Universität St.Gallen

Hochschule für Wirtschafts-,
Rechts- und Sozialwissenschaften sowie Internationale Beziehungen (HSG)

Die strafprozessuale Zwangsverwaltung, Durchsuchung und Überwachung von Online-Verkaufsplattformen, insbesondere im sogenannten Darknet

Masterarbeit im Master in Rechtswissenschaft mit Wirtschaftswissenschaften an der Universität St. Gallen

Vorgelegt von:
Tanja Niederer
Regensdorferstrasse 175
8049 Zürich
Matrikel-Nr.: 15-608-920
tanja.niederer@student.unisg.ch

Referent:
Prof. Dr. Marc Forster

Korreferentin:
Prof. Dr. Nora Markwalder

Eingereicht am: 25. Mai 2021

Inhaltsverzeichnis

Literaturverzeichnis

Anmerkung:

Wenn nichts anderes vermerkt ist, werden die Werke mit Nachnamen des Autors beziehungsweise der Autorin sowie mit Seitenzahl und/oder Randnote/-ziffer (N) zitiert. Weist das Dokument weder Seitenzahlen noch Randnoten auf, so wird die zitierte Fundstelle mittels des Abschnitts (Abschn.) gekennzeichnet. Das vorliegende Verzeichnis umfasst auch Quellen, die im Anhang dieser Arbeit verwendet wurden.

AEPLI MICHAEL, Die strafprozessuale Sicherstellung von elektronisch gespeicherten Daten, Unter besonderer Berücksichtigung der Beweismittelbeschlagnahme am Beispiel des Kantons Zürich, Diss. Universität Zürich, Zürich/Basel/Genf 2004.

AMSTUTZ MARC/REINERT MANI (Hrsg.), Basler Kommentar, Kartellgesetz (KG), 1. Aufl., Basel 2010 (zit. BSK KG-BEARBEITER).

BACHMANN MARIO/ARSLAN NERGIZ, «Darknet»-Handelsplätze für kriminelle Waren und Dienstleistungen: Ein Fall für den Strafgesetzgeber?, NZWiSt 2019, 241 ff.

BÄR WOLFGANG, Transnationaler Zugriff auf Computerdaten, ZIS 2/2011, 53 ff. (zit. BÄR, transnationaler Zugriff).

BÄR WOLFGANG, 28. Kapitel EDV-Beweissicherung, in: Wabnitz Heinz-Bernd/Janovsky Thomas/Schmitt Lothar (Hrsg.), Handbuch Wirtschafts- und Steuerstrafrecht, 5. Aufl., München 2020, N 1 ff. (zit. Bär, EDV-Beweissicherung, Durchsuchungen mit Auslandsbezug).

BANGERTER SIMON, Hausdurchsuchungen und Beschlagnahmen im Wettbewerbsrecht unter vergleichender Berücksichtigung der StPO, Diss. Universität Zürich, Zürich/Basel/Genf 2014.

BERANEK ZANON NICOLE, Datenaufbewahrungspflichten vs. Datenlöschungspflichten Kollision von BÜPF und DSG?, in: Weber Rolf/Thouvenin Florent (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich/Basel/Genf 2012, 131 ff.

BETSCHMANN SIMON, Randdatenerhebung im Fernmeldeverkehr gemäss Art. 273 StPO, AJP 2019, 358 ff.

BIEDERMANN AUGUST, Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 6. Oktober 2000, ZStrR 120/2002, 77 ff.

BIEMANN JENS, «Streifenfahrten» im Internet, Die verdachtsunabhängigen Ermittlungen der Polizei im virtuellen Raum, Stuttgart 2013.

BISCHOFF PATRICK/LANTER MARKUS, Verdeckte polizeiliche Ermittlungshandlungen in Chatrooms, Jusletter vom 14. Januar 2008.

BOMMER FELIX, Löschung als Einziehung von Daten, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, 171 ff.

BOTTINELLI NICOLAS, L'obtention par l'autorité pénale des données informatiques situées à l'étranger, AJP 2016, 1327 ff.

BRICH STEPHANIE/HASENBALG CLAUDIA, Kompakt-Lexikon Wirtschaftsinformatik, 1.500 Begriffe nachschlagen, verstehen, anwenden, Wiesbaden 2013.

BÜRGE LUKAS, Polizeiliche Ermittlung und Untersuchung, Charakteristik, Abgrenzungen und Auswir-

kungen auf die Beschuldigtenrechte, Diss. Universität Bern, Bern 2018.

BURCHARD CHRISTOPH, Der grenzüberschreitende Zugriff auf Clouddaten im Lichte der Fundamentalprinzipien der internationalen Zusammenarbeit in Strafsachen – Teil 2, Hintergründe des Kommissionsentwurfs zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln im Strafermittlungsverfahren wie auch zum sog. Microsoft Ireland Case, ZIS 7-8/2018, 249 ff.

BURCKHARDT PETER/RYSER ROLAND M., Die erweiterten Beschlagnahmeverbote zum Schutz des Anwaltsgeheimnisses insbesondere im neuen Strafverfahren, AJP 2013, 159 ff.

DALBY JAKOB, Grundlagen der Strafverfolgung im Internet und in der Cloud: Möglichkeiten, Herausforderungen und Chancen, Wiesbaden 2016.

DEL GIUDICE LUDOVICA, Wann beginnt das polizeiliche Ermittlungsverfahren? Wann beginnt das staatsanwaltschaftliche Untersuchungsverfahren?, ZStrR 2/2010, 116 ff.

DOMBROWSKI NADINE, Extraterritoriale Strafrechtsanwendung im Internet, Freiburg i.Br. 2014.

DONATSCH ANDREAS/LIEBER VIKTOR/SUMMERS SARAH/WOHLERS WOLFGANG (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung StPO, Art. 196-457, 3. Aufl., Zürich/Basel/Genf 2020 (zit. BEARBEITER, StPO-Kommentar, Art. 1 N 1).

DONATSCH ANDREAS/SCHMID ALBERT, Der Zugriff auf E-Mails im Strafverfahren – Überwachung (BÜPF) oder Beschlagnahme?, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, 151 ff.

DONATSCH ANDREAS/SCHWARZENEGGER CHRISTIAN/WOHLERS WOLFGANG, Strafprozessrecht, 2. Aufl., Zürich/Basel/Genf 2014.

EIHOLZER LEO, «Es war das einzige Mittel», Interview mit Stephan Walder, Rheintaler vom 22. Februar 2021, (zit. EIHOLZER, Frage).

FORSTER MARC, Marksteine der Bundesgerichtspraxis zur strafprozessualen Überwachung des digitalen Fernmeldeverkehrs, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schindler Benjamin/Wildhaber Isabelle (Hrsg.), Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, 615 ff. (zit. FORSTER, Marksteine BGer-Praxis).

GAYARD LAURENT, Darknet, Geopolitics and Uses, Volume 2, London/Hoboken 2018.

GERCKE MARCO, Brauchen Ermittlungsbehörden zur Bekämpfung von Kinderpornographie im sog. «Darknet» weitergehende Befugnisse?, CR 7/2018, 480 ff. (zit. GERCKE, Kinderpornographie).

GERCKE MARCO, Die Bekämpfung der Internetkriminalität als Herausforderung für die Strafverfolgungsbehörden, MMR 2008, 291 ff. (zit. GERCKE, Internetkriminalität).

GERCKE MARCO, Strafrechtliche und strafprozessuale Aspekte von Cloud Computing und Cloud Storage, CR 5/2010, 345 ff. (zit. GERCKE, Cloud Computing).

GERHARD FIOLKA/LAUPER NICOLAS, Bundesgericht, Strafrechtliche Abteilung, Urteil 6B_504/2019 vom 29. Juli 2019, A. gegen Staatsanwaltschaft der Republik und des Kantons Neuenburg, schwere Widerhandlung gegen das Betäubungsmittelgesetz; Willkür, Unschuldsvermutung (Original in französischer Sprache, Übersetzung durch die Verfasser), AJP 2020, 662 ff.

GERMANN SANDRO/WICKI-BIRCHLER DAVID, Hacking und Hacker im Schweizer Recht, AJP 2020, 83 ff.

GLESS SABINE, Beweisverbote in Fällen mit Auslandsbezug, JR 8/2008, 317 ff. (zit. GLESS, Beweisverbote).

GLESS SABINE, Heimliche Ermittlungsmassnahmen im Schweizer Strafprozess, ZSTW 2012, 440 ff. (zit. GLESS, heimliche Ermittlungsmassnahmen).

GLESS, SABINE, Sinn und Unsinn von Beweisverwertungsverboten – strafprozessuale Wahrheitssuche und ihre Grenzen im Rechtsvergleich, ZStrR 137/2019, 1 ff. (zit. GLESS, Beweisverwertungsverbote).

GLESS SABINE, Strafverfolgung im Internet, ZStrR 130/2012, 3 ff. (zit. GLESS, Strafverfolgung im Internet).

GRAF DAMIAN K., Aspekte der strafprozessualen Siegelung, AJP 2017, 553 ff. (zit. GRAF, Siegelung).

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

GRAVE CARSTEN/BART CHRISTOPH, Von «Dawn Raids» zu «eRaids», Zu den Befugnissen der Europäischen Kommission bei der Durchsuchung elektronischer Daten, EuZW 2014, 369 ff.

GYARMATI NIKOLAUS, Phänomen Cybercrime und seine Bekämpfung, SZK 1-2/2019, 86 ff.

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

HANSJAKOB THOMAS, Die neuen Bestimmungen zu verdeckter Fahndung und Ermittlung, forumpoenale 4/2013, 214 ff. (zit. HANSJAKOB, Bestimmungen der VF und VE).

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

HANSJAKOB THOMAS, Verdeckte polizeiliche Tätigkeit im Internet, forumpoenale 4/2014, 244 ff. (zit. HANSJAKOB, verdeckte polizeiliche Tätigkeit).

HAUSER-SPÜHLER GABRIELA, Challenges from a compliance point of view, in: Innovation vs. Regulation, Law & Management Praxis, Zürich 2017, 115 ff.

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

HEIMGARTNER STEFAN, Strafprozessuale Beschlagnahme, Wesen, Arten und Wirkungen, Habilitationsschrift Universität Zürich, Zürich/Basel/Genf 2011 (zit. HEIMGARTNER, Beschlagnahme).

HENKEL TIM, Darknet – die dunkle Seite des Internets?, in: Rüdiger Thomas-Gabriel/Bayerl Petra Saskia (Hrsg.), Cyberkriminologie, Kriminologie für das digitale Zeitalter, 175 ff.

HEROLD HELMUT/LURZ BRUNO/WOHLRAB JÜRGEN, Grundlagen der Informatik, 2. aktualisierte Aufl., Hallbergmoos 2012.

HESS MARTIN/LIENHARD STEPHANIE, Übertragung von Vermögenswerten auf der Blockchain, Darstellung der technischen Grundlagen und der Übertragungsformen de lege lata et ferenda, Jusletter vom 4. Dezember 2017.

HORTEN BARBARA/GRÄBER MARLEEN, Cyberkriminalität, Übersicht zu aktuellen und künftigen Erscheinungsformen, Forensische Psychiatrie Psychologie Kriminologie 2020, 234 ff.

HOSTETTLER OTTO, Darknet, Die Schattenwelt des Internets, Zürich 2017 (zit. HOSTETTLER, Darknet).

HOSTETTLER OTTO, Hilflose Ermittler. Warum Kriminelle im Darknet wenig zu befürchten haben, APuZ 46–47/2017, 10 ff. (zit. HOSTETTLER, Hilflose Ermittler).

HOSTETTLER YANNICK, Das Mass der zulässigen Einwirkung bei der verdeckten Ermittlung bzw. Fahndung gemäss Art. 293 StPO, insbesondere bei Drogengeschäften, forumpoenale 3/2018, 192 ff. (HOSTETTLER, zulässige Einwirkung bei VF und VE).

HUG BEELI GUSTAV, Betäubungsmittelgesetz (BetmG), Kommentar zum Bundesgesetz über die Betäubungsmittel und die psychotropen Stoffe vom 3. Oktober 1951, 1. Aufl., Basel 2016.

HUSMANN MARKUS, Bundesgericht, I. öffentlich-rechtliche Abteilung, Urteil 1B_164/2019 vom 15. November 2019, A. gegen Staatsanwaltschaft des Kantons Waadt, Strafprozess, Nichtberücksichtigung von Aktenstücken, AJP 2020, 364 ff.

IHWAS SALEH R., «Die digitale Unterwelt» – Strafprozessuale Ermittlungsmöglichkeiten im Darknet, WiJ 3/2018, 138 ff.

JEANNERET YVAN/KUHN ANDRÉ/PERRIER DEPEURSINGE CAMILLE (édit.), Commentaire Romand, Code de procédure pénale suisse (CPP), 2e édition, Bâle 2019 (zit. BEARBEITER, Commentaire Romand).

JOSITSCH DANIEL/MULLE FRANZISKA, Die StPO-Revision in Bezug auf die Bestimmungen über die verdeckte Ermittlung, AJP 2014, 491 ff.

JOSITSCH DANIEL/POULIKAKOS GEORGE, Beschlagnahme als Zwangsmassnahme, Wie lange ist zu Lange?, ContraLegem 2/2019, 151 ff.

KLAUS SAMUEL/MATHYS ROLAND, «The Best of BÜPF» – Was ändert sich mit der Revision?, Jusletter IT vom 22. September 2016.

KLEIJSSEN JAN/PERRI PIERLUIGI, Chapter 7, Cybercrime, Evidence and Territoriality: Issues and Options, in: Kuijer Martin/Werner Wouter (eds.), Netherlands Yearbook of International Law 2016, The Changing Nature of Territoriality in International Law, The Hague 2017, 3 ff.

