Universität St. Gallen
Hochschule für Wirtschafts-,
Rechts- und Sozialwissenschaften,
sowie Internationale Beziehungen

Strafprozessuale Fernmeldeverkehr-Teilnehmeridentifikation per Antennensuchlauf

---

Eine Anwendung der bundesgerichtlichen Rechtsprechung auf die Fälle „Rupperswil“ und „Emmen“

Seminararbeit im Bachelor-Programm Rechtswissenschaft mit Wirtschaftswissenschaften

Referent: Prof. Dr. Marc Forster

Vorgelegt am 18. April 2017

Judith Rothen
Innerer Sonnenweg 1
9000 St.Gallen
+41 (0)78 696 96 72
judith.rothen@student.unisg.ch
Matrikel – Nr.: 14-610-596

Inhaltsverzeichnis

Abbildungs- und Tabellenverzeichnis

Abkürzungsverzeichnis

a.a.O.	am angeführten Ort
a.M.	anderer Meinung
abg. v.	abgerufen von
Abs.	Absatz
AG	Kanton Aargau
AI	Kanton Appenzell Innerrhoden
AJP	Aktuelle Juristische Praxis
Anh.	Anhang
AR	Kanton Appenzell Ausserrhoden
Art.	Artikel
As	Antennensuchlauf, Antennensuchläufe
AS	Amtliche Sammlung des Bundesrechts
Auff.	Auffassung
Aufl.	Auflage
AZ	Aargauer Zeitung
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
Bd.	Band
BE	Kanton Bern
bez.	bezüglich
BGE	Entscheidungen des Schweizerischen Bundesgerichts
BGer	Schweizerisches Bundesgericht
BL	Kanton Basel-Land
BS	Kanton Basel-Stadt
BSK	Basler Kommentar
bspw.	beispielsweise
bzw.	beziehungsweise
CHF	Schweizer Franken
d.h.	das heisst
DBA	Dienst für besondere Aufgaben
ders.	derselbe
dies.	dieselben
diesbez.	diesbezüglich
E.	Erwägung
EDV	Elektronische Datenverarbeitung
EJPD	Eidgenössisches Justiz- und Polizeidepartement

etc.	et cetera
f., ff.	folgende, fortfolgende
FDA	Fernmeldedienstanbieter(n)
folg.	folglich
form.	formell(e(n))
FP	forum poenale
FR	Kanton Freiburg
GE	Kanton Genf
gesetzl.	gesetzlich(e)
GL	Kanton Glarus
gl.M.	Gleicher Meinung
GR	Kanton Graubünden
h.L.	herrschende Lehre
Hrsg.	Herausgeber
i.c.	in casu = im vorliegenden Fall
i.d.F.	in der Folge
i.d.R.	in der Regel
IMSI	International Mobile Subscriber Identity
insb.	insbesondere
insg.	insgesamt
IP	Internet Protocol
i.V.m.	in Verbindung mit
JU	Kanton Jura
kt.	kantonal(e)
Kap.	Kapitel
Komm.	Kommunikation(en)
lit.	litera = Buchstabe
LU	Kanton Luzern
LZ	Luzerner Zeitung
m.a.W.	mit anderen Worten
m.E.	meines Erachtens
mat.	materiell
max.	maximal
mind.	mindestens
Mio.	Millionen
N	Note
NE	Kanton Neuenburg

Nr.	Nummer
NW	Kanton Nidwalden
NZZ	Neue Zürcher Zeitung
Obj.	Objekt(e)
öff.	öffentlich(e(s))
PTT	Post-, Telefon- und Telegrafenbetriebe
RK UVEK	Rekurskommission des Eidgenössischen Departements für Umwelt, Verkehr, Energie und Kommunikation
Rupp.	Rupperswil
Rz.	Randziffer
S.	Seite
SG	Kanton St.Gallen
SH	Kanton Schaffhausen
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht
SMS	Short Message Service
SO	Kanton Solothurn
sog.	sogenannte(n)
SR	Systematische Sammlung des Bundesrechts der Schweizerischen Eidgenossenschaft
SRF	Schweizer Radio und Fernsehen
StA	Staatsanwalt(schaft)
SZ	Kanton Schwyz
TA	Tagesanzeiger
Tab.	Tabelle
teilw.	teilweise
TG	Kanton Thurgau
TI	Kanton Tessin
u.a.	unter anderem
URL	Uniform Resource Locator
U.	Urteil
u.U.	unter Umständen
ÜPF	Dienst Überwachung Post- und Fernmeldeverkehr
ÜV	Übergangsverordnung
V.	Verordnung
VD	Kanton Waadt
versch.	verschiedene
Vf.	Verfügung

vgl.	vergleiche
VS	Kanton Wallis
z.Z.	zur Zeit
ZBJV	Zeitschrift des Bernischen Juristenvereins
ZH	Kanton Zürich
Ziff.	Ziffer
zit.	zitiert
ZM	Zwangsmassnahme(n)
ZStrR	Schweizerische Zeitschrift für Strafrecht

Erlassverzeichnis

BetmG	Bundesgesetz über die Betäubungsmittel und die psychotropen Stoffe (Betäubungsmittelgesetz) vom 3. Oktober 1951 (SR 812.121).
BGG	Bundesgesetz über das Bundesgericht (Bundesgerichtsgesetz) vom 17. Juni 2005 (SR 173.110).
BStP	Bundesgesetz über die Bundesstrafrechtspflege vom 15. Juni 1934 (AS 50 685).
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 6. Oktober 2000 (SR 780.1).
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101).
E-BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs. Entwurf (noch nicht in Kraft; die Referendumsfrist ist am 7. Juli 2016 unbenutzt ausgelaufen).
E-VÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs. Entwurf März 2017 (noch nicht in Kraft; die Verordnung steht seit dem 22. März 2017 bis zum 29. Juni 2017 in der Vernehmlassung).
FMG	Fernmeldegesetz vom 30. April 1997 (SR 784.10).
GebV-ÜPF	Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs vom 7. April 2004 (SR 780.115.1).
NDG	Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz) vom 25. September 2015 (noch nicht in Kraft).
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0).
StPO	Schweizerische Strafprozessordnung (Strafprozessordnung) vom 5. Oktober 2007 (SR 312.0).

ÜV	Verordnung vom 1. Dezember 1997 über den Dienst für die Überwachung des Post- und Fernmeldeverkehrs (AS 1997 3022) (zit. ÜV).
VÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 31. Oktober 2001 (SR 780.11).
VwVG	Bundesgesetz über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz) vom 20. Dezember 1968 (SR 172.021).

Literaturverzeichnis

BASTEN PASCAL, Rasterfahndung: Proaktive polizeiliche Massnahme der Rasterfahndung. Ihre Geschichte in Gesetz und Praxis, Kriminalistik 3 (2011) 197 ff.

BOMMER FELIX/KAUFMANN ANDREA, Die strafrechtliche Rechtsprechung des Bundesgerichts im Jahr 2011 (ohne Entscheide betreffend die internationale Zusammenarbeit in Strafsachen), ZBJV 151 (2015) 873 ff.

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

DIES. (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung (StPO) (Zürich 2010) (zit. Kommentar StPO 2010/BEARBEITER, Art. x N y).

EHRENZELLER BERNHARD/SCHINDLER BENJAMIN/SCHWEIZER RAINER J./VALLENDER KLAUS A. (Hrsg.), Die Schweizerische Bundesverfassung: St. Galler Kommentar, Bd. 2 (3. Aufl. St. Gallen 2014) (zit. SG Kommentar BV/BEARBEITER, Art. x N y).

FELLMANN JEREMIAS, Unverhältnismässige Randdatenerhebung beim Privatkläger, ius.focus 12 (2015).

FORSTER MARC, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs. Probleme der grenzüberschreitenden Strafverfolgung bei Delikten über soziale Netzwerke und den mobilen Internetverkehr, 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 2015) 615 ff.

GLESS SABINE/GLETH CHRISTOPHER, Antennensuchlauf und Rasterfahndung – Neue Fragestellungen in der Debatte um Sicherheit und Freiheit, in: Kuhn André/Margot Pierre/Aebi Marcelo F./Schwarzenegger Christian/Donatsch Andreas/Jositsch Daniel (Hrsg.), Kriminologie, Kriminalpolitik und Strafrecht aus internationaler Perspektive: Festschrift für Martin Killias zum 65. Geburtstag = Criminologie, politique criminelle et droit pénal dans une perspektive internationale = Criminology, Criminal Policy and Criminal Law in an International Perspective (Bern 2013) 1033 ff.

HANSJAKOB THOMAS, Das neue BÜPF, ZStrR 134 (2016) 429 ff. (zit. HANSJAKOB Das neue BÜPF).

DERS., Wichtige Entwicklungen der Bundesgerichtspraxis zu Überwachungen des Post- und Fernmeldeverkehrs, FP 3 (2013) 173 ff. (zit. HANSJAKOB Entwicklungen).

DERS., Zur Zulässigkeit von Antennensuchläufen, Jusletter vom 5. März 2012 (zit. HANSJAKOB Zulässigkeit).

DERS., BÜPF/VÜPF. Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs. Schriftenreihe des Instituts für Rechtswissenschaft und Rechtspraxis, Bd. 44 (2. Aufl. 2006 St. Gallen) (zit. HANSJAKOB Kommentar BÜPF/VÜPF 2006).

DERS., BÜPF/VÜPF. Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs. Schriftenreihe des Instituts für Rechtswissenschaft und Rechtspraxis, Bd. 7 (1. Aufl. 2002 St. Gallen) (zit. HANSJAKOB Kommentar BÜPF/VÜPF 2002).

DERS., Die ersten Erfahrungen mit dem Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs, ZStrR 120 (2002) 265 ff. (zit. HANSJAKOB Erfahrungen).

HEIMGARTNER STEFAN, Auslegungs- und Rechtfindungsmethodik im Strafprozessrecht, AJP (2016) 3 ff.

HEINIGER ANDREAS, Schrankenlose Fernmeldeüberwachung aufgrund eines konzeptionellen Fehlers im BÜPF?, Jusletter vom 17. September 2012.

JEKER KONRAD/ROOS EVELINE, Antennensuchlauf im Rahmen einer Rasterfahndung, FP 3 (2012) 175 ff.

KARNUSIAN PHILIP, Der Tatverdacht und seine Quellen, FP 6 (2016) 350 ff.

KUHN ANDRÉ/JEANNERET YVAN (HRSG.), Code de procédure pénale suisse. Commentaire Romand (Basel 2011) (zit. CR StPO/ BEARBEITER, Art. x N y).

NIGGLI MARCEL A./HEER MARIANNE/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar. Schweizerische Strafprozessordnung. Jugendstrafprozessordnung, Bd. 2 (2. Aufl. Basel 2014) (zit. BSK StPO/BEARBEITER, Art. x N y).

PETRI THOMAS, Informationsbearbeitung im Polizei- und Strafverfahrensrecht (Kapitel G), in: Lisken Hans/Denninger Erhard (Hrsg.), Handbuch des Polizeirechts: Gefahrenabwehr, Strafverfolgung, Rechtsschutz (5. Aufl. 2012 München) 717 ff.

SCHLAURI SIMON, Fernmeldeüberwachung à discrétion?, sic! (2012) 238 ff.

SCHMID NIKLAUS, Schweizerische Strafprozessordnung: Praxiskommentar (2. Aufl. 2013 Zürich) (zit. SCHMID 2013, Art. x N y).

DERS., Schweizerische Strafprozessordnung: Praxiskommentar (1. Aufl. 2009 Zürich) (zit. SCHMID 2009, Art. x N y).

WALDER HANS/HANSJAKOB THOMAS, Kriminalistisches Denken (10. Aufl. 2016 Heidelberg).

WALDMANN BERNHARD/BELSER EVA MARIA/EPINEY ASTRID (Hrsg.), Bundesverfassung. Basler Kommentar (2015 Basel) (zit. BSK BV/BEARBEITER, Art. x N y).

Materialien- und Rechtsprechungsverzeichnis

Materialien:

Begleitschreiben von Bundesrätin Simonetta Sommaruga zur Anhörung bezüglich der Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF) sowie der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs vom 8. Juni 2011, verfügbar unter <https://www.admin.ch/ch/d/gg/pc/documents/2090/Brief_Ueberwachung-und-GebV_08062011_unterzeichnet_de.pdf> (zuletzt abgerufen am 8. April 2017) (zit. Begleitschreiben SOMMARUGA Änderung VÜPF/GebV-ÜPF).

Botschaft zu den Bundesgesetzen betreffend die Überwachung des Post- und Fernmeldeverkehrs und über die verdeckte Ermittlung vom 8. September 1998, BBl 1998 IV 4241 ff. (zit. Botschaft BÜPF).

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

Erläuternder Bericht des Eidgenössischen Justiz- und Polizeidepartement zum Erlass der VÜPF vom 28. September 2001 (zit. Bericht EJPD VÜPF).

Erläuternder Bericht Zur Totalrevision der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs (GebV-ÜPF). Entwurf März 2017 (zit. Bericht Revision GebV-ÜPF).

Erläuternder Bericht zur Totalrevision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF). Entwurf März 2017 (zit. Bericht Revision VÜPF).

Rechtsprechung:

BGer 1B_256/2015, U. vom 4. November 2015.

BGer 1B_344/2014, U. vom 14. Januar 2015.

BGer 1B_251/2013, U. vom 30. August 2013.

BGer 1B_481/2012, U. vom 22. Januar 2013.

BGer 1B_563/2012, U. vom 6. November 2012.

BGer 1B_376/2011, U. vom 3. November 2011.

BGer 1A_185/2003, U. vom 13. April 2004.

Medien- und Internetquellenverzeichnis

ALTERMATT SVEN, „Die Behörden prüften im Vierfachmord Rupperswil 30'000 Handys“, AZ vom 13. März 2016, verfügbar unter <http://www.aargauerzeitung.ch/schweiz/die-behoerden-prueften-im-vierfachmord-rupperswil-30000-handys-131103651> (zuletzt abgerufen am 7. April 2017) (zit. ALTERMATT, AZ vom 13. März 2016).

DERS., „Nach «Rupperswil» und «Emmen»: Behörden überprüfen massenhaft Handydaten“, AZ vom 18. März 2016, verfügbar unter <http://www.aargauerzeitung.ch/schweiz/nach-rupperswil-und-emmen-behoerden-ueberpruefen-massenhaft-handydaten-130140980> (zuletzt abgerufen am 7. April 2017) (zit. ALTERMATT, AZ vom 18. März 2016).

ASUT, Stellungnahme zur Anhörung zur Änderung der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs VÜPF sowie der Verordnung über die Gebühren und Entschädigungen für die Überwachung des Post- und Fernmeldeverkehrs, vom 29. Juli 2011, verfügbar unter <https://www.ejpd.admin.ch/dam/data/ejpd/aktuell/news/2011/2011-11-23/ve-organisationen.pdf> (zuletzt abgerufen am 7. April 2017).

AZ, „Zwei Drittel der Schweizer wollen persönliche Freiheit für mehr Sicherheit beschränken“, vom 10. November 2016, verfügbar unter <http://www.aargauerzeitung.ch/schweiz/zwei-drittel-der-schweizer-wollen-persoenliche-freiheit-fuer-mehr-sicherheit-beschraenken-130708525> (zuletzt abgerufen am 8. April 2017) (zit. AZ vom 10. November 2016).

AZ, „Vierfachmord Rupperswil: War Thomas N. zu unvorsichtig? Er soll vor der Tat oft die Familie Schauer gegoogelt haben“, vom 9. Juni 2016, verfügbar unter <http://www.aargauerzeitung.ch/aargau/kanton-aargau/war-thomas-n-zu-unvorsichtig-er-soll-vor-der-tat-oft-die-familie-schauer-gegoogelt-haben-130335931> (zuletzt abgerufen am 7. April 2017) (zit. AZ vom 9. Juni 2016).

AZ, „Vierfachmord Rupperswil: Neues Ermittlungsverfahren: Haben seine Huskies den Mörder Thomas N. verraten?, vom 6. Juni 2016, verfügbar unter <http://www.aargauerzeitung.ch/aargau/kanton-aargau/war-thomas-n-zu-unvorsichtig-er-soll-vor-der-tat-oft-die-familie-schauer-gegoogelt-haben-130335931> (zuletzt abgerufen am 8. April 2017) (zit. AZ vom 6. Juni 2016).

KPMG, Bericht „Erhebung und Analyse der Kosten der Post- und Fernmeldeüberwachung“, vom 12. Juni 2012 im Auftrag des Informatik Service Center ISC-EJPD, Leiter Dienst ÜPF, verfügbar unter <https://www.bj.admin.ch/dam/data/bj/sicherheit/gesetzgebung/fernmeldeueberwachung/ber-isc-ejpd-fda-pda-d.pdf> (zuletzt abgerufen am 8. April 2017).

KOPP SIMON, in: SRF, „Gespräch mit Simon Kopp, Sprecher Staatsanwaltschaft Luzern (21. Juli 2016)“ (Podcast), verfügbar unter <http://www.srf.ch/news/regional/zentralschweiz/vergewaltigung-in-emmen-ermittler-geben-nicht-auf> (zuletzt abgerufen am 8. April 2017) (zit. KOPP in Gespräch mit SRF vom 21. Juli 2016).

LZ, „Überprüfung tausender Handynutzer ohne Erfolg – Personen im Ausland im Visier“, vom 21. Juli 2016, verfügbar unter <http://www.luzernerzeitung.ch/nachrichten/ zentralschweiz/luzern/Vergewaltigung-in-Emmen-Auch-Handydaten-helfen-nicht-weiter;art92,784729> (zuletzt abgerufen am 6. April 2016) (zit. LZ vom 21. Juli 2016).

NZZ, „Vierfachmord von Rupperswil: Ermittler werten tausende Handy-Daten aus“, vom 11. März 2016, verfügbar unter <https://www.nzz.ch/panorama/ungluecksfaelle-und-verbrechen/vierfachmord-von-rupperswil-ermittler-werten-tausende-von-handy-daten-aus-ld.7105> (zuletzt abgerufen am 6. April 2017) (zit. NZZ vom 11. März 2016).

NZZ, „Chronologie des Vierfachmords von Rupperswil: Ein Einfamilienhausbrand entpuppt sich als Tötungsdelikt“, vom 13. Mai 2016, verfügbar unter <https://www.nzz.ch/panorama/chronologie-im-vierfachmord-von-rupperswil-ein-einfamilienhausbrand-entpuppt-sich-als-toetungsdelikt-ld.82504> (zuletzt abgerufen am 7. April 2017) (zit. NZZ vom 13. Mai 2016).

NZZ, „Vergewaltigung von Emmen: Angreifer nannte während der Tat seinen Namen“, vom 13. Februar 2017, verfügbar unter <https://www.nzz.ch/panorama/aktuelle-themen/vergewaltigung-von-emmen-angreifer-nannte-waehrend-der-tat-seinen-namen-ld.145201> (zuletzt abgerufen am 7. April 2017) (zit. NZZ vom 13. Februar 2017).

TA, „Fall Emmen: Staatsanwaltschaft sucht nach «Aron/Aaron»“, vom 13. Februar 2017, verfügbar unter <http://www.tagesanzeiger.ch/news/standard/fall-emmen-staatsanwaltschaft-sucht-nach-aronaaron/story/27227282> (zuletzt abgerufen am 8. April 2017) (zit. TA vom 13. Februar 2017).

ÜPF, Detaillierte Statistiken des Dienstes der Jahre 2011-2016, verfügbar unter <https://www.li.admin.ch/de/themen/statistik> (zuletzt abgerufen am 1. April 2017) (zit. ÜPF Statistik).

VEREIN DIGITALE GESELLSCHAFT, Vorratsdatenspeicherung, verfügbar unter <https://www.digitale-gesellschaft.ch/vorratsdatenspeicherung/ => Antennensuchläufe/Funkzellenabfragen> (zuletzt abgerufen am 8. April 2017).

1 Einführung[1]

„Nach «Rupperswil» und «Emmen»: Behörden überprüfen massenhaft Handydaten“,[2] so und ähnlich[3] titulierten Schweizerische Tageszeitungen, seit zwei der aktuell berühmtesten Kriminalfälle der Schweiz, die Frage nach der Zulässigkeit von strafprozessualer Fernmeldeverkehr-Teilnehmeridentifikation per Antennensuchlauf (As) in den Fokus der Öffentlichkeit rückte. Vornehmlich Art. 269 StPO[4] stipuliert die Bedingungen, unter welchen die Schweizerischen Strafverfolgungsbehörden As nach Art. 16 lit. e VÜPF durchführen dürfen. As, im Zeitalter von Smartphones und anderen mobilen Endgeräten an Bedeutung gewinnende strafprozessuale Ermittlungsmethoden, bieten aber auch einiges an Konfliktpotential, da sie sich im Spannungsfeld zwischen Sicherheit und Freiheit bewegen. Fest steht, dass die staatliche Überwachung des Fernmeldeverkehrs zwecks Strafverfolgung heutzutage unumgänglich ist. In der Diskussion zwischen „mehr Sicherheit“ oder „mehr Freiheit“ geht es folg. nicht um die grundsätzliche Zulässigkeit solcher Methoden, sondern um deren Ausgestaltung.[5] Z.Z. scheint das Bedürfnis der Bevölkerung nach einem „Mehr an Sicherheit“ zu überwiegen, zumindest in Anbetracht aktueller Abstimmungstendenzen.[6]

Der Verein «Digitale Gesellschaft» befürchtet nichtsdestotrotz, dass bei rückwirkender Rasterfahndung, zu denen der As zählt, hunderte oder tausende Personen gezwungen sind, ihre Unschuld darzulegen.[7] Dies würde entgegen der strafprozessualen Ideologie stehen, dass nur diejenigen Individuen Eingriffe in ihre Rechtssphäre befürchten müssen, die tatsächlich strafverdächtig sind. Zwangsmassnahmen (ZM), die in die Grundrechte nicht beschuldigter Personen eingreifen, dürfen nämlich nur besonders zurückhaltend eingesetzt werden.[8] Rechtsanwalt Konrad Jeker andererseits, echauffiert sich über die fehlende Transparenz der Massnahme, weil Betroffene nicht über die Datenerhebung informiert werden.[9]

---

1 *Leserhinweis:* Stand der Einarbeitung von Literatur und Rechtsprechung ist der 10. April 2017. Auf eine Verwendung von Paarformen und Doppelbezeichnungen wird verzichtet; stets steht die männliche Form auch für die weibliche. Abkürzungen, die nicht geläufig sind, werden nachfolgend bei erstmaliger Verwendung in Klammern angegeben.

2 ALTERMATT, AZ vom 18. März 2016.

3 Bspw. NZZ vom 11. März 2016.

4 Das BGer orientiert sich in 1B_376/2011 vom 3. November 2011 an den in Art. 269 StPO postulierten Voraussetzungen bei Prüfung der Zulässigkeit von As. Vgl. dazu Kap. 6.1.

