgt, würde Art. 32 lit. b CCC in der Praxis nur selten zur Anwendung gelangen, was dem Ziel und Zweck des Übereinkommens zuwiderlaufen würde.

B. Anordnung zur Herausgabe von Bestandesdaten (Art. 18 CCC)

Gemäss Art. 18 Abs. 1 lit. a CCC kann die zuständige Strafverfolgungsbehörde jede Person dazu verpflichten, sich in ihrem Besitz befindliche, gespeicherte Computerdaten herauszugeben. Diese Bestimmung deckt sich mit Art. 263 ff., insb. Art. 265 StPO. Lit. a bezieht sich auf Personen, die sich im Hoheitsgebiet des Vertragsstaats befinden. Gemäss Abs. 18 lit. b CCC werden Dienstanbieterinnen[199], die ihre Dienste im Hoheitsgebiet des Vertragsstaats *anbieten*, verpflichtet, auf Anordnung der zuständigen Strafverfolgungsbehörden Bestandesdaten[200], jedoch keine Verkehrs-[201] oder Inhaltsdaten, mitzuteilen.[202]

Art. 18 CCC richtet sich an den inländischen Gesetzgeber und verpflichtet die Vertragsstaaten, Massnahmen zu erlassen, die es den inländischen Strafverfolgungsbehörden ermöglichen, auf inländische Bestandesdaten zuzugreifen. Diese Massnahmen stehen sowohl für inländische Ermittlungen als auch für den Vollzug von Rechtshilfeersuchen zur Verfügung.[203] Derweil ergibt sich aus Art. 18 Abs. 1 lit. b CCC kein zusätzlicher Anspruch (über Art. 32 CCC hinaus) auf grenzüberschreitende Datenerhebung[204]. Die Heraushabe der Daten hat auf dem Rechtshilfeweg zu erfolgen.[205]

---

[199] Unter „Dienstanbieterinnen" sind „Service Provider" zu verstehen, vgl. Explanatory Report No. 185, Ziff. 26.

[200] „Bestandesdaten" im Sinne von Art. 18 Abs. 3 CCC sind „alle in Form von Computerdaten oder in anderer Form enthaltene Informationen, die bei einem Dienstanbieter über Teilnehmer seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten, und durch die die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Massnahmen und die Dauer des Dienstes (lit. a); die Identität des Teilnehmers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen (lit. b); andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen (lit. c)". Dazu gehört z.B. die Identität des Kunden, vgl. BBl 2010 4697, 4720.

[201] „Verkehrsdaten" i.S.v. Art. 1 lit. d CCC sind „alle Computerdaten in Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum, der Umfang oder die Dauer der Kommunikation oder die Art des für die Kommunikation benutzten Dienstes hervorgeht".

[202] BBl 2010 4697, 4720.

[203] ROTH, Rz. 52–53.

[204] Vgl. dazu ausführlich Kap. III./3./B.

[205] BGE 141 IV 108, E. 6.4; FORSTER, 619; GRAF, Jusletter IT, Rz. 35, Fn. 62.

3. Bekämpfung von Cybercrime im Konflikt mit dem Territorialitätsprinzip

Im technisch dynamischen und hoch komplexen Bereich der Internetkriminalität stellt sich die Frage, wo die Grenzen zwischen innerstaatlichen und grenzüberschreitenden Strafverfolgungsmassnahmen zu ziehen sind. In welchem Rahmen können die Strafverfolgungsbehörden die Anbieterinnen direkt zur Mitwirkung verpflichten (mittels Beschlagnahme, eines Editionsbefehls oder einer Überwachung) und ab wann gilt die Convention on Cybercrime oder der formelle Rechtshilfeweg? Inwieweit verletzen bestimmte hoheitliche Handlungen die Souveränität eines ausländischen Staates? Ist eine wirksame Bekämpfung von (grenzüberschreitender) Cyberkriminalität stärker zu gewichten, als das Territorialitätsprinzip? Und, darf unter bestimmten Voraussetzungen letzteres verletzt werden? Zur Beantwortung dieser heiklen Fragen werden ausgewählte Bundesgerichtsentscheide und verschiedene Lehrmeinungen diskutiert, wobei auch die eigene Meinung der Autorin dargelegt wird.

A. Grenzüberschreitender direkter Zugriff auf Daten oder Rechtshilfeweg?

Das Bundesgericht musste sich in mehreren Entscheiden mit der Frage auseinandersetzen, ob eine grenzüberschreitende Untersuchungshandlung das Territorialitätsprinzip bereits verletzte oder noch zulässig war: In BGE 141 IV 108 ging es darum, ob die Staatsanwaltschaft direkt von Facebook USA die Herausgabe von „IP-Histories" verlangen durfte. Es entschied, dass für die Herausgabe der „IP-History" eine rechtmässige und freiwillige Zustimmung einer herausgabeberechtigen Person hätte vorliegen müssen (Art. 32 lit. b CCC).[206] Den Meinungen von FORSTER, HEIMGARTNER und SEITZ folgend, kommen neben dem ausländischen Internet Service Provider auch die inländische Inhaberin oder Kundin des entsprechenden (E-Mail- oder Social Media-)Kontos als zustimmungsberechtigte Personen infrage.[207] Im gegenständlichen Fall lag jedoch keine Zustimmung der inländischen Kundinnen (oder einer anderen berechtigten Person) vor, weil diese mittels der Datenerhebung erst hätten identifiziert werden müssen. Es galt also, den förmlichen Rechtshilfeweg zu beschreiten.[208]

In BGE 143 IV 21 hatte das Bundesgericht zu entscheiden, ob die Gesellschaft Facebook Switzerland Sàrl (Facebook Schweiz) zur Edition von Daten eines Facebook-Kontos (u.a. IP-Adressen und Inhaltsdaten) an die Staatsanwaltschaft verpflichtet war. Facebook Schweiz verweigerte die Herausgabe mit der Begründung, dass es in der Schweiz nicht die Plattform, sondern nur die Abwicklung des Werbemarktes verwaltet habe bzw. lediglich für die Entwicklung des schweizerischen Marktes für Werbeauftritte zuständig gewesen sei. Facebook Ireland Ltd. (Facebook Irland), wo die Daten gespei-

---

[206] BGE 141 IV 108, E. 5.9; vgl. auch die Ausführungen in BGE 143 IV 270, E. 4.7.

[207] Vgl. dazu bereits oben, Kap. III./2./A. FORSTER, 619, insb. Fn. 14; SEITZ, 371; HEIMGARTNER, Internetstrafälle, 146.

[208] BGE 141 IV 108, E. 5.11–5.12; FORSTER, 619, Fn. 14.

chert werden, gab an, dass der Editionsbefehl auf dem Weg der internationalen Rechtshilfe hätte gestellt werden müssen.[209]

Das Bundesgericht stellte zuerst fest, dass Facebook als Social Media nicht unter das BÜPF und somit auch nicht unter Art. 269 ff. StPO gefallen sei.[210] Weder Facebook Schweiz noch Facebook Irland (oder Facebook USA) seien Fernmeldedienstanbieterinnen i.S.v. Art. 1 Abs. 1 und 2 aBÜPF noch Internetzugangsanbieterinnen i.S.v. Art. 1 Abs. 2 aBÜPF i.V.m. Art. 1 Abs. 2 lit. e aVÜPF gewesen. Zu Recht war also Art. 265 StPO zu prüfen, der an die jeweilige in der Schweiz domizilierte Dateninhaberin bzw. -verwalterin zu richten war. Da Facebook Schweiz jedoch über keinen direkten Zugang oder keine Herrschaft über die entsprechenden Daten verfügt habe, habe der Editionsbefehl nicht in der Schweiz erfolgen können. Auch ein Zugriff gestützt auf das Cybercrime Übereinkommen sei wegen derselben Begründung nicht infrage gekommen[211]. Vielmehr werde der Dienst Facebook von den amerikanischen und irländischen Gesellschaften kontrolliert. Facebook Irland sei alleinige Vertragspartei mit den ausserhalb der USA und Kanada wohnhaften Facebook-Nutzenden und kontrolliere auch allein die Personendaten. Das BGer kam also zum Schluss, dass der Weg der internationalen Rechtshilfe in Strafsachen zu beschreiten war.[212] Nicht ausdrücklich beantwortet wurde aber die Frage, ob ein Editionsbefehl bei Facebook Schweiz möglich gewesen wäre, hätte Facebook Schweiz eine Zugriffsmöglichkeit bzw. -berechtigung auf die in Irland gespeicherten Daten gehabt.[213]

Im gleichentags erschienenen Entscheid hatte das Bundesgericht zu beurteilen, ob die Google Switzerland GmbH mit Sitz in Zürich (Google Schweiz) über Maildaten der Schweizer Kunden verfügte. Wäre dies bejaht worden, hätten die Daten (u.a. IP-Adressen, Verbindungsprotokolle, Inhaltsdaten) durch die zuständige Staatsanwaltschaft Waadt beschlagnahmt werden können; andernfalls wäre der Rechtshilfeweg massgeblich gewesen. Google Schweiz wehrte sich gegen den von der Staatsanwaltschaft erlassenen Beschlagnahmebefehl und machte geltend, dass sie gar nicht passivlegitimiert gewesen sei. Das E-Mail-System von Google werde in Kalifornien von der Google Inc. betrieben. Einzig die in den USA ansässige Google Inc. verfüge über die erforderlichen Daten, so dass die gegenseitige Rechtshilfe hätte ergriffen werden müssen. Die Beschwerdekammer des Kantonsgerichts Waadt ent-

[209] Vgl. dazu den Sachverhalt in BGE 143 IV 21, 21–22.