KRAUSE BENJAMIN, Ermittlungen im Darknet, Mythos und Realität, NJW 2018, 678 ff.

LENTJES MEILI CHRISTIANE, § 32f Informationsbeschaffung im Internet, in: Donatsch Andreas/Jaag Tobias/Zimmerlin Sven, PolG Kommentar zum Polizeigesetz des Kantons Zürich, Zürich 2018, 417 ff.

MEY STEFAN, Darknet, Waffen, Drogen, Whistleblower, Wie die digitale Unterwelt funktioniert (eBook Version), 2. Aufl., München 2018 (zit. MEY, Darknet).

MEY STEFAN, «Tor» In eine andere Welt? Begriffe, Technologien und Widersprüche des Darknets, APuZ 46–47/2017, 4 ff. (zit. MEY, Tor).

MOORE DANIEL/RID THOMAS, Cryptopolitik and the Darknet, Survival 2016, 7 ff.

MÜLLER SEBASTIAN T., Internetermittlungen und der Umgang mit digitalen Beweismitteln im

(Wirtschafts-)Strafverfahren, NZWiSt 2020, 96 ff.

MUGGLI SANDRA, Im Netz ins Netz - Pädokriminalität im Internet und der Einsatz von verdeckten Ermittlern und verdeckten Fahndern zu deren Bekämpfung, Diss. Universität Zürich/Basel/Genf 2014 (zit. MUGGLI, Diss.).

MUGGLI SANDRA, Bekämpfung der Kinderpornografie und des sexuellen Missbrauchs Minderjähriger, Zusammenfassung der 3. internationalen Arbeitstagung für Staatsanwälte/innen und Ermittlungsleiter/innen der Landeskriminalämter in Windischgarsten, Jusletter vom 20. August 2018 (zit. MUGGLI, Arbeitstagung).

NIGGLI MARCEL ALEXANDER, Das Verhältnis von Eigentum, Vermögen und Schaden nach schweizerischem Strafgesetz, Diss. Universität Zürich, Zürich/Basel/Genf 1992.

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

NIGGLI MARCEL ALEXANDER/WIPRÄCHTIGER HANS (Hrsg.), Basler Kommentar, Strafrecht, Strafgesetzbuch und Jugendstrafgesetz (StGB/JStG), 4. Aufl., Basel 2018 (zit. BSK StGB-BEARBEITER).

NIGGLI MARCEL ALEXANDER/HEIMGARTNER STEFAN (Hrsg.), Basler Kommentar, Internationales Strafrecht (IRSG, GwÜ), 1. Aufl., Basel 2015 (zit. BSK IRSG-BEARBEITER).

OBENHAUS NILS, Cloud Computing als neue Herausforderung für Strafverfolgungsbehörden und Rechtsanwaltschaft, NJW 2010, 651 ff.

RIEDO CHRISTOF/FIOLKA GERHARD/NIGGLI MARCEL ALEXANDER, Strafprozessrecht sowie Rechtshilfe in Strafsachen, Basel 2011.

RIEKKINEN JUHANA, Evaluation of Evidence in Dark Web Drug Cases: The Approach of the Finnish Supreme Court, Jusletter IT vom 30 September 2020.

RIKLIN FRANZ, StPO Kommentar: Schweizerische Strafprozessordnung mit JStPO, StBOG und weiteren Erlassen, 2. Aufl., Zürich 2014 (zit. RIKLIN, Kommentar StPO).

RONC PASCAL/VAN DER STROOM SANDRA/MEYER FRANK, Zur Abgrenzung der verdeckten Ermittlung von der verdeckten Fahndung unter besonderer Berücksichtigung des Internets – zugleich Besprechung des Urteils OGer SB 150205/O/U/eh vom 2. November 2015, forumpoenale 5/2016, 302 ff.

RONC PASCAL/VAN DER STROOM SANDRA, Das Ende der verdeckten Ermittlung im Internet – Besprechung des Urteils BGE 143 IV 27, forumpoenale 5/2017, 344 ff.

ROTH SIMON, Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess, Jusletter vom 17. August 2015 (zit. ROTH, grenzüberschreitende Edition).

RÜCKERT CHRISTIAN, Das Darknet: Blick in eine Schattenwelt, Politische Studien 479/2018, 12 ff.

RÜCKERT CHRISTIAN/GOGER THOMAS, Neue Waffe im Kampf gegen Kinderpornografie im Darknet, Neuregelung von § 184b Abs. 5 S. 2 StGB und § 110d StPO, MMR 2020, 373 ff.

RÜCKERT CHRISTIAN/SAFFERLING CHRISTOPH, Das Strafrecht und die Underground Economy, Analysen und Argumente der Konrad Adenauer Stiftung 2018, 1 ff.

RYSER DOMINIC, «Computer Forensics», eine neue Herausforderung für das Strafprozessrecht, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian S. (Hrsg.), Internet-Recht und Strafrecht, 4. Tagungsband, Bern 2005, 553 ff.

SCHMID NIKLAUS, Strafprozessrecht, Eine Einführung auf der Grundlage des Strafprozessrechtes des Kantons Zürich und des Bundes, 4. Aufl., Zürich/Basel/Genf 2004 (zit. SCHMID, Strafprozessrecht).

SCHMID NIKLAUS, Strafprozessuale Fragen im Zusammenhang mit Computerdelikten und neuen Informationstechnologien im allgemeinen, ZStrR 111/1993, 81 ff. (zit. SCHMID, Computerdelikte).

SCHMID NIKLAUS/JOSITSCH DANIEL, Schweizerische Strafprozessordnung, Praxiskommentar, 3. Aufl., Zürich/St. Gallen 2018. (zit. SCHMID/JOSITSCH, Praxiskommentar StPO).

SCHMID NIKLAUS/JOSITSCH DANIEL, Handbuch des schweizerischen Strafprozessrechts, 3. Aufl., Zürich/St. Gallen 2017 (zit. SCHMID/JOSITSCH, Handbuch StPO).

SCHWARZENEGGER CHRISTIAN, Die Internationalisierung des Wirtschaftsstrafrechts und die schweizerische Kriminalpolitik: Cyberkriminalität und das neue Urheberstrafrecht, ZSR 2/2008, 399 ff.

SCHWEINGRUBER SANDRA, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, Jusletter vom 10. November 2014.

SIMMLER MONIKA/SELMAN SINE/BURGERMEISTER DANIEL, Beschlagnahme von Kryptowährungen im Strafverfahren, AJP 2018, 963 ff.

SINGELNSTEIN TOBIAS, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmassnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co., NStZ 2012, 593 ff.

SUI DANIEL/CAVERLEE JAMES/RUDESILL DAKOTA, The Deep Web and the Darknet: A look inside the Internet's massive Black Box, STIP 03/2015, 1 ff.

SUSSMANN MICHAEL A., The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium, Duke Journal of Comparative & International Law 1999, 451 ff.

TEICHMANN FABIAN, Unzulässigkeit von Onlinedurchsuchungen, Anwaltsrevue 10/2017, 427 ff.

THOUVENIN FLORENT/STILLER BURKHARD/HETTICH PETER/BOCEK THOMAS/REUTIMANN KENTO, Keine Netzsperren im Urheberrecht, sic! 2017, 701 ff. (zit. THOUVENIN ET AL.).

TIEFENTHAL JÜRG MARCEL, Kantonales Polizeirecht der Schweiz, Zürich/Basel/Genf, 2018.

TZANETAKIS MEROPI, Drogenhandel im Darknet: Gesellschaftliche Auswirkungen von Kryptomärkten, APuZ 46–47/2017, 41 ff.

VOGT SABINE, Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale «Kaufhaus» der Kriminellen?, Die Kriminalpolizei 2/2017, 4 ff.

WHITE RYAN/KAKKAR PUNEET V./CHOU VICKI, Prosecuting Darknet Marketplaces: Challenges and Approaches, DOJ Journal of Federal Law and Practice 2019, 65 ff.

WICKER MAGDA, Durchsuchung in der Cloud - Nutzung von Cloud-Speichern und der strafprozessuale Zugriff deutscher Ermittlungsbehörden, MMR 2013, 765 ff.

WITTMER SANDRA/STEINEBACH MARTIN, Computergenerierte Kinderpornografie zu Ermittlungszwecken im Darknet, MMR 2019, 650 ff.

WOHLFEIL STEFAN, Sicherheit im Internet I – Ergänzungen, Kurseinheit 1: Benutzersicherheit, Fakultät für Mathematik und Informatik der Fernuniversität in Hagen, Hagen 2019.

YOUSSEF OMAR ABO, Smartphone-User zwischen unbegrenzten Möglichkeiten und Überwachung, ZStrR 130/2012, 92 ff.

ZÖLLER MARK, Strafbarkeit und Strafverfolgung des Betreibens internetbasierter Handelsplattformen für illegale Waren und Dienstleistungen, KriPoZ 5/2019, 274 ff.

ZULAUF RENA/SIEBER MAJA, Social Media als privatsphärenfreier Raum?, AJP 2017, 548 ff.

Rechtsprechungsverzeichnis

Anmerkung:

Die Zitation der Urteile in den entsprechenden Fussnoten erfolgt in abgekürzter Form, welche in der linken Spalte zu finden ist. Die Urteile sind nach Datum sortiert.

Amtlich publizierte Urteile des Bundesgerichts:

BGE 146 IV 36	Urteil vom 15. November 2019
BGE 144 IV 74	Urteil vom 17. Januar 2018
BGE 143 IV 270	Urteil vom 24. Mai 2017
BGE 143 IV 21	Urteil vom 16. November 2016
BGE 143 IV 27	Urteil vom 28. September 2016
BGE 142 IV 34	Urteil vom 4. November 2015
BGE 141 IV 108	Urteil vom 14. Januar 2015
BGE 140 I 353	Urteil vom 1. Oktober 2014
BGE 140 IV 181	Urteil vom 28. Mai 2014
BGE 140 IV 86	Urteil vom 27. März 2014
BGE 138 IV 225	Urteil vom 10. Oktober 2012
BGE 137 IV 340	Urteil vom 3. November 2011
BGE 137 IV 189	Urteil vom 4. April 2011
BGE 136 II 508	Urteil vom 8. September 2010
BGE 134 IV 266	Urteil vom 16. Juni 2008
BGE 130 II 193	Urteil vom 11. Februar 2004
BGE 126 II 495	Urteil vom 17. November 2000
BGE 126 I 50	Urteil vom 5. April 2000
BGE 106 IV 413	Urteil vom 13. März 1980
BGE 108 IV 145	Urteil vom 23. Dezember 1982

Nicht amtlich publizierte Urteile des Bundesgerichts:

BGer 1B_233/2020	Urteil vom 15. Februar 2021
BGer 1B_547/2020	Urteil vom 3. Februar 2021
BGer 1B_164/2020	Urteil vom 29. April 2020
BGer 1B_153/2019	Urteil vom 11. Dezember 2019
BGer 1B_185/2019	Urteil vom 26. November 2019
BGer 6B_504/2019	Urteil vom 29. Juli 2019
BGer 1C_598/2016	Urteil vom 2. März 2018
BGer 6B_656/2015	Urteil vom 16. Dezember 2016
BGer 1B_351/2016	Urteil vom 16. November 2016

BGer 1B_142/2016	Urteil vom 16. November 2016
BGer 5A_195/2016	Urteil vom 4. Juli 2016
BGer 1B_360/2013	Urteil vom 24. März 2014
BGer 1B_136/2012	Urteil vom 25. September 2012

Weitere Urteile:

BStGer BG.2019.31	Beschluss des Bundesstrafgerichts vom 30. Juli 2019
Urteil 502 2019 297	Urteil der Strafkammer des Kantonsgerichts Freiburg vom 17. Dezember 2019

Materialienverzeichnis

Anmerkung:

Die Materialien werden in den Fussnoten in abgekürzter Form zitiert, welche in der Klammer nach der Materialie ersichtlich ist.

Botschaft über die Änderung des Betäubungsmittelgesetzes vom 9. März 2001, BBl 2001 3715 (zit. Botschaft 2001 BetmG).

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

Botschaft zu den Bundesgesetzen betreffend die Überwachung des Post- und Fernmeldeverkehrs und über die verdeckte Ermittlung vom 1.Juli 1998, BBI 1998 4241 (zit. Botschaft 1998 BÜPF).

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

Botschaft zur Änderung des Betäubungsmittelgesetzes (Pilotversuche mit Cannabis) vom 27. Februar 2019, BBI 2019 2529 (zit. Botschaft 2019 BetmG).

Botschaft zur Vereinheitlichung des Strafprozessrechts vom 21. Dezember 2005, BBl 2006 1085 (zit. Botschaft StPO).

Bundesamt für Justiz (BJ), Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens über den Bericht und den Vorentwurf zur Änderung der Strafprozessordnung (Umsetzung der Motion 14.3383, Kommission für Rechtsfragen des Ständerates, Anpassung der Strafprozessordnung) vom August 2019 (zit. BJ, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zur StPO).

Council of Europe, Discussion paper, Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?, Version August 31, 2010, Internet: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df (Abruf 23.05.2021) (zit. Council of Europe, Cloud Computing).

Council of Europe, Draft Discussion paper, Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from «Cloud Computing Providers» Project on Cybercrime, Strasbourg, January 15, 2010, prepared by Joseph J. Schwerha IV Trace Evidence, LLC, Internet: https://rm.coe.int/16802fa3dc (Abruf 23.05.2021) (zit. Council of Europe, Project on Cybercrime)

Council of Europe, Draft Protocol Version of Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence of April 12, 2021, Internet: https://rm.coe.int/2nd-additional-protocol-budapest-convention-en/1680a2219c (Abruf 23.05.2021) (zit. Council of Europe, Draft Protocol Version April 12, 2021).