5 GLESS SABINE/GLETH CHRISTOPHER, S. 1034.

6 Bspw. Abstimmung zum NDG am 25. September 2016; AZ vom 10. November 2016.

7 VEREIN DIGITALE GESELLSCHAFT.

8 Art. 197 Abs. 2 StPO.

9 ALTERMATT, AZ vom 18. März 2016.

Zudem stellt sich in den Fällen „Rupperswil“ (Rupp.) und „Emmen“ die Frage, ob die bestehende gesetzl. Grundlage und die bundesgerichtliche Konkretisierung für die Zulassung der Beweiserhebungsmethode ausreicht. Diesen problematischen Aspekten widmet sich die vorliegende Arbeit: Unter Berücksichtigung der bisherigen Rechtsprechung zur Thematik wird der Frage nachgegangen, ob die strafprozessuale Fernmeldeverkehr-Teilnehmeridentifikation per As in den Praxisbeispielen „Rupp.“ und „ Emmen“ überhaupt auf die erfolgte Art und Weise hätte angewendet werden dürfen.

In einem ersten Schritt werden in Kap. 2 die wesentlichen Begrifflichkeiten erläutert. Danach folgt eine Sachverhaltsdarstellung der Fälle „Rupp.“ und „Emmen“. An dieser Stelle ist zudem anzumerken, dass sich die vorliegende Arbeit ausschliesslich auf die Überwachung per As fokussiert, da andere den Fernmeldeverkehr betreffende Ermittlungsmethoden für die Fälle „Rupp.“ und „Emmen“ von untergeordneter Bedeutung sind. Weiter wird in Kap. 4 ein Überblick über das bisherige Ausmass der Überwachungen mittels As in der Schweiz verschafft. Eine systematische Analyse der rechtlichen Rahmenbedingungen und Rechtsprechung in Kap. 5 soll Aufschluss über die Systematik, die gesetzl. Grundlage und rechtsstaatlichen Problematiken des As liefern. Auf Basis der gewonnenen Erkenntnisse soll im Anschluss eine Einschätzung abgegeben werden, ob die in der Rechtsprechung ausgearbeiteten Kriterien in den Fällen „Rupp.“ und „Emmen“ erfüllt sind. Abschliessend wird die Arbeit in Kap. 7 mit einem Fazit über die Zulässigkeit der Beweiserhebung mittels As in den Fällen „Rupp.“ und „Emmen“ zusammengefasst, sowie eine Würdigung vorgenommen.

2 Begriffsqualifikation

As lassen sich nur schwer einer konkreten Kategorie von im Fernmeldeverkehr eingesetzten Überwachungstypen zuordnen, weil sie entgegen den üblichen Methoden keine im Voraus individualisierte Person anvisieren. Das BGer bezeichnet den As in einem viel beachteten U. deswegen auch als „rückwirkende Rasterfahndung“ und erklärt ihn zu einer komplett neuen Kategorie von Überwachungsmethoden, die jedoch bis anhin ohne form.-gesetzl. Grundlage existiert.[10] Doch bevor man sich mit diesen rechtsstaatlich heiklen Aspekten befassen kann und um die Problematik und das Konfliktpotential von strafprozessualer Fernmeldeverkehr-Teilnehmeridentifikation per As besser verstehen zu können, ist eine Definition der zentralen Begriffe von grundlegender Bedeutung.

2.1 Antennensuchlauf

Primär gilt es den strafprozessualen Begriff des As zu definieren. Das Gesetz statuiert den As seit dem Jahr 2012 in Art. 16 lit. e VÜPF als „rückwirkende Eruierung aller an einem bestimmten Standort angefallenen mobilen Kommunikations-Vorgänge während eines bestimmten Zeitraumes, sofern es zum Aufbau einer Kommunikation gekommen ist“. As geben demgemäss den ermittelnden Behörden im Nachhinein Auskunft über bestimme Antennenstandorte bzw. Auskunft über gespeicherte Daten mobiler Kommunikation (Komm.), die über besagte Antenne geführt wurden. Dies impliziert, dass As im Gegenteil zur herkömmlichen strafprozessualen Mobilfunküberwachung nicht eine individualisierte Telefonnummer überwachen, sondern den Strafverfolgungsbehörden eine Menge an Telefonnummern zur Verfügung stellen, aus der es die zu ermittelnde Telefonnummer zwecks Identifizierung eines Fernmeldeverkehr-Teilnehmers herauszufiltern gilt. Allein aus diesem Umstand lässt sich ableiten, dass es sich beim As um eine selten eingesetzte Überwachungsmassnahme handelt, die sich nur für einen begrenzten Anwendungskreis eignet.

2.1.1 Anwendungsbereich

Konkret eignet sich der As für dreierlei Ermittlungsvorgänge:[11] Erstens für die Untersuchung von Straftaten, bei der die verdächtige Täterschaft zu einem bestimmten Zeitpunkt beim mobilen Kommunizieren beobachtet wurde, aber die konkret benutzte Telefonnummer unbekannt ist. Je exakter der Zeitpunkt bekannt ist – bspw. durch Observation der Zielperson – desto wahrscheinlicher lässt sich die gesuchte Rufnummer mittels As filtern, da sich so die

---

10 BOMMER/KAUFMANN, S. 919.

11 A.M. HANSJAKOB Zulässigkeit, Rz. 5, der von 2 Gründen, die für die Durchführung eines As sprechen, ausgeht. Er erachtet insb. die beiden ersten hier erwähnten Konstellationen als geeignet um einen As einzuleiten.

Zahl der in Frage kommenden Nummern minimieren lässt. Zweitens eignen sich As für die Aufdeckung von mind. zwei ähnlichen Straftaten, die vermutungsweise durch die selbe Täterschaft an unterschiedlichen Antennenstandorten begangen wurden. Bei dieser Konstellation muss mit genügend hoher Wahrscheinlichkeit davon ausgegangen werden können, dass die Täterschaft jeweils zur ungefähren Tatzeit am oder in der Nähe des Tatorts mobil kommuniziert hat. Ist dies der Fall, kann mittels Konstruktion der Schnittmenge, der jeweils an den Tatorten anwesenden Rufnummern, die Täterschaft mit hoher Wahrscheinlichkeit ermittelt werden.

Es gibt aber auch einen dritten denkbaren Anwendungsfall für die Durchführung von As und zwar für Straftaten, bei der die Täterschaft unbekannt, aber bspw. der genaue Ort und Zeitpunkt des Tathergangs bekannt ist. Obwohl ein As bei dieser Konstellation wenig erfolgsversprechend scheint, weil die in Frage kommende Anzahl an Telefonnummern mit keiner anderen Menge zur Konstruktion einer Schnittmenge vereinigt werden kann, liefert ein As den Ermittlungsbehörden nichtsdestotrotz wichtige Erkenntnisse. Der primäre Grund für die Durchführung eines solchen As besteht darin, Rufnummern von potentiell verdächtigen Personen mit dem erhobenen Datensatz abzugleichen. Es geht demzufolge in erster Linie um Alibiabklärungen.[12]

Neben dem begrenzten Anwendungsbereich von As ist auch anzumerken, dass diese nur durchführbar sind, wenn es zum Aufbau mobiler Komm. gekommen ist. Zum Aufbau mobiler Komm. kann es einerseits durch aktiven Beitrag des Mobiltelefonbenutzers kommen, indem dieser bspw. jemanden anruft oder via Internet mobile Daten benützt. Andererseits fällt unter mobile Komm. aber auch eine Art passive Haltung des Mobiltelefonbenutzers, weil Verkehrsdaten auch dann registriert werden, wenn der Mobiltelefonbenutzer angerufen wird oder eine E-Mail empfängt.[13]

2.1.2 Funktionsweise

Um zu erklären wie ein strafprozessualer As funktioniert, gilt vorweg festzuhalten, dass jedes Mobiltelefon fortwährend Verbindung zur nächstgelegenen Mobilfunkantenne aufnimmt, damit eingehende Anrufe oder Mitteilungen auf das richtige Gerät weitergeleitet werden können. Die Antennen verfügen dabei über eine Reichweite von mehreren hundert Metern in der Stadt bzw. wenigen Kilometern auf dem Land und werden von privaten FDA[14] betrieben. Jede Antenne besteht aus 3 Zellen, die jeweils ein Gebiet von 120 Grad um die Antenne herum abdecken. Die zuständigen FDA können aufgrund der fortwährenden Verbindungs-

---

12 Hansjakob stützt die These. Interview Hansjakob, Anh. 1, S. 41.

13 Ders., a.a.O. S. 45.

14 In der Schweiz sind dies die Swisscom, Salt und Sunrise.

aufnahme der einzelnen Mobiltelefone genau in Erfahrung bringen, welche Telefone sich während eines bestimmten Zeitraumes im Einzugsgebiet einer gewissen Antenne befunden bzw. gegebenenfalls über diese Antenne mobil kommuniziert haben. Dabei ist den FDA nicht nur die spezifische Antenne, sondern auch die Hauptstrahlrichtung bekannt, wodurch sich genau ermitteln lässt in welchem Segment von 120 Grad um die Antenne sich das überwachte Gerät befindet.[15] Bewegungsmuster, bzw. Daten über die reine Anwesenheit im Erfassungsbereich einer spezifischen Antenne, werden fortlaufend mit aktuellen Daten überschrieben. Gespeichert werden nur die sog. Komm.-Daten, also Daten über Telefonate und Textnachrichten, sowie Internetverbindungen. Da As Auskunft über eine Vielzahl an Telefonnummern geben, ist es im Hinblick auf die Verhältnismässigkeit stringent, dass nicht die konkreten Komm.-Inhalte weitergegeben werden, sondern nur Eckdaten über die Komm.[16]

2.2 Daten des Fernmeldeverkehrs

Das Gesetz kennt eine Vielzahl von Daten des Fernmeldeverkehrs, wobei es sich teilw. einer verwirrlichen Terminologie bedient.[17] Die Datenarten sind sich im Grunde sehr ähnlich, was aber auf den ersten Blick oft nicht erkennbar ist. Es ist jedoch wichtig, die versch. Datenarten auseinanderzuhalten, da die Voraussetzungen und Konsequenzen unterschiedlich ausfallen.

2.2.1 Daten zur Teilnehmeridentifikation

Das Gesetz bzw. Art. 273 StPO kennt dreierlei Daten: Abs. 1 lit. a regelt die Erhebung von Daten, die Aufschluss über Verbindungen geben, lit. b die Auskunft über Verkehrs- und Rechnungsdaten. Demzufolge gibt es gemäss Gesetz Verbindungs-, Verkehrs- und Rechnungsdaten, wobei alle 3 Arten unter dem Oberbegriff der Teilnehmeridentifikation subsumiert werden. Teilnehmeridentifikation bedeutet, dass an konkreten Fernmeldeverbindungen über einen gewissen Zeitraum hinweg Teilnehmer identifiziert werden (Verbindung hat oder gehabt hat).[18] Teilnehmeridentifikation ist ein Begriff, der auch für den As prägend ist, da er als schlussendlicher Zweck der Massnahme bezeichnet werden kann. Obwohl die Rechtsprechung entgegen der Lehrmeinung entschieden hat, dass der As nicht unter Art. 273 StPO subsumiert werden kann, lassen sich die sprachlichen Feinheiten in der Abgrenzung der Datenarten auf den As anwenden.

Die h.L. geht davon aus, dass Verbindungs- und Verkehrsdaten eigentlich deckungsgleiche Begriffe sind, wobei allerdings Verkehrsdaten um die Daten über den Standort oder der EDV-Anlagen ergänzt sind. Rechnungsdaten andererseits werden soweit nicht als Daten, die

---

15 HANSJAKOB Zulässigkeit, RZ. 1.

16 DERS. a.a.O. Rz. 3.

17 Kommentar StPO 2014/HANSJAKOB, Art. 273 N 2.

18 BGer 1B_344/2014 E. 6.2.

dem Fernmeldegeheimnis unterstehen, bezeichnet, solange sie keine Rückschlüsse auf die Daten einzelner Verbindungen zulassen.[19] Wenn sie detailliert nach einzelnen Gesprächen aufgeschlüsselt sind, sind Rechnungsdaten nichts anderes als Verkehrsdaten. Die Begriffe Verkehrs- und Rechnungsdaten lassen sich demgemäss u.U. synonym verwenden, während der Begriff der Verbindungsdaten keine Angaben über den Standort zulässt. Für den As sind Standortdaten jedoch von entscheidender Bedeutung, weswegen im Zusammenhang mit der Durchführung von As immer von Verkehrs- allenfalls von Rechnungsdaten-Abfragen die Rede sein muss.

Zu den Rechnungsdaten zählen neben Hinweisen zum Rechnungsempfänger, auch Aufzeichnungen über die geführten Komm.-Verbindungen, damit der geschuldete Rechnungsbetrag an den FDA gemäss den Tarifen ermittelt werden kann. Der FDA muss bspw. wissen ob Gespräche ins Ausland oder auf andere heimische Netze geführt wurden und wie lange diese gedauert haben. Konkret registriert und weitergegeben werden im Sinn einer Abfrage von Rechnungs- bzw. Verkehrsdaten mittels As, der Zeitpunkt und die Länge der geführten Gespräche, der Zeitpunkt des Versendens oder Empfangens von Textnachrichten, die ausgehende und eingehende Telefonnummer, sowie die sendende Antenne und die Hauptstrahlrichtung.[20] Da die Daten während der Analyse durch die Polizei zur Wahrung des Fernmeldegeheimnisses anonymisiert behandelt werden, dürfen Hinweise zum Inhaber erst nach Eingrenzung auf einige wenige Verdächtige eingeholt werden.

2.2.2 Bestandes- und Verkehrsdaten

Bei der Betrachtung von Daten des Fernmeldeverkehrs ergibt sich noch eine zweite terminologische Unklarheit, nämlich in der Abgrenzung zwischen Bestandes- und Verkehrsdatenabfragen. Was Verkehrsdaten sind, wurde bereits eingehend erläutert. Bestandesdaten-Auskünfte andererseits sind in Art. 14 Abs. 1 BÜPF festgesetzt. Dabei sind den Strafverfolgungsbehörden die entsprechenden Fernmeldeanschlüsse bekannt und ihnen werden Auskünfte über Abonnementenverhältnisse erteilt .[21] Es werden jedoch keine Verkehrsdaten zu Komm. erhoben.[22] In diesem Sinn müsste angenommen werden, dass sich die Abgrenzung dieser unterschiedlichen Arten von Datenerhebungen einfach gestaltet, dies v.a. auch in Anbetracht der Tatsache, dass die Begrifflichkeiten unterschiedliche gesetzl. Anforderungen stellen. Bei Bestandesdaten-Auskünften ist die Eingriffsschwere deutlich kleiner, weswegen sie keiner Bewilligung seitens des ZM-Gerichts bedürfen und auch alleine von der Polizei

---

19 Kommentar StPO 2014/HANSJAKOB, Art. 273 N 2.

20 DERS. Zulässigkeit, RZ. 3.

21 DERS. Kommentar BÜPF/VÜPF 2006, Art. 14 N 11 ff.

22 BGer 1B_344/2014 E.6.2.

ohne Mitwirkung der StA abgefragt werden können.[23] Dass die Begriffe klar unterschieden werden können ist jedoch insb. im Bereich des mobilen Internetverkehrs nicht so,[24] da das Gesetz die Begriffe teilw. vermischt und sich selbst das BGer mit der sprachlichen Differenzierung schwer tut.[25]

Im Hinblick auf den As kann festgehalten werden, dass dieser primär den Verkehrsdatenabfragen zugeordnet werden kann, da gestützt auf diese Daten Teilnehmer identifiziert werden. Ist im Zuge der Auswertung der erhobenen Daten eine Eingrenzung erfolgt oder sollen die erhobenen Nummern personenbezogen analysiert werden, erfolgt eine Bestandesdatenabfrage.

2.3 Rasterfahndung

Aus der vorhergehenden Analyse lässt sich ableiten, dass jeder As auch eine Rasterfahndung beinhaltet, da die gewonnen Daten noch weiter ausgewertet werden müssen. Aus der Vielzahl an ermittelten Telefonnummern muss nämlich die eine, dem Täter gehörende Nummer, herausgefiltert werden, was sich mittels eines Rasters bewerkstelligen lässt. Die Rasterfahndung definiert sich als – i.d.R. automatisiertes – Massendatenverarbeitungsverfahren mit dem Ziel bestimmte Personen zu ermitteln. Wichtig dabei ist, dass diese Art von kriminalistischer Methode den Zweck verfolgt, gewisse Straftaten aufzudecken, indem diese mit ihren Tätern in Verbindung gebracht werden.[26] Die Rasterfahndung ermöglicht insoweit die Ermittlung von bisher unbekannten Tatverdächtigen.[27] Folg. geht es um das „Finden und Fangen“ von Personen.[28]

Bei der Rasterfahndung wird die Annahme getroffen, dass die Täterschaft gewisse unterschiedliche Merkmale auf sich vereinigt, die in der Summe nur auf wenige Verdächtige zutreffen. Die Merkmale basieren meist auf Zeugenaussagen, Überwachungsaufnahmen oder begründeten Annahmen der Polizei und werden dann mit öff. oder privat zugänglichen Daten gerastert, d.h. abgeglichen. Das Problem besteht darin, dass die Merkmale in erster Linie

---

23 HANSJAKOB Entwicklungen, S. 176.

24 FORSTER, S. 622 f. Internetadressen bekommen i.d.R. alle Session eine neue IP-Adresse zugewiesen, weswegen eine Identifizierung des registrierten Inhabers nicht ohne weiteres möglich ist. Damit der Teilnehmer identifiziert werden kann, muss der Provider alle zugewiesenen IP-Adressen abspeichern. Wenn bspw. Kunden von sozialen Netzwerken identifiziert werden sollen, muss die „IP-History“ des Netzwerk-Providers eingeholt werden. Zudem stellen sich Abgrenzungsschwierigkeiten, wenn kein typischer Fall einer Bestandesdaten-Abfrage vorliegt, weil der Internet-Anschluss unbekannt ist.

25 BGer 1B_481/2012.

26 PETRI, S. 880.

27 WALDER/HANSJAKOB, S. 99.

28 BASTEN, S. 197.

keinen direkten Zusammenhang mit der Straftat haben müssen.[29] Bspw. wird die Annahme getroffen, dass der Täter vom Tatort mit einem Personenwagen eines bestimmten Autotyps geflüchtet ist. Aus der Datenbank des Motorfahrzeugamts können nun Angaben über sämtliche Halter dieses Typs von Personenwagen eingeholt werden. Dabei muss im Auge behalten werden, dass es grundsätzlich unverdächtig ist, Halter eines solchen Personenwagens zu sein. Die Wahrscheinlichkeit, dass sich der Täter tatsächlich in der gerasterten Schnittmenge befindet, hängt von der Zahl und Schlüssigkeit der Merkmale ab. Es besteht auch die Möglichkeit, dass die gerasterte Schnittmenge ein Produkt des Zufalls ist, weil die angenommenen Merkmale in Tat und Wahrheit täterfern sind.[30]

Beim As gestaltet sich die Rasterfahndung unterschiedlich: Handelt es sich um eine Straftat, die von der selben Täterschaft mehrmals, an jeweils versch. Orten, begangen wurde, ist das Raster einfach zu konstruieren. Es muss die Schnittmenge der Telefonnummern der versch. Antennen, die sich rund um die jeweiligen Tatorte befinden, ermittelt werden.[31] Beim dritten Anwendungsfall des As gestaltet sich die Konstruktion eines Rasters schwieriger. Zumindest erstellt die Polizei aber üblicherweise ein Täterprofil, welches sich mit der Datenmenge vergleichen lässt. Dafür müssen die bis anhin anonymisiert behandelten Daten deanonymisiert werden. Es stellt sich die Frage ob ein solches Vorgehen bei Vorhandensein von sehr grossen Datenmengen überhaupt zielführend und wenn ja verhältnismässig ist. Bei Schnittmengen, die auf Basis von an zwei oder mehr versch. Orten durchgeführten As konzipiert wurden, ermöglicht ein vorhandenes Täterprofil ein zweistufiges Vorgehen.

---

29 HANSJAKOB Erfahrungen, S. 275.

30 JEKER/ROOS, S. 176 f.

31 Interview Hansjakob, a.a.O. S. 39 f.

3 Praxisbeispiele

Nach der theoretischen Einführung in die Thematik, folgt ein Überblick über die Sachverhaltslage der konkret zu betrachtenden Anwendungsfälle.

3.1 Der Fall „Rupperswil“

Am 21. Dezember 2015 fand die Feuerwehr im aargauischen Rupp. die Leichen von 4 Personen: einer Frau, ihren beiden Söhnen und der Freundin des ältesten Sohnes. Die Feuerwehr war ausgerückt, um den gemeldeten Brand eines Wohnhauses zu löschen, wobei sie noch während den Löscharbeiten die Leichen fand. Im Zuge der Ermittlungen stellte sich heraus, dass die 4 Menschen bereits vor Brandausbruch getötet wurden.[32] Der Kriminalfall löste aufgrund der Kaltblütigkeit seiner Ausführung grosse Bestürzung in der Bevölkerung und ein regelrechtes Medienspektakel aus. Der grosse Druck auf die Ermittlungsbehörden zur Aufklärung des grausamen Verbrechens führte dazu, dass die Ermittlungen für die Schweiz aussergewöhnliche Ausmasse annahmen. Rund 40 Ermittler kümmerten sich ausschliesslich um die Lösung des Falles, wobei eine Belohnung in Höhe von CHF 100'000 ausgesetzt wurde. Die Polizei ging diversen Hinweisen nach und setzte sämtlich möglichen Aufklärungsmethoden ein. 146 Tage nach der Tat konnte der mutmassliche Täter festgenommen werden. Z.Z. läuft gegen ihn ein Verfahren, wobei allerdings noch kein konkretes Verhandlungsdatum festgesetzt wurde. Wie aktuell bekannt wurde, sind zur Aufklärung der Tat über 30'000 Handydaten in 48 As erhoben worden, was den Kanton um die CHF 800'000 kostet. Inwiefern die Auswertung der Handydaten erfolgte und zielführend war, wurde bis anhin aus ermittlungstaktischen Gründen nicht veröffentlicht.[33]

3.2 Der Fall „Emmen“

Am 21. Juli 2015 hat ein bislang unbekannter Täter eine 26-jährige Frau bei Emmen LU vom Velo gerissen und brutal vergewaltigt.[34] Die Frau erlitt derart schlimme Verletzungen, dass sie seither vom 5. Halswirbel an abwärts gelähmt ist. Auch dieser Fall hat in der Schweizer Bevölkerung aufgrund seiner Brutalität für Aufsehen gesorgt. Die Luzerner Strafvollzugsbehörden haben i.d.F. alles Mögliche versucht um den Täter zu fassen: Es wurden knapp 10'000 Personendaten überprüft, 371 Männer zum Massen-DNA-Test gebeten und tausende Handydaten mittels As erhoben. Von diesen Daten wurden 1'863 näher überprüft und i.d.F. weitere 32 Personen zum DNA-Abgleich aufgeboten, wobei 29 Proben bereits erhoben und

---

32 NZZ vom 13. Mai 2016.

33 ALTERMATT, AZ vom 13. März 2016.

34 LZ vom 21. Juli 2016.

untersucht werden konnten.[35] Trotz genauer Täterbeschreibung durch das Opfer, zahlreichen Mithilfe-Aufrufen und Hinweisen aus der Bevölkerung, der Aussetzung einer Belohnung von mittlerweile CHF 20'000, dem Beizug externer Experten und 3 bisherigen Festnahmen, ist der Täter nach wie vor nicht identifiziert.[36] Aktuell prüfen die Ermittlungsbehörden einen möglichen Zusammenhang mit dem Namen Aron/Aaron.[37]

35 KOPP in Gespräch mit SRF vom 21. Juli 2016.

36 NZZ vom 13. Februar 2017.

37 TA vom 13. Februar 2017.

4 Dimension von Antennensuchläufen in der Schweiz

Der As ist der breiten Öffentlichkeit erst seit den Fällen „Rupp." und „Emmen" ein Begriff, obwohl er zuvor natürlich auch in weniger berühmten Fällen eingesetzt wurde. Generell lässt sich aber festhalten, dass der As eine selten eingesetzte Ermittlungsmethode ist, da er sich wie bereits beschrieben nur für eine begrenzte Anzahl an Anwendungsmöglichkeiten eignet. In der Schweiz erhebt der ÜPF Daten, die Aufschluss darüber geben, wie viele As bewilligt wurden. Diese Statistik wird im Hinblick auf den As nachfolgend genauer analysiert. Im Anschluss gilt festzustellen, ob sich die Zahl der Durchführungen in den letzten 6 Jahren[38] gesamthaft oder je nach Kanton erhöht hat und ob diese Zahl eine zusehends bedenkliche Höhe erreicht. Zudem lassen sich aus den Statistiken die Gründe ablesen, für welche Art von Straftatbeständen As ermittlungstechnisch eingesetzt werden.