[210] Damit hat das BGer seine Praxis wiederholt bestätigt, vgl. auch bspw. BGE 143 IV 270, E. 7.1; 141 IV 108, E. 5.13; 143 IV 21, E. 3.1; BGer 1B_142/2016, E. 3.1.

[211] Das BGer stellt folgende Regelung auf: „Aus den Bestimmungen der CCC [...] als auch der StPO [...] ergibt sich [...], dass die vom Herausgabebefehl betroffene Person der Inhaber oder der Besitzer der betreffenden Daten sein oder zumindest die Kontrolle darüber haben muss, das heisst tatsächlich und rechtlich eine Verfügungsgewalt über die Daten haben muss."

[212] BGE 143 IV 21, E. 3.1, 3.4; vgl. auch die Ausführungen in BGE 143 IV 270, E. 4.8.

[213] GRAF, Jusletter IT, Rz. 27

schied jedoch, dass Google Schweiz passivlegitimiert gewesen sei und die entsprechenden Daten habe herausgeben müssen. Daraufhin erhob Google Schweiz Beschwerde beim Bundesgericht.[214]

Auch in diesem Entscheid stellte das Bundesgericht zuerst fest, dass Google als Anbieterin eines abgeleiteten Internetdienstes unter altem Recht nicht dem BÜPF und den Art. 269 ff. StPO unterstanden habe. Art. 265 StPO war deshalb einschlägig.[215] Das BGer kam zum Schluss, dass die Frage, ob Google Schweiz einen direkten Zugang oder Herrschaft über die Daten ausgeübt habe, nicht abschliessend geklärt worden sei, weshalb es die Vorinstanz anwies, die Frage zu klären.[216] Das BGer ging im Google-Entscheid also einen Schritt weiter als in BGE 143 IV 21 und erlaubte die Edition sämtlicher (auch ausländischer) Daten, auf welche die Anbieterin zugreifen konnte[217]. Gemäss der hier vertretenen Auffassung hätten (wäre eine Zugriffsberechtigung bejaht worden) Google und Facebook Schweiz ihre Zustimmung zur Herausgabe der im Ausland gespeicherten Daten geben dürfen[218].

GRAF und HEIMGARTNER können der bundesgerichtlichen Auffassung, soweit sie sich auf die schweizerische StPO stützt, nicht folgen: „Eine inländische Person darf nicht gestützt auf inländisches Strafprozessrecht verfügungsweise aufgefordert werden, für die Strafverfolgungsbehörden im Ausland verfügbare Beweismittel zu beschaffen, auch wenn es sich dabei um Daten handelt, hinsichtlich derer sie zugriffsberechtigt ist“[219]. Mittels dieses Vorgehens werde eine Privatperson für staatliche Zwecke instrumentalisiert und die internationale Rechtshilfe unterlaufen. Demzufolge sind für GRAF Zwangsmassnahmen, die sich an in- oder ausländische Internetdienste richten, unzulässig, sofern dies das Rechtshilferecht nicht zulässt.[220] Ein direkter (eigenhändiger) Zugriff der Strafverfolgungsbehörden auf im Ausland gespeicherte Daten sei nur insoweit zulässig, als dass es sich bei den Daten, auf die zugegriffen wird, um öffentlich zugängliche Daten handle. Hier bestehe keine Zwangsausübung, weshalb auf solche Daten im Ausland frei zugegriffen werden könne. Werde auf nicht öffentlich zugängliche (insb. passwortgeschützte) Daten im Ausland zugegriffen, wirke sich dies mit hoher Intensität auf das ausländische („digitale“) Hoheitsgebiet aus.[221] Ein grosser Teil der Lehre wertet einen Zugriff von Ermittlungsbehörden auf im Ausland befindliche Daten als Eingriff in fremdes Hoheitsgebiet. An die

[214] Urteil 1B_142/2016, Sachverhalt, E. 3, 3.6; vgl. dazu auch Chambre des recours pénal VD 2014/540.

[215] Urteil 1B_142/2016, E. 3.1.

[216] Urteil 1B_142/2016, E. 3.6, 4.

[217] Die Argumentation des Bundesgerichts bezieht sich auf eine Edition mittels Art. 18 Abs. 1 lit. b CCC (bzw. Art. 265 StPO). Dass Art. 18 Abs. 1 lit. b CCC keinen Anspruch auf grenzüberschreitende Bestandesdatenerhebung gewährt, wurde bereits oben, Kap. III./2./B., kurz angesprochen und wird in Kap. III./3./B. nochmals diskutiert.

[218] Gl.M. FORSTER, Fn. 14; SEITZ, 371; BURGERMEISTER, 37, 40. Dazu folgen jedoch unten, Kap. III./3. und IV./2., noch weitere Ausführungen.

[219] GRAF, Jusletter IT, Rz. 28.

[220] GRAF, Jusletter IT, Rz. 28; gl.M. ist auch HEIMGARTNER, Beschlagnahme, 266–267.

[221] GRAF, Rz. 29–30; HEIMGARTNER, Beschlagnahme, 266–267.

Daten könne bloss mittels internationaler Rechtshilfe oder direkt, falls dies ein internationales Übereinkommen vorsehe, gelangt werden.[222]

Einzelne Stimmen[223] fordern jedoch auch eine weniger strenge Beachtung des Territorialitätsprinzips und tolerieren einen grenzüberschreitenden direkten Zugriff auf Datenverarbeitungs- und Speicherungsanlagen im Ausland. Die Durchsuchung und Sicherstellung von im Ausland befindlichen Daten durch Schweizer Behörden stelle keine Souveränitätsverletzung dar. Als Begründung wird auf das sog. *Zugriffsprinzip*, welches die Folge der Unkörperlichkeit von elektronischen Daten ist, abgestellt. Danach liegt die Datenherrschaft bei derjenigen Person, welche zugriffsberechtigt ist, und nicht bei derjenigen, die sich im physischen Besitz des Datenträgers befindet.[224] SCHMID hat die Problematik bereits 1993 erkannt und sich wie folgt dazu geäussert: „Werden internationale Datenübertragungs- und Verarbeitungsnetze mit direkten Zugriffsmöglichkeiten betrieben, so wird von der jeweils betroffenen nationalen Gesetzgebung toleriert, dass die Informationen nicht nur am Ort, an dem sie primär gespeichert sind, sondern auch jederzeit in anderen Ländern abgerufen werden können. Daraus könnte gefolgert werden, dass keine Verletzung der nationalen Souveränität vorliegt, wenn nun nicht die Datenberechtigten selbst, sondern die Strafverfolgungsbehörden von dieser grenzüberschreitenden, ubiquitären Verfügbarkeit der Daten Gebrauch machen“[225]. Aufgrund der heutigen stets zunehmenden Internationalisierung der Datenverarbeitung kann diese Argumentation m.E. mehr denn je Geltung beanspruchen[226].

Auch wenn nun die Anbieterinnen abgeleiteter Kommunikationsdienste neu dem BÜPF unterstellt sind, besteht das Problem der grenzüberschreitenden Datenerhebung weiter. So hat auch der Bundesrat in der Botschaft zum BÜPF betont, dass keine allzu grossen Hoffnungen in die Ausweitung des persönlichen Geltungsbereichs gesetzt werden sollen, weil viele bedeutende Anbieterinnen abgeleiteter Internetdienste ihren Sitz und ihre Infrastruktur im Ausland haben[227]. Sie könnten also nicht zur Mitwirkung verpflichtet werden, auch dann nicht, wenn sie eine in der Schweiz ansässige Vertretung hätten, solange die Daten dort nicht verwaltet würden.[228] HANSJAKOB formuliert einen Lösungsvorschlag, mit welchem die Problematik der strafprozessualen Überwachung ausländischer Internetdienstanbieterinnen entschärft würde: Und zwar könnten ausländische Anbieterinnen von Internetdiensten dazu

---

[222] U.a. RYSER, 575–576; HEIMGARTNER, Internetstraffälle, 136; DERS., Beschlagnahme, 93; AEPLI, 130–131, der jedoch erwähnt, dass zum Zeitpunkt seiner Dissertation (2004) noch von einer Souveränitätsverletzung habe ausgegangen werden müssen.

[223] BANGERTER, 280–282, der sich auf den Ansatz von SCHMID, 108–109, bezieht. Gl.M. ist auch BURGERMEISTER, 22–23.

[224] BANGERTER, 281–282; gl.M. BURGERMEISTER, 22–23; SEITZ, 356; ansatzweise auch FORSTER, Fn. 14.

[225] SCHMID, 109.

[226] Gl.M. auch BANGERTER, 281.

[227] BBl 2013 2683, 2708, als Beispiel werden im Ausland eröffnete E-Mail-Konten, die von Personen mit Wohnsitz in der Schweiz eröffnet wurden, genannt.