Council of Europe, Explanatory Report No. 185 of 23 November 2001 to the Convention on Cybercrime, Internet: https://rm.coe.int/16800cce5b (Abruf 23.05.2021) (zit. Council of Europe, Explanatory Report).

Council of Europe, Final report of the T-CY Cloud Evidence Group, Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, September 16, 2016, Internet: https://rm.coe.int/16806a495e (Abruf 23.05.2021) (zit. Council of Europe, T-CY).

Der Vorsteher des Sicherheits- und Justizdepartements (SJD) des Kantons Obwalden, Stellungnahme vom 12. März 2018 bezüglich Änderung der Strafprozessordnung (Umsetzung der Motion 14.3383, Kommission für Rechtsfragen des Ständerates, Anpassung der Strafprozessordnung), Internet: https://www.ow.ch/dl.php/de/5aa9547552cb3/Stn_Strafprozessordnung.pdf (Abruf 24.05.2021) (zit. Vorsteher des SJD des Kt. Obwalden, Stellungnahme StPO).

Europäische Kommission, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, Strassburg, 17. April 2018, COM(2018) 226 final, Internet: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52018PC0226&from=DE (Abruf 23.05.2021) (zit. Europäische Kommission, Vorschlag für Richtlinie).

Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnung und Sicherungsordnungen für elektronische Beweismittel in Strafsachen, Strassburg, 17. April 2018, COM(2018) 225 final, 2018/0108(COD), Internet: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN und https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52018PC0225&from=EN (Abruf 23.05.2021) (zit. Europäische Kommission, Vorschlag für Verordnung).

European Commission, Commission Staff Working Document, Impact Assessment, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Brussels, April 17, 2018, SWD(2018) 118 final, Internet: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A118%3AFIN (Abruf 23.05.2021) (zit. European Commission, Working Document).

Interpellation Bregy (19.3288) «Cyberkriminalität. Wie sieht es insbesondere bei der Ausbildung der Strafverfolgungsbehörden aus?» vom 21. März 2019 (zit. Interpellation Bregy (19.3288)).

Kommission für Rechtsfragen des Nationalrates (RK-N), Medienmitteilung vom 6. November 2020, Kommission schliesst Beratung zur Revision der Strafprozessordnung ab, Internet: https://www.parlament.ch/press-releases/Pages/mm-rk-n-1-2020-11-06.aspx (Abruf 23.05.2021) (zit. RK-N, Medienmitteilung vom 6.11.2020).

Kommission für Rechtsfragen des Nationalrates (RK-N), Bericht vom 3. Februar 2012 betreffend Parlamentarische Initiative Präzisierung des Anwendungsbereichs der Bestimmungen über die verdeckte Ermittlung, BBI 2012 5991 (zit. RK-N, Bericht von 2012 zur VE).

Nationalrat, Führjahressession 2021, fünfzehnte Sitzung vom 18. März 2021, Strafprozessordnung Änderung, Internet: https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=52440 (Abruf 23.05.2021) (zit. Nationalrat, Frühjahressession 2021).

Regierungsrat des Kantons Zug, Vernehmlassung vom 6. März 2018, Änderung der Strafprozessordnung (Umsetzung der Motion 14.3383, Kommission für Rechtsfragen des Ständerates, Anpassung der Strafprozessordnung), Internet: https://www.zg.ch/behoerden/regierungsrat/vernehmlassungen/aenderung-der-strafprozessordnung-umsetzung-der-motion-14-3383-kommission-fuer-rechtsfragen-des-staenderates-anpassung-der-strafprozessordnung (Abruf 23.05.2021) (zit. Regierungsrat Kt. Zug, Vernehmlassung StPO).

Verzeichnis der Internetquellen

Anmerkung:

Wenn nichts anderes vermerkt ist, werden die Werke mit Nachnamen des Autors beziehungsweise der Autorin sowie mit Seitenzahl und/oder Randnote/-ziffer (N) zitiert. Weist das Dokument weder Seitenzahlen noch Randnoten auf, so wird die zitierte Fundstelle mittels des Abschnitts (Abschn.) gekennzeichnet. Das vorliegende Internetquellenverzeichnis umfasst auch Quellen, die im Anhang dieser Arbeit verwendet wurden.

AVARIKIOTI GEORGIA/BRUNNER ROMAN/KIAYIAS AGGELOS/WATTENHOFER ROGER/ZINDROS DIONYSIS, Structure and Content of the Visible Darknet, Internet: https://arxiv.org/pdf/1811.01348.pdf (Abruf 23.05.2021) (zit. AVARIKIOTI ET. AL).

AWUKU YAW, Was ist eigentlich eine IP-Adresse, t-online vom 28. Januar .2019, Internet: https://www.t-online.de/digital/hardware/wlan-dsl/id_47922534/was-ist-eigentlich-eine-ip-adresse-und-was-verraet-sie-ueber-den-nutzer-.html#:~:text=Ein%20bekanntes%20Beispiel%20f%C3%BCr%20eine,n%C3%A4chsten%20mit%20einem%20Punkt%20getrennt (Abruf 23.05.2021).

BALL MATTHEW/BROADHURST RODERIC/NIVEN ALEXANDER/TRIVEDI HARSHIT, Data Capture and Analysis of Darknet Markets Australian National University (ANU) Cybercrime Observatory, September 11, 2019, Internet: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3344936 (Abruf 23.05.2021).

BAUMGARTNER FABIAN, Tötungsdelikt im Zürcher Seefeld: Tobias K. und die Falle der Australier, NZZ online vom 27. Mai 2017, Internet: https://www.nzz.ch/zuerich/toetungsdelikt-im-zuercher-seefeld-tobias-k-und-die-falle-der-australier-ld.1296973 (Abruf 23.05.2021).

Berner Zeitung, Aargauer Polizei überführt Drogenhändler im Darknet, 8. August 2017, Internet: https://www.bernerzeitung.ch/panorama/vermischtes/kapo-aargau-ueberfuehrt-drogenhaendler-im-darknet/story/31291338 (Abruf 23.05.2021).

BEUTH PATRICK, Alles Wichtige zum NSA-Skandal, Zeit online vom 28. Oktober 2013, Internet: https://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal (Abruf 23.05.2021).

BOSCAINI MATTHIAS, Beweisschwierigkeiten bei Betäubungsmitteldelikten – vom Tatverdacht zum anklagereifen Sachverhalt (rechtliche Möglichkeiten und Grenzen bei der Aufklärung von Betäubungsmitteldelikten), Masterarbeit Universität Luzern, MAS Forensics, Internet: https://www.unilu.ch/fileadmin/fakultaeten/rf/institute/staak/MAS_Forensics/dok/Masterarbeiten_MAS_5/Boscaini_Matthias.pdf (Abruf 23.05.2021).

BÜHLMANN LUKAS, MLL News vom 9. Februar 2017, BGer: Anfragen zu IP-Adresse und Provider von strafbaren E-Mails erfordern Genehmigung des Zwangsmassnahmengerichts, Internet: https://www.mll-news.com/bger-anfragen-zu-ip-adresse-und-provider-von-strafbaren-e-mails-erfordern-genehmigung-des-zwangsmassnahmengerichts/ (Abruf 23.05.2021).

BÜHLMANN LUKAS/REINLE MICHAEL, MLL News vom 10. September 2020, BVGer: Threema gilt als Anbieterin abgeleiteter Kommunikationsdienste im Sinne des BÜPF, Internet: https://www.mll-news.com/bvger-threema-gilt-als-anbieterin-abgeleiteter-kommunikationsdienste-im-sinne-des-buepf/ (Abruf 23.05.2021).

Bundesamt für Kommunikation (BAKOM), Bekämpfung der Internetkriminalität, Internet: https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/internet/bekaempfung-der-internetkriminalitaet.html (Abruf 23.05.2021) (zit. BAKOM, Liste).

Bundesamt für Polizei (fedpol), Die Schweiz und Europol – Fragen und Antworten, Internet: https://www.fedpol.admin.ch/fedpol/de/home/polizei-zusammenarbeit/international/europol/Fragen_und_Antworten.html (Abruf 23.05.2021) (zit. Fedpol, Die Schweiz und Europol).

Bundesamt für Polizei (fedpol), Fingerabdrücke und AFIS, Internet: https://www.fedpol.admin.ch/fedpol/de/home/sicherheit/personenidentifikation/fingerabdruecke.html (Abruf 23.05.2021) (zit. Fedpol, Fingerabdrücke und AFIS).

Bundesamt für Polizei (fedpol), Medienmitteilung vom 23. April 2013, Markanter Anstieg der KOBIK-Verdachtsmeldungen im Bereich Wirtschaftsdelikte, Internet: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-48600.html (Abruf 23.05.2021) (zit. Fedpol, KOBIK).

Bundesamt für Sicherheit in der Informationstechnik (BSI) von Deutschland, Darknet und Deep Web – wir bringen Licht ins Dunkle, Internet: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Darknet-und-Deep-Web/darknet-und-deep-web_node.html (Abruf 23.05.2021) (zit. BSI, Abschn.).

BURGERMEISTER DANIEL, Masterarbeit, Beweiserhebung in der Cloud, Masterarbeit Universität Luzern, MAS Forensics, Internet: https://www.unilu.ch/fileadmin/fakultaeten/rf/institute/staak/MAS_Forensics/dok/Masterarbeiten_MAS_5/Burgermeister_Daniel.pdf (Abruf 23.05.2021).

BURRI DANIEL/EMMENEGGER GUIDO/KOPP SIMON, Jahresbericht 2019, Oberstaatsanwaltschaft des Kantons Luzern, Februar 2020, Internet: https://staatsanwaltschaft.lu.ch/-/media/Staatsanwaltschaft/Dokumente/Downloads/Jahresbericht_2019.pdf?la=de-CH (Abruf 23.05.2021).

Check Point Software Technologies Ltd, Check Point Blog March 30, 2021, A passport to freedom? Fake COVID-19 test results and vaccination certificates offered on Darknet and hacking forums, Internet: https://blog.checkpoint.com/2021/03/22/a-passport-to-freedom-fake-covid-19-test-results-and-vaccination-certificates-offered-on-darknet-and-hacking-forums/ (Abruf 23.05.2021) (zit. Check Point).

CHEN ADRIAN, The Underground Website Where You Can Buy Any Drug Imaginable, Gawker June 1, 2011, Internet: https://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160 (Abruf 23.05.2021).

CHRISTENSSON PER, Login Definition, Tech Terms August 12, 2017, Internet: https://techterms.com/definition/login (Abruf 23.05.2021).

CHRISTIAN JON, The «Exit Scam» Is the Darknet's Perfect Crime, Vice online February 4, 2015, Internet: https://www.vice.com/en/article/xyw7xn/darknet-slang-watch-exit-scam (Abruf 23.05.2021).

Council of Europe, T-CY News from April 14, 2021, Towards a Protocol to the Convention on Cybercrime: additional stakeholder consultations, Internet: https://www.coe.int/en/web/cybercrime/-/towards-a-protocol-to-the-convention-on-cybercrime-additional-stakeholder-consultatio-1 (Abruf 23.05.2021) (zit. Council of Europe, T-CY News).

Darknetstats.com, All the darkweb news you need and more, Internet: https://www.darknetstats.com/ (Abruf 23.05.2021).

Dienst Überwachung Post- und Fernmeldeverkehr (ÜPF), Statistik, Internet: https://www.li.admin.ch/de/stats (Abruf 23.05.2021) (zit. Dienst ÜPF, Statistik).

Dropbox, Behördliche Auskunftsanfragen an Dropbox, Internet:

https://help.dropbox.com/de-de/accounts-billing/security/legal-requests (Abruf 23.05.2021) (zit. Dropbox).

Dienst Überwachung Post- und Fernmeldeverkehr (Dienst ÜPF), Merkblatt «FDA - AAKD» Abgrenzung zwischen Fernmeldedienstanbieterinnen (FDA) und Anbieterinnen abgeleiteter Kommunikationsdienste (AAKD), Stand: 16. April 2019, Internet: https://www.li.admin.ch/sites/default/files/2019-04/Merkblatt%20FDA_AAKD%20DE.pdf (Abruf 23.05.2021) (zit. Dienst ÜPF, Merkblatt «FDA - AAKD»).

DUSANEK LAURA, Probleme der strafprozessualen Überwachung abgeleiteter Internetdienste wie Facebook, Skype oder Whatsapp, Lösungen im neuen BÜPF?, Masterarbeit Universität St. Gallen, Internet: https://www.marc-forster-strafrecht.com/dissertationen-und-masterarbeiten-hsg/ (Abruf 23.05.2021)

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Erläuterungen zu Cloud Computing, Internet: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html (Abruf 23.05.2021) (zit. EDÖB).

Europarat, Vertragsbüro, Unterschriften und Ratifikationsstand des Vertrags 185, Übereinkommen über Computerkriminalität, Internet: https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=zw38jIZt (Abruf 23.05.2021) (zit. Europarat, Ratifikationsstand der CCC).

European Monitoring Centre for Drugs and Drug Addiction (EMCDDA)/ Europol, Drugs and the darknet: Perspectives for enforcement research and policy 2017, Internet: https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy (Abruf 23.05.2021) (zit. EMCDDA/Europol).

Europol, Joint Cybercrime Action Taskforce (J-CAT), Internet: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce (Abruf 23.05.2021) (zit. Europol, J-CAT).

Europol, Press Release of December 4, 2020, Europol predictions correct for fake covid-19 vaccines, Internet: https://www.europol.europa.eu/newsroom/news/europol-predictions-correct-for-fake-covid-19-vaccines (Abruf 23.05.2021) (zit. Europol, Covid-19).