4.1 Schweizweit und nach Kantonen

Bei Betrachtung der Tab. 1 über die Dimension von As in der Schweiz, fällt auf, dass die Zahl der schweizweit durchgeführten As seit dem Jahr 2011, in dem mit 218 die meisten durchgeführt wurden, eher abgenommen bzw. sich auf einem ungefähr gleichbleibenden Niveau eingependelt hat und jeweils zwischen 07% bis max. 1,76% der total durchgeführten Überwachungen ausmacht.[39] Wird in Abb. 1 die Zahl der Durchführungen verteilt auf die einzelnen Kantone betrachtet, fällt auf, dass bis Ende 2016 5 Kantone verbleiben, die noch nie einen As durchgeführt haben und es Kantone gibt, die nur einmalig As durchführten, wobei es sich dabei um mehrheitlich kleine und bevölkerungsarme Kantone handelt.[40] Auffallend ist, dass es relativ viele Kantone gibt, die zu Anfang viele und im Verlauf der Jahre eher wenig bis gar keine As mehr durchführten.[41] Es stellt sich die Frage ob dies reiner Zufall ist, oder ob sich diesbez. eine Art Lerneffekt eingestellt hat. Immerhin besteht die Möglichkeit, dass die Ermittlungsbehörden gelernt haben, mit weniger Suchanfragen das selbe Ergebnis zu erzielen oder feststellen mussten, dass As nicht zum erhofften Ziel führen. Diese Argumentationsweise ist jedoch nicht ganz schlüssig, da es auch Kantone gibt, bei denen die Zahlen ungefähr konstant blieben[42] oder über die Jahre zunahmen.[43] Es lässt sich aber immerhin eine gewisse Tendenz erahnen, dass weniger As durchgeführt werden, da im Jahr

---

38 Die Statistiken wurden von 2011-2016 ausgewertet. Für das Jahr 2017 sind bis anhin keine zuverlässigen Statistiken bekannt.

39 Anh. 3, S. 40 ff.

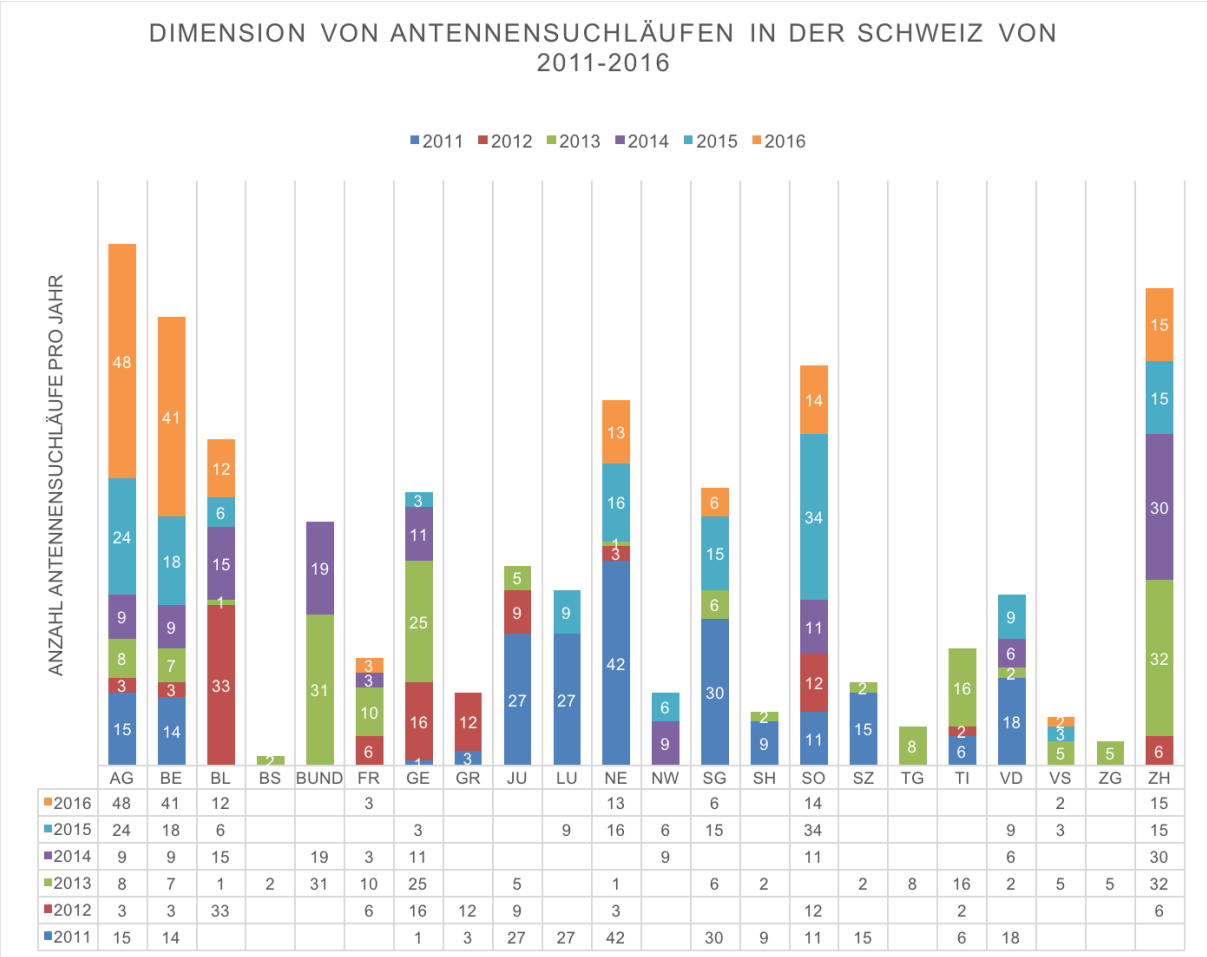
40 Keine bspw. AI, AR oder GL. Einmalig: BS, TG und ZG.

41 Wie bspw. BL, Bund, GR, LU, SH, SZ, VD oder ZH.

42 FR oder VS.

43 AG und BE.

2016 nur 8 Kantone As durchführten im Gegensatz zu 13 Kantone im Jahr 2011. Aus Abb. 1 lässt sich zudem ablesen, dass i.d.R. 1-15 Durchläufe pro Ermittlung reichen und nur in Ausnahmefällen mehr als 30 Durchläufe nötig sind.[44] Zusammenfassend kann festgehalten werden, dass die Zahl, der in der Schweiz durchgeführten As, weder schweizweit noch pro Kanton eine bedenkliche Höhe erreicht hat.[45]



	AG	BE	BL	BS	BUND	FR	GE	GR	JU	LU	NE	NW	SG	SH	SO	SZ	TG	TI	VD	VS	ZG	ZH
2016	48	41	12			3					13		6		14					2		15
2015	24	18	6				3			9	16	6	15		34				9	3		15
2014	9	9	15		19	3	11					9			11				6			30
2013	8	7	1	2	31	10	25		5		1		6	2		2	8	16	2	5	5	32
2012	3	3	33			6	16	12	9		3				12			2				6
2011	15	14					1	3	27	27	42		30	9	11	15		6	18			

Abbildung 1: Dimension von Antennensuchläufen in der Schweiz von 2011-2016, aufgeschlüsselt nach Kantonen. Quelle: selbst erstellt i.A.a. ÜPF Statistik.

44 Bericht Revision VÜPF, S. 59. Der ÜPF führt jede Datenabfrage pro Zelle für einen Zeitraum von 2 h einzeln in der Statistik auf. Deswegen sind meist mehrere Anordnungen für einen As nötig sind, was folg. zu mehreren Durchläufen pro Ermittlung führt.

45 Das Total der pro Jahr durchgeführten As ist in Tab. 1 a.a.O. ersichtlich.

4.2 Straftatbestände

Hinsichtlich der versch. Straftatbestände, die zur Durchführung eines As führten, lässt sich Folgendes festhalten: Am meisten As wurden zur Aufdeckung von Räuben (262), Vorsätzlichen Tötungen (194) und Diebstählen (186) eingesetzt. Danach folgen Freiheitsberaubungen und Entführungen (66), teilw. unter erschwerenden Umständen (55), und schwere Sachbeschädigungen (62). Diese sind als Verbrechen zu qualifizieren, da sie mit Strafen über 3 Jahre bedroht sind.[46] Auffallend ist aber, dass As ebenso zur Aufdeckung von Vergehen oder Übertretungen eingesetzt wurden, nämlich in bisher 57 Fällen von total 803 betrachteten Durchläufen.[47] Diese Vorgehensweise wäre gemäss BGer-Rechtsprechung eigentlich unzulässig, da dieses den „Tatverdacht auf ein schweres Verbrechen" als Voraussetzung des As proklamiert.[48] Der Grossteil der As wird aber zur Aufklärung von Verbrechen eingesetzt. 23 As wurden anscheinend falsch in der Statistik aufgeführt, da sie entweder zur Rubrik der Bestandesdaten-Auskünften oder der Teilnehmeridentifikation zu zählen sind.

Aus Tab. 1 lassen sich zudem auch die in den Fällen „Rupp." und „Emmen" durchgeführten As ablesen, nämlich 48 im Jahr 2016 zur Aufdeckung des Tatbestands von StGB 111 (Vorsätzliche Tötung) im AG und mutmasslich 9 zur Aufdeckung des Tatbestands von StGB 122 i.V.m. 190 (schwere Körperverletzung und Vergewaltigung) im Jahr 2015 in LU.[49]

---

46 Art. 10 StPO.

47 Bei der Aufzählung wurden Straftatbestände, die als Vergehen oder als Übertretung zu qualifizieren sind aber i.V.m. einem Verbrechen verübt wurden, nicht mitgezählt.

48 Vgl. Kap. 6.2.

49 A.a.O. S. 54.

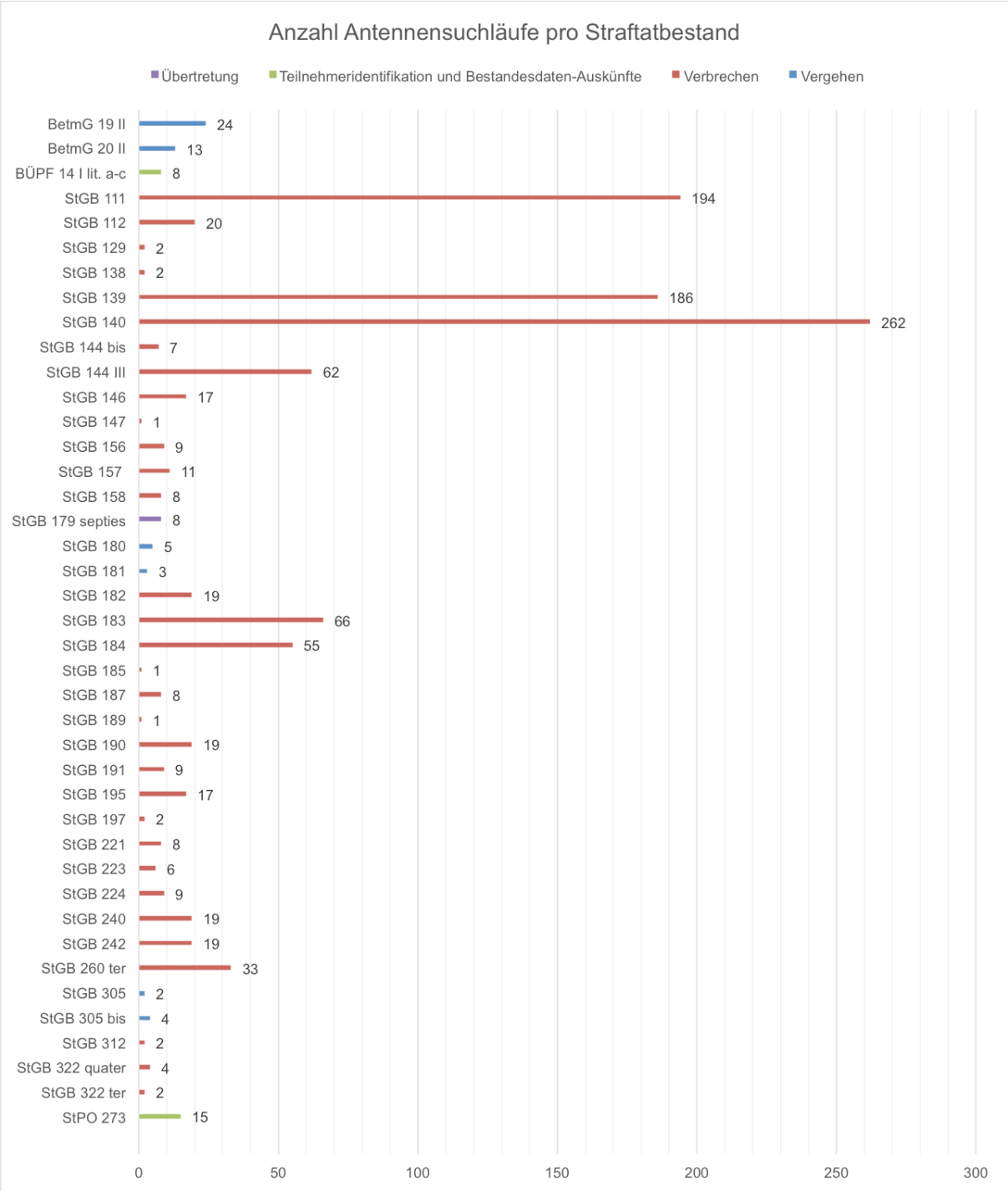


Abbildung 2: Anzahl Antennensuchläufe pro Straftatbestand. Quelle: selbst erstellt i.A.a. ÜPF Statistik.

5 Analyse der rechtlichen Rahmenbedingungen des Antennensuchlaufs

5.1 Systematische Einordnung

Systematisch ist der As sowohl strafprozessualen als auch verwaltungsrechtlichen Bestimmungen zuzuordnen. Dies hat eine historische Ursache: Fernmeldeverkehrsüberwachungen sind in der Schweiz seit dem Jahr 1922 gesetzl. geregelt, waren aber aufgrund der technisch beschränkten Möglichkeiten eher rudimentär ausgestaltet.[50] Zudem war der Telefonmarkt verstaatlicht und die PTT einziger FDA. In den 1970er Jahren schuf der Bund in Art. 66 BStP die bis heute prägende Grundlage: Überwachungen sind zulässig, sofern sie zur Aufdeckung von Verbrechen und Vergehen dienlich sind, deren Schwere oder Eigenart die Überwachung legitimieren. Zudem bedarf es einer richterlichen Genehmigung.[51]

Nach der Privatisierung des Marktes stiegen die Anforderungen an die gesetzl. Rahmenbedingungen und das Koordinationsbedürfnis. Es bedurfte einer einheitlichen Koordinationsstelle zur Zusammenarbeit zwischen kt. Strafvollzugsbehörden und privaten FDA, weswegen im Jahr 1998 auf Grundlage der ÜV der DBA[52] gegründet wurde. Im Jahre 2000 wurde das BÜPF beschlossen und 2002 in Kraft gesetzt. Darin waren nun die Fernmeldeverkehrsüberwachungen national einheitlich verankert und sämtliche, in strafprozessualer und verwaltungsrechtlicher Hinsicht, relevanten Bestimmungen zentriert geregelt. Auch der DBA wurde dem BÜPF unterstellt, wobei er einige Jahre später zu ÜPF umbenannt wurde. Ergänzend wurden die Bestimmungen in der VÜPF konkretisiert und die GebV-ÜPF gab Aufschluss über die Kosten der Überwachung. Im Jahr 2011 kam der Erlass der StPO und die strafprozessualen Bestimmungen wurden darin integriert, damit nicht ein wesentlicher Teil des mat. Strafprozessrechts in einem anderen Gesetz geregelt war.[53] Die verwaltungsrechtlichen Bestimmungen verblieben im BÜPF. Die VÜPF und die GebV-ÜPF blieben in Kraft, wobei erstere im Jahr 2011 totalrevidiert wurde.[54] Im Zuge dieser Revision fand u.a. auch der As seinen Einzug in die V. Aktuell wird das BÜPF und damit einhergehend auch die VÜPF totalrevidiert. Dies um dem technischen Fortschritt und dem gesteigerten Koordinationsbedürfnis gerecht zu werden.[55]

---

50 Kommentar StPO 2014/HANSJAKOB, Art. 269 N 1.

51 Botschaft BÜPF, S. 4246 f.

52 Der Dienst betreibt insb. die EDV-Anlage, welche die Daten der Überwachung von den FDA entgegennimmt und den Polizeibehörden übergibt.

53 Interview Hansjakob, a.a.O. S. 35.

54 Kommentar StPO 2014/DERS., Art. 269 N 1.

55 Interview Ders., a.a.O. S. 36; Botschaft Revision BÜPF, S. 2689.

5.2 Erste Anträge

Schon in den 1990er Jahren wurden erste Anträge an die Swisscom herangetragen, Daten für As bereitzustellen. Die Swisscom wies die Anträge allesamt ab mit dem Hinweis ab, dass ein As keinen bestimmten Anschluss überwacht, sondern eine „Fläche“ um eine Antenne herum und daher rechtlich unzulässig sei. In einzelnen schwerwiegenden Ausnahmefällen erwies sich die Swisscom jedoch kooperativ und stellte den Strafvollzugsbehörden nichtsdestotrotz die Daten zur Verfügung. Dies nur in den Fällen, in denen sie As unter den Tatbestand des geltenden Rechts subsumieren konnte. Dafür bedurfte es gemäss der Swisscom die Versicherung, dass der gesuchte Anschluss individualisiert werden könne, bspw. mittels Schnittmengen-Konstruktion der Antennenstandorte, an denen ein Polizist eine verdächtige Person zu versch. Zeitpunkten telefonieren sah. Die Ermittlung des individualisierten Anschlusses verblieb zu Handen der FDA und dieser leitete zur Wahrung des Fernmeldegeheimnisses nur die individualisierten Daten an die Strafvollzugsbehörden weiter. Bei andersartigen Anfragen, bei denen eine Individualisierbarkeit schon von Anfang an ausgeschlossen werden konnte, weigerte sich die Swisscom weiterhin Daten bereitzustellen. Vor Erlass des BÜPF stellte diese Handhabung der FDA kein Problem dar, da keine Bundesbehörde sie zur Durchführung der Überwachung zwingen konnte. Diese Praxis liess auch die ÜV von 1997 zu.[56]

5.3 Erste Urteile

Erst als 2002 das BÜPF in Kraft trat, tauchte der Begriff des As zum ersten Mal in der ordentlichen Gerichtspraxis auf. Im Jahr 2002 weigerte sich die Swisscom einen As durchzuführen, weil sie diesen aufgrund einer fehlenden gesetzl. Grundlage für unzulässig hielt. Der DBA erliess nun gewissermassen unfreiwillig und entgegen seiner früheren Haltung eine Vf., die die Swisscom zur Durchführung des As zwang. Die Swisscom klagte i.d.F. vor der RK UVEK gegen diese Vf. Die RK UVEK anerkannte der Swisscom zwar eine generelle Beschwerdelegitimation zu, da es sich bei der Anordnung des DBA um eine Vf. nach Art. 5 VwVG handelt, konnte die Legitimationsbasis aber keiner Bestimmung des BÜPF zuordnen. Durch Auslegung füllte die RK UVEK die uneigentliche Gesetzeslücke dahingehend, dass sie der Swisscom die Rechtsmittelmöglichkeit trotzdem einräumte, da eine solche anscheinend vergessen wurde und dies nicht Sinn und Zweck des Gesetzgebers sein könne. Obwohl somit grundsätzlich auf die Beschwerde eingetreten war, wurde der Swisscom dennoch die Möglichkeit verwehrt die Legalität der Überwachungsart zu rügen.[57]

---

[56] HEINIGER, Rz. 36 ff.

[57] DERS., Rz. 14 ff.

Fernmeldeüberwachungen werden bei Vorliegen gewisser Voraussetzungen vom StA angeordnet und durch ein ZM-Gericht genehmigt. Der zuständige Dienst erteilt daraufhin gemäss BÜPF dem FDA den Auftrag zur Durchführung der Überwachung. Die Problematik besteht insb. darin, dass der FDA sich nicht gegen diese zweistufige Anordnung wehren kann. Er kann sich erstens nicht gegen die kt. Anordnung des StA bzw. des ZM-Gerichts wehren, da diese nicht an ihn direkt, sondern an den Dienst gerichtet ist, und zweitens auch nicht gegen die i.d.F. durch den Dienst erlassene Vf.. Der Dienst legt nämlich Art. 13 Abs. 1 lit. a BÜPF, der seine Aufgaben definiert, wörtlich aus, weswegen er weder die technische Realisierbarkeit noch die Legalität der Massnahme überprüft. In der ÜV konnte der neugegründete DBA noch prüfen ob die Überwachung dem anwendbaren Recht entspricht.[58] Heute prüft der ÜPF lediglich ob die Überwachung von einer dafür zuständigen Behörde angeordnet wurde und ob eine Straftat im Sinn des Straftatbestandskatalogs vorliegt. Sind diese Voraussetzung erfüllt, bleibt dem Dienst nichts anderes übrig, als auch Durchführungen von Überwachungen anzuordnen, die ohne gesetzl. Grundlage verlangt werden. Im Endeffekt kann sich der FDA nicht gegen die Vf. zur Wehr setzen, weil eine allfällige Beschwerdekommission keine Kognition hat, die über diejenige des Dienstes hinaus geht. Es fehlt m.a.W. eine Bundesbehörde, welche die Pflichten der FDA eingehender reguliert.[59]

Die Swisscom gab sich mit dem Entscheid der RK UVEK nicht zufrieden und zog das Verfahren weiter bis vor BGer. In BGer 1A.185/2003 wurde das Beschwerderecht der Swisscom, welches ihr die RK UVEK durch Auslegung zugestand, bestätigt.[60] Das BGer stimmte allerdings mit der RK UVEK überein, dass die Swisscom keine angeordnete und durch sie umzusetzende Massnahme als unzulässig rügen könne. Es kam lediglich zur Konklusion, dass sich FDA gegen für sie aus technisch oder organisatorischen Gründen nicht durchführbare Überwachungen wehren können. Da die Swisscom schon früher in Ausnahmefällen As durchgeführt hat, kann sie sich folg. auf keine solche Unmöglichkeit berufen. Das BGer stellte zudem fest, dass die Legitimität von Überwachungen ohne gesetzl. Grundlage wie dem As sowieso indirekt gegeben sei, weil die überwachten Personen nach Mitteilung der Überwachung nachträglich gegen diese Beschwerde führen können. Auf diesem Weg könne die allfällige Unzulässigkeit der Massnahme gerügt werden.[61] Somit ebnete das

---

58 Art. 6 Abs. 1 lit. a ÜV.

59 HEINIGER, RZ. 5, spricht dahingehend von einem konzeptionellen Fehler im BÜPF. Dieser Fehler soll insb. durch die aktuelle Revision behoben werden. Botschaft Revision BÜPF S. 2696. Art. 16 lit. b E-BÜPF.