[228] HANSJAKOB, Überwachungsrecht, Rz. 1367.

verpflichtet werden, einen Sitz in der Schweiz zu eröffnen, der die Daten von Nutzern in der Schweiz verwaltet oder zumindest Zugang zu ihnen hat.[229]

B. Aufweichung des Territorialitätsprinzips durch die Convention on Cybercrime

Art. 31 Abs. 1 CCC sieht explizit den Rechtshilfeweg für die Durchsuchung, Sicherstellung und Beschlagnahme sowie die Weitergabe von Daten, die auf Computersystemen gespeichert sind, welche sich im Hoheitsgebiet einer anderen Vertragspartei befinden, vor. Gemäss GRAF haben die Vertragsstaaten damit nicht das Territorialitätsprinzip zugunsten eines Zugriffsprinzips aufweichen wollen.[230] Mit Art. 32 CCC wurde eine Grundlage geschaffen, mittels derer auf die Notwendigkeit eines Rechtshilfeersuchens in zwei Konstellationen verzichtet werden kann[231]. Die Vertragsstaaten haben somit verbindlich festgelegt, unter welchen Umständen ein Staat direkt auf im Ausland befindliche Daten zugreifen kann und wann ein förmliches Rechtshilfeersuchen zu stellen ist. Dies impliziert nach Auffassung von GRAF, dass der Zugriff auf ausländische Daten prinzipiell als Eingriff in die Territorialität zu werten sei. Eine Verletzung des Territorialitätsgrundsatzes sei v.a. dann anzunehmen, wenn ein solches Verhalten in seinen Wirkungen einem Hoheitsakt direkt auf fremdem Staatsgebiet gleichkomme.[232] Sodann hat das Bundesgericht noch im Jahre 2015 anerkannt, dass sich die Vertragsstaaten mit Art. 32 CCC auf einen minimalen (restriktiven) Konsens für einen grenzüberschreitenden Zugriff geeignet hätten.[233] Es hielt insbesondere fest, dass „aus Art. 23, 25 Abs. 4 und Art. 39 Abs. 3 CCC folgt, dass in allen Fällen, bei denen die (Ausnahme-) Voraussetzungen von Art. 32 CCC nicht gegeben sind, die fragliche Datenerhebung bzw. rückwirkende Überwachung im Ausland auf dem förmlichen Rechtshilfeweg [...] zu beantragen ist. Die Vertragsstaaten des Übereinkommens haben sich

---

[229] Vgl. dazu HANSJAKOB, Überwachungsrecht, Rz. 1369.

[230] GRAF, Jusletter IT, Rz. 24, 34.

[231] Einerseits ist ein direkter Zugriff dann zulässig, wenn die Daten öffentlich zugänglich sind (Art. 32 lit. a CCC), und andererseits, wenn die rechtmässige und freiwillige Zustimmung einer herausgabeberechtigten Person vorliegt (Art. 32 lit. b CCC), vgl. dazu oben, Kap. III./2./A.

[232] GRAF, Jusletter IT, Rz. 36. DOMBROWSKI macht eine Unterscheidung zwischen „Hoheitsakten auf fremdem Staatsgebiet“ und „extraterritorialen Hoheitsakten“. Generell unzulässig seien Hoheitsakte, die ohne Einwilligung durch auf fremdem Staatsgebiet physisch befindliche staatliche Behörden vorgenommen werden. Es liege ein Eingriff in die Souveränität des anderen Staates vor. Um einen extraterritorialen Hoheitsakt handle es sich, wenn die hoheitliche Handlung zwar auf eigenem Staatsgebiet erfolge, die Handlung sich jedoch auf ein fremdes Hoheitsgebiet auswirke. Im Gegensatz zu den Hoheitsakten auf fremdem Staatsgebiet könnten extraterritoriale Hoheitsakte u.U. zulässig sein. Ein extraterritorialer Hoheitsakt ist nach DOMBROWSKI insb. dann rechtswidrig, „wenn er die Gebietshoheit des fremden Staates unmittelbar verletzt, *der Hoheitsakt in seinen Wirkungen einem Hoheitsakt auf fremdem Staatsgebiet gleichkommt* oder die Sicherheit und Ordnung des fremden Staates beeinträchtigt“ (Hervorhebung durch die Verfasserin). Als Beispiel für einen extraterritorialen Hoheitsakt nennt DOMBROWSKI den Zugriff auf Computersysteme im Ausland. Ein extraterritorialer Hoheitsakt gelte nur dann als zulässig, wenn er die Voraussetzungen von Art. 32 CCC erfülle. Vgl. zum Ganzen DOMBROWSKI, 12–14, 143 ff.

[233] BGE 141 IV 108, E. 5.9.

(über die Bestimmungen von Art. 32 CCC hinaus,) nicht auf weitergehende „extraterritoriale" Zugriffe von Strafverfolgungsbehörden einigen können"[234].

Das Bundesgericht ist in BGE 143 IV 270[235] einer gegenteiligen Ansicht (insbesondere jener von BANGERTER[236]) gefolgt, indem es das Zugriffsprinzip als Begründung für die Zulässigkeit einer Durchsuchung und Beschlagnahme von im Ausland befindlichen Daten durch die Schweizer Behörden heranzog. Demnach soll die Zulässigkeit eines (direkten) Online-Zugriffs von der Rechtsmässigkeit der inländischen Ermittlungshandlung abhängen. Das BGer begründete seinen Entscheid folgendermassen: „Wer über einen Internetzugang im Inland einen abgeleiteten Internetdienst benutzt, der von einer ausländischen Firma angeboten wird, handelt nicht im „Ausland". Auch der blosse Umstand, dass die elektronischen Daten des betreffenden abgeleiteten Internetdienstes auf Servern (bzw. Cloud-Speichermedien) im Ausland verwaltet werden, lässt eine von der Schweiz aus erfolgte gesetzeskonforme Online-Recherche nicht als unzulässige Untersuchungshandlung auf ausländischem Territorium (im Sinne der dargelegten Praxis) erscheinen"[237]. GRAF bringt diesbezüglich den Einwand vor, dass der Zugriff im Ausland Datenverarbeitungsvorgänge auslöse und nachvollziehbare Spuren im Zielstaat hinterlasse und demnach einen *grenzüberschreitenden* direkten Zugriff auf im Ausland gespeicherte Daten darstelle. Demzufolge argumentiert er, dass die Convention on Cybercrime einen grenzüberschreitenden direkten Zugriff auf im Ausland befindliche Daten bereits in beschränktem Masse erlaube und damit, (e contrario) jede darüberhinausgehende Beweisbeschaffung als Eingriff in die Souveränität des ausländischen Staates zu werten sei.[238]

Für GRAF erscheint es unbegreiflich, wieso die in BGE 141 IV 108 statuierte Praxis nun nicht mehr gelten soll. Würde der eben zitierte Entscheid eine implizite Praxisänderung darstellen, wäre eine solche nicht gerechtfertigt: Falls anerkannt werde, dass ein Zugriff auf im Ausland gespeicherte Daten über den Rechtshilfeweg erfolgen müsse, soweit Art. 32 CCC nicht anwendbar sei, bleibe kein Raum für die bundesgerichtliche Erwägung, dass die Strafverfolgungsbehörde in diesem Fall nicht im Ausland handle und der inländische Durchsuchungsbefehl demnach ausreiche. Nationale Durchsuchungsbefugnisse könnten derartige Eingriffe in fremde Souveränitätsrechte nicht rechtfertigen.[239]

HANSJAKOB sieht hinsichtlich der Tatsache, dass sich die Daten im zitierten Entscheid im Ausland befinden, kein echtes Problem: Sofern jeder private Nutzer die Daten einsehen könne, falls er einen

---

[234] BGE 141 IV 108, E. 5.12.

[235] In BGE 143 IV 270 haben die Strafverfolgungsbehörden die Zugangsdaten zu einem Facebook-Konto eines Untersuchungshäftlings in Erfahrung bringen können, weil der Häftling diese Daten aus dem Gefängnis schmuggeln wollte. In der Folge nahm die Polizei (im Auftrag der Staatsanwaltschaft) Zugriff auf die (im Ausland gespeicherten) Daten und stellte sie sicher. Vgl. zu diesem Fall auch oben, Kap. II./3./B./c.

[236] Vgl. dazu BANGERTER, 280–282.

[237] BGE 143 IV 270, E. 7.10.

[238] GRAF, Jusletter IT, Rz. 32.

[239] GRAF, Jusletter IT, Rz. 39.