Europol, Press Release of July 20, 2017, Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation, Internet: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (Abruf 23.05.2021) (zit. Europol, Criminal Dark Web).

Facebook Ireland Ltd., Datenrichtlinie, Internet: https://de-de.facebook.com/policy.php# (Abruf 23.05.2021) (zit. Facebook).

FEUSI ALOIS, «Wer hier arbeitet, traut eher jedem alles zu»: Eine Spezialabteilung der Zürcher Polizei spürt Pädokriminelle auf. Ein Berufsporträt, NZZ online vom 16. Oktober 2019, Internet: https://www.nzz.ch/zuerich/zuerich-wie-detektive-paedokriminelle-im-internet-aufspueren-ld.1512385 (Abruf 23.05.2021).

FORSTER MARC, Territorialitätsgrundsatz und strafrechtliches Zugriffsprinzip bei Facebook, Whatsapp, Google und Co. – Gefährliche «Postkutschenromantik» im 21. Jahrhundert, 2. September 2019, Internet: https://www.marc-forster-strafrecht.com/2019/09/02/territorialit%C3%A4tsgrundsatz-und-internationalstrafrechtliches-zugriffsprinzip-bei-facebook-whatsapp-google-und-co-gef%C3%A4hrliche-postkutschenromantik-im-21-jahrhundert/ (Abruf 23.05.2021) (zit. FORSTER, Territorialitätsgrundsatz).

Gabler Wirtschaftslexikon, Browser, Definition: Was ist «Browser»?, Internet: https://wirtschaftslexikon.gabler.de/definition/browser-29143 (Abruf 23.05.2021) (zit. Gabler Wirtschaftslexikon, Browser).

Gabler Wirtschaftslexikon, E-Marketplace, Definition: Was ist «E-Marketplace»?, Internet: https://wirtschaftslexikon.gabler.de/definition/e-marketplace-51868 (Abruf 23.05.2021) (zit. Gabler Wirtschaftslexikon, E-Marketplace).

Gabler Wirtschaftslexikon, Internet, Definition: Was ist «Internet»?, Internet: https://wirtschaftslexikon.gabler.de/definition/internet-37192 (Abruf 23.05.2021) (zit. Gabler Wirtschaftslexikon, Internet).

Gabler Wirtschaftslexikon, IP-Adresse, Internet: https://wirtschaftslexikon.gabler.de/definition/ip-adresse-41676 (Abruf 23.05.2021) (zit. Gabler Wirtschaftslexikon, IP-Adresse).

Gabler Wirtschaftslexikon, Soziale Medien, Definition: Was ist «Soziale Medien»?, Internet: https://wirtschaftslexikon.gabler.de/definition/soziale-medien-52673#:~:text=Definition:%20Was%20ist%20%22Soziale%20Medien%22?%20Soziale%20Medien%20(Social,2.0,%20das%20Mitmachweb,%20ist%20wesentlich%20durch%20sie%20 (Abruf 23.05.2021) (zit. Gabler Wirtschaftslexikon, Soziale Medien).

Gabler Wirtschaftslexikon, World Wide Web (WWW), Definition: Was ist «World Wide Web (WWW)»?, Internet: https://wirtschaftslexikon.gabler.de/definition/world-wide-web-www-49260 (Abruf 23.05.2021) (zit. Gabler Wirtschaftslexikon, WWW).

Generalsekretariat Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD), Medienmitteilung vom 17. November 2020, Verstärkter Einsatz der Kantone gegen Cyber- und Pädokriminalität, Internet: https://www.kkjpd.ch/newsreader/verst%C3%A4rkter-einsatz-der-kantone-gegen-cyber-und-p%C3%A4dokriminalit%C3%A4t.html (Abruf 23.05.2021) (zit. KKJPD).

Google, Entdecken Sie die Standorte unserer Rechenzentren, Internet: https://www.google.com/intl/de/about/datacenters/locations/ (Abruf 23.05.2021) (zit. Google, Rechenzentren).

Google, Datenschutzerklärung und Nutzungsbedingungen, Wie Google mit behördlichen Ersuchen zu Nutzerdaten umgeht, Internet: https://policies.google.com/terms/information-requests?hl=de (Abruf 23.05.2021) (zit. Google, Datenschutzerklärung).

GOTSCH LARS/RENSCH CHRISTIAN, Schweizer Darknet-Dealer: Ecstasy und Kokain frei Haus, 10vor10 vom 30. November 2018, Internet: https://www.srf.ch/news/schweiz/schweizer-darknet-dealer-ecstasy-und-kokain-frei-haus (Abruf 23.05.2021).

Hochschule Luzern, Ressourcen für empirische Methoden, Auswahl der Erhebungsmethode, Internet: https://www.empirical-methods.hslu.ch/forschungsprozess/qualitative-forschung/auswahl-der-erhebungsmethode/ (Abruf 23.05.2021).

Interpol, Darknet and Cryptocurrencies, Internet: https://www.interpol.int/How-we-work/Innovation/Darknet-and-Cryptocurrencies (Abruf 23.05.2021).

Kantonspolizei Aargau, Medienmitteilung vom 8. August 2017, Aargau: Die Polizei ist auch im Darknet präsent, Internet: https://www.ag.ch/de/weiteres/aktuelles/medienportal/medienmitteilung_kapo/medienmitteilungen_kapo/medienmitteilungen_kapo_details_81986.jsp (Abruf 23.05.2021).

KOPP SIMON, Medienmitteilung der Staatsanwaltschaft Luzern vom 28. Mai 2018, Rund 800 Drogendeals im Darknet: Drogendealer überführt, Internet: https://newsletter.lu.ch/inxmail/html_mail.jsp?id=0&email=newsletter.lu.ch&mail-ref=000dr4y000fru000000000gcwqtpd50j (Abruf 23.05.2021).

KÜTTEL KILIAN, Luzerner Polizei schnappt Darknet-Dealer, Luzerner Zeitung online vom 28. Mai 2018, Internet: https://www.luzernerzeitung.ch/zentralschweiz/luzern/luzerner-polizei-schnappt-darknet-dealer-ld.1024200 (Abruf 23.05.2021).

LUBER STEFAN/SCHMITZ PETER, Definition Brute Force, Was ist ein Brute-Force-Angriff?, Security Insider vom 17. Januar 2018, Internet: https://www.security-insider.de/was-ist-ein-brute- force-angriff-a-677192/ (Abruf 23.05.2021).

MEIER ANDREAS, Cybercrime, Polizei Basel-Landschaft, Präsentation vom 26. November 2019, https://www.baselland.ch/politik-und-behorden/direktionen/sicherheitsdirektion/polizei/downloads/referat-cybercrime-26-11-2019.pdf/@@download/file/Referat_Cybercrime_26.11.2019.pdf (Abruf 23.05.2021).

MEY STEFAN, Die Banalität des Dark Commerce: Das Darknet als Einkaufsmeile, Heise Medien vom 26. Dezember 2015, Internet: https://www.heise.de/ct/artikel/Die-Banalitaet-des-Dark-Commerce-Das-Darknet-als-Einkaufsmeile-3052700.html (Abruf 23.05.2021) (zit. MEY, Banalität des Darknet Commerce).

Minsters of Justice of the European Union, Informal Meeting of the Justice and Home Affairs Ministers, Discussion Paper on tackling cybercrime, Amsterdam January 25-26, 2016, Internet: https://perma.cc/KJS2-SQ9C (Abruf 23.05.2021) (zit. Ministers of Justice EU).

MUTH MAX, Polizei knackt Telegram-Drogenmärkte, SZ online vom 30. Oktober 2020, Internet: https://www.sueddeutsche.de/digital/cybercrime-telegram-drogenhandel-1.5099730 (Abruf 23.05.2021).

NAJJAR MOHAMED/SCHWASS HANNAH, Das Darknet - Im Licht der Öffentlichkeit, Seminar Informatik und Gesellschaft im Sommersemester 2019 geleitet durch Prof. Dr. Paul Molitor am Institut für Informatik an der Naturwissenschaftlichen Fakultät III der Martin-Luther-Universität Halle-Wittenberg, Internet: https://blogs.urz.uni-halle.de/informatikundgesellschaft/files/2019/10/Najjar_und_Schwass.pdf (Abruf 23.05.2021).

Nationales Zentrum für Cybersicherheit (NCSC), Das NCSC, Internet: https://www.ncsc.admin.ch/ncsc/de/home/ueber-ncsc/das-ncsc.html (Abruf 23.05.2021) (zit. NCSC).

NZZ online vom 13.02.2015, Tamedia übernimmt Tutti.ch und Car4you.ch ganz, Internet: https://www.nzz.ch/wirtschaft/tamedia-uebernimmt-tuttich-und-car4youch-ganz-1.18482328 (Abruf 23.05.2021) (zit. NZZ vom 13.2.2015).

PAVLOVIC ALEXANDRA, Missbrauchsfall in St. Galler Kita: Pädophiler Betreuer muss für vier Jahre und sechs Monate ins Gefängnis, Tagblatt online vom 21. Januar 2020, Internet: https://www.tagblatt.ch/ostschweiz/stgallen/prozess-zum-missbrauchsfall-in-stgaller-kita-richter-verkuendet-urteil-angeklagter-ist-gestaendig-was-ich-gemacht-habe-tut-mir-unendlich-leid-ld.1186031 (Abruf 23.05.2021).

PETERSON RACHEL, Data centers year in review, January 1, 2019, Internet: https://engineering.fb.com/2019/01/01/data-center-engineering/data-centers-2018/ (Abruf 23.05.2021).

ROTH SIMON, Das Bundesgericht bestätigt das Territorialitätsprinzip bei grenzüberschreitenden Straf-

untersuchungen, Lex Futura Legal Service Provider vom 10. Januar 2020, Internet: https://www.lexfutura.ch/was-uns-gerade-beschaeftigt/artikel/das-bundesgericht-bestaetigt-das-territorialitaetsprinzip-bei-grenzueberschreitenden-strafuntersuchungen/ (Abruf 23.05.2021) (zit. ROTH, Territorialitätsprinzip).

SCHOOP FLORIAN/BAUMGARTNER FABIAN, «Warum haben Sie einen Mann erstochen, den Sie gar nicht kennen?» – Wie eine Freundschaft hinter Gittern in einer Bluttat endet, NZZ online vom 29. Januar 2020, Internet: https://www.nzz.ch/zuerich/toetungsdelikt-seefeld-eine-fatale-freundschaft-hinter-gittern-ld.1537354 (Abruf 23.05.2021).

SCHOOP FLORIAN, Dealer im Darknet: Wie «Happy Olaf» und «Swiss Flakes» aus dem Verkehr gezogen wurden, NZZ online vom 7. August 2018, Internet: https://www.nzz.ch/zuerich/dealer-im-darknet-wie-happy-olaf-und-swiss-flakes-aus-dem-verkehr-gezogen-wurden-ld.1409615 (Abruf 23.05.2021) (zit. SCHOOP, Dealer im Darknet).

Schweizer Radio und Fernsehen (SRF), Regionaljournal Ostschweiz vom 7. Februar 2019, Betreuer soll sich an Buben vergangen haben, Internet: https://www.srf.ch/news/regional/ostschweiz/verdacht-missbrauch-in-kita-betreuer-soll-sich-an-buben-vergangen-haben (Abruf 23.05.2021) (zit. SRF).

SIEGLE JOCHEN, Die BBC startet einen News-Dienst im Darknet, NZZ online vom 25. Oktober 2019, Internet: https://www.nzz.ch/digital/bbc-im-darknet-nachrichten-im-news-untergrund-umgehen-zensur-ld.1517792 (Abruf 23.05.2021) (zit. SIEGLE, BBC im Darknet).

Stadt Bern, Kriminalität und Strafrecht 19, Kriminalstatistik 285, Internet: https://www.bern.ch/themen/stadt-recht-und-politik/bern-in-zahlen/publikationen/jahrbuch/einzelne-kapitel/19-kriminalitat-und-strafrecht.pdf/view (Abruf 23.05.2021) (zit. Stadt Bern).

SULIAK HASSO, Interview mit Deutschlands führendem Darknet-Ermittler: «Unser Strafrecht ist auf dem Stand des vergangenen Jahrhunderts», LTO online vom 20. September 2018, Internet: https://www.lto.de/recht/justiz/j/darknet-ermittlungen-osta-andreas-may-waffen-drogen-interview/ (Abruf 23.05.2021) (zit. SULIAK, Frage).

SVERDLIK YEVGENIY, eBay Designs Own Servers, Decentralizes Data Center Strategy, DataCenter Knowledge, September 8, 2018, Internet: https://www.datacenterknowledge.com/ebay/ebay-designs-own-servers-decentralizes-data-center-strategy (Abruf 23.05.2021).

Tails, How Tails works, Internet: https://tails.boum.org/about/index.de.html (Abruf 23.05.2021) (zit. Tails).

Telegram, Fragen und Antworten, Internet: https://telegram.org/faq/de (Abruf 23.05.2021) (zit. Telegram, Frage:)

The Tor Project, About History, Internet: https://www.torproject.org/about/history/ (Abruf 23.05.2021) (zit. Tor Project, About History).

The Tor Project, Servers, Internet: https://metrics.torproject.org/networksize.html (Abruf 23.05.2021) (zit. Tor Project, Servers).

The Tor Project, Some statistics about onions, February 26, 2015, Internet: https://blog.torproject.org/some-statistics-about-onions (Abruf 23.05.2021) (zit. Tor Project, statistics).

The Tor Project, Users, Internet: https://metrics.torproject.org/userstats-relay-country.html (Abruf 23.05.2021) (zit. Tor Project, Users).