60 DERS, Rz. 17. A.M., SCHLAURI, S. 239. SCHLAURI kommt zum Schluss, dass das BGer gar nie auf die Beschwerde eingetreten ist.

61 BGer 1A.185/2003 E. 2.2.3. Dazu kritisch HEINIGER., RZ. 18. Ihm ist in der Annahme zuzustimmen, dass im Normalfall nicht sämtliche durch As betroffene Personen über die Datenerhebung informiert werden. Dass Betroffene kein Informationsrecht haben wurde aktuell auch auf S. 2764 der Botschaft Revision BÜPF fest-

BGer den Strafvollzugsbehörden den Weg gesetzl. ungeregelte Überwachungsmassnahmen anzuordnen, da sich die FDA nicht gegen solche Anordnungen wehren können. Obwohl sich das BGer nicht direkt mit der Zulässigkeit des As beschäftigte, legitimierte es dessen Praxis indirekt, weswegen die Durchführung von As zur Regel wurde.

5.4 Grundsatzurteil und gesetzliche Grundlage

As sind Ermittlungstechniken, die selten eingesetzt und normalerweise nur vor einem nicht öff.-tagenden ZM-Gericht beurteilt werden, weswegen es zur Thematik äusserst wenige Gerichts-U. gibt. Es erstaunt daher nicht, dass sich das BGer erst 2011 erstmals direkt mit der Zulässigkeit von As beschäftigte. Dies war möglich, weil diesmal kein FDA Beschwerdeführer war, sondern ein StA, der nach Art. 81 Abs. 1 Ziff. 3 BGG gegen den Nichtgenehmigungsentscheid seines ZM-Gerichts klagte. In diesem Fall war folg. der konzeptionelle Fehler nach Art. 13 Abs. 1 lit. a BÜPF irrelevant. In BGer 1B_376/2011 wurde der viel beachtete Entscheid gefällt, dass As nicht ausdrücklich gesetzl. geregelt sind. Um sie aber dennoch für zulässig zu erklären und entsprechend der bisherigen Praxis zu agieren, definierte das BGer teilw. aus Art. 269 StPO abgeleitete einschränkende Kriterien, die erfüllt sein müssen, um As durchzuführen.[62] Die Problematik, dass sich FDA nicht gegen unzulässige As wehren können, besteht diesbez. aber weiterhin, weil FDA nicht berechtigt sind, die Nichteinhaltung der BGer-Kriterien zu rügen.

Problematisch scheint auch, dass das BGer in diesem Grundsatz-U. davon ausgeht, dass die FDA nur anonymisierte Daten an die Ermittler weitergeben. Dies ist zwar richtig, weil nur Telefonnummern ohne die Angabe von Benutzerdaten herausgegeben werden. Da die Telefonnummern aber real existieren und die Polizei gemäss Art. 14 BÜPF berechtigt ist Bestandesdaten-Auskünfte einzuholen, können die Nummern immer eindeutig einem Kunden zugeordnet werden, wodurch der Schutz des Fernmeldegeheimnisses umgangen wird. Anbieter dürfen Kundendaten nämlich nur an Dritte – zu denen auch die Polizei zählt – weitergeben, wenn es dafür einen Rechtfertigungsgrund gibt, der vorliegend aufgrund der fehlenden Gesetzesbestimmung gerade nicht gegeben ist.[63]

---

gehalten. Dies erklärt die in der Einführung durch Jeker (in ALTERMATT, AZ vom 18. März 2016) bemängelte Transparenz der Massnahme. Vielen Betroffenen ist nicht bewusst, dass sie Gegenstand von Ermittlungen sind. Solange sie deswegen aber keine Nachteile erleiden, scheint fraglich, inwiefern sie diesbez in ihren Rechten tangiert werden. Nachteile lassen sich zumeist erst ab diesem Zeitpunkt erahnen, ab dem die Betroffenen sowieso wissen, dass sie Gegenstand von Ermittlungen sind, bspw. weil sie zur Befragung berufen werden.

62 Die Kriterien werden in Kap. 6 vertieft analysiert.

63 HEINIGER, Rz. 57.

Im Jahr 2012 wurde der As schliesslich auf Begehren des EJPD in die VÜPF in Art. 16 lit. e aufgenommen und gesetzl. somit zumindest auf V.-Stufe verankert. Dieser Entscheid war bereits vor Bekanntgabe von BGer 1B_376/2011 gefällt worden.[64] Im Jahr 2001 hielt das EJPD den As noch für unzulässig, da er keiner Bestimmung des BÜPF oder der StPO zugeordnet werden konnte.[65] Obwohl sich am form. Gesetz in der Zwischenzeit nichts geändert hatte, sah das EJPD die Notwendigkeit der „Nachführung der geltenden Verordnung".[66] Damit spielte das EJPD auf BGer 1A.185/2003 an, indem As unglücklicherweise indirekt für zulässig befunden wurden, obwohl direkt nie gerichtlich über deren Zulässigkeit befunden wurde. Ein direkter Entscheid über die Zulässigkeit erfolgte eben genaugenommen erst 2011, was allerdings zeitlich zu spät erfolgte und somit bei Neugestaltung der VÜPF keine Beachtung mehr fand. Diesbez. besteht eine Diskrepanz zwischen Rechtsprechung und Gesetz: Laut VÜPF sind As voraussetzungslos durchzuführen, gemäss BGer-Rechtsprechung nur unter Einhaltung einschränkender Kriterien.[67]

5.5 Gebühren und Bestimmungen des BÜPF

Neben der VÜPF ist in gesetzl. Betrachtungsweise des As auch die GebV-ÜPF massgebend. Aus ihr werden einerseits die Kosten der Überwachung, andererseits aber auch der genaue Ablauf eines As ersichtlich. Nachdem die Ermittlungsbehörden die Durchführung durch Bewilligung des ZM-Gerichts erwirkt haben, werden die Angaben über den Ort und das betreffende Zeitintervall an den ÜPF dirigiert, welcher die Angaben an den FDA mit der entsprechenden Vf. weiterleitet. In einem ersten Schritt wird untersucht, welche Antennne den Ort bedienen, bspw. auch welche Zellen überhaupt in die Richtung des Tatorts senden. Dies können die Ermittlungsbehörden entweder durch den Dienst abklären lassen, was gemäss GebV-ÜPF einmalig CHF 2'310 kostet[68] oder durch den Einsatz eines IMSI-Catchers,[69] was gebührenfrei ist. Sind die potentiellen Antennen ermittelt, muss die StA entscheiden, welche Antennendaten am ehesten erfolgsversprechend sind. Meistens beschränken sich die Ermittlungsbehörden auf die Antennen, die durch den in der Bevölkerung bevorzugten FDA betrieben werden.[70] Von den ausgewählten Zellen werden nun Daten eingeholt, was pro Zelle für einen zu betrachtenden Zeitraum von 2 h und pro Datentyp – Telefonie oder

---

64 DERS., Rz. 46.

65 HANSJAKOB Kommentar BÜPF/VÜPF 2002, Art. 16 VÜPF RZ. 15; Bericht EJPD VÜPF, S. 10.

66 Begleitschreiben SOMMARUGA Änderung VÜPF/GebV-ÜPF. Der Satz erntete in der Vernehmlassung Kritik:. ASUT, S. 1 ff., insb. Kap. 1.3.

67 HEINIGER, RZ. 47.

68 Ermittlung der geografischen Koordinaten gemäss Art. 2 GebV-ÜPF (CS 5).

69 Interview Hansjakob, a.a.O. S. 44. Der IMSI-Catcher ist ein Ermittlungstechnisches Gerät, welches u.a. die Fähigkeit hat, sämtliche in der Nähe zur Verfügung stehenden Antennen anzuzeigen.

70 Ders, a.a.O. S. 45.

Internet – CHF 630 kostet.[71] Will man Aufschluss über beide Verkehrsdaten-Arten müssen pauschal CHF 1'260 bezahlt werden. Schlussendlich muss auch noch pro Bestandesdaten-Auskunft CHF 5 Gebühr bezahlt werden.[72] Die Kosten der Überwachung können demnach wie folgt berechnet werden:[73]

$$\text{Gebühr pro Zelle} \times \text{Anzahl Zellen} \times \text{Datentyp} \times \frac{\text{Überwachungsdauer}}{2} + (\text{Gebühr pro Bestandesdaten-Auskunft})$$

Wie sich erahnen lässt, schiessen die Kosten in ihrer Summe schnell in die Höhe. Die Gebühren sind auch aus Gründen der Verhältnismässigkeit so hoch angesetzt, damit nicht in jedem kleineren Fall Telefonüberwachungen angeordnet werden. Sie fungieren somit als Art künstliche Hürde.[74] Der grösste Teil dieser durch den ÜPF erhobenen Gebühren wird den FDA zur Deckung ihrer Kosten, die ihnen aufgrund des zusätzlichen Aufwands und Ressourceneinsatzes entstehen, überlassen.[75] Z.Z. steht anlässlich der Revision der GebV-ÜPF zur Disskussion die Gebühren aufgrund des kleinen Kostendeckungsgrades von 50% nochmals zu erhöhen.[76]

Aktuell wurde die Debatte über die Kosten der Fernmeldeüberwachung in der Öffentlichkeit aufgegriffen, nachdem bekannt wurde, dass die im Fall „Rupp." angewandte Handy-Analyse per As die Aargauer Justiz CHF 800'000 kostet. Die Höhe der Rechnung erntete viel Kritik, da offenbar aus Zeitgründen von Seiten der Strafvollzugsbehörden kein Mengenrabatt verlangt wurde. Ein solcher ist zwar in der GebV-ÜPF nicht vorgesehen, wäre aber angebracht gewesen, da der Rechnungsbetrag kaum dem Prinzip der Kostendeckung, welcher der GebV zugrunde liegt, entspricht. Der Rechnungsbetrag ist insb. daher so hoch, weil die Antennendichte in Rupp. sehr hoch ist (siehe Abb. 3), ein Zeitraum von deutlich über 2 h betrachtet wurde und vollständige Datensätze erhoben worden sind.[77]

---

71 Art. 2 GebV-ÜPF (CS 6). Dass für beide Datentypen bezahlt werden muss ergibt sich aus der Praxis und ist nicht ausdrücklich im Gesetz geregelt, was mit Revision der GebV-ÜPF behoben werden soll.

72 Art. 2 GebV-ÜPF (A 0).

73 Interview Umbricht, Anh. 2, S. 48.

74 Interview Hansjakob, a.a.O. S. 45.

75 Gemäss KPMG. S. 32 ff., liegt der Aufwand insb. in Betriebs- (u.a. Server zur Datenspeicherung) und Personalkosten (eine FDA führt bspw. Überwachungen mit 13 eigens dafür angestellten Vollzeitstellen durch).

76 Bericht Revision GebV-ÜPF, S. 2.

77 Interview Umbricht, a.a.O. S. 48.

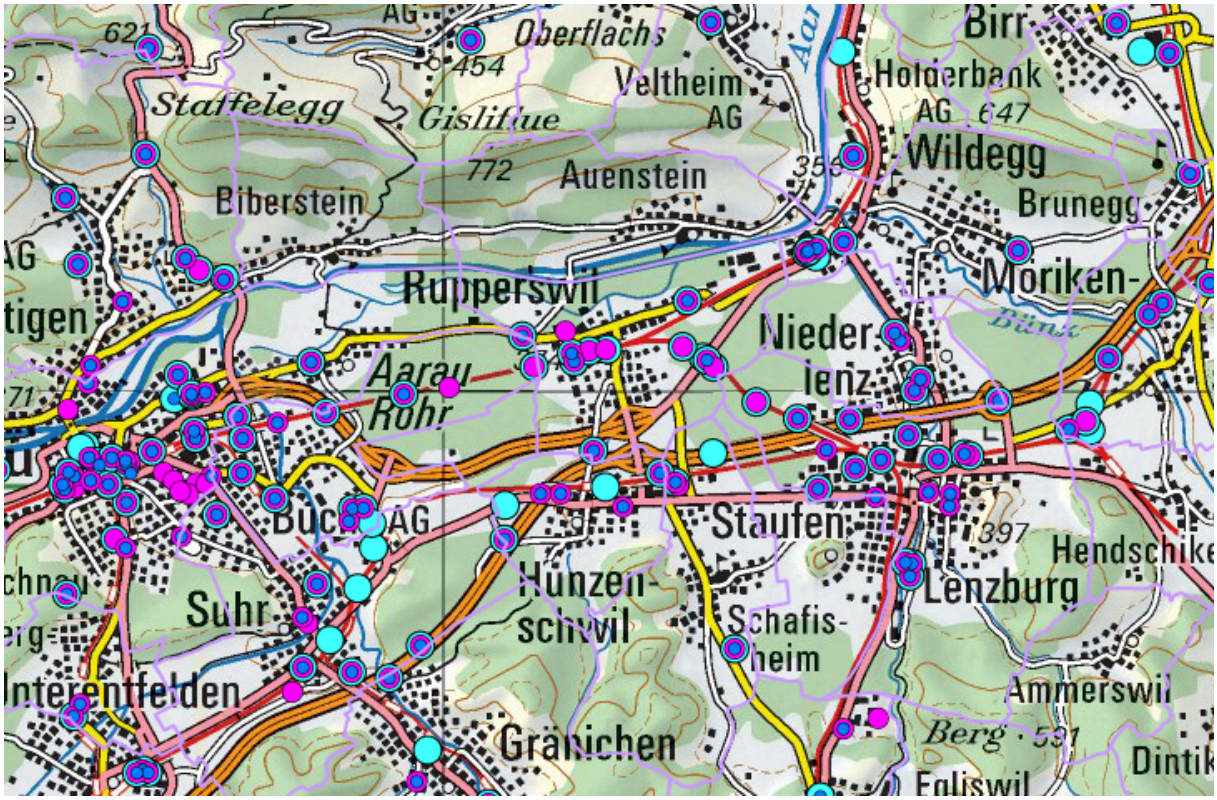


Abbildung 3: Antennendichte in Rupp. abg. v.: <https://map.geo.admin.ch>

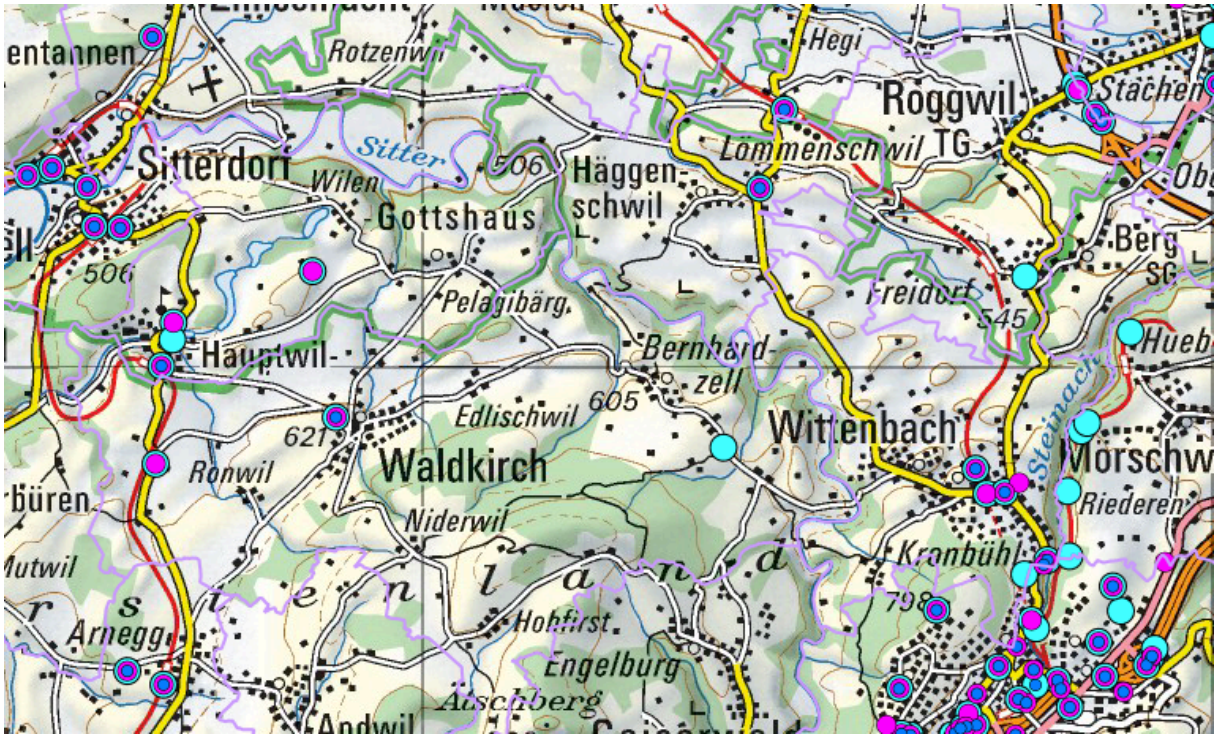


Abbildung 4: Zum Vergleich: Antennendichte in Wittenbach (weshalb siehe Interview, S. 39) und Umgebung. Die hohe Antennendichte unten rechts ist jene der Stadt St.Gallen. abg. v.: <https://map.geo.admin.ch>

Neben der VÜPF und der GebV-ÜPF sind für den As auch andere Bestimmungen des BÜPF von Bedeutung. Art. 15 Abs. 3 BÜPF regelt die Aufbewahrung der Verkehrsdaten durch die FDA. Diese müssen die Daten während mind. 6 Monaten speichern um sie den Strafverfol-

gungsbehörden auf Antrag rückwirkend aushändigen zu können. Die Daten werden während dieser Zeit von den Anbietern entsprechend den gesetzl. Bestimmungen über den Datenschatz behandelt.[78] Nach Ablauf der Frist dürfen die Daten überschrieben werden, was aber aus buchhalterischen Gründen meist nicht sofort geschieht, da die Daten zur Rechnungsstellung benötigt werden.[79] Zudem ist auch der bereits erwähnte Art. 14 BÜPF bezüglich der Bestandesdaten-Auskunft von Belang.

5.6 Rechtsstaatliche Problematik

Bei einer Auseinandersetzung mit dem As muss immer auch beachtet werden, dass er gewisse rechtsstaatliche Risiken birgt.

5.6.1 Eingriff in die Privatsphäre und Qualifikation als Zwangsmassnahme

Erstens stellt der As einen Eingriff in die Privatsphäre dar, welche verfassungsrechtlich in Art. 13 BV geschützt ist.[80] Das Recht auf Schutz vertraulicher Komm., worunter auch Randdaten fallen, ist Teilgehalt des Rechts auf Privatsphäre.[81] Strafprozessuale Einschränkungen von Grundrechten müssen deshalb immer den Anforderungen von Art. 36 BV genügen, sprich auf einer gesetzl. Grundlage basieren, aufgrund eines öff. Interessens erfolgen, verhältnismässig sein und den Kerngehalt unangetastet lassen. Beim As ist die erste Voraussetzung seit dem Jahr 2012 erfüllt. Ein As stellt i.d.R. aus mehreren Gründen keinen schweren Grundrechtseingriff dar, weswegen die Normstufe als genügend bezeichnet werden kann.[82] Das öff. Interesse an Überwachungen des Fernmeldeverkehrs besteht in der Strafverfolgung[83] und kann als gewichtiges Eingriffsinteresse qualifiziert werden, da es dem Schutz von Polizeigütern dient. Ob die Verhältnismässigkeit der Massnahme – d.h. deren Eignung, Erforderlichkeit und Zumutbarkeit – und die Wahrung des Kerngehalts gegeben ist, muss im Einzelfall eruiert werden.

Zusätzlich müssen strafprozessuale Grundrechtseinschränkungen Art. 196 ff. StPO erfüllen und können didaktisch als ZM bezeichnet werden. ZM sind nach Gesetz Verfahrenshandlungen, die dazu dienen Beweise zu sichern, die Anwesenheit von Personen im Verfahren sicherzustellen oder die Vollstreckung des Endentscheides zu gewährleisten. Der Katalog von

---

78 Bspw. Art. 43 und 45b FMG.

79 HANSJAKOB Das neue BÜPF, S. 441 f.

80 JEKER/ROOS, S. 180.

81 BSK BV/DIGGELMANN, Art. 13 N 29 ff.

82 Schwere Grundrechtseingriffe müssen gemäss Art. 36 Abs. 1 formell.-gesetzl. verankert sein. Der Grundrechtseingriff wird vom BGer als nicht schwer qualifiziert, weil zur Schnittmengen-Konstruktion nicht alle Verkehrsdaten personenbezogen überprüft werden. Gl.M. HEIMGARTNER, S. 8, soweit der Datenabgleich manuell vorgenommen und somit das Recht auf informationelle Selbstbestimmung nur virtuell tangiert wird.

83 Botschaft BÜPF, S. 4256 f.

zulässigen ZM ist seit Erlass der StPO einheitlich in ihr geregelt und als abschliessend zu betrachten. Da es dem Gesetzgeber aber grundsätzlich frei steht, weitere ZM zu erlassen, scheint die neuerliche Konkretisierung der zulässigen Fernmeldeverkehrsüberwachungen in der VÜPF legitim. Das Problem besteht aber dahingehend, dass Art. 197 Abs. 1 StPO ähnlich wie Art. 36 Abs. 1 BV eine gesetzl. Grundlage verlangt, dabei aber weiter als die Verfassung geht, da er ein Gesetz im form. Sinn verlangt und nicht wie die BV nur für schwere Eingriffe.[84] Folg. genügt rein theoretisch die gesetzl. Grundlage auf V.-Stufe nicht.