Facebook-Zugang habe, so müsse dies auch für die Polizei möglich sein. Allenfalls lässt der Facebook-Entscheid den Weg einer aktiven Überwachung offen, wenn sich die Anbieterin eines abgeleiteten Internetdienstes zwar im Ausland befindet und dort auch die Daten verwaltet, aber die Erhebung der Daten mittels (rechtmässig erhobener) Zugangsdaten zum Konto ohne Mitwirkung der Anbieterin möglich ist. Wenn die Anbieterin dem Benutzer aus der Schweiz Zugang zu seinen eigenen Daten ermöglicht und wenn auch seine Kommunikationspartner in der Schweiz diese Daten ohne Weiteres abrufen können, ist nicht einzusehen, weshalb die Strafverfolgungsbehörden dies nicht auch tun dürfen, wenn sie die Zugangsdaten besitzen.[240]

Einen weiteren Ansatz schildert SCHWEINGRUBER in ihrem Artikel im Jusletter vom 10. November 2014. Sie erklärt das von Belgien vertretene Vorgehen: Nach Art. 43bis der belgischen Strafprozessordnung kann die Betreiberin eines elektronischen Kommunikationsnetzes („operator of an electric communications network") oder die Anbieterin eines elektrischen Kommunikationsdienstes („provider of an electronic communications service") verpflichtet werden, Auskunft über Daten zu geben, welche die Identifikation der Nutzerin ermöglichen. Dabei ist kein Rechtshilfeweg nötig. Die Bestimmung bezieht sich nicht nur auf Internet Service Provider in Belgien, sondern richtet sich an alle „operator" und „provider", die auf belgischem Territorium präsent sind bzw. ihre Dienste dort anbieten. SCHWEINGRUBER fordert eine weniger strenge Beachtung des Territorialitätsprinzips und sieht für das Schweizer Recht in Art. 18 CCC eine ähnliche Regelung wie Art. 43bis der belgischen Strafprozessordnung: Nach Art. 18 CCC hätten ausländische Internet Service Provider allfällige Bestandesdaten (ohne Rechtshilfeweg) herauszugeben, falls sie ihre Dienste im Vertragsstaat anböten. Sollten Verkehrsdaten von ausländischen Service Providern eingeholt werden, sei Art. 32 CCC zu prüfen. Seien auch die Voraussetzungen von Art. 32 CCC nicht erfüllt, so müsse schliesslich der ordentliche Rechtshilfeweg beschritten werden. Zwar biete das CCC bereits Instrumente, die das Territorialitätsprinzip stellenweise aufweichen, doch müssten in Zukunft noch weitere Möglichkeiten entwickelt werden, die einen schnellen Zugriff auf im Ausland gespeicherte Daten erlauben würden.[241]

Es stellt sich also auch die Frage, ob Art. 18 Abs. 1 lit. b CCC die Strafverfolgungsbehörden ermächtigt, grenzüberschreitend und direkt Bestandesdaten bei ausländischen Providern einzufordern. SCHWEINGRUBER, die sich dafür ausspricht, argumentiert, dass der Wortlaut von Art. 18 Abs. 1 CCC von „anordnen" spreche, wodurch die Strafverfolgungsbehörde die Provider direkt verpflichten könne, Daten herauszugeben. Dasselbe lasse sich aus dem Titel des Art. 18 „Anordnung zur Herausgabe" ableiten. Zudem wäre Art. 18 CCC obsolet, wenn doch der Rechtshilfeweg ergriffen werden müsste,

[240] HANSJAKOB, Überwachungsrecht, Rz. 329, 331.

[241] SCHWEINGRUBER, Rz. 33–45; gl.M. ist auch BURGERMEISTER, 40–41.

weil dann kein Grund mehr bestünde, die Modalitäten zur Erhebung von Bestandesdaten bei einer Dienstanbieterin speziell zu regeln.[242]

Das Bundesgericht hat in BGE 141 IV 108 festgehalten, dass eine Abfrage von ausländischen Bestandesdaten des Internetverkehrs nicht mittels Art. 18 Abs. 1 lit. b CCC (und somit über Art. 32 CCC hinaus) erfolgen dürfe. Das Rechtshilfeverfahren sei massgeblich.[243] In der Schweiz domizilierte Dienstanbieterinnen, zu denen auch die „Server Farms" von ausländischen Providern gehören, müssten die in der Schweiz gespeicherten Bestandesdaten gestützt auf Art. 14 Abs. 4 aBÜPF (neu Art. 21 BÜPF) herauszugeben.[244] Im Urteil 1B_142/2016 hat das Bundesgericht hingegen darauf hingewiesen, dass Art. 18 Abs. 1 lit. b CCC die Edition aller (auch ausländischer) Daten erlaube, auf welche die Verfügungsadressatin zugreifen könne.[245]

Die Argumente von SCHWEINGRUBER für eine grenzüberschreitende Datenerhebung mittels Art. 18 Abs. 1 lit. b CCC erscheinen m.E. allesamt nicht überzeugend. Auch wenn die bundesgerichtliche Rechtsprechung in Bezug auf die Auslegung von Art. 18 Abs. 1 lit. b CCC ambivalent ist, ist meiner Ansicht nach das Vorgehen in BGE 141 IV 108 zu bevorzugen. Art. 18 CCC bezieht sich auf die innerstaatlich zu erlassenden verfahrensrechtlichen Bestimmungen, die es den Strafverfolgungsbehörden ermöglichen, auf im Inland gespeicherte Bestandesdaten zuzugreifen. Dies dient einerseits den eigenen Ermittlungen der inländischen Behörden und andererseits dem Vollzug von Rechtshilfegesuchen. In systematischer und historischer Hinsicht wird klar ersichtlich, dass Art. 32 CCC den Minimalkonsens der Vertragsstaaten hinsichtlich grenzüberschreitenden Handelns darstellt. Es wäre folglich verwunderlich, wenn die Verfassenden der Konvention weitere Bestimmungen mit grenzüberschreitenden Befugnissen hätten einbauen wollen.[246] Weshalb Art. 18 CCC bei dieser Auslegung obsolet sein sollte, ist m.E. also nicht nachvollziehbar.

Auch GRAF spricht sich gegen die Argumentation von SCHWEINGRUBER aus und kritisiert darüber hinaus den Entscheid 1B_142/2016 des Bundesgerichts. Das Bundesgericht verkenne, dass Art. 18 CCC nicht self-executing sei und Art. 265 StPO keine extraterritorialen Befugnisse bereithalte. Würde Art. 18 CCC tatsächlich so interpretiert, dass er eine Ermächtigung zu einem grenzüberschreitenden direkten Zugriff auf im Ausland gespeicherte Bestandesdaten erlaube, bräuchte es hierfür eine Gesetzesänderung. Auch FORSTER und ROTH weisen zu Recht darauf hin, dass Art. 18 Abs. 1 lit. b CCC (über Art. 32 CCC hinaus) keine Grundlage für eine grenzüberschreitende Datenerhebung darstellt.[247]

---

[242] SCHWEINGRUBER, Rz. 25–27.

[243] BGE 141 IV 108, E. 6.4–6.5; gl.M. auch FORSTER, 619–620 und ROTH, Rz. 50–53.

[244] BGE 141 IV 108, E. 6.4.

[245] BGer 1B_142/2016, E. 3.6.

[246] ROTH, Rz. 51–53.

[247] GRAF, Jusletter IT, Rz. 35, Fn. 62; FORSTER, 619–620; ROTH, Rz. 44, 50–53.

Aufgrund der (bereits erwähnten) stetig voranschreitenden Digitalisierung und der damit einhergehenden Internationalisierung des Datenverkehrs stossen strafprozessuale Instrumente zur (grenzüberschreitenden) Beweisbeschaffung an ihre Grenzen. Das klassische Verständnis des Territorialitätsprinzips muss in diesem Bereich also überdacht werden und ggf. zugunsten einer effektiven Strafverfolgung zurücktreten.[248] Dementsprechend ist m.E. das Vorgehen des Bundesgerichts in BGE 143 IV 270 und die Aufweichung des Territorialitätsprinzips zugunsten des Zugriffprinzips zu begrüssen[249]. Der Erwägung, dass nicht im Ausland handle, wer über einen Internetzugang im Inland einen abgeleiteten Internetdienst benutze, der von einer ausländischen Firma angeboten werde, wird zugestimmt. Eine von Schweizer Strafverfolgungsbehörden von der Schweiz aus erfolgte Online-Recherche betreffend auf ausländischen Servern gespeicherter Daten tangiert folglich das Territorialitätsprinzip nicht.[250]

Eine Abweichung vom Territorialitätsprinzip ist unerlässlich, wenn in Zukunft eine effiziente Strafverfolgung im Bereich des Cybercrime gewährleistet sein soll. Dazu braucht es Rechtsgrundlagen, die den Strafverfolgungsbehörden einen schnellen, unkomplizierten und internationalen Zugriff auf Daten ermöglichen. Mit der Convention on Cybercrime wurden bereits erste Instrumente geschaffen, um an im Ausland liegende Daten zu kommen. Nichtdestotrotz sind weitere Lösungsansätze zu entwickeln, welche eine Aufweichung des Territorialitätsprinzips erlauben und für eine wirksame Strafverfolgung von Cybercrime sorgen[251].

---

[248] SCHWEINGRUBER, Rz. 2, 6; GRAF, Jusletter IT, Rz. 49; BANGERTER, 281.

[249] Auch der Erwägung des Bundesgerichts in BGer 1B_142/2016, E. 3.6, 4, dass Google Schweiz direkt herausgabeberechtigt sei, sofern ein direkter Zugang zu oder Herrschaft über die Daten bestünde, ist zuzustimmen. Die Datenherausgabe würde allerdings über Art. 32 lit. b CCC (und Art. 265 StPO), und nicht Art. 18 Abs. 1 lit. b CCC erfolgen.

[250] Vgl. dazu BGE 143 IV 270, E. 7.10.