TSCHIRREN JÜRG, Will die EU verschlüsselte Kommunikation bei WhatsApp verbieten?, Echo der

Zeit vom Dienstag 17. November 2020 (Artikel vom 21. November 2020), Internet: https://www.srf.ch/news/panorama/verschluesselte-kommunikation-will-die-eu-verschluesselte-kommunikation-bei-whatsapp-verbieten (Abruf 23.05.2021).

Twitter Inc., Richtlinien für Strafverfolgungsbehörden, Internet: https://help.twitter.com/de/rules-and-policies/twitter-law-enforcement-support#:~:text=Nicht%20%C3%B6ffentliche%20Informationen%20%C3%BCber%20Twitter,einschl%C3%A4gigen%20rechtsg%C3%BCltigen%20Verfahrens%20mitgeteilt%2C%20z (Abruf 23.05.2021) (zit. Twitter, Titel).

U.S. Department of Justice (DoJ), U.S. Attorney's Office, Southern District of New York, Press Release Number: 13-322 of October 25, 2013 (updated May 18, 2015), Manhattan U.S. Attorney Announces Seizure Of Additional $28 Million Worth Of Bitcoins Belonging To Ross William Ulbricht, Alleged Owner And Operator Of «Silk Road» Website, Internet: https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-seizure-additional-28-million-worth-bitcoins-belonging (Abruf 23.05.2021) (zit. DoJ, U.S. Attorney's Office).

VINTON KATE, The Feds Explain How They Seized The Silk Road Servers, Forbes online September 8, 2014, Internet: https://www.forbes.com/sites/katevinton/2014/09/08/the-feds-explain-how-they-seized-the-silk-road-servers/ (Abruf 23.05.2021).

VON GEHLEN DIRK, «Dark Social» - Ich poste was, was du nicht siehst, SZ online vom 16. Januar 2019, Internet: https://www.sueddeutsche.de/digital/dark-social-media-gruppen-whatsapp-telegram-facebook-habeck-1.4289076 (Abruf 23.05.2021).

VON HEIN MATTHIAS, Deutschlands grösste Online-Dealer vor Gericht, DW online vom 4. August 2020, Internet: https://www.dw.com/de/deutschlands-gr%C3%B6%C3%9Fte-online-dealer-vor-gericht/a-54435047 (Abruf 23.05.2021).

WhatsApp LLC, WhatsApp Datenschutzrichtlinie vom 4. Januar 2021, Internet: https://www.whatsapp.com/legal/updates/privacy-policy/?lang=de (Abruf 23.05.2021) (zit. WhatsApp, Titel).

WILSON EMILY, The truth about the dark web fraud trade, Fraud Magazine, November/December 2019, Internet: https://www.fraud-magazine.com/cover-article.aspx?id=4295009061 (Abruf 23.05.2021).

Rechtsquellenverzeichnis

BetmG	Bundesgesetz über die Betäubungsmittel und die psychotropen Stoffe vom 3. Oktober 1951 (SR 812.121).
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (SR 780.1).
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101).
CCC	Übereinkommen über die Cyberkriminalität vom 23 November 2001 (SR 0.311.43).
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1)
FMG	Fernmeldegesetz vom 30. April 1997 (SR 784.10).
IRSG	Bundesgesetz über internationale Rechtshilfe in Strafsachen vom 20. März 1981 (SR 351.1).
KG	Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen vom 6. Oktober 1995 (SR 251)
PG	Postgesetz vom 17. Dezember 2010 (SR 783.0).
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (311.0).
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0).
VID	Verordnung über Internet-Domains vom 5. November 2014 (SR 784.104.2).
VStrR	Bundesgesetz über das Verwaltungsstrafrecht vom 22. März 1974 (SR 313.0).
VÜPF	Verordnung über die Überwachung des Post- und Fernmeldeverkehrs vom 15. November 2017 (SR 780.11).
WG	Bundesgesetz über Waffen, Waffenzubehör und Munition vom 20. Juni 1997 (SR 514.54).

Tabellenverzeichnis

Abkürzungsverzeichnis

Anmerkung:

Im Anhang wurden die Abkürzungen zugunsten der besseren Leserlichkeit der Interviews nicht konsequent verwendet.

A.M.	Anderer Meinung
AAKD	Anbieterinnen abgeleiteter Kommunikationsdienste
Abs.	Absatz
Abschn.	Abschnitt
AFIS	Automatisiertes Fingerabdruckidentifizierungssystem
AGB	Allgemeine Geschäftsbedingungen
AJP / PJA	Aktuelle Juristische Praxis /Pratique Juridique Actuelle
Anh.	Anhang
AP	Associated Press
APuZ	Aus Politik und Zeitgeschichte
Art.	Artikel
Aufl.	Auflage
BAKOM	Bundesamt für Kommunikation (der Schweizerischen Eidgenossenschaft)
BBC	British Broadcasting Corporation
BBI	Bundesblatt
BGE	Leitentscheide des Bundesgerichts
BGer	Bundesgericht
BJ	Bundesamt für Justiz
BSI	Bundesamt für Sicherheit in der Informationstechnik (der Bundesrepublik Deutschland)
BSK	Basler Kommentar
bspw.	beispielsweise
BStGer	Bundesstrafgericht
BVGer	Bundesverwaltungsgericht
bzw.	beziehungsweise
ca.	circa
CHF	Schweizer Franken
CR	Computer und Recht
Dienst ÜPF	Dienst Überwachung Post- und Fernmeldeverkehr
d.h.	das heisst
DDos	Distributed Denial of Service (deutsch: Verweigerung des Dienstes)
DEA	United States Drug Enforcement Administration

Diss.	Dissertation
DNA	Desoxyribonukleinsäure
DOJ	United States Department of Justice
DW	Deutsche Welle
E.	Erwägung
EC3	European Cybercrime Center
édit	éditeur (frz.)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
eds.	editor (engl.)
EDV	Elektronische Datenverarbeitung
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMCDDA	The European Monitoring Centre for Drugs and Drug Addiction
engl.	englisch
et al.	t alii = und weitere
etc.	et cetera (lat.)
ETH Zürich	Eidgenössische Technische Hochschule Zürich
EU	Europäische Union
Europol	The European Union's law enforcement agency
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
evtl.	eventuell
f. / ff.	folgend(e) / fortfolgende
FBI	United States Federal Bureau of Investigation
FDA	Anbieterinnen von Fernmeldediensten
Fedpol	Bundesamt für Polizei
FN	Fussnote
frz.	französisch
gem.	gemäss
Gl.M.	Gleicher Meinung
GovWare	GovernmentWare
h.L.	heutige Lehre
Hrsg.	Herausgeber
HTML	Hypertext Markup Language
http	Hypertext Transfer Protocol
i.d.R.	in der Regel
i.e.S.	im engeren Sinn(e)
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit

i.w.S.	im weiteren Sinne
Inc.	incorporated (engl.)
insb.	insbesondere
Interpol	International Criminal Police Organisation
IP-Adresse	Internet Protocol
IPv4 / IPv6	Internet Protocol Version 4 und 6
ISC-EJPD	Informatik Service Center des Eidgenössischen Justiz- und Polizeidepartement EJPD
IT	Informationstechnik
J-CAT	Joint Cybercrime Action Taskforce
JR	Juristische Rundschau
jur.	juristisch
Kap.	Kapitel
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
KOBIK	Die Koordinationsstelle zur Bekämpfung der Internetkriminalität
KriPoZ	Kriminalpolitische Zeitschrift
Kt.	Kanton
lat.	lateinisch
lit.	litera
LSD	Lysergsäurediethylamid
LTO	Legal Tribune Online
m.a.W.	mit anderen Worten
m.E.	meines Erachtens
m.w.H.	mit weiteren Hinweisen
Mio.	Million(en)
MLL	Meyerlustenberger Lachenal
MMR	Multimedia und Recht
N	Note
nat.	natürlich
NCSC	Nationales Zentrum für Cybersicherheit
NEDIK	Netzwerk digitale Ermittlungsunterstützung Internetkriminalität
NJW	Neue Juristische Wochenschrift
No.	Number (engl.)
Nr.	Nummer
NSA	National Security Agency
NStZ	Neue Zeitschrift für Strafrecht
NZWiSt	Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht
NZZ	Neue Zürcher Zeitung

PolG	Polizeigesetz
resp.	respektive
RK-N	Kommission für Rechtsfragen des Nationalrates
sic!	Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht
sog.	sogenannt(e)
SRF	Schweizer Radio und Fernsehen
StA	Staatsanwalt; Staatsanwaltschaft
STIP	Science and Technology Innovation Program, Woodrow Wilson Center
SZ	Süddeutsche Zeitung
SZK	Schweizerische Zeitschrift für Kriminologie
T-CY	The Cybercrime Convention Committee
Tor	The Onion Routing oder The Onion Router
u.a.	unter anderem
U.S.	United States
u.U.	unter Umständen
v.a.	vor allem
VE	Verdeckte Ermittlung
VF	Verdeckte Fahndung
vgl.	vergleiche
vs.	versus
WiJ	Journal der Wirtschaftsstrafrechtlichen Vereinigung e.V.
WLAN	Wireless Local Area Network
WWW	World Wide Web
z.B.	zum Beispiel
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik
zit.	zitiert
ZMG	Zwangsmassnahmengericht
ZSR	Zeitschrift für Schweizerisches Recht
ZStrR	Schweizerische Zeitschrift für Strafrecht
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

I. Einleitung*

A Ausgangslage

«Making small talk with your pot dealer sucks. Buying cocaine can get you shot. What if you could buy and sell drugs online like books or light bulbs? Now you can: Welcome to Silk Road»[1] schrieb der Journalist ADRIAN CHEN 2011 in einem Exposee für den Blog «Gawker» über die inzwischen gelöschte Darknet-Verkaufsplattform Silk Road. CHEN's Artikel wurde überraschenderweise von diversen Medien aufgegriffen, was nicht nur die Bekanntheit von Silk Road und der Kryptowährung Bitcoin steigerte, sondern auch amerikanische Behörden dazu bewegte, Ermittlungen gegen den Betreiber von Silk Road aufzunehmen.[2] Diese Ermittlungen verliefen erfolgreich und endeten in der Ausserbetriebnahme der Plattform im Jahre 2013. Seither sind im Darknet, das über den sog. Tor Browser aufgerufen wird, unzählige neue Verkaufsplattformen entstanden.[3] Die Nutzung des Tor Netzwerks mit den dort gelegenen «Hidden Services» bietet Verkäufern und Käufern von illegalen Waren und Dienstleistungen die Möglichkeit, ihre Geschäfte über das Internet unter der Wahrung ihrer Anonymität abzuwickeln. Der Gebrauch dieser neuen Technologien stellt die Strafverfolgungsbehörden vor bedeutende Herausforderungen. Einerseits ergeben sich bereits bei der Ermittlung von allfälligen Straftätern resp. der Überwachung dieser Verkaufsplattformen gewisse tatsächliche und rechtliche Schwierigkeiten, weil «gängige» Ermittlungsmethoden nicht angewendet werden können.[4] Andererseits resultieren aber auch bei einem Ermittlungserfolg weitere Herausforderungen, v.a. dann, wenn die Strafverfolgungsbehörden direkt Daten eines Benutzerkontos bei einer Darknet-Verkaufsplattform sicherstellen und durchsuchen möchten.

B Zielsetzung und Aufbau

In der vorliegenden Arbeit sollen die oben aufgeworfenen Herausforderungen für die Strafverfolgungsbehörden bei der Ermittlungstätigkeit sowie der Beweissicherung in tatsächlicher und rechtlicher Hinsicht erläutert und analysiert werden. Nach einer Einführung in die Grundlagen liegt der erste Schwerpunkt der Arbeit auf den Schwierigkeiten, die sich bei den Ermittlungen im Darknet ergeben sowie den Anwendungsmöglichkeiten von strafprozessualen Zwangsmassnahmen in Form von geheimen Überwachungsmassnahmen, die zur Lokalisation und Identifikation von Verkäufern und Käufern auf Darknet-Verkaufsplattformen eingesetzt werden können. Ausgangssituation für den zweiten Forschungsfokus bilden zwei Entscheide des Bundesgerichts,[5] bei denen mutmassliche Drogenverkäufer im Darknet durch die Zürcher Strafbehörden lokalisiert und identifiziert sowie deren E-Mail- und Benutzerkonten für Handelsplattformen im Darknet sichergestellt wurden. Im Zusammenhang mit diesen beiden Entscheiden wird die Bundesgerichtspraxis zur strafprozessualen Zwangsverwaltung von Darknet-Benutzerkonten sowie deren Durchsuchung hinsichtlich ihrer Sachgerechtigkeit anhand von einschlägiger Cybercrime-Literatur analysiert und auf die Herausforderungen der Beweissicherung eingegangen. Da sich gewisse Parallelen zur Datenerhebung bei Cloud-Speicherplätzen und Social Media Benutzerkonten ergeben, werden die Vorgehensweisen in Bezug auf diese Service Provider vergleichsweise beigezogen.

* Ein herzlicher Dank geht an Prof. Dr. Marc Forster für den Vorschlag zur Auseinandersetzung mit der vorliegenden Materie und die Übernahme des Referats, sowie Prof. Dr. Nora Markwalder für die Annahme des Koreferats. Ebenfalls herzlich danken möchte ich meinen Interviewpartnern: Frau Sabrina Werren, Herrn Heinz Zaugg, Herrn lic. iur. Stephan Walder, Herrn Andreas Eugster und Herrn Reto Waldmeier für die hilfreichen Einblicke aus der Praxis und die breitwillige Unterstützung.
Hinweis zur Gender-Formulierung: Bei allen Bezeichnungen, die auf Personen bezogen sind, meint die gewählte Formulierung beide Geschlechter, auch wenn aus Gründen der leichteren Lesbarkeit nur die männliche Form verwendet wird.
[1] CHEN, Abschn. 1.
[2] HOSTETTLER, Darknet, 110 f.
[3] HOSTETTLER, Darknet, 114 f.; HAUSER-SPÜHLER, 119, N 79-81.
[4] Zum Ganzen RÜCKERT/SAFFERLING, 2.
[5] BGer 1B_185/2019; BGer 1B_153/2019.