Um die rechtsstaatliche Problematik des Aspekts der fehlenden form.-gesetzl. Grundlage, die im Hinblick auf die Durchführung von ZM erforderlich wäre, zu heilen, scheint es angebracht eine solche in der StPO zu verankern. [85] Systematisch sinnvoll ist eine Ergänzung von Art. 273 StPO, weil in diesem die Teilnehmeridentifikation geregelt ist, zu der sich auch der As zählen lässt. Leider hat der Gesetzgeber die Chance, die sich mit der aktuellen Revision des BÜPF und der damit einhergehenden Anpassung der StPO anbietet, verpasst und eine form.-gesetzl. Verankerung des As als unnötig erachtet.[86] Der As wird zukünftig in Art. 64-66 E-VÜPF geregelt sein.

5.6.2 Tangierung Dritter

ZM richten sich normalerweise nur gegen den Beschuldigten. Wenn aber Dritte tangiert werden, muss nach Art. 197 Abs. 2 StPO besondere Zurückhaltung ausgeübt werden.[87] Bei einer ZM wie dem As werden jedoch zwangsläufig immer Dritte betroffen sein, da anders als bei herkömmlichen Überwachungsmassnahmen nicht der Anschluss einer bestimmten Person, sondern Daten sämtlicher Personen, die über eine bestimmte Antenne mobil kommuniziert haben, überwacht werden. In der Konsequenz, dass durch den As notwendigerweise Daten unbescholtener Dritter ins Visier genommen werden, besteht dessen zweite rechtsstaatliche Problematik.

Randdatenerhebungen Dritter sind in Art. 270 lit. b StPO geregelt. Der Wortlaut von Art. 270 lit. b Ziff. 1 und 2 ist zunächst auf die aktive und geheime Überwachung von Fernmeldeanschlüssen zugeschnitten.[88] Anschlüsse von Dritten dürfen geheim überwacht werden, wenn angenommen werden kann, dass entweder die beschuldigte Person den Anschluss der Drittperson benutzt oder die Drittperson für die beschuldigte Person bestimmte Mitteilungen entgegennimmt oder von dieser stammende Mitteilungen an eine weitere Person weiterlei-

---

84 Kommentar StPO 2014/Hug/SCHEIDEGGER, Art. 197 N 1; SG Kommentar BV/SCHWEIZER, Art. 36 N 1 f.

85 Interview Hansjakob, a.a.O. S. 44.

86 Botschaft Revision BÜPF, S. 2748 f. Dies u.a. deswegen, weil der Grundrechtseingriff durch As nicht besonders schwer ist.

87 Kommentar StPO 2014/Hug/SCHEIDEGGER, Art. 197 N 21 ff.

88 BGer 1B_563/2012; BGer 1B_251/ 2013 E. 5.3 ff.

tet.[89] Die Voraussetzungen an die aktive Überwachung von Dritten sind somit hoch. Der As zählt jedoch zu den rückwirkenden Randdatenerhebungen, weswegen eine „Benutzung" oder voraussichtliche „Entgegennahme" oder „Weiterleitung" von Mitteilungen durch Dritte von Vornherein ausgeschlossen ist. Das BGer schliesst aber eine Randdatenerhebung bei Dritten, die nicht zugleich Anschlussinhaber oder Nachrichtenmittler sind, nicht grundsätzlich aus,[90] verlangt jedoch mit Verweis auf die einschlägige Rechtsprechung bei rückwirkenden Erhebungen nach Art. 273 StPO einen direkten Sachzusammenhang zwischen der Überwachungsmassnahme und dem untersuchten Delikt.[91]

Zudem hält das BGer fest, dass Art. 270 lit. b StPO das Ziel verfolgt, die Privatsphäre unschuldiger Dritter zu schützen,[92] wobei der angestrebte Schutz hinfällig wird, sobald die betroffene Drittperson der Überwachung zustimmt oder sie aus Eigeninteressen wünscht.[93] Dies bedeutet jedoch nicht, dass die Zustimmung der Drittperson die gesetzlichen Voraussetzungen der Überwachung zu derogieren vermag.[94] Die Voraussetzungen zur Überwachung nach Art. 269-273 StPO – insb. jenes der richterlichen Genehmigung – sind somit auch dann zwingend einzuhalten.

Beim Versuch diese Rechtsprechung auf den As zu übertragen, fallen gleich 4 Problembereiche ins Auge: Erstens werden beim As Dritte überwacht, die weder Anschlussinhaber noch Nachrichtenmittler sind, was eigentlich nicht dem Wortlaut von Art. 270 lit. b StPO entspricht. Da das BGer jedoch rückwirkende Randdatenerhebungen von Drittpersonen nicht grundsätzlich ausschliesst, kann dieser Punkt vernachlässigt werden. Dies auch in Anbetracht dessen, dass Art. 270 lit. b StPO auf die aktive Randdatenerhebung zugeschnitten ist, aber beim As keine Gesprächsinhalte eingeholt werden und die Daten zusätzlich gerastert werden. Zweitens erfolgt die i.c. streitige Randdatenerhebung Dritter nicht geheim und die Drittperson hat ihr ausdrücklich zugestimmt. Der As ist jedoch eine geheime Massnahme, weswegen eine Zustimmung der betroffenen Dritten unmöglich ist. Da eine solche aber sowieso nicht die gesetzl. Voraussetzungen derogiert, kann auch dieser Punkt unbeachtet bleiben. Drittens besteht wiederum das Problem der fehlenden form.-gesetzl. Grundlage. Gemäss obiger Analyse müssen bei Randdatenerhebungen Dritter die gesetzl. Voraussetzungen beachtet werden, worunter eben auch der bereits im vorherigen Kap. beschriebene Art.

---

89 BGer 1B_256/2015.

90 FELLMANN.

91 BGer 1B_251/2013 E. 5.5.

92 Dies ergibt sich aus der Entstehungsgeschichte und dem Sinn und Zweck der Norm. Dazu BGer 1B_563/2012 E. 5; BGer 1B_251/2013 E. 5.5

93 BGer 1B_256/2015 E. 4.2.3.

94 FELLMANN.

197 StPO fällt. Viertens wurde die rückwirkende Randdatenerhebung eines Dritten u.a. wegen eines fehlenden direkten Sachzusammenhangs zwischen der Überwachung und dem untersuchten Delikt als unzulässig erklärt. Beim As bei dem u.U. sehr viele Personen gleichzeitig überwacht werden, ist kaum vorstellbar, dass sich zwischen jeder Überwachung und dem zu untersuchenden Delikt ein sachlicher Zusammenhang finden lässt. Ein solcher ist nur bei der ermittelten Täterschaft klar anzunehmen. Wird jedoch der As gesamthaft als Überwachungsmassnahme betrachtet und nicht jede Datenerhebung als einzelne Massnahme, lässt sich ein sachlicher Zusammenhang erkennen, da das Ergebnis des As für die Aufklärung der Straftat von wesentlicher Bedeutung ist.

5.6.3 Tatverdachtsbegründung

Ein As wird zumeist angewendet, bevor man einen konkreten Verdacht gegen eine bestimmte Person hat. Der Tatverdacht stellt aber Dreh- und Anfangspunkt von strafprozessualen Ermittlungen dar, da er gemäss Art. 197 Abs. 1 StPO gesetzl. Voraussetzung für die Ergreifung einer ZM ist und zudem das öff. Interesse an der Verfolgung der Straftat darstellt.[95] Ermittlungen ohne Anfangsverdacht sind dem Beweisverwertungsverbot unterworfen, da es sich um Ergebnisse der Beweisausforschung handelt.[96] Die vom BGer gesetzte Hürde zur Annahme eines Anfangsverdachts ist jedoch sehr tief angesetzt.[97] Das Problem beim As verbleibt aber dennoch: Wenn man den individuell zurechenbaren Tatverdacht als rechtsstaatliche Voraussetzung zum Grundrechtseingriff mittels ZM erachtet, so sollten verdachtsfreie Ermittlungshandlungen per se unzulässig sein. Das Gesetz kennt jedoch ausser dem As noch weitere verdachtsfreie ZM, nämlich bspw. die Haft wegen Ausführungsgefahr gemäss Art. 221 Abs. 2 StPO, die DNA-Massenuntersuchung nach Art. 256 StPO und die Aufbewahrung und Verwendung von erkennungsdienstlichen Unterlagen nach Art. 261 Abs. 1 lit. b StPO.[98] In diesem Sinn stellt die Verdachtsfreiheit des As keine Singularität dar. Das Besondere ist aber, dass diese anderen ZM form.-gesetzl. verankert sind und demzufolge demokratisch legitimiert sind. Beim As ist diese rechtsstaatliche Absicherung nicht gegeben. Immerhin schafft der Umstand, dass As einer Bewilligung seitens des ZM-Gerichts bedürfen, Linderung. Zudem muss auch festgehalten werden, dass ein Verdächtiger nie alleine aufgrund der Ergebnisse eines As verurteilt werden kann. Im Allg. bedarf es weiterer Beweise, die auf Basis der Ermittlung der Täterschaft mittels As gewonnen werden.[99] Es stellt sich nichtsdestotrotz die Frage, ob diese pragmatische Haltung im Hinblick auf die Verhältnismässigkeit in den Fällen „Rupp." und „Emmen" weiterhin angebracht scheint.

---

95 Das Gesetz kennt dabei keine Legaldefinition des Tatverdachts.

96 BSK StPO/GFELLER/THORMANN, Art. 243 N 39 ff.

97 KARNUSIAN, S. 352.

98 DERS., S. 354.

99 Interview Hansjakob, a.a.O. S. 44 f.

6 Analyse der Kriterien und deren Anwendung auf die Praxisbeispiele

Wie bereits verdeutlicht besteht eine Diskrepanz zwischen der VÜPF und der BGer-Rechtsprechung bez. den Voraussetzungen des As. Aufgrund der fehlenden form.-gesetzl. Verankerung der rückwirkenden Rasterfahndung, empfiehlt sich zur Wahrung der Verhältnismässigkeit die weitere Anwendung der in BGer 1B_376/2011 ausgearbeiteten Kriterien. Um zu prüfen ob diese in den Fällen „Rupp." und „Emmen" eingehalten wurden, müssen sie zuerst genauer analysiert und erklärt werden.

6.1 Gesetzliche Grundlage

Das erste durch das BGer betrachtete Kriterium ist jenes der gesetzl. Grundlage.[100] Die bisherige Lehre subordinierte den As unter Art. 269 und 273 StPO, welche die Voraussetzungen der Fernmeldeüberwachung und die Erhebung von Verbindungs-, Verkehrs und Rechnungsdaten der „überwachten Person" regeln.[101] Der Wortlaut von Art. 273 StPO setzt voraus, dass die Person schon individualisiert ist, was beim As eben nicht der Fall ist. Die einhellige Lehre hat zuvor angenommen, dass der Begriff der „überwachten Person" dem Ergebnis der Rasterung der Datenmenge gleichgesetzt werden kann, da dies ein rein technischer Vorgang sei. Dem hat das BGer widersprochen und den As einer komplett neuen Kategorie von Fernmeldeverkehrsüberwachungen zugeordnet: der systematischen Rasterfahndung, die nicht ausdrücklich in Art. 273 StPO geregelt sei. Das BGer hat i.d.F. auf die geplante Aufnahme des As in die V. hingewiesen. In der Zwischenzeit liegt die gesetzl. Grundlage in Art. 16 lit. e VÜPF vor, die aber eigentlich gemäss Art. 197 StPO auf einer zu niederen Normstufe rangiert. Das Kriterium der gesetzl. Grundlage ist in den Fällen „Rupp." und „Emmen" zwar nicht als vollumfänglich erfüllt zu betrachten, was mit Blick auf das Legalitätsprinzip problematisch ist, allerdings muss angenommen werden, dass dieser Umstand vor BGer nicht zur Unzulässigkeitserklärung der Beweiserhebung führen wird, da das BGer jedoch selbst bei Vorliegen gar keiner gesetzl. Grundlage die Zulässigkeit von As bejaht hat.

---

100 BGer 1B_376/201 E. 5.1 ff.

101 CR StPO/ BACHER/ZUFFEREY, Art. 273 N 4; Kommentar StPO 2010/HANSJAKOB, Art. 273 N. 4; SCHMID 2009, Art. 273 N. 5.

6.2 Dringender Tatverdacht auf ein schweres Verbrechen

Das BGer hat weiter festgehalten, dass die nicht ausdrücklich gesetzl. geregelte Erhebung von Verkehrs-Randdaten per As im Rahmen einer Rasterfahndung gegen Unbekannt in Anlehnung an Art. 269 Abs. 1 lit. a und b, sowie Abs. 2 StPO das Vorliegen eines dringenden Tatverdachts auf ein Verbrechen verlangt.[102] Obwohl das BGer den As nicht direkt unter Art. 269 StPO subordiniert, wendet es dessen Voraussetzungen an die Überwachung des Fernmeldeverkehrs ansatzweise analog an. Dieses Vorgehen ist kritisch zu hinterfragen, da geheime Überwachungsmassnahmen bisher ohne Erhebung von Komm.-Inhalten gemäss Art. 273 StPO auch zur Aufklärung von Vergehen zulässig waren, bzw. die Erhebung von Komm.-Inhalten nur bei Vorliegen einer in Art. 269 StPO aufgeführten Katalogtat. Durch die neue BGer-Rechtsprechung gibt es fortan 3 Kategorien: Erstens die Teilnehmeridentifikation für Verbrechen und Vergehen, zweitens die Erhebung von Komm.-Daten bei Vorliegen einer Katalogtat und drittens As, die nur bei Verbrechen zulässig sind. Das Kriterium des Verbrechens soll wohl die Verhältnismässigkeit von As wahren, wobei dies zu strikt greift.[103] Der Katalog von Art. 269 StPO beinhaltet neben Verbrechen nämlich noch weitere Deliktarten, weswegen die Einschränkung der Zulässigkeit von As auf Verbrechen sinnlos scheint. Die Erhebung von Komm.-Inhalten ist ein schwererer Eingriff in die Grundrechte, während die Eingriffsschwere des As niedriger anzusetzen ist, weswegen es kaum Sinn macht die Hürden an den As höher zu stellen. Es hätte ausgereicht die Voraussetzungen jenen des Kataloges von Art. 269 gleichzustellen. Zudem kann sogar die Ansicht vertreten werden, dass der As durchaus auch für die Aufklärung von Vergehen nützlich sein kann und die Beschränkung auf Verbrechen somit erschwerend für die Ermittlungsbehörden sein könnte. Die Voraussetzungen von Art. 273 StPO – das Vorliegen eines Verbrechens oder Vergehens – sind passender.[104] Dies wiederspiegelt sich auch in der Praxis, in der As auch zur Aufklärung von Vergehen eingesetzt werden.[105]

Was aber primär festgehalten werden muss, ist, dass ein As kein präventiver Suchlauf ist, wenn er nicht das Ziel verfolgt Straftaten zu finden, sondern erst eingesetzt wird, nachdem bereits ein Delikt begangen wurde,[106] was in den Fällen „Rupp." und „Emmen" zu bejahen ist. Der Tatverdacht auf ein schweres Verbrechen liegt vor: Im Fall „Rupp." kann die Straftat als vierfache vorsätzliche Tötung bzw. u.U. vierfacher Mord qualifiziert werden, da der Täter

---

102 BGer 1B_376/2011 E. 6.1

103 HANSJAKOB Zulässigkeit, Rz. 16.

104 DERS. a.a.O. Rz. 17 f.

105 Siehe Kap. 4.2.

106 SCHMID 2014, Art. 269 N 7.

besonders verwerflich vorging und seine Motive sexueller und finanzieller Natur waren.[107] Im Fall „Emmen“ liegt ebenfalls ein schweres Verbrechen vor, namentlich eine Vergewaltigung i.V.m. schwerer Körperverletzung, aufgrund derer das Opfer bleibend körperlich geschädigt ist.[108] Somit ist diese Voraussetzung erfüllt und die grundsätzliche Kritik an der bundesgerichtlichen Einschränkung bleibt i.c. irrelevant.

6.3 Individualisierbarkeit

Das BGer hält fest, dass alleine der Umstand, dass ein Tatverdacht auf ein schweres Verbrechen noch keiner Person individuell zugerechnet werden kann, unerheblich ist, solange die noch unbekannte und flüchtige Täterschaft im Rasterergebnis grundsätzlich identifizierbar ist.[109] Somit stimmt das BGer der einschlägigen Lehre zu, dass das Ergebnis der Rasterung eine Individualisierbarkeit zulässt, zieht aber nicht wie diese den Rückschluss, dass aufgrund dieser Auslegung der As Art. 273 StPO zugeordnet werden kann. Das BGer sieht die Individualisierbarkeit viel mehr als Voraussetzung zur Durchführung eines As. Diese Haltung erinnert an jene, die die Swisscom bereits in den 90er-Jahren vertreten hat. Das BGer wendet das Kriterium i.d.F. auf den konkret zu betrachtenden Fall an.

Um die konkrete Anwendung nachvollziehen zu können bedarf es einiger Hintergrundinformationen: Der BGer 1B_376/2011 zugrunde liegende Sachverhalt stellt sich so dar, dass es im Zeitraum vom 13. Januar 2011 und dem 9. März 2011 an 3 versch. Orten – Lachen SZ, Berikon AG und Schaffhausen – zu 3 qualifizierten Raubüberfällen gegen Bijouteriegeschäfte gekommen ist, bei denen Obj. im Wert von CHF 2,2 Mio. entwendet wurden. Aufgrund der bis zum Zeitpunkt des Verfahrens erfolgten Untersuchungsergebnisse, gehen die Ermittlungsbehörden davon aus, dass die Überfälle zumindest teilw. von der selben Täterschaft begangen wurden und diese vor und nach der Tat und insb. auch vor Beschaffung eines Fluchtfahrzeugs mobil kommuniziert hat. Aufgrund dessen hält das BGer klar fest, dass i.c. der dringende Tatverdacht auf ein schweres Verbrechen gegeben ist, da die Raubüberfälle bewaffnet ausgeführt wurden, es zu Gewaltanwendungen kam und die erbeutete Deliktsumme sehr hoch war. Nun stellt sich gemäss BGer-Auslegung die Frage, ob die Täterschaft im Rasterergebnis grundsätzlich identifizierbar ist, da ansonsten die Unerheblichkeit der individuellen Zurechnung nicht gegeben ist. I.c. ist dies klar zu bejahen, da die Durchführung an 3 versch. Orten erfolgt und ein Abgleich der Telefonnummern der versch. Antennenstandorten mit grösster Wahrscheinlichkeit zu einem konkreten Ergebnis führen wird. Zudem wurden die Täter auch von Zeugen beobachtet, was einen weiteren Abgleich ermöglicht. Das BGer

---

107 Art. 112 StGB.

108 Art. 190 i.Vm. 122 StGB.

109 A.a.O. E. 6.1

verwendet im Anschluss einen ganzen Abschnitt um ausdrücklich darauf hinzuweisen, dass entgegen der Ansicht der Vorinstanz der hier streitige As nicht dafür dient einen inexistenten Tatverdacht originär zu begründen oder nach Straftaten zu suchen, sondern „der Individualisierung und Identifizierung der Täterschaft bei bereits objektiv konkretisiertem dringendem Tatverdacht“ dienlich ist.[110]

Versucht man diese Logik auf die Fälle „Rupp.“ und „Emmen“ anzuwenden, lassen sich gewisse Schwierigkeiten erahnen: Das BGer erachtete die Wahrscheinlichkeit als hoch aufgrund der Triage eine eindeutige Individualisierung der Täterschaft zu ermöglichen. In den Fällen „Rupp.“ und „Emmen“ fehlt diese Konnexität, da es sich um Einzeltaten handelt, die von Einzeltätern begangen wurden. Daran ändert auch der Umstand nichts, dass in Rupp. drei verschiedene Antennenstandorte überwacht wurden.[111] Es handelt sich nämlich anscheinend um Orte, die sehr nahe beieinander liegen, weswegen die Wahrscheinlichkeit sehr gross ist, dass sich an allen 3 Orten ähnliche Personen aufgehalten haben. Aufgrund dessen, dass es sich um Einzeltäter handelt ist auch nicht anzunehmen, dass während der Tat mobil kommuniziert werden musste, bspw. um sich mit jemandem abzusprechen. Zumindest im Fall „Emmen“ war dieser Umstand sehr bald bekannt, da das Opfer spätestens wenige Wochen nach der Tat, vernommen werden und das alleinige Vorgehen des Täters beschreiben konnte. Beim Fall „Rupp.“, wo Zeugen fehlten, kann aufgrund fehlender Einsicht in die Ermittlungsakten nicht genau eruiert werden, ab welchem Zeitpunkt die Ermittlungsbehörden wussten, dass nur ein einzelner Täter am Werk war. Es kann jedoch angenommen werden, dass die Behörden alsbald von einem Einzeltäter ausgehen konnten, da nur eine DNA-Spur gefunden wurde und die Opfer nacheinander getötet wurden. Da die Möglichkeit der Schnittmengen-Konstruktion nicht gegeben ist bzw. aufgrund des aktuellen Erkenntnisstandes als nicht sehr erfolgsversprechend einzustufen ist, bleibt fraglich wie eine Individualisierung der Täterschaft erfolgen soll.

Es stellt sich nun die Frage ob die As in den Fällen „Rupp.“ und „Emmen“ rein der Ermittlung einer bisher unbekannten Täterschaft dienten oder ob die Datenmenge vielmehr für Alibiabklärungen verwendet wurde. Während ersteres unzulässig ist, da ein möglicher Abgleich eher schwierig scheint, muss der zweite Fall als zulässig erachtet werden, da sich in dieser Konstellation der Tatverdacht ja bereits vor einer allfälligen Rasterung gegen eine bestimmte Person richtet und somit individuell zurechenbar ist. Das Kriterium der Individualisierbarkeit wäre deshalb erfüllt. Schlussfolgernd dürfte ein solcher As erst ab dem Zeitpunkt durchgeführt werden, ab dem ein erster Tatverdächtiger ermittelt wurde. Angesichts der hohen Kosten im Fall „Rupp.“ und der Medienaussagen im Fall „Emmen“, die auf eine personenbezo-

110 A.a.O. E. 6.3

111 Interview Umbricht, a.a.O. S. 48.

gene Handydaten-Analyse schliessen lassen, ist die Annahme der Erhebung zu reinen Alibi-Abklärungen aber als unwahrscheinlich einzustufen.

Im Fall „Emmen“ liegt eine konkrete Täterbeschreibung durch das Opfer vor. Obwohl somit eine Schnittmengen-Konstruktion in räumlicher Hinsicht nicht möglich scheint, besteht zumindest die Möglichkeit der Rasterung mittels Täterprofil. Das Problem hierbei ist aber, dass dafür sämtlich erhobenen Daten deanonymisiert gerastert werden müssten, da dazu ein Abgleich von Personendaten und nicht reinen Telefonnummern erforderlich wäre. Dieses Vorgehen entspricht nicht der Auffassung des BGer, dass As keinen schweren Eingriff in die Privatsphäre darstellen, da nur anonymisierte Randdaten betrachtet werden. Somit ist auch im Fall „Emmen“ bei Anwendung der BGer-Kriterien die Durchführung des As erst möglich, sobald ein konkreter Tatverdächtiger ermittelt worden ist.