[251] Die Staaten haben sich in der Präambel des CCC für eine wirksame Bekämpfung der Cyberkriminalität ausgesprochen. Erreicht werden soll dies durch zügig und gut funktionierende internationale Zusammenarbeit in Strafsachen. Die in dieser Arbeit diskutierte Problematik zur grenzüberschreitenden Bekämpfung von Internetkriminalität zeigt, dass Handlungsbedarf in diesem (äussert wichtigen) Bereich besteht. Das Problem wurde wohl erkannt und soll in einem Zusatzprotokoll zur Konvention, das den grenzüberschreitenden Zugriff der Strafverfolgungsbehörden auf Daten zum Gegenstand haben soll, geregelt werden. Vgl. dazu den Final Report T-CY, Rz. 144. Auch der Bundesrat hat das Problem erkannt und sich dafür ausgesprochen, dass das Problem der grenzüberschreitenden Datenerhebung durch internationale Kooperation zu lösen ist. Es soll im Rahme der Cybercrime Convention eine praxisgerechte Lösung gefunden werden. Vgl. dazu SRF, Facebook Schweiz soll Daten herausrücken.

IV. Bedeutung und Auswirkungen der Erkenntnisse auf die Praxis

In der vorliegenden Arbeit wurden zahlreiche Theorien zu den verschiedenen Arten der Daten, Datenerhebungen, Kommunikationsinfrastrukturen und -kanälen geführt. Des Weiteren wurde die Problematik zur grenzüberschreitenden Strafverfolgung von Cybercrime theoretisch beleuchtet und ausführlich diskutiert. Nun stellt sich jedoch die Frage, ob sich ein klar strukturiertes und verlässliches Vorgehen aus Theorie und Praxis herauskristallisieren lässt. Dieser Rechtsbereich ist durch eine technische und rechtliche Komplexität geprägt, die es bedeutend erschwert, einen Durchblick zu gewinnen. Deshalb bieten die folgenden zwei Unterkapitel die Möglichkeit, ein klares Verständnis in Form zweier strukturierter Schemas zu gewinnen.

1. Zwangsmassnahmen zur Datenerhebung in der Schweiz

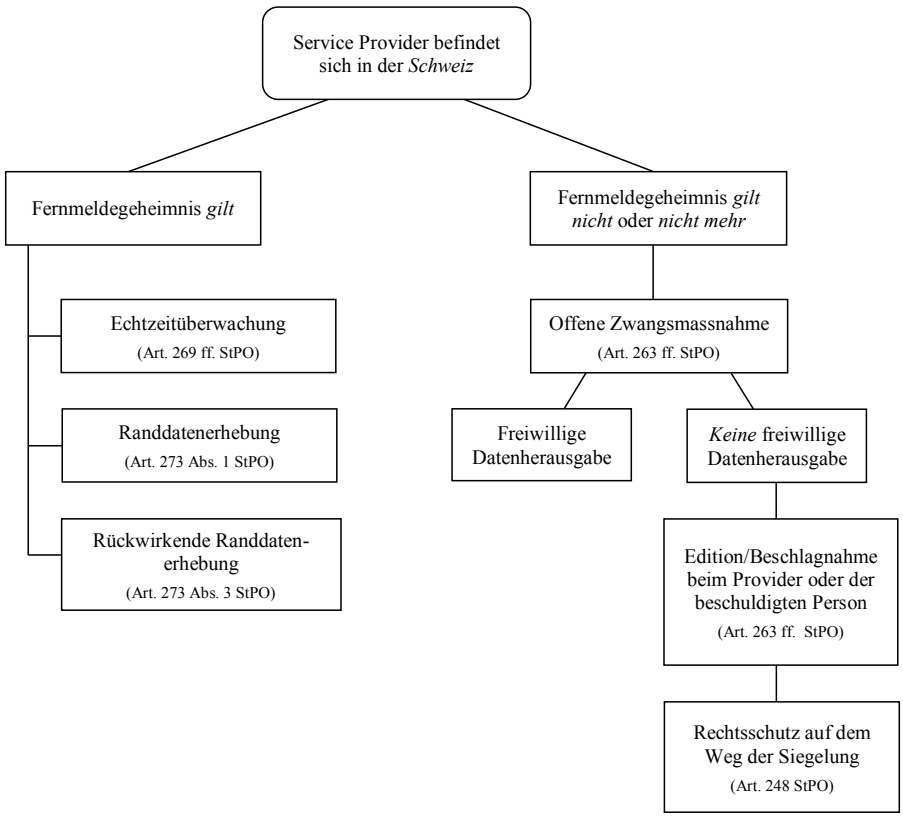


Abbildung 1: Schema Zwangsmassnahmen zur Datenerhebung in der Schweiz

Das dargestellte Schema bezieht sich auf die in dieser Arbeit untersuchten Anbieterinnen abgeleiteter Internetdienste, wie bspw. Facebook, Skype und Whatsapp. Wie bereits oben in Kapitel II./2./D./c. beschrieben, können die Anbieterinnen abgeleiteter Dienste als Anbieterinnen abgeleiteter Kommuni-

kationsdiene oder Fernmeldedienstanbieterinnen qualifiziert werden[252]. Je nach Kategorisierung treffen die Anbieterinnen unterschiedliche Pflichten. Auf die jeweiligen Pflichten wird in diesem Kapitel nicht näher eingegangen.[253]

In der gegenständlichen Arbeit wurden verschiedene Zwangsmassnahmen zur Datenerhebung des Internetverkehrs erklärt. Diese Zwangsmassnahmen lassen sich grob in zwei Kategorien aufteilen: Einerseits die *geheime* Überwachung nach Art. 269 ff. StPO und andererseits die *offene* (d.h. für die betroffene Person erkennbare) Edition/Beschlagnahme nach Art. 263 ff. StPO. Damit eine geheime Überwachung angeordnet werden kann, müssen bestimmte Voraussetzungen erfüllt sein, insbesondere muss es sich bei der zu überwachenden Kommunikation um *Fernmeldeverkehr* handeln, welcher den Schutz des *Fernmeldegeheimnisses* geniesst. Internetkommunikationen via E-Mail, Internettelefonie und Messenger (wie bspw. Syke, Whatsapp, Facebook-Messenger und Google) unterliegen grundsätzlich dem Fernmeldegeheimnis und sind als Fernmeldeverkehr zu qualifizieren. Charakteristisch für die *offenen* Zwangsmassnahmen ist, dass sie für die betroffene Person erkennbar sind und dass die zu erhebenden Daten nicht (oder nicht mehr) vom Fernmeldegeheimnis erfasst sind.[254]

Hinsichtlich des Fernmeldegeheimnisses gilt es also zu prüfen, ob dieses für die zu erhebenden Daten überhaupt gilt. Werden *Inhalts*-, *Verbindungs*- oder *Randdaten* erhoben, welche durch das Fernmeldegeheimnis geschützt sind, gelten die Regeln von Art. 269 ff. StPO und die Datenerhebung bedarf einer Genehmigung des Zwangsmassnahmengerichts; handelt es sich um eine *Bestandesdaten*erhebung (Art. 21 bzw. 22 BÜPF) kommen wiederum die Art. 263 ff. StPO zur Anwendung. Auskünfte nach Art. 21 BÜPF unterliegen nicht dem Fernmeldegeheimnis.[255]

Es wurde bereits mehrfach betont, dass das Bundesgericht regelmässig mit Abgrenzungsschwierigkeiten bei der Datenerhebung des Internetverkehrs zu kämpfen hat. Auch die gesetzliche Trennung der Datenarten bedient sich einer verwirrlichen Terminologie, weshalb eine klare Abgrenzung alles andere als einfach ist. Trotzdem wird vorliegend versucht, eine (klare) Trennung der Datenarten vorzunehmen:

Eine *Bestandesdatenerhebung* nach Art. 21 BÜPF liegt vor, wenn die Daten Auskunft über eine Vertragsbeziehung eines Kunden mit einer Anbieterin, über den Abonnenten eines bestimmten Anschlusses oder darüber, wer ein bestimmtes Gerät oder eine dynamische Internetadresse benutzt, geben. Wird eine Straftat über das Internet begangen, kommt Art. 22 BÜPF zur Anwendung. Ein bestimmter Internetverkehr kann einer IP-Adresse zugeordnet werden, wie ein bestimmter Telefonanruf einer Ruf-

[252] Als Oberbegriff für die Anbieterinnen abgeleiteten Dienste, wird der Begriff „Provider“ bzw. „Service Provider“ verwendet, dabei kann es sich fernmelderechtlich um Anbieterinnen i.S.v. Art. 2 lit. c oder lit. b BÜPF handeln.

[253] Vgl. dazu Kap. II./2./D./c.

[254] Vgl. dazu Kap. II./2./A.–D.