Dabei wird wie folgt vorgegangen: Um die strafprozessualen Herausforderungen bezüglich des Phänomens Darknet zu erläutern, werden zuerst die verschiedenen Bereiche des Internets sowie deren Funktionsweise voneinander abgegrenzt und erklärt sowie der Aufbau von Verkaufsplattformen im Darknet erläutert. Anschliessend werden die relevanten Straftatbestände bezüglich der Aktivitäten auf diesen Plattformen kurz erläutert und ausgewählte bedeutende Ermittlungserfolge in der Schweiz präsentiert (Kap. II.). Nach einem kurzen Überblick zu den Herausforderungen für Ermittlungen im Darknet werden die rechtlichen Grundlagen zu den Zwangsmassnahmen dargelegt (Kap. III.). Im Anschluss erfolgt die Thematisierung der Anwendungsmöglichkeiten von geheimen Überwachungsmassnahmen anhand der aus den Interviews gewonnen Erkenntnissen von verschiedenen kantonalen Strafbehörden (Kap. IV.). Darauffolgend wird die bundesgerichtliche Rechtsprechung bezüglich der bereits erwähnten Entscheide erläutert und anhand Rechtsprechung und Lehrmeinungen betreffend deren Sachgerechtigkeit reflektiert (Kap. V). Im letzten Kapitel werden die gewonnen Erkenntnisse der Arbeit und insb. die heutigen strafprozessualen Möglichkeiten zur Zwangsverwaltung, Durchsuchung und Überwachung von Online-Verkaufsplattformen im Darknet sowie deren Herausforderungen resümiert (Kap. VI.). Da das Darknet im Kontext des Strafprozessrechts in der Deutschen Lehre resp. auf europäischer Ebene ausführlicher diskutiert wird als in der Schweizer Lehre, wird punktuell auf die Rechtslage und die Diskurse in Deutschland verwiesen. Aufgrund des beschränkten Rahmens der vorliegenden Arbeit werden die internationale Rechtshilfe in Strafsachen sowie das Übereinkommen über Cyberkriminalität (CCC) nur einzeln aufgegriffen.

C Methodik

Als Methodik der vorliegenden Arbeit liegen die Recherche von ausgewählter juristischer Literatur sowie die gewonnen Erkenntnisse aus drei halbstrukturierten Experteninterviews[6] und einem beantworteten Fragebogen zugrunde. Die gewählte Methodik hat sich einerseits angeboten, weil es sich bei den kriminellen Aktivitäten auf Verkaufsplattformen im Darknet um eine neuere Erscheinungsform handelt und deshalb die juristische Fachliteratur insb. mit Blick auf die Schweiz noch sehr spärlich vorhanden ist und andererseits, weil die zu klärenden Fragestellungen einen sehr praxisnahen Bezug aufweisen. Die Auswahl der Interviewpartner erfolgte mittels Anschreiben an alle sechs vom BAKOM anerkannten Stellen für die Bekämpfung der Cyberkriminalität aus der Deutschschweiz sowie an das Kompetenzzentrum Cybercrime der Kantonspolizei St. Gallen und der Polizei Basel-Landschaft.[7] Alle angefragten Stellen[8] gaben Rückmeldung, wobei die meisten mitteilten, dass sie u.a. wegen der zur Verfügung stehenden Ressourcen noch keine oder fast keine Erfahrungen zu Ermittlungen im Zusammenhang mit dem Darknet sammeln konnten. Die verantwortlichen Personen von drei Stellen, namentlich der Kriminalabteilung der Kantonspolizei Bern, der Fachbereich Cyberermittlung bei der Zuger Polizei sowie die Staatsanwaltschaft (StA) II in Zürich antworteten, dass sie bereits Ermittlungen im Darknet durchgeführt haben und stellten sich für ein persönliches Interview zur Verfügung.[9] Die Anfrage zur Beantwortung

[6] Als Grundlage für die Interviews diente ein Gesprächsleitfaden, der alle Fragen umfasste. Es gab sog. «Schlüsselfragen», die in jedem Interview und sog. «Eventualfragen», die je nach Gesprächsverlauf gestellt wurden. Durch diese Interviewform konnte sichergestellt werden, dass spezifische Aspekte angesprochen werden konnten und gleichzeitig das Ziel der Vergleichbarkeit der Interviewergebnisse gegeben war (Hochschule Luzern, Abschn.2).

[7] Vom BAKOM anerkannte Stellen gem. Art. 15 Abs. 3 VID sind: das Nationale Zentrum für Cybersicherheit (NCSC), Kantonspolizei Zürich Abteilung Cybercrime, Kantonspolizei Bern Kriminalabteilung, Bundesamt für Polizei fedpol, Zuger Polizei Fachbereich Cyberermittlung, Kantonspolizei Schwyz Fachbereich Cybercrime (BAKOM, Liste).

[8] Die beiden Stellen des Bundes verwiesen auf die Strafverfolgungsbehörden der Kantone. Die verantwortlichen Personen bei den Cybercrime Abteilungen der Kantone Schwyz, St. Gallen und Basel-Landschaft verwiesen wiederum auf Strafverfolgungsbehörden der grösseren Kantone Bern und Zürich.

[9] Siehe Anh. 1: Interview WERREN/ZAUGG, S. XXVII ff.; Anh. 2: Interview WALDER, S. XXXIX ff.; Anh. 3: Interview EUGSTER, S. LII ff.

eines Fragebogens an die StA Brugg-Zurzach[10] erfolgte zu einem späteren Zeitpunkt, da durch die Literaturrecherche zutage kam, dass eben genannte StA im Jahr 2017 erfolgreich im Darknet ermittelte und zwei Benutzerkonten von Darknet-Plattformen «beschlagnahmen» konnte.[11]

II. Definitionen und Grundlagen

Um die Thematik der strafprozessualen Zwangsmassnahmen im Zusammenhang mit Online-Verkaufsplattformen im Darknet zu einem späteren Zeitpunkt analysieren zu können, müssen vorliegend gewisse Definitionen sowie technische Funktionsweisen näher erklärt werden.

A Die verschiedenen Bereiche des Internets

1. Clearnet, Deep Web und Darknet

Das Internet ist, vereinfacht umschrieben, ein globales Netz von vielen heterogenen Computernetzwerken, auf dessen Infrastruktur verschiedene Dienste angeboten werden.[12] Das Internet kann grundsätzlich in die Bereiche: Clearnet, Deep Web und Darknet unterteilt werden.[13] Unter dem *Clearnet*[14] versteht man das Internet, welches mit den gängigen Browserprogrammen,[15] wie z.B. Microsoft Internet Explorer, Mozilla Firefox und Google Chrome aufgerufen werden kann,[16] und auf welchem man unter Verwendung von Standard-Suchmaschinen[17] die Suchergebnisse direkt aufrufen resp. indizieren kann.[18] Die Inhalte dieses Bereichs sind unverschlüsselt und umfassen bspw. Online-Shops und Nachrichten-Seiten. Diese Websites können anhand ihrer Domain (Internetadresse) mit den kennzeichnenden Endungen von Top-Level-Domains wie «.ch», «.com» oder «org.» erkannt werden.[19]

Das *Deep Web*[20] ist ebenfalls ein Teil des gewöhnlich genutzten Internets.[21] Im Unterschied zum Clearnet sind die im Deep Web gelagerten Daten jedoch wegen zweier Gründe nur mit grösserem Aufwand ersichtlich. Einerseits sind die Seiten nicht mit dem Suchmaschinen-Algorithmus verlinkt, d.h. sie werden bei einer Suchanfrage mit einer üblichen Suchmaschine nicht als Ergebnis erscheinen.[22] Andererseits sind die Inhalte im Deep Web vielfach in geschützten Bereichen und in eigenen Netzwerken abgelegt sowie durch Zugangsbeschränkungen wie Bezahlung oder Passwörter geschützt.[23] Zu den Inhalten des Deep Webs werden u.a. Datenbanken, Online Speicher sowie Foren und Internetseiten von Social Media gezählt, welche eine Registration und Anmeldung erfordern.[24] Das *Darknet*[25] gilt wiederum als spezieller Teil des Deep Webs.[26] Aufgrund zweier bedeutender Unterschiede müssen das Deep Web und

---

[10] Siehe Anh. 4: Fragebogen WALDMEIER, S. LVII ff.
[11] Vgl. Kantonspolizei Aargau, Abschn. 5.
[12] Gabler Wirtschaftslexikon, Internet.
[13] SUI/CAVERLEE/RUDESILL, 6; GAYARD, 9 f.; NAJJAR/SCHWASS, 4; BSI, Abschn. 1.
[14] Die Begrifflichkeiten sind uneinheitlich. Das Clearnet wird teilweise auch als Surface Web oder Visible Web bezeichnet (NAJJAR/SCHWASS, 4).
[15] Der Browser bezeichnet ein Programm, welches http unterstützt und mit dem die grafischen Inhalte des WWW dargestellt werden können (Gabler Wirtschaftslexikon, Browser).
[16] VOGT, 4.
[17] Als Standard-Suchmaschinen gelten bspw. Google, bing, Yahoo.
[18] MEY, Tor, 4; GAYARD, 10.
[19] NAJJAR/SCHWASS, 4.
[20] Die Begrifflichkeiten sind uneinheitlich. Das Deep Web wird zum Teil auch Hidden Web oder Invisible Web genannt (NAJJAR/SCHWASS, 4; VOGT, 4; SUI/CAVERLEE/RUDESILL, 6).
[21] NAJJAR/SCHWASS, 4.
[22] VOGT, 4; SUI/CAVERLEE/RUDESILL, 6.
[23] MEY, Tor, 4; VOGT, 4.
[24] RÜCKERT, 13.
[25] Die Begrifflichkeiten sind uneinheitlich. Das Darknet wird zum Teil auch als Dark Web, Dark Net oder Dark Internet bezeichnet (SUI/CAVERLEE/RUDESILL, 6).
[26] IHWAS, 138.

das Darknet jedoch klar voneinander abgegrenzt werden.[27] Zum einen wird das Surfen im Deep Web im Normalfall nicht anonymisiert, wie dies aufgrund der angewendeten Verschlüsselungstechnologien im Darknet der Fall ist. Zum anderen kann das Deep Web mit Hilfe von Standard-Browsern erreicht werden, wogegen für das Aufrufen des Darknets spezifische Browser erforderlich sind (vgl. Kap. II. A 3.).[28]

2. Die technische Funktionsweise des Internets

Um die technische Funktionsweise des Darknets zu verstehen, wird vorliegend zuerst in stark vereinfachten Ausführungen die Funktionsweise des Internets (resp. Clearnet) erläutert. Damit Computer im Internet miteinander kommunizieren können, benötigen sie einen gemeinsamen Standard, eine Sprache zum Datenaustausch. Im Zusammenhang mit dem World Wide Web (WWW[29]) ist dies meistens das Hypertext Transfer Protocol (http). Zudem brauchen Computer eine einheitliche Programmiersprache, die Hypertext Markup Language (HTML) sowie eine standardisierte Benutzeroberfläche, den Browser. Damit eine Information überhaupt an ihr Ziel gesendet werden kann, muss sie mit einer Adresse, einer sog. Internet Protocol Adresse (kurz: IP-Adresse), versehen sein.[30] Jedes Endsystem, welches mit dem Internet verbunden ist (z.B. Laptops, Server oder mobile Geräte) und jedes Zwischensystem im Internet (z.B. Router) verfügt somit über eine IP-Adresse (z.B. 192.168.0.1.[31]), die als Absender- oder Empfängeradresse in der Kommunikation zwischen den Geräten als eindeutige Identifikation verwendet wird.[32] Bestimmte Websites, die immer unter derselben Internetadresse aufrufbar sein sollen sowie Server oder Netzwerk-Drucker haben in der Regel eine statische IP-Adresse.[33] Statische IP-Adressen werden einmal vergeben und anschliessend nicht mehr geändert.[34] Da es momentan noch keine ausreichende Anzahl IP-Adressen gibt,[35] damit alle Internetnutzer eine statische Adresse haben können, werden die bestehenden IP-Adressen dynamisch den einzelnen Nutzern neu zugeordnet.[36] Dynamische IP-Adressen kommen v.a. bei privaten Anwendern zum Einsatz, welche mit Hilfe eines Internet Access Providers[37] den Zugang zum Internet erhalten. Dabei verbindet sich der Computer des Anwenders per Telefonkabel, Glasfaserleitung oder drahtlos (via WLAN) mit dem Provider, der ihm dann vorübergehend eine seiner IP-Adressen überlässt.[38]

Da jede Information, die im Internet versendet wird, sowohl die IP-Adressen des Absenders und des Empfängers umfasst, kann der Urheber dieser Information wie folgt ermittelt werden. Wenn der Absender eine statische IP-Adresse besitzt, erfolgt eine direkte Identifizierung. Handelt es sich hingegen um eine dynamische IP-Adresse, so kann der Provider prüfen, welchem Kunden er seine IP-Adresse zum entsprechenden Zeitpunkt zur Verfügung gestellt hatte.[39] Ruft man im Internet eine Website, wie z.B.