6.4 Subsidiarität und keine inhaltliche Überwachung

Das BGer verlangt im Sinne von Art. 269 Abs. 1 lit. c, dass der As nur subsidiär, d.h. als ultima ratio eingesetzt wird.[112] Im BGer 1B_376/2011 zugrunde liegenden Sachverhalt war dies dahingehend erreicht, dass die bereits umfangreichen Untersuchungsanstrengungen – namentlich DNA-Spurenauswertungen, Zeugenbefragungen, Personen- und Fahrzeugüberprüfungen, Publikation von Phantombildern, usw. – erfolglos verblieben sind. Die Subsidiarität ist somit zu bejahen. Analog lässt sich eine solche auch in den Fällen „Rupp.“ und „Emmen“ erkennen, da wie bereits verdeutlicht, die dortigen Ermittlungsbemühungen grosse Ausmasse annahmen. Im Fall „Rupp.“ wurde die Nachbarschaft eingehend befragt, Computer-Daten analysiert,[113] DNA-Spuren – sogar von Hunden – ausgewertet[114] und eine Belohnung im Wert von CHF 100'000 ausgesetzt. Erst im Januar, knapp einen Monat nach der Tat, wurden Anträge für die Durchführung eines As gestellt, weswegen eine Subsidiarität zu bejahen ist. Im Fall „Emmen“ sieht dies ähnlich aus: Es wurden 10'000 Personendaten überprüft, Massen-DNA-Tests durchgeführt, Mithilfe-Aufrufe an die Bevölkerung übers Radio und Fernsehen veröffentlicht und eine Belohnung von CHF 20'000 ausgesetzt. Somit ist auch dort die „ultima ratio“ gegeben.

Gemäss BGer-Rechtsprechung ist als weiteres Kriterium die Voraussetzung zu prüfen, dass „keine inhaltliche Überwachung erfolgt“. Eine solche bedarf einer weiteren Bewilligung seitens des ZM-Gerichts und stellt einen gröberen Eingriff in die Privatsphäre dar. Es dürfen daher nur Verkehrsdaten erhoben werden und keine Komm.-Daten. Dieses Kriterium stellt

---

112 A.a.O. E. 6.3.

113 AZ vom 9. Juni 2016.

114 AZ vom 5. Juni 2016.

semantisch einen Pleonasmus dar, da bereits die Definition des AS deutlich macht, dass dieser immer nur zur Erhebung von Verkehrs- und eben nie für Komm.-Inhalte eingesetzt wird. Deswegen ist davon auszugehen, dass dieses Kriterium in sämtlichen Fällen erfüllt ist.

6.5 Kleine Schnittmenge

Das letzte durch das BGer betrachtete Kriterium der „kleinen Schnittmenge“ hat einige Ähnlichkeit mit jenem der „Individualisierbarkeit“. Während letzteres dafür sorgt, dass der Tatverdacht schliesslich einem Täter bzw. den Tätern konkret zugeordnet werden kann, sorgt ersteres dafür, dass nicht zu viele Personen als allfällige Täter, denen der Verdacht zugerechnet werden könnte, in Frage kommen. Das Kriterium der „kleinen Schnittmenge“ sorgt demgemäss dafür, dass nicht zu viele Daten deanonymisiert behandelt werden und das Fernmeldegeheimnis gewahrt bleibt.

Das BGer hält fest, dass die Rasterung aus Praktikabilitätsgründen durch die StA erfolgen soll und nicht direkt durch die FDA. Dies würde die Wahrung des Fernmeldegeheimnisses nicht beeinträchtigen, da die Analyse von anonymisierten Daten keinen schweren Grundrechtseingriff darstellt. Eine personenbezogene Identifizierung rechtfertige sich erst beim Ergebnis der Rasterung.[115] Die klageführende StA versicherte vor BGer ausdrücklich, dass bis zur Schnittmengen-Eruierung keine Feststellung von Personalien erfolge. Dafür muss aber die Möglichkeit zur sachgerechten und gezielten Eingrenzung von einigen wenigen tatverdächtigen Personen bestehen, was vorliegend durch Ortsbasierte-Rasterung möglich war. Das BGer erachtete i.c. die Wahrscheinlichkeit als sehr hoch nur eine kleine Schnittmenge von Verdächtigen als Ergebnis der Rasterung vorzufinden, da die Orte der Raubüberfälle und der Fluchtfahrzeug-Beschaffung weit auseinander liegen und es praktisch ausgeschlossen scheint, dass sich noch weitere unverdächtige Personen zufällig an allen Antennenstandorten zur fraglichen Zeit aufhielten.

Diese Argumentation scheint schlüssig, obwohl sich einige Problembereiche erahnen lassen: Erstens ist die kleine Schnittmenge immer eine Mutmassung. Ob die Schnittmenge tatsächlich klein ist, kann erst im Nachhinein festgestellt werden. Zweitens ist das Kriterium dann als besonders problematisch einzustufen, wenn keine anderen Beweise wie bspw. DNA-Spuren vorliegen, die es ermöglichen würden, rein zufällig gerasterte Personen als mögliche Täter auszuschliessen. Diese wären gezwungen ihre Unschuld darzulegen, da die Stochastik ihre Beteiligung an der Straftat als sehr wahrscheinlich erachtet.[116]

---

115 BGer 1B_376/2011 E. 6.5.

116 JEKER/ROOS, S. 180.

Zudem besteht das Problem, dass sich die Argumentationsweise nicht beliebig auf sämtlich mögliche Fälle übertragen lässt. Im Fall „Emmen“ sind keine Anhaltspunkte für eine Ortsbasierte-Rasterung ersichtlich. Denkbar ist eine Rasterung durch den Abgleich mit dem Signalement der Täterschaft, das allenfalls Angaben über das Geschlecht, das Alter oder die mutmassliche Nationalität erlaubt. Gemäss Hansjakob muss im Einzelfall entschieden werden ob die Qualität des Profils die Deanonymisierung einer grösseren Datenmenge rechtfertigt. Dies hängt zudem auch von der Schwere der aufzuklärenden Straftat ab. Hansjakob hält es bspw. für zulässig auch mehrere Dutzend Telefonnummern personenbezogen zu überprüfen, wenn das Opfer einer schweren Straftat den genauen Zeitpunkt einer mobilen Komm. benennen und weitere Angaben über das Aussehen des Täters machen kann.[117]

Diese Haltung scheint prinzipiell richtig. Es besteht jedoch ein grosser Unterschied ob mehrere Dutzend oder eben allenfalls mehrere Hundert oder sogar Tausend Nummern deanonymisiert betrachtet werden, was anscheinend im Fall „Emmen“ geschehen ist. Dort wurden 1'863 Handydaten eingehender überprüft und im Anschluss 32 Personen zum DNA-Test aufgeboten. Es kann die Annahme getroffen werden, dass die 1'863 Daten auf das durch das Opfer beschriebene und auch veröffentlichte Signalement des Täters geprüft wurden und schliesslich 32 Männer im Raster hängen blieben. Diese Schnittmenge wurde nicht aus einer anonymen Datenmenge gebildet, sondern aus einer deanonymisierten. Dies widerspricht der Argumentationsweise des BGer, dass das Fernmeldegeheimnis nur intakt bleibt, wenn eine kleine Menge an Daten personenbezogen analysiert wird. Diese Annahme ist jedoch nicht belegt, da sich die Luzerner Ermittlungsbehörden aus taktischen Gründen über die genaue Vorgehensweise bedeckt halten.

Ähnlich verhält es sich im Fall „Rupp.“, bei dem ebenfalls nicht bekannt ist, wie die Ermittler die 30'000 Daten genauer analysiert haben. Das Einzige was diesbez. neu in Erfahrung gebracht werden konnte, ist, dass As an 3 versch. Standorten durchgeführt wurden, wobei jedoch angenommen werden muss, dass diese sehr nahe beieinander liegen. In den beiden Fällen besteht gerade auch das Problem, dass die Masse an abgefangenen Daten sehr hoch ist, weil in Rupp. in der Nähe des Tatorts die Autobahn A1 und die Bahnlinie Aarau/Zürich verläuft und in Emmen die Autobahn A14, sowie teilw. die A2. Die Antennen registrieren deshalb überproportional viele Rufnummern, was die Wahrscheinlichkeit, dass sich ein unbeteiligter Dritter zufällig im Rasterergebnis befindet, erhöht. Auf Basis der Annahmen ist das Kriterium der „kleinen Schnittmenge“ wohl in beiden Fällen nicht erfüllt, da eine zu grosse Menge an Daten deanonymisiert betrachtet werden müsste. Wenn die Daten aber zu Alibi-Abklärungen erhoben wurden, fällt die Problematik der Nichteinhaltung des Kriteriums dahin.

---

117 HANSJAKOB Zulässigkeit, Rz. 23.

7 Fazit

As sind immer noch selten eingesetzte Ermittlungsmethoden, führen jedoch eine Reihe von Problemen mit sich: Erstens bewegen sie sich im Spannungsfeld zwischen Sicherheit und Freiheit. Zweitens greifen sie als ZM trotz fehlender form.-gesetzl. Verankerung in die Grundrechtsphäre des Einzelnen ein und drittens gibt es eine bundesgerichtliche Konkretisierung der Zulässigkeitsvoraussetzungen, welche in der Praxis jedoch teilw. mehr als Richtlinie, denn als verbindliche Vorgabe verstanden wird. Dies insb. deshalb, weil sich gewisse Kriterien nicht auf sämtliche Anwendungsfälle übertragen lassen oder zu strikt greifen. In der Praxis wird bspw. das Kriterium des „Tatverdachts auf ein schweres Verbrechen" in knapp 8% der total durchgeführten As nicht erfüllt.[118]

Zwar fällt es angesichts der fehlenden vollumfänglichen Einsicht in die Ermittlungsakten schwierig, ein abschliessendes U. über die Zulässigkeit des As in den Fällen „Rupp." und „Emmen" zu treffen, auf Basis der getroffenen Annahmen, muss jedoch festgehalten werden, dass die Kriterien – haupts. jenes der „Individualisierbarkeit" und der „kleinen Schnittmenge" – wohl nicht eingehalten werden konnten. Dies aufgrund dessen, dass es sich um Einzeltaten handelt und sich keine erfolgsversprechende Möglichkeit zur Schnittmengen-Konstruktion anbietet. Wurden die As zu reinen Alibi-Abklärungen eingesetzt, verhält sich die Sachlage anders, weil somit der Tatverdacht individuell zurechenbar und die Kriterien-Einhaltung zu bejahen ist. Angesichts der Kosten der Überwachung im Fall „Rupp." und den Medienaussagen im Fall „Emmen" ist die Erhebung zum Zweck der reinen Alibi-Abklärung aber eher unrealistisch. Die Kriterien „Subsidiarität", „keine inhaltliche Überwachung" und „Tatverdacht auf ein schweres Verbrechen" sind in den Fällen „Rupp." und „Emmen" erfüllt. Das Kriterium der „gesetzlichen Grundlage" ist zumindest auf V.-Stufe normiert.

Was die Folgen der Nichteinhaltung der bundesgerichtlichen Kriterien in den Fällen „Rupp." und „Emmen" sein könnten, lässt sich zum jetzigen Zeitpunkt und auf Basis dieser Analyse nicht abschätzen. Um aber Bezug auf die einführende Divergenz zwischen „mehr Sicherheit" oder „mehr Freiheit" zu nehmen, kann argumentiert werden, dass das öff. Interesse an der Aufklärung eines schweren Verbrechens die Deanonymisierung einer grösseren Datenmenge rechtfertigt. Dies in Anbetracht dessen, dass niemand alleine auf Basis eines As angeklagt werden kann. Eine Grenze zu ziehen, bei welchen Verbrechen wie viele Daten betrachtet werden dürfen, ist jedoch eine schwierige Abgrenzungsfrage.

---

[118] Vgl. Kap. 4.2.

Der Gesetzgeber hat aktuell die Chance zur form.-gesetzl. Verankerung des As, die sich mit der Totalrevision des BÜPF und der damit einhergehenden Anpassung der StPO bietet, ungenutzt verstreichen lassen, da er den As als nicht schweren Grundrechtseingriff erachtet. Dabei wird jedoch ausser Acht gelassen, dass es bei der form.-gesetzl. Verankerung des As auch viel mehr darum geht, die bundesgerichtlichen Zulässigkeitsvoraussetzungen zu diskutieren, gegebenenfalls anzupassen und die Grenzen des As national einheitlich und klar zu regeln. Die form.-gesetzl. Verankerung soll nicht dem Täterschutz dienen, sondern vielmehr der strafprozessualen Ideologie Rechnung tragen, dass ZM in demokratisch legitimierter Art und Weise angewendet werden. Damit der Grundrechtseingriff für Dritte auch weiterhin klein bleibt, muss insb. ein Verbot der Deanonymisierung sehr grosser Datenmengen in Betracht gezogen werden. Der Grundrechtsschutz Dritter ist zwar in Art. 197 Abs. 2 und 270 lit. b StPO gewährleistet, kann aber unter der aktuellen Rechtslage durch die Polizei umgangen werden. Damit sich Diskussionen um die Zulässigkeitsvoraussetzungen von As bzw. deren allfälligen Verletzung nicht in weiteren Fällen wiederholen, sollten die Fälle „Rupp." und „Emmen" als Chance betrachtet und eine Diskussion zwischen Gesetzgeber, Praxis und rechtssprechenden Organen um die optimale Ausgestaltung der ZM eröffnet werden. Die diskutierten Zulässigkeitsvoraussetzungen sollten sich anschliessend im form. Gesetz wiederfinden.

Anhang

Anhang 1: Interview mit Dr. Thomas Hansjakob

Das Gespräch fand am 12. Januar 2017 von 10:00-11:00 Uhr in St.Gallen statt. Dr. Thomas Hansjakob ist Erster Staatsanwalt von St.Gallen und führender Experte auf dem Gebiet des As, sowie generell von strafprozessualen Telefonüberwachungen. Er hat u.a. den Kommentar zum BÜPF verfasst, sowie den in dieser Arbeit mehrmalig zitierten Kommentar zu den Art. 269-273 StPO.

Frage 1:[119] Die StPO wurde 2011 erlassen. Im Zuge dieses Erlasses gliederte man die strafprozessualen Bestimmungen des Fernmeldeverkehrs aus dem BÜPF aus, um sie in die StPO zu integrieren. Die verwaltungsrechtlichen Angelegenheiten verblieben im BÜPF. Warum?

Eine Alternative wäre gewesen, dass man trotz Erlass der StPO das BÜPF in seiner damaligen Form belassen hätte. Dann wären aber wesentliche strafprozessuale Bestimmungen ausserhalb der StPO, sprich in einem anderen Gesetz, geregelt gewesen. Aus dieser Sicht war die Übernahme der materiell-rechtlichen Bestimmungen in die StPO richtig. Ob diese Integration einheitlich war ist eine andere Frage. Ich als Staatsanwalt muss sagen, dass ich das BÜPF seit diesem Schritt gar nicht mehr zur Hand nehme. Das steht eigentlich nun nichts mehr drin, was mich für meine tägliche Arbeit interessiert.

Also sind nun nur noch rein verwaltungsrechtliche Begebenheiten im BÜPF geregelt?

Ja, eigentlich schon. Es gibt Ausnahmen, also gewisse Bestimmungen, die eine Reflexwirkung haben, die sich auch auf das materielle Recht auswirken. Aber im Wesentlichen sind die rein verwaltungsrechtlichen Bestimmungen im BÜPF verblieben. Ja, das kann man so sagen. Dies ist auch völlig richtig so. Die materiell-rechtlichen Bestimmungen sind und gehören in die StPO. Es ist auch in allen umliegenden Ländern so geregelt, dass die Voraussetzungen für die fernmeldeverkehrliche Überwachung in der StPO geregelt sind.

Also gibt es aus ihrer Sicht nur Vorteile, dass man die materiell-rechtlichen Bestimmungen aus dem BÜPF ausgegliedert hat?

Ja.

---

[119] Das Gespräch ist wortwörtlich wiedergegeben, weswegen an dieser Stelle auf die in dieser Arbeit verwendeten Abkürzungen verzichtet wird. Ausnahmen werden bei Gesetzen gemacht, da auch während des Gesprächs die geläufigen Kurzformen verwendet wurden.

Keine Nachteile? Ich habe zum Beispiel gelesen, dass es nun Koordinationsprobleme in der Anwendung von strafprozessualen und verwaltungsrechtlichen Bestimmungen gibt?

Ja, das stimmt. Aber das gibt es überall. Das gibt es auch im Bereich des Strafvollzuges oder in der Abgrenzung was nun materiell-rechtlich Strafrecht und was Strafprozessrecht ist. Solche Probleme gibt es schlichtweg immer. Das ist von untergeordneter Bedeutung und die Ausgliederung war überzeugend.

Frage 2: Nun wird das BÜPF totalrevidiert. Was sind die Gründe, die für diese Revision sprechen?

Der Hauptgrund ist, dass man der technischen Entwicklung folgen muss. Das ist sehr interessant, denn das was wirklich für uns materiell-rechtlich neu ist, ist nicht in der Region des BÜPF selber geregelt, sondern das sind die Änderungen im Anhang der StPO. Die wesentlichen Punkte sind: die Zulässigkeit des Einsatzes von IMSI-Catchern und GovWares und die Notsuche. Alles was eigentlich wesentlich neu im BÜPF steht, interessiert uns Staatsanwälte nur am Rande. Aber um nochmals zu betonen: im Wesentlichen geht es um die Anpassung an den technischen Fortschritt. Es ist auch so, dass man nun eine ganz andere Organisation im Hintergrund hat. Die Sachen werden immer komplexer. Als man das BÜPF erlasen hatte, hatte der Dienst noch einigermassen einfache Apparaturen. Es war im Wesentlichen klar, wie Überwachungen praktisch funktionieren. Mittlerweile sind Überwachungen sehr viel komplexer geworden. Auch der Dienst ist sehr viel grösser geworden und hat neue Möglichkeiten gebraucht, v.a. auch gegenüber den Anbietern. Früher, also 2002, als das BÜPF in Kraft trat, war es sehr einfach den Anbietern aufzuzeigen, was diese an Daten zu liefern hatten. Heute ist dies aufgrund der neuen komplexen Technologien anders. Nun müssen auch die Anbieter einen relativ grossen Aufwand leisten, damit sie überhaupt das erfüllen können, was von ihnen verlangt oder gebraucht wird. Der Dienst muss dies den Anbietern vorschreiben können und deshalb braucht es hier eine neue Bestimmung. Bis anhin war das im BÜPF eigentlich nicht so vorgesehen, dass man den Anbietern im grossen Stil sagen muss, wie und warum Überwachungen umzusetzen sind. Der Dienst muss deshalb auch Sanktionsmöglichkeiten bekommen. Das hatte man unter dem alten BÜPF nicht. Wenn ein Anbieter etwas nicht macht, was er eigentlich müsste, konnte man ihn bis anhin nicht sanktionieren. Deshalb braucht es neue Bestimmungen.

Hat man dies dann 2002 verpasst?

Nein, das war damals kein Problem. Geschichtlich muss man sehen, dass bis zum Jahr 1998 die Telekommunikation rein staatlich geregelt war. Die Swisscom oder die damalige

PTT hatte ein Monopol und war eine staatliche Organisation. Vor 1998 haben wir der PTT einfach gesagt was wir brauchen und die PTT hat dies gemacht. Damals haben auch Kosten keine so grosse Rolle gespielt. Man hat die Kosten einfach auf die Preise für die Kunden abgewälzt. Diese Kosten waren jetzt aber auch nicht immens gross, sondern ein eher vernachlässigbarer Posten. Und dann kam im Jahr 1998 die Privatisierung und man hat festgestellt, dass man nun mit Privaten zusammenarbeiten muss und dass es diesbezüglich einer Koordinationsstelle bedarf. Man gründete den Dienst bereits 1998 (also vor dem BÜPF) um diese Koordination zu bewerkstelligen. Man musste aber Überwachungen des Fernmeldeverkehrs trotzdem noch gründlicher und klarer regeln. Von der technischen Seite her, hat man 1998 im Wesentlichen nur Festnetzanschlüsse überwacht, was technisch wenig anspruchsvoll ist. Erst allmählich hat man begonnen Mobilfunkanschlüsse zu überwachen. Das war damals auch nicht besonders schwierig, weil Mobiltelefone hauptsächlich nur über die Telefonier-Funktion verfügten. Man hatte damals gar keinen Bedarf den Anbietern genauere Weisungen zu übertragen. Jedem war klar, wer was zu tun hatte, weil alles relativ einfach umzusetzen war.

Hätte man nicht bis zu einem gewissen Punkt antizipieren können, dass hier technische Erneuerungen kommen würden?

Ja, gewisse Leute haben dies kommen sehen. Aber die Entwicklung des Fernmeldemarktes ist sehr interessant und manchmal auch sehr irrational. SMS bspw. ist eigentlich ein Medium, dass unglaublich mühsam ist. Dass Menschen im grossen Stil tatsächlich über diese Textnachrichten kommunizieren würden, hat niemand erwartet, als man das BÜPF lancierte. Man muss auch sagen, dass Swisscom weltweit die Ersten waren, die diese SMS-Technologie entwickelt haben. Aber die Swisscom dachte damals, dass dies eine technische Anwendung für irgendwelche Spinner sei und sich niemals durchsetzen würde. Dann kam der grosse Schritt mit der Internetfähigkeit der Mobiltelefone. Man hat schon erkannt, dass dies kommen würde aber vor 10 Jahren wurde nicht erkannt, dass sich dies wirklich in so grossem Umfang durchsetzen würde. Kürzlich hatte man den Wechsel von SMS zu Whatsapp. Dies hätte man voraussehen können. Aber was man nicht voraussehen konnte war die Schnelligkeit mit der die Gesellschaft das Medium gewechselt hat. Nun vergrössert sich Whatsapp noch einmal. Mittlerweile überschneidet sich wieder alles mit der Telefonie indem Sprachnachrichten, etc. für die Menschen wieder interessant werden. Von daher sind wir plötzlich wieder viel näher bei der Telefonie. Es kann sein, dass die Menschen nun wiedererkennen, dass es eigentlich viel einfacher wäre kurz zu telefonieren als 17 Kurznachrichten hin und her zu schicken. Aber eben, solche Entwicklungen sind manchmal irrational, manchmal haben sie aber auch mit den Preisen zu tun. Der Wechsel von SMS zu Whatsapp war eine reine Preisfrage für die meisten Leute. Da ist auch interessant, dass die Anbieter eigentlich zu spät gekommen sind

und zu spät bemerkt haben, dass sie eigentlich bei den SMS massiv die Preise hätten senken müssen, wenn sie überhaupt im Markt bleiben wollen. Jetzt ist der Zug abgefahren. Wenn die Tarifstruktur anders gewesen wäre, wäre niemand auf Whatsapp umgestiegen. Interessant ist z.B. auch, dass Skype ein Medium wäre, dass eigentlich die Telefonie hätte verdrängen sollen. Das ist aber bislang nicht passiert. Skype wird eigentlich nur für Gespräche ins Ausland benötigt. Es ist eigentlich unlogisch, dass Menschen innerhalb der Schweiz kein Skype brauchen, aber heute, wo wir alle eine Flatrate haben, ist Skype genau aus diesem Grund uninteressant geworden. Wenn die Anbieter aber später mit dieser Flatrate gekommen wären, könnte es durchaus sein, dass wir nun alle Skype benützen würden.