[255] Vgl. dazu Kap. II./3./A./a.–b.

nummer. Die Ermittlung dieser Registrierungsdaten (bzw. der „IP-History“) stellt in jenen Fällen eine *Bestandesdatenerhebung* dar, in denen der Strafverfolgungsbehörde bereits ein Internetanschluss oder eine E-Mail-Adresse bekannt ist und die Anbieterin nur die entsprechenden Registrierungsdaten herausgeben muss oder wenn eine bekannte statische IP-Adresse betroffen ist. Eine *Verbindungs-Randdatenerhebung* liegt demgegenüber vor, wenn der Strafverfolgungsbehörde lediglich strafbare Internetkommunikationsaktivitäten bekannt geworden sind und über die Verbindungs-Randdaten die zugewiesenen IP-Adressen und registrierten Kunden erst eruiert werden müssen. Die Erhebung der Verbindungs-Randdaten ist als Randdatenerhebung zu qualifizieren und fällt unter Art. 273 StPO. Randdaten können aktiv bzw. in Echtzeit (Art. 273 Abs. 1 StPO) oder rückwirkend (Art. 273 Abs. 3 StPO) erhoben werden. *Inhaltsdaten* geniessen den Schutz des Fernmeldegeheimnisses und dürfen nur nach Art. 269–272 StPO (geheim) in Echtzeit erhoben werden.[256]

Wurde nun festgestellt, dass es sich um Daten handelt, die grundsätzlich unter dem Schutz des Fernmeldegeheimnisses stehen, muss geprüft werden, ob das Fernmeldegeheimnis *noch* gilt. Ausschlaggebend hierfür ist der *Kommunikationsvorgang*. Wie das Bundesgericht in BGE 140 IV 181 zu Recht präzisiert hat, gilt das Fernmeldegeheimnis nur während des Kommunikationsvorgangs bzw. bis zum Zeitpunkt, indem die Empfängerin über die Nachricht verfügen kann; es ist eine genehmigungspflichtige Echtzeitüberwachung anzuordnen. Hat die Empfängerin die Nachricht abgerufen, kann die Nachricht beschlagnahmt werden. Befinden sich die (abgerufenen) Nachrichten noch auf dem Server des (Service) Providers, können sie dort beschlagnahmt werden. Nach bundesgerichtlicher Rechtsprechung liegt grundsätzlich auch keine Überwachung (oder rückwirkende Randdatenerhebung) vor, wenn bspw. Smartphones oder andere digitale Kommunikationsgeräte beschlagnahmt und die darauf gespeicherten Daten (also Verbindungsdaten, abgerufene SMS- oder E-Mail-Nachrichten etc.) ausgewertet werden. Der Rechtsschutz erfolgt auf dem Weg der Siegelung.[257]

Der einfachste Weg an die Daten zu gelangen ist eine *freiwillige* Datenherausgabe durch die beschuldigte Person. Dabei handelt es sich nicht um eine Zwangsmassnahme. Die beschuldigte Person kann im Rahmen einer Einvernahme ihre Benutzerdaten für bestimmte Benutzerkonten mitteilen oder die Daten selbst an die Strafverfolgungsbehörden herausgeben.[258] Mittels bekanntgegebener Benutzerdaten darf die Strafverfolgungsbehörde auf das entsprechende Benutzerkonto zugreifen und die Daten erheben. In diesem Fall steht der beschuldigten Person das Recht auf Siegelung zu.[259] Erfolgt keine freiwillige Herausgabe, ist eine Zwangsmassnahme anzuordnen.

---

[256] Vgl. dazu Kap. II./3./A./a.–c. und II./3./B./a.

[257] Vgl. dazu Kap. II./3./A./d und II./3./B./b. Die zum E-Mail-Verkehr entwickelte Rechtsprechung dürfte nun analog für die Kommunikation über abgeleitete Dienste gelten.

[258] AEPLI, 127 und BURGERMEISTER, 19.

[259] Vgl. dazu die Einführung zu Kap. II./2.

Der Strafverfolgungsbehörde stehen, im Rahmen der gegenständlich untersuchten Zwangsmassnahmen, acht Möglichkeiten der Datenerhebung zur Verfügung:

1. Es kann eine geheime inhaltliche Echtzeitüberwachung nach Art. 269–272 StPO angeordnet werden. Dabei werden Inhalts- und Randdaten in Echtzeit erhoben. Es bedarf einer Genehmigung des Zwangsmassnahmengerichts (Art. 272 Abs. 1 StPO).[260]

2. Es kann eine geheime Randdatenerhebung in Echtzeit nach Art. 273 Abs. 1 StPO angeordnet werden. Es bedarf einer Genehmigung durch das Zwangsmassnahmengericht (Art. 273 Abs. 2 StPO).[261]

3. Eine Randdatenerhebung kann auch rückwirkend erfolgen (Art. 273 Abs. 3 StPO). Dabei handelt es ich um eine rückwirkende Überwachung, welche ebenfalls einer Genehmigung des Zwangsmassnahmengerichts bedarf (Art. 273 Abs. 2 StPO).[262]

4. Es kann ein Gerät physisch sichergestellt und die darauf befindlichen (abgerufenen) Daten ausgewertet werden. Hierbei können rückwirkend neben den Verbindungs- oder Randdaten auch Inhaltsdaten erhoben werden. Die Regeln über die Beschlagnahme (Art. 263 ff. StPO) und die Siegelung (Art. 248 StPO) sind massgeblich.[263]

5. Der (Service) Provider kann von den Strafverfolgungsbehörden mittels Editionsbefehl (Art. 265 StPO) aufgefordert werden, die bei ihm gespeicherten (abgerufenen) Daten (wie Verbindungs-, Rand- und Inhaltsdaten) herauszugeben. Auch in diesem Fall hat die beschuldigte Person das Recht, ein Siegelungsgesuch zu stellen. Dasselbe kann auch gegenüber der beschuldigten Person selbst angeordnet werden.[264]

---

[260] Vgl. dazu HANSJAKOB, Überwachungsrecht, Rz. 1677. Hier ist anzumerken, dass bei Überwachungen von Kommunikationen mit End-zu-End-Verschlüsselung regelmässig verschlüsselte Informationen geliefert werden, welche den Strafverfolgungsbehörden nicht viel nützen. Kann selbst die Anbieterin den Kommunikationsverkehr nicht entschlüsseln, schafft der Einsatz von GovWare (Art. 269ter StPO) Abhilfe. Vgl. dazu oben, Kap. II./2./D./e. Fernmeldedienstanbieterinnen trifft denn auch die Pflicht, die von ihnen angebrachte Verschlüsselung (soweit sie dies überhaupt können) zu entfernen (Art. 26 Abs. 2 lit. c BÜPF).

[261] Vgl. dazu oben, Kap. II./2./D./c./bb. und II./2./D./d.

[262] Dabei müssen die Anbieterinnen abgeleiteter Kommunikationsdienste nur diejenigen Randdaten liefern, welche sie für die eigenen Zwecke gespeichert haben. Die Fernmeldedienstanbieterinnen trifft hingegen die Pflicht, die Randdaten der letzten sechs Monate zu speichern (Art. 26 Abs. 5 BÜPF).

Bei der rückwirkenden Randdatenerhebung handelt es sich um eine spezielle Form der Edition von der Beschlagnahme unterliegenden Daten, allerdings mit der Besonderheit, dass das Verfahren nach Art. 273 StPO zu beachten ist. Vgl. dazu oben, Kap. II./2./D./c./bb.

[263] Weil der Kommunikationsverkehr regelmässig von den Anbieterinnen verschlüsselt wird und die Anbieterinnen selbst nicht in der Lage sind, die Verschlüsselung zu entfernen, war es bisher umso wichtiger, die Nachrichten unverschlüsselt aus den beschlagnahmten Geräten auslesen zu können, vgl. dazu Kap. II./3./A./e.

[264] Vgl. dazu Kap. II./2./B. und C.

6. Die Strafverfolgungsbehörden haben zudem die Möglichkeit, den Datenverkehr mittels Verwendung von Zugangsdaten[265] zu überwachen. Mittels Zugangsdaten bzw. Login-Daten können sie sich in das Mail- oder Facebook-Konto der beschuldigten Person einloggen und auf diese Weise den Kommunikationsverkehr überwachen. Vorausgesetzt wird, dass die Zugangsdaten rechtmässig erhoben wurden. Sie können bspw. im Rahmen einer Hausdurchsuchung sichergestellt werden. Sie können sich auch auf einem sichergestellten Smartphone oder Computer befinden. Eine aktive Überwachung auf diese Weise ist nach Art. 269 ff. StPO insofern zulässig, als dass eine Genehmigung des Zwangsmassnahmengerichts vorliegt. Auf diesem Weg können Verbindungs-, Rand- und Inhaltsdaten in Echtzeit erhoben werden; Randdaten können auch rückwirkend nach Art. 273 Abs. 3 StPO erhoben werden. Kommunikationsinhalte der Vergangenheit sind bei einer Echtzeitüberwachung jedoch nicht erhältlich.[266]

7. Die Zugangsdaten können auch zur Durchsuchung (Art. 246 StPO) eines Facebook- oder E-Mail-Kontos und zur anschliessenden Beschlagnahme (Art. 263 StPO) beweisrelevanter Daten verwendet werden. Auch hier gilt, dass die Zugangsdaten rechtmässig beschafft werden müssen. Auf diesem Weg dürfen alle Daten (wie bei der Beschlagnahme eines physischen Geräts, vgl. unter 4.) erhoben werden. Der Rechtsschutz erfolgt auf dem Weg der Siegelung[267].[268]

8. Will die Strafverfolgungsbehörde Bestandesdaten erheben, liegt eine spezielle Form der Durchsuchung oder Beschlagnahme vor. Die Daten können vorerst ohne Wissen der beschuldigten Person erhoben werden und eine Genehmigung des Zwangsmassnahmengerichts ist nicht erforderlich.[269]

---

[265] Eine Datenerhebung mittels Zugangsdaten stellt eine äusserst interessante Möglichkeit für die zuständigen Behörden dar, weil sie mit niedrigem Aufwand verbunden ist und (im Falle von Kommunikationen mit End-zu-End-Verschlüsselung) unverschlüsselte Kommunikationsdaten liefert.