---

[27] NAJJAR/SCHWASS, 4; IHWAS, 139.
[28] Zum Ganzen RÜCKERT, 13; IHWAS, 139.
[29] Das World Wide Web ist ein Interaktives Informationssystem, das den globalen Austausch von digitalen Dokumenten ermöglicht und aus Hypertext-Systemen besteht. Dieses wird auch als Website bezeichnet. Eine Website setzt sich normalerweise aus mehreren zusammenhängenden Webdokumenten zusammen. Für den Zugriff auf die Dokumente ist ein Browser notwendig (Gabler Wirtschaftslexikon, WWW).
[30] Zum Ganzen HANSJAKOB, Überwachungsrecht, N 189 f.
[31] Diese IP-Adressen werden aktuell im IPv4-Format dargestellt und setzen sich aus vier durch Punkte abgetrennte Zahlenblöcke zusammen (HEROLD/LURZ/WOHLRAB, 454; Gabler Wirtschaftslexikon, IP-Adresse).
[32] THOUVENIN ET AL, 704.
[33] AWUKU, Abschn. 4.
[34] HEROLD/LURZ/WOHLRAB, 454.
[35] Da auf absehbare Zeit zu erkennen war, dass es im aktuellen IPv4-Format zu wenig Adresskombinationen gibt, wurde der neue Standard IPv6 definiert. Die Umstellung auf diese neue 128 Bit (statt 32 Bit) lange Adresse ist jedoch immer noch nicht abgeschlossen (HEROLD/LURZ/WOHLRAB, 454; Gabler Wirtschaftslexikon, IP-Adresse).
[36] BGE 136 II 508 E. 3.3 S. 514 f.; MUGGLI, Diss., 8 f;
[37] Wird auch als Internetzugangsanbieterin oder Provider bezeichnet.
[38] MUGGLI, Diss., 8 f.
[39] Zum Ganzen HANSJAKOB, Überwachungsrecht, N 194 f.

www.facebook.com, auf, so sieht einerseits der Provider, welche Website vom Nutzer besucht wurde. Andererseits sieht Facebook, mit welcher IP-Adresse ihre Website aufgerufen wurde und kann so den Nutzer identifizieren.[40] Die Geheimhaltung von illegalen Aktivitäten wird dadurch im Internet praktisch verunmöglicht.[41]

3. Die technische Funktionsweise des Darknets am Beispiel des Tor Browsers

Für den Begriff des «Darknets» gibt es bis anhin keine einheitliche Definition. In der medialen Diskussion wird das Darknet häufig in einem negativen Kontext dargestellt, weil es vielfach als ein Ort für illegale Tätigkeiten bezeichnet wird.[42] Allgemein wird das Darknet oft als Synonym für die bedeutendste und am meisten verbreitetste Darknet-Software dem sog. «Tor Browser» verstanden.[43] Zudem gibt es aber noch diverse weitere frei erhältliche Software-Programme und dazugehörige Darknets,[44] wie das Invisible Internet Project (I2P), The Freenet oder Retroshare.[45] Diese Programme ermöglichen eine anonyme Kommunikation und anonymes Surfen.[46] Wie dies beim Tor Browser funktioniert, wird nachfolgend erklärt.

«Tor» war anfänglich ein Akronym für «The Onion Routing».[47] Die Entwickler dieser Technologie verglichen den Aufbau ihrer Erfindung mit einer Zwiebel. Bei dieser ist der «Kern» unter zahlreichen Schalen verborgen, während bei Tor eben die Identität und Aktivität der einzelnen Internetnutzer unter mehreren Anonymisierungsschichten versteckt ist.[48] Der Tor Browser kann öffentlich verfügbar im Clearnet heruntergeladen und auf dem Endgerät des Nutzers installiert werden.[49] Er gewährt seinen Nutzern zwei Funktionen: Einerseits verbirgt seine Anonymisierungstechnologie die IP-Adressen seiner Nutzer und ermöglicht dadurch anonymes Surfen auch im Clearnet. Andererseits ermöglicht der Browser den Zugriff auf das Tor-basierte Darknet, welches mit anderen gewöhnlichen Browsern nicht aufgerufen werden kann.[50] Um das Surfen und die Kommunikation zu anonymisieren, umfasst Tor ein globales Netzwerk von ca. 7'000 ehrenamtlichen Nutzern,[51] die ihren Computer als sog. Tor Nodes zur Verfügung stellen.[52] Wenn nun ein Tor-Nutzer eine Website (z.B. Facebook) aufruft, wird keine direkte Verbindung zu dieser Website aufgebaut, sondern nach dem Zufallsprinzip eine Verbindung über drei dieser Tor Nodes hergestellt.[53] Damit keiner dieser Tor Nodes den ganzen Weg der Daten nachvollziehen kann, werden die versendeten Daten (mindestens) dreifach verschlüsselt. Dabei erhält jeder mitwirkende Tor Node vom Browser nur den Schlüssel für eine einzige Schicht. Entschlüsselt der erste Node, der sog. Entry Node, die erste Verschlüsselungsschicht, so bekommt er lediglich die Information an welchen Middle Node er die Daten weiterschicken muss. Dieser vermag wiederum die zweite Schicht zu entschlüsseln und erfährt hierdurch an welchen dritten Node, den sog. Exit Node, die Daten weiterzugeben sind. Der Exit Node entfernt mithilfe seines Schlüssels die letzte Schicht und stellt eine Verbindung zum

[40] IHWAS, 138.
[41] MUGGLI, Diss., 9.
[42] HOSTETTLER, Darknet, 7.
[43] IHWAS, 139.
[44] Es ist wichtig zu erwähnen, dass es nicht nur «das Darknet», sondern mehrere Darknets gibt (GAYARD, 10; MEY, Tor, 4.)
[45] Abruf der Darknets unter: https://geti2p.net/de/about/intro; https://freenetproject.org/; https://retroshare.cc/.
[46] IHWAS, 139; HOSTETTLER, Darknet, 19.
[47] Tor Project, About History, Abschn. 5; VOGT, 5; HENKEL, 176.
[48] MEY, Tor, 5; HENKEL, 177.
[49] IHWAS, 139; Adresse für den Download: https://www.torproject.org/de/download/
[50] Zum Ganzen MOORE/RID, 15 f.; MEY, Tor, 5; RÜCKERT, 14 f.
[51] Tor Project, Server, Grafik; TZANETAKIS, 41.
[52] Die Begrifflichkeiten sind uneinheitlich. Die Tor Nodes (deutsch: Tor-Knoten) werden auch Tor Router oder Onion-Router genannt (WOHLFEIL, 14).
[53] WOHLFEIL, 14 f.

ursprünglich gesuchten Dienstanbieter, resp. zum Server der Website her.[54] In diesem System kennt somit jeder Tor Node nur die IP-Adresse des vorangehenden Nodes.[55] Der Entry Node verfügt zwar über Kenntnisse über den Absender, er weiss aber nichts über den Inhalt oder den Endempfänger. Der Exit Node kennt hingegen den Inhalt und den Endempfänger, er weiss aber nicht, wer die Nachricht anfänglich versendet hat.[56] Der Einzige, der auf seinem Computer alle durchlaufenen Nodes und deren IP-Adressen einsehen kann, ist der Tor-Nutzer.[57] Um den Weg der Daten zu rekonstruieren, müsste man alle drei Tor Nodes kontrollieren können. Damit genau eine solche Kontrolle verhindert werden kann, wechselt der Tor Browser in regelmässigen Zeitintervallen von ca. 10 Minuten die genutzten Tor Nodes.[58]

Die eben erklärte dezentrale Struktur des Verbindungsaufbaus ermöglicht, dass der Access Provider des Internetnutzers nicht nachvollziehen kann, welche Adresse er aufgerufen hat. Zugleich kann aber auch der Dienstanbieter (im verwendeten Beispiel: Facebook) nicht erkennen, von wo der Zugriff auf seine Website erfolgt. Er kennt einzig die IP-Adresse des Exit Nodes.[59] Die Mehrheit der Tor-Nutzer verwenden die Software i.S. der eben gemachten Ausführungen, um damit sicherer und anonym im Internet zu surfen. Verhältnismässig wenige Tor-Nutzer nutzen den Browser in seiner zweiten Funktion und rufen damit das Tor-basierte Darknet auf,[60] wo sich die Websites mit der Domain «.onion», die sog. «Hidden Services» befinden.[61] Diese .onion-Adressen werden durch Zufall von der Tor-Software berechnet und setzen sich aus einer Folge von 16 Zeichen, wie bspw. expyuzz4wqqyqhjn.onion zusammen.[62] Mithilfe dieser .onion-Adressen werden verschlüsselte Verbindungen zu einem neutralen Tor Node aufgebaut, über den die Kommunikation zwischen dem Nutzer und Dienstanbieter abgewickelt wird. Die .onion-Adresse gewährleistet, dass nicht nur die IP-Adressen und damit die Identität der Tor-Nutzer, sondern auch die Identität der Dienstanbieter verschleiert wird.[63] Damit die Nutzer auf solche Websites gelangen, müssen sie zwingend deren .onion-Adresse kennen.[64] Da diese Adressen so kompliziert und die Suchfunktionen im Darknet beschränkt sind, helfen Verzeichnisse wie das Hidden Wiki oder das Undernet Directory bei der Suche nach der gewünschten .onion-Adresse.[65]

B Die Bedeutung und Nutzung des Tor-basierten Darknets

1. Geschichte des Tor Projects

Die Idee des Tor Project entstand Mitte der 1990er Jahre aufgrund der Befürchtung, dass die Sicherheit des Internets mangelhaft war, und dieses zur Verfolgung und Überwachung genutzt wird. Drei Forscher des U.S. Naval Research Laboratory entwickelten im Jahre 1995 den Prototypen von Tor, welcher in den darauffolgenden Jahren laufend verbessert wurde.[66] Anfangs wurde Tor v.a. unter Aktivisten und technisch versierten Nutzern, die an Privatsphäre interessiert waren, eingesetzt. Mit der Entwicklung

[54] Zum Ganzen WOHLFEIL, 14 f; RÜCKERT, 14 f.
[55] IHWAS, 139.
[56] IHWAS, 139; WOHLFEIL, 14 f.; RÜCKERT/SAFFERLING, 3.
[57] RÜCKERT/SAFFERLING, 3.
[58] RÜCKERT, 15.
[59] Zum Ganzen IHWAS, 139; RÜCKERT/SAFFERLING, 3.
[60] MOORE/RID, 16; Gemäss eigenen statistischen Erhebungen aus dem Jahr 2015 schätzt Tor Project, dass das Aufrufen der versteckten Websites nur etwa 3-6% des gesamten Datentransfers im Tor Browser ausmacht (Tor Project, statistics, Abschn. 3).
[61] MEY, Tor, 5.
[62] MEY, Tor, 5.
[63] Zum Ganzen RÜCKERT, 15 f.
[64] MOORE/RID, 18; RÜCKERT, 16; MEY, Tor, 5.
[65] RÜCKERT, 16; IHWAS, 141; MEY, Tor, 7.
[66] Tor Project, About History, Abschn. 3.

des heutigen Tor Browsers im Jahre 2008 wurde Tor aber auch für alltägliche Internetnutzer zugänglicher gemacht. Dies erklärt auch, weshalb Tor bspw. während des Arabischen Frühlings ab Ende 2010 zu einem wichtigen Instrument wurde. Tor konnte einerseits die Online-Identität der Personen schützen und ermöglichte ihnen andererseits den Zugriff auf kritische Ressourcen, Social Media und Websites,[67] die für sie blockiert waren.[68] Dank der Enthüllungen von Edward Snowden[69] über die Massenüberwachung des weltweiten Internetverkehrs durch die National Security Agency (NSA) der USA im Jahre 2013 hat sich die Anzahl Internetnutzer, welche mit dem Tor Browser surfen, im Vergleich zum Jahr 2012 verdoppelt.[70] Laut aktuellen Schätzungen des Tor Projects wird der Tor Browser täglich von ca. 2 bis 2.5 Mio. Nutzern aufgerufen.[71] Neben dem Militär, den Strafverfolgungsbehörden und Journalisten wird der Browser v.a. auch von Leuten verwendet, welche in Ländern mit eingeschränktem Internetzugang, in autokratischen Staaten, Diktaturen oder Kriegsgebieten leben und damit die staatliche Überwachung und Zensur umgehen können.[72]

2. Das Tor-basierte Darknet als digitale Handelsplattform für Kriminelle

Die Tor-Technologie bietet jedoch auch ein beachtliches Missbrauchspotenzial. Die dadurch erzielte Anonymität ist v.a. für Kriminelle sehr attraktiv und führt zur Etablierung einer kontinuierlich grösser werdenden Schattenwirtschaft im Darknet, in der praktisch alle illegalen Güter gehandelt werden.[73] Für die Strafbehörden sind dabei insb. der Verkauf von Drogen, Betäubungsmitteln, Waffen, illegaler Pornografie sowie das Angebot von Cybercrime-Dienstleistungen[74] und rechtswidrig erworbenen Datensätzen von grosser Bedeutung.[75] Im Zuge der Corona-Pandemie wird das Darknet aber auch zum beliebten Handelsplatz für gefälschte Impfpässe, negative Corona-Tests oder sogar gefälschte oder angeblich echte Impfstoffe.[76]

Die Infrastruktur für den Handel im Darknet unterteilt sich dabei, vereinfacht gesagt, in zwei Geschäftsmodelle: Foren und Darknet-Marktplätze (sog. Verkaufsplattformen[77]). Die Betreiber der Foren[78] stellen ihren Nutzern einen «Treffpunkt» sowie eine Kommunikationsinfrastruktur zur Verfügung, um Themen wie Meinungsfreiheit oder IT-Sicherheit zu diskutieren, aber auch um strafrechtlich relevante Geschäfte anzubahnen und auszuhandeln.[79] Im Fokus der vorliegenden Arbeit stehen jedoch die strafrechtlich relevanteren Verkaufsplattformen. Diese zeichnen sich durch zwei essenzielle Merkmale aus: Einerseits werden die als Hidden Services ausgestalteten Onion-Websites dieser Verkaufsplattformen im Darknet