Was gibt es sonst für wesentliche Änderungen im BÜPF? Relevant ist sicher auch dies mit der allfälligen Änderung der Vorratsdatenspeicherung?

Im Endeffekt hat sich diesbezüglich ja nun gar nichts geändert. Wir haben immer noch die gleiche Regelung wie vorher. Es lässt sich darüber diskutieren was richtig ist. Ich war immer der Meinung, dass man die Möglichkeit hätte schaffen sollen, mit den Vorratsdaten weiter zurückzugehen, aber unter strengeren Vorgaben. Dass man bspw. nur bei Verbrechen 12 Monate zurückgehen darf und bei Vergehen weiterhin nur 6 Monate. Das Bedürfnis zur Ausdehnung der Frist besteht ja nur deshalb, weil man bei Kapitaldelikten oftmals nicht binnen 6 Monaten einen Verdächtigen finden kann. Wenn man ausserhalb dieser 6 Monate ist, lassen sich keine Alibi-Abklärungen mehr durchführen. Aber das spielt nur bei Tötungsdelikten, schweren Vergewaltigungen, etc. eine Rolle, also bei Ausnahmefällen. Das sind vielleicht gesamtschweizerisch 500 Fälle pro Jahr, bei denen überhaupt ein Interesse daran bestehen würde diese Frist auszudehnen. In der Regel reichen 6 Monate. Bei Drogendelikten, mit denen ich mich meist beschäftige, muss man auch sagen, dass die meisten Drogendealer gar nicht 6 Monate lang, die gleiche Nummer benützen. Von da her spielt das sowieso keine Rolle.

Frage 3: Hat die Revision des BÜPF auch Einfluss auf den Antennensuchlauf?

Nein, komischerweise nicht. Dabei ist das Interessante, dass das Bundesgericht sagt, dass die Voraussetzungen für den Antennensuchlauf darin bestehen, dass es ein Verbrechen sein muss. Diesen Umstand hätte man eigentlich ins Gesetz nehmen sollen. Dies hat man aber wahrscheinlich vergessen, weswegen weiterhin die Bundesgerichtspraxis gelten wird – zumindest nach meinem Dafürhalten. Es gibt keinen Grund warum das Bundesgericht seine Haltung ändern sollte, aber dieser Umstand steht halt einfach nicht im Gesetz.

Wie sieht es dann im Hinblick auf die Fälle Rupperswil und Emmen aus - insbesondere auch betreffend das Kriterium der Individualisierbarkeit?

Da besteht nun einmal ein Problem. Hier ist es definitiv eine Frage der Verhältnismässigkeit. Wenn ich einen Antennensuchlauf habe, also jetzt am konkreten Beispiel Rupperswil, wenn ich also 30'000 Menschen (ich glaube diese Zahl stand auch in den Medien) habe, die über eine Antenne telefonieren, dann stellt sich natürlich die Frage, was man da genau braucht und wer nun wirklich davon betroffen ist, dass seine Daten erhoben und bearbeitet werden. Es gibt hier gewisse Raster, die interessant sind und wenn man die 30'000 Daten durch dieses Raster laufen lässt, verbleiben vielleicht noch 1'000 Daten. Diese kann man dann individuell angucken und dann bleiben vielleicht noch 30 Individuen übrig, die wirklich interessieren. Betroffen sind die 30'000 also nur unmerklich, der Eingriff ist nicht spürbar. Deswegen finde ich den Eingriff rechtsstaatlich auch eher unproblematisch. Die Frage ist aber einfach wie sich das entwickelt auch mit den immer neuen Möglichkeiten der Datenbearbeitung, also Stichwort „Big Data". Je mehr Daten wir haben um irgendwelche Suchläufe zu machen, desto heikler wird es für den Einzelnen, weil sich die Daten natürlich immer besser verknüpfen lassen um ein konkretes Ergebnis zu erzielen. Auf der anderen Seite muss man sagen, dass gewisse Daten rein elektronisch herausgefiltert werden, wo ich persönlich zugeben muss, dass mir das egal wäre, wenn diese rein elektronisch von einem Computer gefiltert werden. Interessant oder heikel wird es erst, wenn ein Polizist meint, dass eine bestimmte vielleicht auch rein zufällige Verknüpfung von Daten verdächtig erscheint. Vorher kann einem das egal sein.

Was mir persönlich noch nicht ganz klar ist, ist wie sich dieses Raster zusammensetzt. Wer stellt es auf und wie wird das gemacht?

Dies ist immer eine heikle Frage – ein Problem – und nicht ganz einfach. In der Regel ist das Raster beim Antennensuchlauf so gestaltet, dass man 2 Tatorte und 2 Tatzeitpunkte hat und sich dort eine Übereinstimmung finden lässt. Man muss das Raster dann so engmaschig gestalten, dass nicht allzu viele Personen darin hängen bleiben. Um ein konkretes Beispiel zu geben: Wir hatten kürzlich einen Banküberfall in Steinach und kurz darauf einen in Wittenbach. Es war der gleiche Täter, das wussten wir aufgrund von Überwachungskameraaufnahmen und dort haben wir dann einen Antennensuchlauf machen lassen. In einem ersten Umgang haben wir 17 Anschlüsse gefiltert, die an beiden Orten aufgetaucht sind. Mit 17 Datensätzen kann man arbeiten. Man hat dann überprüft was das für Personen sind und konnten dann 12 bereits ausscheiden, weil dies unverdächtige Personen waren wie bspw. eine 75-jährige Frau. Das lässt sich relativ schnell erkennen. Konkret hangen blieb schlussendlich ein Verdächtiger. Dieser hatte dann auch das passende Auto, sprich den passenden Autotyp, welcher an einem der beiden Tatorte beobachtet wurde. Diesen Verdächtigen hat man

dann näher überprüft. Leider kam dann heraus, dass es sich bei dieser Person eindeutig nicht um den Tatverdächtigen handeln kann. Das Problem für uns ist, dass wir nicht abstrakt formulieren können nach was wir genau suchen. Mir müssen unter Umständen einfach wirklich die Daten selbst bearbeiten können, weil Ideen vielleicht auch erst bei der Bearbeitung der Daten entstehen und so auch Ideen für mögliche Raster entstehen. Von da her ist die Idee des Bundesgerichts, dass man die Triage den Anbietern oder dem ÜPF überlassen soll, in der Praxis nicht praktikabel. Dies muss die Polizei übernehmen. Bei anderen Konstellationen kann es aber auch möglich sein, dass ein Staatsanwalt bei Betrachtung der Daten auf gewisse Ideen kommt und weiss nach was er suchen muss. Dies auch einfach aufgrund dessen, da er alle verfügbaren Daten, wie bspw. ein Signalement, Telefon-Randdaten oder DNA-Ergebnisse, aus der man bspw. das Geschlecht bestimmen kann, zu Händen hat. Die Kombination von allen diesen Erkenntnissen liefert dann oftmals das Raster. Dazu braucht man die Daten. In Rupperswil war es so, dass man natürlich genau überlegen musste was man mit diesen 30'000 Daten anstellt. Man kann nicht 30'000 Daten überprüfen. Letztendlich wäre aber vielleicht auch nichts anderes übrig geblieben. Es gibt auch einen bekannten Fall den „Yorkshire Ripper", bei dem man von einem der Morde Pneu-Spuren hatte. Aufgrund dieser Erkenntniss konnte cirka 30'000 Automobilisten identifiziert werden. Man hat angefangen diese zu überprüfen. Nach 5'000 hat man aufgehört, weil sich ein Zeuge an eine bestimmte Automarke erinnern konnte. Man hat sich dann auf diese bestimmte Automarke konzentriert. Am Schluss musste man aber feststellen, dass sich der Zeuge geirrt hat und die falsche Automarke genannt hat. Diese Spur hat also in die Leere geführt. Wenn man aber weiterhin die 30'000 Automobilisten überprüft hätte, wäre der Täter darunter gewesen. Dies hat man alles jedoch erst im Nachhinein erfahren. Bei Rupperswil ist es vielleicht so, dass wenn nichts anderes zum Ergebnis geführt hätte, man tatsächlich begonnen hätte die 30'000 Randdaten systematisch abzuarbeiten. Dann ist klar, dann überprüft man zuerst diejenigen die vom Alter her cirka passen, man kann bspw. die unter 15 und die über 50 herausfiltern. Dann konzentriert man sich bspw. auf die Vorbestraften. Es stellt sich immer die Frage wie am besten vorzugehen ist und wie das Raster genau erstellt werden soll, bei solch riesigen Datenmengen. Das Ziel vom Antennensuchlauf müsste ja eigentlich laut Bundesgericht sein, dass man so präzise sein kann, dass schlussendlich nur eine Person – der Täter – im Raster hängen bleibt. Bei diesen Banküberfällen war einfach das Problem, dass Wittenbach und Steinach sehr nahe beieinander liegen und dann die Chance gross ist, dass sich 2 Personen am gleichen Ort befinden, die überhaupt nichts mit dem Vorfall zu tun haben.

War es denn so, gerade jetzt beim Beispiel Steinach und Wittenbach, dass man zuerst die ganzen Daten anonymisiert behandelt hat und dann erst die 17 Überschneidungen deanonymisiert hat?

Ja, natürlich.

Angenommen in Rupperswil, wäre man so wie sie gerade erwähnt haben vorgegangen. Dann hätte man aber alle 30'000 Daten deanonymisieren müssen?

Ja, aber da ist ja auch das Problem, dass man nur einen Tatort und einen Zeitpunkt hat. Man hätte so oder so deanonymisieren müssen um zu filtern. Aber der Sinn war primär erst einmal, dass wenn man einen Verdächtigen hat, der auf ein Signalement passt, man überprüfen kann ob er anwesend war. Bspw. wenn man einen Vorbestraften hat, kann man überprüfen ob sich dessen Telefonnummer auf dem Datensatz des Antennensuchlaufs finden lässt oder nicht. Und wenn nicht, dann kann man in wahrscheinlich ausschliessen. Daher ist es genau auch wichtig, dass die Daten im Besitz der Ermittlungsbehörden sind und die Triage nicht bei den Anbietern gemacht wird, weil das sonst alles verkomplizieren würde. Aber eben, dass sind sowieso immer die Fälle, die schwierig sind, wenn man nur einen Tatort hat, jetzt hinsichtlich eines Antennensuchlaufs.

Frage 4: Abgesehen vom BÜPF will man ja auch die VÜPF teilrevidieren. Was ist dort der Stand der Dinge?

Es gibt da eine verwaltungsinterne Expertengruppe die sich um diese Frage kümmert. Was für den Dienst klar ist, ist, dass sie die Revision der Verordnung gleichzeitig mit dem Gesetz veröffentlichen wollen. Bei den Verordnungen ist materiell sowieso nichts Interessantes geregelt. Das braucht Sie gar nicht gross zu interessieren. Es wird alles nur konkretisiert.

Aber gerade der Antennensuchlauf ist ja nur in der Verordnung geregelt?

Ja, schon, dort wird er definiert, aber dies ergibt sich eigentlich auch schon aus dem Gesetz. Die Frist (6 Monate) bleibt gleich. Genau diese Frist ist beim Antennensuchlauf ja auch kein Problem, weil da wo man Antennensuchläufe machen lässt, sind die Tatorte ja bereits bekannt, weswegen die Frist eigentlich immer eingehalten werden kann.

Dann hat eigentlich auch die Revision der VÜPF keinen Einfluss auf den Antennensuchlauf?

Nein, nicht direkt. Ich glaube nicht, dass dies einen Einfluss haben wird. Es regelt einfach genau was die Anbieter in diesem Zusammenhang liefern müssen. Und vielleicht wer wie für die Verarbeitung zuständig ist. Nein ich denke nicht, dass dies eine Rolle spielt.

Dann ist es für Sie auch stringent, dass der Antennensuchlauf nicht formell gesetzlich geregelt ist?

Nein, es wäre natürlich gut gewesen, wenn man bei der Randdatenerhebung auch den Antennensuchlauf geregelt hätte, weil dieser aus meiner Sicht eine Form von Randdatenerhebung darstellt. Konkret hätte man explizit erwähnen müssen, dass Antennensuchläufe nur bei Verbrechen zulässig sind. Mehr müsste man nicht machen. Das hätte man regeln können.

Und warum macht man dies dann nicht?

Ja, weil man dies wahrscheinlich vergessen hat.

Könnte man dies dann nicht nachtragen?

Ja, dies könnte man theoretisch, aber dies wäre eine Gesetzesänderung, die dem Referendum untersteht und ins Parlament muss. Das ist das Problem.

Dann haben Sie das Gefühl der Antennensuchlauf ist nicht referendumsfähig?

Doch, sehr wohl. Das ist nicht das Problem. Aber man weiss ja schon jetzt, wie die Rahmenbedingungen sind, weil das Bundesgericht diese festgehalten hat. Der Bedarf wäre nur gegeben, wenn das Bundesgericht etwas beschlossen hätte, was in der Praxis als nicht sinnvoll erachtet worden wäre oder wenn ein Parlamentarier der Meinung wäre man hätte diesen ganz verbieten müssen. Das Heikle am Antennensuchlauf, rechtsstaatlich gesehen, liegt darin und das ist zentral, dass dieser verdachtsbegründend ist und nicht einen vorbestehenden Verdacht gegen eine gewisse Person erhärtet. Der Antennensuchlauf dient dazu, den unbekannten Täter zu identifizieren. Man hat zwar einen Verdacht auf eine Straftat, aber man hat keinen konkreten Tatverdacht gegen eine bestimmte Person. Im Grunde genommen – und das ist genau jener Umstand der Antennensuchläufe bedenklich macht – geht Art. 269 StPO davon aus, dass man eine bestimmte Person im Visier hat und deren Telefon überwacht. Man geht auch bei Randdatenerhebungen davon aus, dass man konkreten Personen als Beschuldigte benennen kann und deren Randdaten, oder gegebenenfalls Randdaten von Dritten, also Personen, die aber mit dem Beschuldigten zu tun haben, erheben will. Und der Punkt besteht darin, dass die Person individualisierbar sein muss, nicht identifizierbar. Bspw. wenn man einen Drogendealer sucht, der eine konkrete Telefonnummer benützt. Damit ist er hinreichend individualisiert, damit man einen Tatverdacht gegen eine bestimmte Person hat. Aber beim Antennensuchlauf ist es natürlich so, dass man weiss man sucht einen Bankräuber, aber von diesem weiss man gar nichts, auch keine Telefonnummer. Und trotzdem werden nun Daten gesucht und zwar Daten von Menschen, gegen die wir keinen Tatverdacht

haben. Diese Daten werden dann abgeglichen und erst aus dieser Abgleichung ergibt sich allenfalls ein Tatverdacht. Das ist das Problematische. Aber dies ist nicht etwas singuläres. Dies gibt es auch bei anderen Ermittlungsmethoden, bspw. bei DNA-Abgleichungen. Dort nehmen wir auch eine DNA-Spur und lassen diese durch eine Datenbank laufen. Dann haben wir den Täter und zwar auch erst mit dieser Massnahme. Von da her kann man den Antennensuchlauf eigentlich mit einem Fingerabdruck, der am Tatort zurückgelassen wird, vergleichen, ausser dass es sich hierbei um eine digitale Spur handelt. Dass der Antennensuchlauf aber verdachtsbegründend ist, ist aus rechtsstaatlicher Sicht wirklich ein Problem.

Frage 5: Ist Ihnen irgendein Fall bekannt, in dem man durch einen Antennensuchlauf einen falschen Täter begründet hat und sich dann auf diesen eingeschossen hätte? Gerade bei dem von Ihnen erwähnten Fall in „Wittenbach / Steinach" wäre ja schon ein gewisses Risiko dazu bestanden?

Dort ist natürlich klar: Man darf gegen solche Personen kein Verfahren eröffnen. Wir wussten vom Täter aufgrund der Videoaufnahmen, dass dieser um die 30 Jahre alt ist, einen Bart trägt und aufgrund einer Zeugenaussage, dass dieser mit einem blauen Seat Ibiza davon gefahren ist. Nachdem wir den Antennensuchlauf durchgeführt hatten, konnten wir eine Schnittmenge von 17 Personen konstruieren, die wir überprüft haben. Und genau eine Person hatte einen Bart und einen blauen Seat Ibiza. Dann hatte ich natürlich das Gefühl, dass wir den Täter gefunden haben. Dann hat man diesen Mann näher überprüft und dann hat man herausgefunden, dass dieser direkt neben der Bank arbeitet. Die Anwesenheit zum zweiten Zeitpunkt am zweiten Tatort, lässt sich also aufgrund dessen erklären. Dann hat man eine DNA-Probe genommen, die mit derjenigen des mutmasslichen Täters nicht übereingestimmt hat. Schliesslich hat man ihn befragt, was er zum anderen Zeitpunkt in Steinach gemacht hat und er hat dann angegeben, dass er seine Tochter in die Krippe gebracht hat. All diese Angaben konnten einfach überprüft werden, weswegen sich die Sache erledigt hat. Das war eine normale Alibi-Abklärung. Wenn jemand bei der Polizei angerufen hätte: „Sie, mein Nachbar fährt einen blauen Seat Ibiza und trägt einen Bart", wären wir wahrscheinlich genau gleich vorgegangen. Das ist nicht heikel im rechtsstaatlichen Sinn. Aber dennoch hat der Antennensuchlauf in diesem Fall etwas gebracht, weil man so eine Person aktiv ausschliessen konnte.

Und was wäre, wenn man dies vielleicht nicht so einfach gekonnt hätte?

Dann wäre dies aber ein grosser Zufall gewesen, wenn er für beide Zeiten kein konkretes Alibi gehabt hätte. Und auch dann hätte man allein aufgrund eines Antennensuchlaufs kein Verfahren eröffnen können. Dies hätte allein als Beweis nicht gereicht.

Dann ist dies gar nicht möglich, dass man Jemanden allein aufgrund eines Antennensuchlaufs als Täter festnagelt?

Nein, der Punkt ist eben auch – das ist das, was ich immer sage im Zusammenhang mit Telefonüberwachungen – dass es nur relativ wenige Gerichtsurteile gibt, die sich mit der Zulässigkeit von Überwachungen beschäftigen. Dies kommt daher, dass man zwar aufgrund von Telefonüberwachungen den Täter identifizieren kann, aber wenn man ihn erst hat, sind wir aufgrund der Telefonüberwachung so gut dokumentiert, dass man über weitere Beweismittel verfügt. Wenn ich bspw. eine Telefonüberwachung eines potentiellen Drogendealers mache und dann feststelle, dass dieser tatsächlich mit Drogen dealt, dann richte ich das natürlich so ein, dass ich den Dealer direkt während einem Drogendeal überführe. Dann hat man die Drogenübergabe und dann ist die Frage im Verfahren ob man aufgrund von Telefongesprächen noch andere Sachverhalte nachweisen kann, bspw. weil man auch die Abnehmer identifizieren und befragen kann. Für den Verteidiger besteht dann gar keine Veranlassung mehr die Zulässigkeit der Telefonüberwachung in Frage zu stellen, weil der Beweis dann eben auf andere Art und Weise erbracht wird. Es gibt so eine Untersuchung aus Deutschland, die immer wieder von Gegnern der Überwachung zitiert wird, wo behauptet wurde, Ergebnisse von Telefonüberwachungen spielen im Endeffekt gar keine Rolle mehr. Dies ist vor Gericht ganz richtig, aber in der Praxis liefern sie eben doch Ermittlungsansätze. Wir müssen ja zuerst wissen, wo überhaupt gesucht werden soll.

Frage 6: Angenommen man würde trotzdem den Antennensuchlauf formell gesetzlich festlegen, wo wäre dieser systematisch einzuordnen. In die StPO?

Ja genau, in die StPO irgendwo bei Art. 269 ff. Ein Satz müsste man dort einfügen. Dies würde reichen.

Frage 7: Wie läuft denn ein Antennensuchlauf praktisch genau ab?

Die rechtlichen Hürden sind nämlich gar nicht so sehr von Bedeutung. Das Problem sind die Kosten. Ich muss Ihnen kurz erklären wie das funktioniert, also jetzt gerade wieder am Beispiel „Wittenbach / Steinach“: Wir haben 2 Tatorte, an denen jeweils ein Banküberfall passiert ist. Wenn ich da einen Antennensuchlauf durchführen will, muss ich als erstes wissen, mit welchen Antennen der Täter rund um die Bank allenfalls überhaupt in Kontakt hätte kommen können. Das ist eine technische Abklärung, die ich durch den Dienst machen lassen kann. Dies kostet mich aber 2'000 Franken pro Standort. Ich kann dies auch durch die Polizei machen lassen, die dies mittels eines IMSI-Catchers macht. Welche Antennen in der Nähe sind, muss ich wissen. Konkret, zahle ich somit bereits 4'000 Franken nur um zu wissen, welche Antennen in Frage kommen. Im Fall Wittenbach / Steinach war das Ergebnis,

dass der Täter mit 31 verschiedenen Antennen hätte Kontakt haben können. Am einen Ort 15 und am anderen Ort 16 Antennen. Wenn ich nun die Randdaten will, kostet mich das CHF 600 pro Antennenelement und pro Art der Daten. Das heisst ich muss mich entscheiden ob ich Telefonranddaten oder Internetranddaten haben möchte. Für den Zeitraum von 2 h würde dies jeweils CHF 600 kosten. Dann muss man sich entscheiden, ob man wirklich die Daten von allen 31 Antennen will und ob man bei allen Antennen die vollständigen Daten erheben will. Vollständig würde ja dann 31 x CHF 1'200 kosten. Wenn man nur Internetranddaten erheben will, würde das 31 x CHF 600 kosten. Im Fall „Wittenbach / Steinach", habe ich dann beschlossen, dass dies zu teuer kommen würde. Wir haben angenommen, dass es sich beim Bankräuber um einen Einzeltäter handelt, weswegen er eigentlich kein Interesse gehabt haben dürfte zu telefonieren. Er hätte höchstens während der Tat Internetverkehr gehabt.

Würde darunter dann auch fallen, dass er nur passiv ein E-Mail empfangen hat und nicht aktiv eines versendet hat?