[266] Vgl. dazu Kap. II./3./B./c.

[267] Besteht Gefahr in Verzug oder andere Verdunkelungshandlungen, dürfen die Beweismittel vorläufig sichergestellt werden (Art. 263 Abs. 3 StPO), wobei das Recht, sich zum Inhalt der Aufzeichnungen zu äussern und das Recht auf Siegelung der Inhaberin erst nach vorläufiger Sicherstellung gewährt werden kann.

[268] Vgl. dazu Kap. II./3./B./c.

[269] Vgl. dazu Kap. II./3./A./a.

2. Zwangsmassnahmen zur Datenerhebung im Ausland

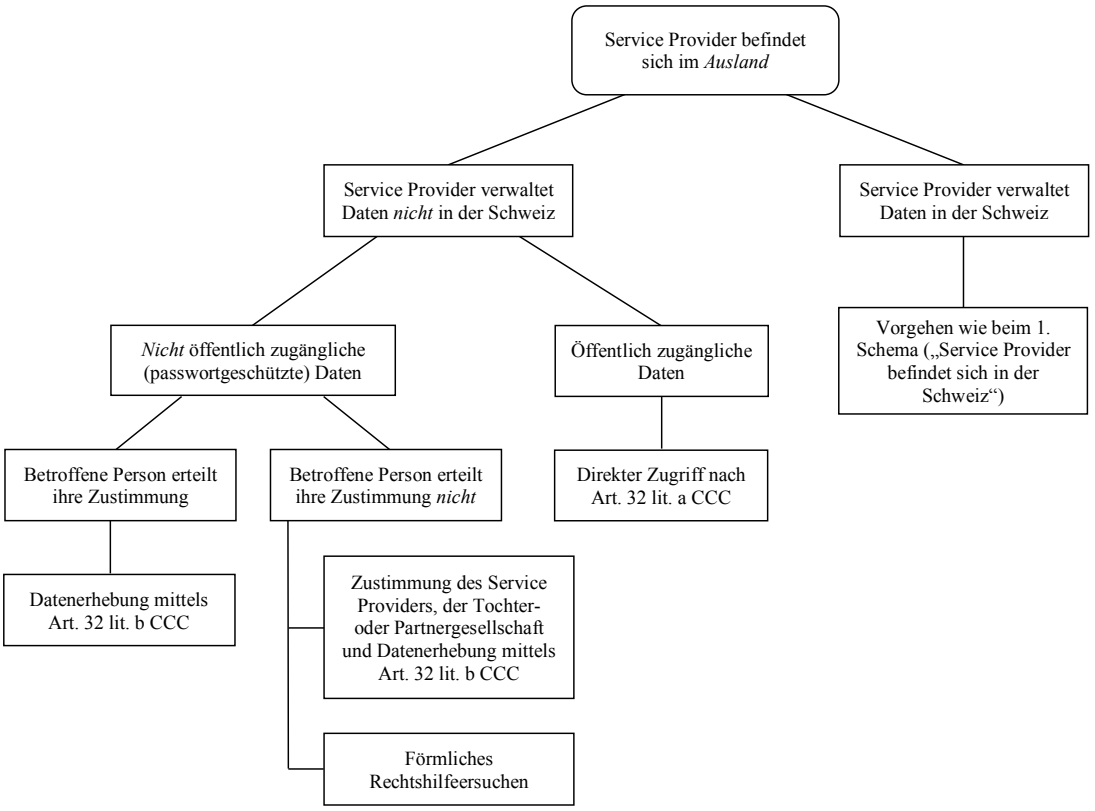


Abbildung 2: Schema Zwangsmassnahmen zur Datenerhebung im Ausland

Die Problematik zur grenzüberschreitenden Datenerhebung wurde bereits in den vorangehenden Kapiteln ausführlich diskutiert. In diesem Kapitel wird ein Schema skizziert, an dem sich die Strafverfolgungsbehörden bei einer grenzüberschreitenden Datenerhebung zu orientieren haben[270]. Erstens muss festgestellt werden, ob der ausländische Service Provider einen Sitz in der Schweiz hat und dort die für die Strafverfolgungsbehörden relevanten Benutzerdaten speichert bzw. verwaltet. Werden an der schweizerischen Niederlassung die Daten gespeichert, spricht man von „Server Farms", auf welche das schweizerische Landesrecht (StPO und BÜPF) Anwendung findet. In diesem Fall gestaltet sich das Vorgehen wie beim ersten Schema zur Datenerhebung in der Schweiz[271].

Hat der ausländische Service Provider einen *Sitz* in der Schweiz, an welchem jedoch *keine* Daten *verwaltet* bzw. *gespeichert* werden oder hat er *keinen* Sitz in der Schweiz, muss geprüft werden, ob die Daten mithilfe von Art. 32 CCC erhoben werden können. Nach Art. 32 lit. a CCC kann ein Vertragsstaat ohne Genehmigung eines anderen Vertragsstaates *direkt* auf *öffentlich zugängliche* Daten zugrei-

[270] Dem Schema zugrundgelegt wird, dass es sich beim ausländischen Staat um einen CCC-Mitgliedsstaat handelt. Sollen Daten in einem Staat erhoben werden, welcher die Convention nicht unterzeichnet hat, muss der formelle Rechtshilfeweg beschritten werden. Der formelle Rechtshilfeweg kennt insb. keine Massnahmen zur vorläufigen Datensicherung, weshalb er regelmässig wenig erfolgsversprechend ist. Vgl. dazu BURGERMEISTER, 34–35.

[271] Vgl. dazu oben, Kap. III./2./A. und III./3./B.

fen, unabhängig davon, wo sich die Daten geografisch befinden. Bei dieser Art von (öffentlichen) Daten sind bspw. öffentliche Facebook-Profile, Postings auf Facebook oder Twitter gemeint.

Will die Strafverfolgungsbehörde auf *nicht öffentliche* (insb. *passwortgeschützte*) Daten im einem anderen Hoheitsgebiet zugreifen, bedarf der Zugriff nach Art. 32 lit. b CCC einer freiwilligen und rechtmässigen Zustimmung einer Person, welche zur Datenweitergabe rechtmässig befugt ist. Zustimmungsberechtigt i.S.v. lit. b sind sowohl inländische als auch ausländische Personen und Gesellschaften. Die Verfügungsberechtigung einer bestimmten Person oder Gesellschaft beurteilt sich nach dem nationalen Recht des Staates, in welchem die betreffende Person handelt. Demzufolge sind ausländische Service Provider, welche sich in ihren Allgemeinen Nutzungsbedingungen ein Weiterleitungsrecht von Daten an in- und ausländische Strafverfolgungsbehörden gegenüber ihren Kunden abbedungen haben, herausgabeberechtigt. Auch inländische Inhaberinnen von E-Mail-Konten und inländische Kunden von sozialen Netzwerken sind direkt zustimmungsberechtigt, ohne dass eine zusätzliche Zustimmung der ausländischen Providerfirma nötig wäre. Art. 32 lit. b CCC gilt auch für den Fall, dass im Inland tätige Tochter- oder Partnergesellschaften zur Herausgabe von Daten gebeten werden, die bei der ausländischen Muttergesellschaft gespeichert sind.[272]

M.E. wäre der für die Strafverfolgungsbehörden einfachste Weg, die inländische Kundin eines bestimmten Kontos (soweit überhaupt bekannt) um Herausgabe der entsprechenden Daten zu bitten. Ist die inländische Kundin nicht bekannt oder erteilt sie ihre Zustimmung nicht und hat der ausländische Provider eine Tochter- oder Partnergesellschaft in der Schweiz, hat sich die Strafverfolgungsbehörde an letztere zu wenden. Damit die Tochter (oder der Partner) die Daten aber herausgeben kann, wird vorausgesetzt, dass sie über einen Zugriff auf die Daten verfügt[273]. Ist dies nicht der Fall, bedarf es einer Zustimmung des ausländischen Providers. Verweigert auch dieser seine Zustimmung, bleibt einzig der formelle Rechtshilfeweg übrig[274].

---

[272] Vgl. dazu Kap. III./2./A. und III./3./A.–B.

[273] Der Lösungsvorschlag von HANSJAKOB, Überwachungsrecht, Rz. 1369, ausländische Anbieterinnen von Internetdiensten dazu zu verpflichten, einen Sitz in der Schweiz zu eröffnen, der die Daten von Nutzenden in der Schweiz verwaltet oder zumindest Zugang zu ihnen hat, würde insoweit helfen, als dass sichergestellt würde, dass die inländischen Töchter und Partner tatsächlich auf die Daten zugreifen und sie herausgeben können.

[274] Das CCC sieht sog. „Quick-Freeze-Procedure“ vor, welche einem reibungslosen Ablauf des Rechtshilfeverfahren dienen. Die Art. 16, 29 und 30 CCC dienen einer (vorläufigen) Datensicherung, damit verhindert wird, dass die Daten während des Rechtshilfeverfahrens gelöscht oder anderweitig beseitigt werden. Vgl. dazu Explanatory Report No. 185, Ziff. 159.

V. Zusammenfassung und Ausblick

Die Ergebnisse der vorliegenden Arbeit lassen sich wie folgt zusammenfassen: Anbieterinnen abgeleiteter Internetdienste fallen neu unter das revidierte BÜPF. Es ist jedoch nicht ganz klar, ob sie nun unter Art. 2 lit. b (die Fernmeldedienstanbieterinnen) oder Art. 2 lit. c BÜPF (die Anbieterinnen abgeleiteter Kommunikationsdienste) fallen. Zur Klärung dieser Unklarheiten hat der Dienst ÜPF ein (nicht unumstrittenes) Merkblatt veröffentlicht, welches die Zuordnung zu einer der beiden Kategorien erleichtern soll. Folglich werden jene abgeleiteten Internetdienste als Fernmeldedienste qualifiziert, welche den klassischen Fernmeldediensten gleichgestellt sind. Nach der hier vertretenen Auffassung ist diese Praxis zu begrüssen, zumal diese Dienste eine erhebliche Konkurrenz für die klassischen Fernmeldedienste darstellen.[275]

Die durch die Revision vorgenommene Ausweitung des persönlichen Geltungsbereichs gibt den Strafverfolgungsbehörden nun die Möglichkeit, auch Anbieterinnen abgeleiteter Internetdienste in Echtzeit zu überwachen. Werden Anbieterinnen abgeleiteter Internetdienste denn auch als Fernmeldedienstanbieterinnen qualifiziert, sind sie verpflichtet, die Randdaten der letzten sechs Monate aufzubewahren, was eine rückwirkende Überwachung i.S.v. Art. 273 Abs. 3 StPO erleichtert. Mit dem neuen Art. 269ter StPO wurde auch eine gesetzliche Grundlage geschaffen, die es ermöglicht, unverschlüsselte Kommunikationsdaten zu erheben. Neben den (neuen) Überwachungsmassnahmen sieht die Schweizerische Strafprozessordung noch weitere (bereits unter altem Recht geltende) Möglichkeiten (Art. 263 ff. StPO) vor, um an die verfahrensrelevanten Daten zu gelangen.[276] Demnach kommt die Autorin zum Schluss, dass den Strafverfolgungsbehörden genügend strafprozessuale Mittel zur Verfügung stehen, Daten von schweizerischen Internetdienstanbieterinnen zu erheben. Schwieriger gestaltet es sich, wenn die Internetdienstanbieterin ihren Sitz im Ausland hat. Für grenzüberschreitende Strafverfolgungsmassnahmen muss regelmässig der Rechtshilfeweg beschritten werden, wobei die Convention on Cybercrime gewisse Instrumente vorsieht, welche die gegenseitige Rechtshilfe erleichtern.

Moderne Kommunikations- und Datenverarbeitungstechnologien stellen eine zunehmend grössere Herausforderung für die Strafverfolgungsbehörden zur Bekämpfung von Internet- und Computerkriminalität dar. Daten können über das globale Netzwerk in kürzester Zeit an beliebige und beliebig viele Empfängerinnen und Empfänger in der ganzen Welt versandt werden.[277] Dabei kennt das Internet keine nationalen Grenzen, so dass die Handlungs- und Erfolgsorte von deliktischem Verhalten geografisch in verschiedenen Staatsgebieten liegen können. Da die grenzüberschreitende Strafverfolgung durch das Territorialitätsprinzip begrenzt wird, braucht es dringend wirksame Instrumente des internationalen Strafrechts, die die Strafverfolgung im Bereich des Cybercrime unterstützen. So erlaubt Art. 32 CCC einen direkten grenzüberschreitenden Zugriff auf im Ausland gespeicherte Daten.

[275] Vgl. zum Ganzen Kap. II./2./D./c./cc.

[276] Vgl. zum Ganzen Kap. II./2. und Kap. II./3.

[277] Vgl. dazu auch FORSTER, 616–617.

Dies gilt einerseits für Daten, die öffentlich zugänglich sind und andererseits, wenn eine berechtigte Person ihre Zustimmung zur Datenherausgabe gibt. M.E. ist der Kreis der Berechtigten weit auszulegen, wonach der ausländische Provider, die inländische Kundin bzw. Inhaberin des entsprechenden Kontos und die inländische Tochter- oder Partnergesellschaft des ausländischen Providers zustimmungsberechtigt sind. Verweigert der ausländische Provider seine Zustimmung und ist die inländische Kundin den Strafverfolgungsbehörden nicht bekannt, ist es besonders wichtig, dass die inländische Tochter, welche ggf. ihre Zustimmung gibt, die Daten auch herausgeben *kann*. Hierfür benötigt sie zumindest einen Zugriff auf die bei der ausländischen Mutter gespeicherten Daten. Eine noch wirksamere Variante bestünde darin, die ausländischen Provider dazu zu verpflichten, einen Sitz in der Schweiz zu eröffnen, an welchem die Daten gespeichert werden.[278]

Des Weiteren plädiert die Autorin für eine weite Auslegung des Territorialitätsprinzips (im Bereich der Verfolgung von Cybercrime) zugunsten des Zugriffsprinzips. Aufgrund der stetig voranschreitenden Digitalisierung und der damit einhergehenden Internationalisierung des Datenverkehrs muss das klassische Verständnis des Territorialitätsprinzips hinterfragt werden und zugunsten einer effektiven Strafverfolgung zurücktreten[279]. Demnach stellt das Einloggen mittels (rechtmässig beschaffter) Zugangsdaten auf ein bestimmtes Benutzerkonto und der damit verbundene Zugriff auf die (auch im Ausland befindlichen) Daten ein für die Strafverfolgungsbehörden einfaches, ressourcensparendes und m.E. zulässig Mittel zur Datenbeschaffung dar.

Der Art. 32 CCC bietet ein wirksames Instrument für die freiwillige Datenherausgabe. Für eine zwangsweise Datenerhebung sieht das CCC allerdings keine Instrumente vor, weshalb nur der langwierige und mühselige formelle Rechtshilfeweg übrigbleibt. Deshalb wird bezüglich einer zwangsweisen grenzüberschreitenden Datenerhebung dafür plädiert, die Convention on Cybercrime entsprechend auszubauen. Gesetzliche Anpassungen und eine Abweichung vom Territorialitätsprinzip sind unerlässlich, damit die Ziele der Convention auch in Zukunft wirksam verfolgt werden können und eine effiziente Strafverfolgung von Cybercrime gewährleistet sein soll. Der effektivste und unumstrittenste Weg wäre, Rechtsgrundlagen zu schaffen, die einen schnellen und unkomplizierten Zugriff auf Daten ermöglichen. Es sind fortlaufend weitere Lösungsansätze zu entwickeln, welche eine Aufweichung des Territorialitätsprinzips erlauben und für eine wirksame Strafverfolgung von Cybercrime sorgen.

Gegenstand dieser Arbeit bildete der technisch hoch komplexe und sich ständig weiterentwickelnde Bereich der digitalen Kommunikation. Zurzeit ist die Literatur und Rechtsprechung in Bezug auf die revidierte BÜPF-Praxis noch überschaubar. Ebenfalls besteht in mehreren Bereichen noch Uneinigkeit und Verwirrung. Es ist also noch viel Grundlagenarbeit zu leisten. Nichtdestotrotz wird es spannend zu sehen sein, wie sich die Rechtspraxis entwickeln wird und welche Theorien und Kritiken an Bedeutung gewinnen werden. Die Autorin blickt also erwartungsvoll und gespannt in die Zukunft.

[278] Vgl. zum Ganzen Kap. III.

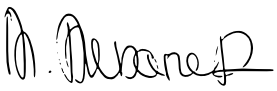
[279] Vgl. dazu auch SCHWEINGRUBER, Rz. 40; GRAF, Jusletter IT, Rz. 49.

Eigenständigkeitserklärung

"Ich erkläre hiermit,

- dass ich die vorliegende Arbeit selbstständig, ohne fremde Hilfe und ohne Verwendung anderer als der angegebenen Hilfsmittel verfasst habe;
- dass ich sämtliche verwendeten Quellen erwähnt und gemäss gängigen wissenschaftlichen Zitierregeln korrekt zitiert habe;
- dass das Thema, die Arbeit oder Teile davon nicht bereits Gegenstand eines Leistungsnachweises einer anderen Veranstaltung oder Kurses waren, sofern dies nicht ausdrücklich mit dem Referenten/der Referentin im Voraus vereinbart wurde und in der Arbeit ausgewiesen wird;
- dass ich ohne schriftliche Zustimmung der Universität keine Kopien dieser Arbeit an Dritte aushändigen oder veröffentlichen werde, wenn ein direkter Bezug zur Universität St. Gallen oder ihrer Dozierenden hergestellt werden kann;
- dass ich mir bewusst bin, dass meine Arbeit elektronisch auf Plagiate überprüft werden kann und ich hiermit der Universität St. Gallen laut Prüfungsordnung das Urheberrecht soweit einräume, wie es für die Verwaltungshandlungen notwendig ist;
- dass ich mir bewusst bin, dass die Universität einen Verstoss gegen diese Eigenständigkeitserklärung sowie insbesondere die Inanspruchnahme eines Ghostwriter-Service verfolgt und dass daraus disziplinarische wie auch strafrechtliche Folgen resultieren können, welche zum Ausschluss von der Universität resp. zur Titelaberkennung führen können."

St. Gallen, 20. Mai 2019



Laura Dusanek