Ja genau. Wenn Sie ihr Handy in der Hosentasche haben, hat dies gegebenenfalls laufend Internetverkehr, weil Sie bspw. die Standortfunktion aktiviert haben. Gewisse Apps machen dann alle 10 Minuten eine Ortsabfrage, was Internetverkehr bewirkt, der sich nachweisen lässt. Aber um zurück zum Fall zu kommen: Auch 31 x 600 Franken, war mir zu teuer. Ich habe mich dann dazu entschieden, dass wir in einem ersten Schritt nur die Daten von Swisscom-Kunden erheben, weil eben immer noch die meisten Menschen bei Swisscom unter Vertrag sind. Erst wenn wir nichts finden nehmen wir in einem zweiten Schritt Salt, weil dies der 2. häufigste Anbieter ist und dann in einem 3. Schritt Sunrise. So oder so war bereits der 1. Schritt teuer, weil auch das – glaube ich – 18 Antennen waren und der Suchlauf somit 18 x 600 Franken gekostet hat. Dies macht ungefähr 11'000 + 4'000 Franken für die Netzanalyse. Diese Kosten sind eigentlich das Problem und stellen in der Praxis ein wesentlich grösseres Hindernis dar, als die rechtsstaatlichen Komplikationen. Beim Fall Rupperswil hat man einen Standort, das bedeutet, dass man mindestens 6 Antennen hat, weil man eigentlich an jedem Punkt in der Schweiz immer mindestens 6 Antennen hat. Also man hat von jedem Anbieter cirka 2 Antennen, in deren Visier man sich befindet, damit man überall abgedeckt ist. Und 6 Antennen sind das Minimum, meistens hat man natürlich mehr. In Rupperswil war ein Antennensuchlauf also eher „billig". Nun hat man aber 30'000 Nummern. Die nächste Frage ist nun, von welchen Nummern man dann tatsächlich Randdaten verlangt. Man könnte von allen 30'000 Nummern Randdaten verlangen, aber pro Nummer würde dies dann wiederum 600 Franken kosten. Dann wären wir kostenmässig irgendwo bei 18 Millionem. Dann hätten wir aber insgesamt alle Randdaten und dann hätten wir den Täter mit sehr grosser Wahrscheinlichkeit. In dieser Situation kann sich das aber niemand leisten. Von da

her ist die Kostenbremse also viel wirksamer, als wenn man rechtsstaatlich an dieser Sache etwas ändern würde.

Wer bewilligt denn das Budget mit dem As durchgeführt werden?

Das wird nicht bewilligt. Der Staatsanwalt kann selbst entscheiden wie viel ihm ein Antennensuchlauf wert ist.

Dann kann man sagen, Sie haben diesbezüglich ein unbegrenztes Budget?

Ja, unbegrenzt natürlich nicht, bspw. gerade bei etwas das 18 Millionen kostet würde man zuerst den Finanzdirektor anfragen, aber es ist natürlich schon so, dass ein Einzelstaatsanwalt grosse Entscheidungskompetenz in solch finanziellen Fragen hat. Antennensuchläufe im Bereich von 20'000 – 30'000 Franken sind problemlos möglich. Bereits psychiatrische Gutachten kosten ja um die 8'000 – 15'000 Franken. Solche Dinge müssen laufend entschieden werden. Da haben wir kein bestimmtes Budget, wie viel wir pro Jahr ausgeben dürfen. Es gibt aber auch Kantone, wie bspw. Zürich, die für Telefonüberwachungen ein konkretes Budget haben. Wenn der Staatsanwalt im November eine Überwachung schalten will, muss er zuerst wissen, ob er dazu noch genügend Geld zur Verfügung hat. Ansonsten muss er bis im Januar warten. Das gibt es in St.Gallen nicht, aber die Kosten sind trotzdem faktisch eine Hürde, weil sie abschrecken. Die Kosten sind eine wirksamere Hürde um die Verhältnismässigkeit der Massnahme zu gewährleisten, weil sich ein Staatsanwalt immer die Frage stellen wird, ob ihm eine Überwachung so viel Geld wert ist. Kein Staatsanwalt würde auf die Idee kommen, bei einem verlorenen Telefon eine Überwachung anzuordnen, weil dies dann einfach 2'400 Franken kosten würde, was natürlich zu viel ist. Das ist praktisch gesehen viel wirksamer, als die rechtsstaatliche Frage, ob eine Überwachung bei einem kleinen Diebstahl überhaupt zulässig sein soll oder nicht.

Frage 8: Wie viele Antennensuchläufe werden pro Jahr ungefähr durchgeführt?

Das sind wenige. In St. Gallen war es dieses Jahr nur den, den ich beschrieben habe. Dies ist etwas sehr seltenes. Da müssen Sie sich an den Dienst wenden oder möglicherweise an ein Zwangsmassnahmen-Gericht, weil dieses natürlich weiss, wie viele Antennensuchläufe es bewilligt hat. In der Regel ist der ÜPF aber sehr grosszügig mit Auskünften und Sie können ja auch sagen, dass Sie nur eine ungefähre Grössenordnung benötigen. Die wissen ja sehr genau wie viele Antennensuchläufe bewilligt worden sind. Am besten fragen Sie beim Zürcher Obergericht nach und rechnen diese Grösse dann für die ganze Schweiz hoch. Sie müssen die Zahl cirka x 4 rechnen, weil Zürich natürlich prozentual viele Erhebungen macht. Wie genau sie das prozentual berechnen müssen, können Sie auch aus der gesamtschweizerischen Statistik ablesen. In den Zentren werden immer mehr Erhebungen gemacht. Im

Appenzell weiss der Staatsanwalt wahrscheinlich gar nicht wie das geht. Das ist leider so. In Zürich haben Sie diesbezüglich eine Routine, weswegen viel eher Erhebungen gemacht werden. Auch wir in St.Gallen mussten zuerst einmal herausfinden, wie Antennensuchläufe genau funktionieren. Wir mussten in Zürich nachfragen. Insbesondere die Netzanalyse war nicht ganz einfach, weil wir nicht wussten, ob wir diese nun an den Dienst überweisen sollen oder selbst durchführen. In Zürich machen sie die Analyse selber und dazu haben wir uns dann auch entschieden. Die Zürcher sind dafür extra nach St.Gallen gekommen und haben uns geholfen. Das funktioniert dann so, dass man den IMSI-Catcher auf den Tisch stellt, einschaltet und dann sucht er die Antennen, die in der Nähe sind. Der IMSI-Catcher macht das Ähnliche wie jedes Mobilfunkgerät, nur sucht er eben alle Anbieter und nicht nur den Eigenen. Er zeigt alle Antennen, in die man sich in der Nähe einloggen kann und das sind dann diejenigen, die für den Antennensuchlauf in Frage kommen. Wir müssen dem Anbieter ja genau sagen, welche Antennen wir wollen. Man muss sogar sagen welches Element einer gewissen Antenne man will. Manchmal braucht man nur 1 Element, weil nur dieses in die entsprechende Richtung des Tatorts sendet. Die anderen 2 Elemente braucht man dann nicht. Dies schränkt die Menge weiter ein.

Vielen Herzlichen Dank für das Gespräch.

Anhang 2: Interview mit Philip Umbricht

Das schriftliche Interview mit Philip Umbricht, leitender Oberstaatsanwalt des Kantons Aargau, fand am 10. April 2017 statt. Philip Umbricht ist zuständiger Staatsanwalt im Fall „Rupp.“. Den Kontakt konnte ich durch Herrn Dr. Hansjakob herstellen, nachdem der ÜPF leider für keine Stellungnahme bez. der Kosten zu erreichen war. Im Zuge des Interviews, dass sich hauptsächlich um die Kosten der Telefonüberwachung mittels As in Höhe von CHF 800'000 im Fall „Rupp.“ drehte, wurden von Herrn Umbricht noch weitere nicht öffentlich bekannte Details verraten:[120]

Judith Rothen, 10. April 2017 um 10:03 Uhr

Wie sich aus der Statistik des ÜPF entnehmen lässt, wurden im Fall „Rupperswil“ 48 Antennensuchläufe eingesetzt. Wie aktuell in den Medien bekannt wurde, soll dies CHF 800’000 an Gebühren gekostet haben. Auch nach eingehender Auseinandersetzung mit der GebV-ÜPF kann ich mir den immensen Rechnungsbetrag nicht erklären.

Beim Antennensuchlauf muss zuerst für die Erhebung der geografischen Koordinaten bezahlt werden. Danach fallen pro Zelle für einen Zeitraum von 2 h Gebühren an. Schliesslich muss pro Datenerhebung (CS oder PS) bezahlt werden. Ich nehme an, dass i.c. nicht beide Datensätze, sondern nur Internetdaten abgefragt wurden. Dies weil es sich um einen Einzeltäter handelt, der wohl während der Tat keinen Anreiz hatte sich telefonisch mit jemanden abzusprechen. Wenn meine Annahmen stimmen, warum ist dann der Rechnungsbetrag trotzdem derart hoch?

Philip Umbricht, 10. April 2017 um 10:32 Uhr

Ihre Annahmen sind teilweise unzutreffend, insbesondere ist zu beachten, dass ein Antennensuchlauf gemäss Statistik mehr als eine Antenne umfassen kann. Die Gesamtkosten ergeben sich aus folgender Formel:

*Kosten pro Zelle * Datentypen * Anzahl Zellen * (Überwachungsdauer/2) + Kosten pro Bestandesdatenabfrage*

Konkret haben wir in Rupperswil beide Datentypen gesucht, die Überwachungsdauer war deutlich über 2 h und die Zellenanzahl aufgrund des Umstandes, dass 3 Standorte abgesucht wurden, die alle in der Nähe der Autobahn und/oder der SBB-Linie waren, sehr hoch. Die Rechnungsstellung des Dienstes ist, rein rechnerisch, korrekt.

---

120 Das Gespräch ist wortwörtlich wiedergegeben, weswegen an dieser Stelle auf die in dieser Arbeit verwendeten Abkürzungen verzichtet wird. Ausnahmen bestehen dort, wo Abkürzungen als solche im Gespräch verwendet wurden.

Anhang 3: Tabelle über die in der Schweiz durchgeführten Antennensuchläufe

Tab. 1[121] zeigt die bisher in der Schweiz durchgeführten As. Die Durchführungen sind nach Jahr und Kanton, sowie Straftatbestand aufgeschlüsselt. Zudem wird die Anzahl durchgeführter Antennensuchläufe ins Verhältnis (%-Anteil) zu den total durchgeführten Telefonüberwachungen (Total Ü) gestellt. Am Ende jedes Jahres steht die totale Anzahl der durchgeführten As (Total AS) auf dem Gebiet der Schweiz.

Die Statistiken des ÜPF wurden jeweils nach den aufgelisteten As sortiert. In den Jahren 2011-2013 waren diese als „Antennensuchlauf“ aufgeführt. Ab dem Jahr 2014 unter den Rubriken „CS 5“ und „CS 6“.

[121] In der Tabelle wurden aus darstellerischen Gründen unbekannte Abkürzungen verwendet: DVA = Datenverarbeitungsanlage; erschw. = erschwerende; gift. G. = gfitige Gase;. Zudem wurden Abs. mit römischen Zahlen wiedergegeben.

Kanton / Bund	Anzahl	Rechtsgrundlage	Delikt	Total AS	Total Ü	%-Anteil
Jahr 2011						
AG	3 6 6	BetmG 19 II StGB 140 StGB 144 III	Diebstahl Raub Schwere Sachbeschädigung	15	435	3,45 %
BE	1 10 3	BetmG 19 II StGB 139 StGB 221 I und II	Verstoss gegen das BetmG, der nicht unter einem Jahr geahndet wird Diebstahl Vorsätzliche Brandstiftung mit Gefahr für Leib und Leben	14	762	1,84 %
GE	1	StGB 189 und 190	Sexuelle Nötigung i.V.m. Vergewaltigung	1	2'298	0,04 %
GR	3	StGB 111	Vorsätzliche Tötung	3	116	2,59 %
JU	6 21	StGB 139 StGB 140	Diebstahl Raub	27	83	32,53 %
LU	18 9	StGB 139 StGB 140	Diebstahl Raub	27	284	9,51 %
NE	3 39	StGB 139 StGB 183 und 184	Diebstahl Freiheitsberaubung und Entführung mit erschw. Umständen	42	354	11,86 %
SG	30	StGB 140	Raub	30	543	5,52 %
SH	9	StGB 140	Raub	9	60	15%
SO	11	StGB 139	Diebstahl	11	223	4,93 %
SZ	6 3 6	StGB 140 StGB 224 StPO 273 und StGB 224 I	Raub Gefährdung durch Sprengstoffen und giftige Gase Teilnehmeridentifikation i.V.m. Gefährdung durch Sprengstoffe und gift. G.	15	135	11,11 %
TI	6	StGB 146	Betrug	6	1'017	0,59 %
VD	3 9 6	StGB 187 II-IV StGB 190 und 191 StGB 223	Sexuelle Handlungen mit Kindern Schändung i.V.m. Vergewaltigung Verursachung einer Explosion	18	1'141	1,57 %
Schweiz				218	12'375	1,76 %

Jahr 2012						
AG	3	StGB 139 und 144 III	Diebstahl i.V.m. schwerer Sachbeschädigung	3	922	0,33 %
BE	3	StGB 140	Raub	3	967	0,31 %
BL	33	StGB 140	Raub	33	456	7,24 %
FR	6	StGB 140	Raub	6	577	1,04 %
GE	9 7	StGB 111 StGB 140	Vorsätzliche Tötung Raub	16	2'908	0,55 %
GR	12	StGB 139	Diebstahl	12	88	13,64 %
JU	9	StGB 140	Raub	9	110	8,18 %
NE	3	StGB 139, 140 und 183	Diebstahl i.V.m. Raub i.V.m. Freiheitsberaubung und Entführung	3	365	0,82 %
SO	6 6	StGB 139 und 144 III StGB 140	Diebstahl i.V.m. schwerer Sachbeschädigung Raub	12	237	5,06 %
TI	2	StGB 146	Betrug	2	1'468	0,14 %
ZH	6	StGB 139	Diebstahl	6	2'522	0,24 %
Schweiz				105	14'968	0,7 %
Jahr 2013						
AG	2 2 2 2	StGB 111 StGB 146 StGB 157, 180 und 181 StGB 180	Vorsätzliche Tötung Betrug Wucher i.V.m. Drohung i.V.m. Nötigung Drohung	8	1'266	0,63 %
BE	3 1 1 2	BetmG 20 II StGB 112 StGB 144 bis, 147 und 156 StGB 179 septies	Gewerbsmässiger Drogenhandel Mord Datenbeschädigung i.V.m. Betrügerischem Missbrauch einer DVA i.V.m. Erpressung Missbrauch einer Fernmeldeanlage	7	1'104	0,63 %
BL	1	StGB 111	Vorsätzliche Tötung	1	503	0,2 %
BS	2	StGB 146	Betrug			

				2	418	0,48 %
Bund	31	StGB 260ter	Kriminelle Organisation			
				31	567	5,47 %
FR	1	BetmG 19 II und StGB 139	Verstoss gegen das BetmG, der nicht unter einem Jahr geahndet wird und Diebstahl			
	2	StGB 139	Diebstahl			
	3	StGB 140	Raub			
	2	StGB 179 septies und 146	Missbrauch einer Fernmeldeanlage und Betrug			
	2	StGB 221 I und II	Vorsätzliche Brandstiftung mit Gefahr für Leib und Leben			
				10	482	2,07 %
GE	8	StGB 111	Vorsätzliche Tötung			
	2	StGB 138	Veruntreuung			
	1	StGB 179 septies	Missbrauch einer Fernmeldeanlage			
	10	StGB 182 und 195	Menschenhandel i.V.m. Förderung der Prostitution			
	2	StGB 305	Begünstigung			
	2	StGB 305 bis Ziff. 2	Schwerer Fall der Geldwäscherei			
				25	2'575	0,97 %
LU	3	BetmG 19 II	Verstoss gegen das BetmG, der nicht unter einem Jahr geahndet wird			
	2	BetmG 20 II	Gewerbsmässiger Drogenhandel			
				5	211	2,37 %
NE	1	StGB 146	Betrug			
				1	326	0,31 %
SG	4	BetmG 20 II	Gewerbsmässiger Drogenhandel			
	2	StGB 111	Vorsätzliche Tötung			
				6	635	0,95 %
SH	2	BetmG 19 II	Verstoss gegen das BetmG, der nicht unter einem Jahr geahndet wird			
				2	20	10%
SZ	2	BetmG 19 II	Verstoss gegen das BetmG, der nicht unter einem Jahr geahndet wird			
				2	80	2,5 %
TG	4	BetmG 20 II	Gewerbsmässiger Drogenhandel			
	1	BÜPF 14 I lit. a-c	Bestandesdaten-Auskünfte (wohl am falschen Ort in der Statistik aufgeführt)			
	3	StGB 179 septies	Missbrauch einer Fernmeldeanlage			
				8	688	1,16 %
TI	1	BetmG 19 II	Verstoss gegen das BetmG, der nicht unter einem Jahr geahndet wird			
	4	BÜPF 14 I lit. a-c	Bestandesdaten-Auskünfte (wohl am falschen Ort in der Statistik aufgeführt)			
	2	StGB 122, 129 und 183	Schwere Körperverletzung i.V.m. Gefährdung des Lebens i.V.m. Freiheitsberaubung und Entführung			
	7	StGB 157, 182 und 195	Wucher i.V.m. Menschenhandel i.V.m. Förderung der Prostitution			
	2	StGB 157 Ziff. 2 und 182	Gewerbsmässiger Wucher i.V.m. Menschenhandel			
				16	1'530	1,05 %
VD	2	StGB 156	Erpressung			
				2	1'737	0,12 %
VS	3	BÜPF 14 I lit. a-c	Bestandesdaten-Auskünfte (wohl am falschen Ort in der Statistik aufgeführt)			
	2	StGB 187 und 197	Sexuelle Handlungen mit Kindern i.V.m. Pornografie			
				5	421	1,19 %
ZG	1	StGB 111, 183 und 185	Vorsätzliche Tötung i.V.m. Freiheitsberaubung und Entführung mit erschwer. Umständen			

	4	StGB 140	Raub	5	143	3,5 %
ZH	2	BetmG 19 II	Verstoss gegen das BetmG, der nicht unter einem Jahr geahndet wird			
	4	StGB 111	Vorsätzliche Tötung			
	2	StGB 140	Raub			
	2	StGB 146	Betrug			
	1	StGB 147	Betrügerischer Missbrauch einer DVA			
	6	StGB 156	Erpressung			
	8	StGB 158 Ziff. 1 III	Ungetreue Geschäftsbesorung mit Absicht			
	1	StGB 180 und 181	Drohung i.V.m. Nötigung			
	2	StGB 260 ter und 305 bis Ziff. 2	Kriminelle Organisation i.V.m. schwerer Fall von Geldwäscherei			
	2	StGB 312 und 322 quater	Amtsmissbrauch i.V.m. sich bestechen lassen			
	2	StGB 322 quater und 322 ter	Sich bestechen lassen i.V.m. bestechen	32	2'806	1,14 %
Schweiz				168	16'015	1,05 %
Jahr 2014						
AG	3	StGB 111	Vorsätzliche Tötung			
	3	StGB 139	Diebstahl			
	3	StGB 140	Raub	9	1'233	0,73 %
BE	9	StGB 139 und 144 III	Diebstahl i.V.m. schwerer Sachbeschädigung	9	918	0,98 %
BL	15	StGB 139 und 140	Diebstahl i.V.m. Raub	15	535	2,8 %
Bund	19	StGB 240 I und 242	Geldfälschung i.V.m. in Umlaufsetzen falschen Geldes	19	588	3,23 %
FR	3	StPO 273	Teilnehmeridentifikation (wohl am falschen Ort in der Statistik aufgeführt)	3	437	0,69 %
GE	5	StGB 111	Vorsätzliche Tötung			
	3	StGB 139 und 144 III	Diebstahl i.V.m. schwerer Sachbeschädigung			
	3	StGB 140	Raub	11	2'055	0,54 %
NW	9	StGB 111	Vorsätzliche Tötung	9	38	23,68 %
SO	6	StGB 139	Diebstahl			
	5	StGB 140 und 183	Raub i.V.m. Freiheitsberaubung und Entführung	11	193	5,69 %
VD	6	StGB 139	Diebstahl	6	1'716	0,35 %
ZH	6	StGB 139	Diebstahl			

	21 3	StGB 140 StPO 273	Raub Teilnehmeridentifikation (wohl am falschen Ort in der Statistik aufgeführt)	30	2'419	1,24 %
Schweiz				122	14'485	0.84%
Jahr 2015						
AG	24	StGB 111	Vorsätzliche Tötung	24	1'219	1,97 %
BE	12 3 3	StGB 111 StGB 139 und 144 III StGB 140	Vorsätzliche Tötung Diebstahl i.V.m. schwere Sachbeschädigung Raub	18	1'012	1,78 %
BL	6	StGB 122	Schwere Körperverletzung	6	574	1,05 %
GE	3	StGB 139	Diebstahl	3	1'925	0,16 %
LU	9	StGB 122 und 190	Schwere Körperverletzung i.V.m. Vergewaltigung	9	254	3,54 %
NE	16	StGB 140, 183 und 184	Raub i.V.m. Freiheitsberaubung und Entführung mit erschwer. Umständen	16	176	9,1 %
NW	6	StGB 111	Vorsätzliche Tötung	6	19	31,58 %
SG	15	StGB 111	Vorsätzliche Tötung	15	439	3,42 %
SO	4 6 24	BetmG 19 II StGB 111 StGB 140	Verstoss gegen das BetmG, der nicht unter einem Jahr geahndet wird Vorsätzliche Tötung Raub	34	332	10,24 %
VD	9	StGB 139	Diebstahl	9	1'713	0,53 %
VS	3	StGB 139	Diebstahl	3	246	1,22 %
ZH	12 3	StGB 139 und 144 III StGB 187	Diebstahl i.V.m. schwerer Sachbeschädigung Sexuelle Handlungen mit Kindern	15	2'236	0,67 %
Schweiz				158	14'313	1,1 %
Jahr 2016						
AG	48	StGB 111	Vorsätzliche Tötung	48	1'072	4,48 %

BE	3 12 12 8	BetmG 19 II StGB 111 StGB 139 und 144 III StGB 140	Verstoss gegen das BetmG, der nicht unter einem Jahr geahndet wird Vorsätzliche Tötung Diebstahl i.V.m. schwerer Sachbeschädigung Raub	41	1'054	3,89 %
BL	9 3	StGB 139 StGB 140	Diebstahl Raub	12	403	2,98 %
FR	3	StGB 221 I und II	Vorsätzliche Brandstiftung mit Gefahr für Leib und Leben	3	506	0,59 %
NE	1 3 6 3	StGB 139 StGB 139 und 144 III StGB 144 bis Ziff. 1 II StPO 273	Diebstahl Diebstahl i.V.m. schwerer Sachbeschädigung Datenbeschädigung mit grossem Schaden Teilnehmeridentifikation (wohl am falschen Ort in der Statistik aufgeführt)	13	220	5,91 %
SG	2 4	StGB 122 StGB 140	Schwere Körperverletzung Raub	6	567	1,06 %
SO	2 12	BetmG 19 II StGB 111	Verstoss gegen das BetmG, der nicht unter einem Jahr geahndet wird Vorsätzliche Tötung	14	203	6,9 %
VS	2	StGB 139 und 144 III	Diebstahl i.V.m. schwerer Sachbeschädigung	2	212	0,94 %
ZH	12 3	StGB 111 StGB 144 III	Vorsätzliche Töung Schwere Sachbeschädigung	15	2'342	0,64 %
Schweiz				154	12'987	1,19 %

Tabelle 1: In der Schweiz durchgeführte Antennensuchläufe. Quelle: selbst erstellt i.A.a. ÜPF Statistik.

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 Leistungs-nachweises 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."

Datum und Unterschrift:

.....

Zeichenzahl (inkl. Leerzeichen und Fussnoten): 78'224