[67] Social Media wie Facebook, aber auch international bekannte Nachrichtendienste und Medienunternehmen wie «The New York Times» oder «BBC» verfügen über eine .onion-Adresse, welche im Tor-basierten Darknet aufgerufen werden kann (SIEGLE, BBC im Darknet, Abschn. 1; MEY, Tor, 6 f.).
[68] Zum Ganzen Tor Project, About History, Abschn. 9 f.
[69] Edward Snowden ist ein US-amerikanischer Whistleblower und früherer NSA-Mitarbeiter. Mit seinen Enthüllungen im Sommer 2013 wurde das Ausmass der weltweiten Überwachungs- und Spionagepraktiken v.a. der NSA bekannt (BEUTH, Abschn. 2).
[70] HOSTETTLER, Darknet, 31.
[71] Die Aussage bezieht sich auf Zahlen von März 2021 bis Mai 2021 (Tor Project, Users).
[72] HOSTETTLER, Darknet, 32 f.; SIEGLE, BBC im Darknet, Abschn. 2 f; RÜCKERT, 17.
[73] RÜCKERT, 17.
[74] Cybercrime-Dienstleistungen werden auch als crime-as-a-service bezeichnet. Dabei werden Dienstleistungen zur Verfügung gestellt, welche die Durchführung von Cybercrime verwirklichen oder erleichtern. Zu diesen Dienstleistungen gehören bspw. Updates für Schadsoftware, Anti-Erkennungsmechanismen sowie die Hilfeleistungen bei technischen Problemen (VOGT, 5).
[75] Detaillierte Erklärungen zu einzelnen Straftatbeständen finden sich in Kap. II. C 1.
[76] Check Point, Abschn. 3 f; Europol, Covid-19, Abschn. 1.
[77] Einfachheitshalber wird in der gesamten Arbeit nur noch von Verkaufsplattformen oder Plattformen gesprochen.
[78] z.B. OnionLand und The Hub.
[79] Zum Ganzen RÜCKERT/SAFFERLING, 4.

über den Tor Browser aufgerufen, und andererseits dienen dort nicht Kreditkarten oder Banküberweisungen sondern virtuelle Kryptowährungen als Zahlungsmittel.[80] Kryptowährungen wie Bitcoin, sind deshalb besonders geeignet, weil sie eine Zahlungsabwicklung jenseits der regulierten Finanzmarktinfrastrukturen ermöglichen.[81] Anstelle der klassischen Bankkonten tritt bei Bitcoin ein kryptografisches Schlüsselpaar: Wobei jedem Nutzer ein Private Key, ein nur ihm bekannter Code zur Freigabe von Transaktionen, und ein Public Key, eine Art öffentliche Kontonummer, zugeordnet wird. Die Verwaltung der Schlüssel erfolgt im sog. Wallet.[82]

Die Kombination der Tor- und Krypto-Technologie gewährleistet den Nutzern dieser Online-Verkaufsplattformen eine nahezu vollständige Anonymität zur Abwicklung ihrer Geschäfte.[83] Diese Plattformen werden jeweils von Administratoren, die über den vollständigen Systemzugriff verfügen, programmiert und hoch professionell betrieben.[84] Die Administratoren finanzieren sich häufig einerseits mit den Anmeldegebühren der Verkäufer, die im Schnitt zwischen 100 und 250 CHF betragen, sowie einer Provision für jeden über die Plattform abgewickelten Verkauf.[85] Die Plattformen gleichen in ihrem Design und Aufbau den konventionellen Plattformen im Clearnet, wie Ebay und Amazon.[86] Die angebotenen Waren und Dienstleistungen sind nach Kategorien übersichtlich sortiert und mit Bildern, Beschreibungen und Preisangaben versehen.[87] Als Käufer muss man sich im Darknet bewusst sein, dass ein grosser Teil der angebotenen Waren von sog. Scammern[88] stammt. Scammer sind Betrüger, welche zwar Waren anbieten, diese nach Eingang der Bezahlung aber nicht liefern können oder wollen.[89] Um diese Problematik zu entschärfen, verfügen viele Plattformen über Foren, in denen über unseriöse Verkäufer, die ihre Waren nicht liefern, berichtet und vor Käufern, die nicht bezahlen, gewarnt wird.[90] Ferner verfügen sie über Bewertungssysteme der Verkäufer, Betrugserkennungssysteme, Messaging-Dienste und Treuhandservices zur Zahlungsabwicklung.[91]

Im Jahr 2013 konnte das FBI den Betreiber der wohl bekanntesten Verkaufsplattform, Silk Road, ausfindig machen und deren Website sowie sämtliche Bitcoins beschlagnahmen.[92] Ironischerweise stieg die Popularität der Darknet-Verkaufsplattformen auch aufgrund der grossen Medienpräsenz bezüglich der Schliessung von Silk Road stark an.[93] Trotz verschiedener weiterer Ermittlungserfolge in den letzten Jahren, florieren die Darknet-Plattformen.[94] Wie eine grossangelegte Studie des European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) und der European Union's law enforcement agency (Europol) zeigt, blieben die beobachteten Darknet-Verkaufsplattformen durchschnittlich nur für ca. acht Monate aktiv.[95] Als Gründe für die Marktschliessungen gelten Polizeizugriffe, Exit Scams, freiwillige

[80] TZANETAKIS, 41.
[81] RÜCKERT/SAFFERLING, 4.
[82] HESS/LIENHARD, N 4 und 9.
[83] RÜCKERT/SAFFERLING, 6.
[84] RÜCKERT/SAFFERLING, 5.
[85] Gemäss HOSTETTLER beträgt die Gebühr pro verkauftes Produkt 5% (HOSTETTLER, Darknet, 75).
[86] RÜCKERT, 17; RÜCKERT/SAFFERLING, 5.
[87] RÜCKERT/SAFFERLING, 5; HENKEL, 181.
[88] Dieses Phänomen wird auch als Exit Scam bezeichnet. Es ist eine Art von Betrug, bei dem ein Betreiber einer Darknet-Verkaufsplattform oder ein einzelner Verkäufer, mit guten Bewertungen im laufenden Geschäftsbetrieb Vorauszahlungen für bestellte Waren oder Dienstleistungen annimmt ohne die vereinbarte Gegenleistung zu erfüllen und nach einer bestimmten Zeit mit den Geldern vom Markt verschwindet (EMCDDA/Europol, 78; CHRISTIAN, Abschn. 4 ff.).
[89] Anh. 1: Interview WERREN/ZAUGG, Frage 1.6; WILSON, Abschn. 2.
[90] HOSTETTLER, Darknet, 75.
[91] RÜCKERT/SAFFERLING, 5.
[92] DoJ, U.S. Attorney's Office, Abschn. 16.
[93] BALL/BROADHURST/NIVEN/TRIVEDI, 4.
[94] RIEKKINEN, N 2.
[95] In der Studie wurden 103 Plattformen untersucht (EMCDDA/Europol, 18 f.).

Schliessungen und Hacks.[96] Die Anzahl der aktuell aktiven Verkaufsplattformen ist nicht genau bekannt.[97] Websites, wie DarknetStats.com, welche auch über das Clearnet zugänglich sind, informieren jedoch über aktive Verkaufsplattformen.[98]

C Strafrechtliche Erfassung der Tätigkeiten auf Online-Verkaufsplattformen und bedeutende Ermittlungserfolge in der Schweiz

Eine Beurteilung der Inhalte des Darknets nach deren Rechtmässigkeit ist schwierig, da diese einerseits vom jeweiligen Rechtssystem abhängig sind und sie andererseits häufig in rechtlichen Grauzonen liegen.[99] Wissenschaftliche Studien gehen von einer Zweiteilung des Darknets in einen klar illegalen und einen grundsätzlich legalen Bereich aus.[100] In ihrer Studie aus dem Jahr 2016 ordneten RID und MOORE vom britischen King's College 57 Prozent aller konsultierten Onion-Websites einer illegalen Nutzungsweise zu, wobei der Handel mit Drogen, Kreditkarten- und Kontodaten, gestohlenen Pässen oder illegaler Pornografie sowie Geldwäscherei am häufigsten und Waffenhandel eher selten vorkam.[101] Eine weitere Studie aus dem Jahr 2018 von Forschern der ETH, der Universitäten Edinburgh und Athen zeigt ein ähnliches Bild. 56 Prozent der Inhalte von Onion-Websites wurden als illegal eingestuft.[102]

1. Straftatbestände aus dem StGB und Nebenstrafrecht

Da die Bedeutung einer Straftat und der hinreichende Tatverdacht im Zusammenhang mit der Rechtfertigung zur Anwendung von strafprozessualen Zwangsmassnahmen von grosser Wichtigkeit ist,[103] werden nachfolgend einige Straftatbestände des StGBs und der Nebengesetze überblicksmässig und nur in Bezug auf die Handelstätigkeiten im Darknet erläutert. Die Auswahl der Straftatbestände erfolgt aufgrund der in den Interviews durch die Autorin gewonnen Erkenntnisse auf die Frage, bei welchen Straftaten die befragten Strafbehörden am häufigsten ermittelten.[104]

Da diese Straftatbestände mit Cybercrimes in Verbindung gebracht werden, soll diese Begrifflichkeit zuerst kurz erläutert werden. Cybercrime oder auch Internetkriminalität sind keine strafrechtlichen Begriffe.[105] Unter Cybercrime werden allgemein strafbare Handlungen verstanden, die im Zusammenhang mit dem Internet oder vernetzten Computersystemen verübt werden.[106] In der strafrechtlichen Literatur werden dabei häufig zwei Deliktsformen differenziert: Bei der einen Form fungiert der Computer als Tatmittel zur Ausübung eines «herkömmlichen», analogen Delikts (Cybercrime im weiteren Sinne[107]). Bei der anderen Deliktsform bieten die Computersysteme selbst eine Angriffsfläche für Delikte, indem

[96] EMCDDA/Europol, 18 f.; MEY, Banalität des Darknet Commerce, Abschn. 1.
[97] HOSTETTLER, Darknet, 119.
[98] Darknetstats.com listet aktuell 13 aktive Darknet-Handelsplattformen auf. Die Website informiert zusätzlich aber auch über Verhaftungen von Verkaufsplattform-Teilnehmer (vgl. darknetstats.com).
[99] AVARIKIOTI ET. AL, 16.
[100] MEY, Darknet, N 64.
[101] RID und MOORE haben in ihrer Studie 2'723 Onion-Websites ausgewertet, wobei 15.5% unter die Kategorie Drogen, 4.5 % unter illegale Pornografie und nur 1.5% unter die Kategorie der Waffen fallen (RID/MOORE, 20 f.).
[102] Die Studie basiert auf einer Analyse von 7'566 Hidden Services, die nutzbare Inhalte angezeigt haben und 7.3 Mio. Pfaden (AVARIKIOTI ET AL., 7 f. und 19).
[103] Art. 197 Abs. 1 lit. b und d StPO.
[104] Anh. 1: Interview WERREN/ZAUGG, Frage 1.4 und 1.6; Anh. 2: Interview WALDER, Frage 1.3 und 1.4; Anh. 3: Interview EUGSTER, Frage 1.4.
[105] SCHWARZENEGGER, 409.
[106] BRICH/HASENBALG, 33; SCHWARZENEGGER, 409.
[107] MEIER, Folie 3; HORTEN/GRÄBER, 234, unterscheiden ebenfalls in Cybercrime i.e.S. von Cybercrime i.w.S.; anders SCHWARZENEGGER, 409 ff., der hingegen die Terminologie der netzwerkunterstützen und -fokussierten Deliktsformen verwendet.

bspw. zur Übermittlung stehende oder abgespeicherte Daten beeinträchtigt werden (Cybercrime im engeren Sinne).[108] Gemäss der Einteilung von GYARMATI können sämtliche Straftaten im Zusammenhang mit Darknet-Verkaufsplattformen, sogar das Anbieten von Ransomware oder DDos-Attacken, unter Cybercrime i.w.S. zusammengefasst werden.[109]

Der Handel über Darknet-Plattformen mit sog. Crime-as-a-service wie Ransomware oder Malware können allenfalls unter die Straftatbestände der unbefugten Datenbeschaffung (Art. 143 StGB), dem unbefugten Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB) oder der Datenbeschädigung (Art. 144bis StGB) fallen.[110] Der Handel, resp. die Verbreitung[111] von verbotener Pornografie, welche sexuelle Handlungen mit Kindern, mit Tieren und/oder Gewalttätigkeiten zum Inhalt hat, wird in Art. 197 Abs. 4 und 5 StGB erfasst und mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe sanktioniert. Personen, die vorsätzlich ohne Berechtigung Waffen, wesentliche Bestandteile davon, Waffenzubehör oder Munition anbieten, übertragen, vermitteln und erwerben, machen sich allenfalls gem. Art. 33 Abs. 1 lit. a WG strafbar, wobei ihnen eine Freiheitsstrafe bis zu drei Jahren oder Geldstrafe droht. Der qualifizierte Tatbestand der Gewerbsmässigkeit sieht gar eine Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe vor.[112] Unbefugte Handlungen, vom Anbau über den Verkauf bis zum Konsum von Betäubungsmitteln, können unter den Art. 19 Abs. 1 BetmG fallen und zu einer Freiheitsstrafe bis zu drei Jahren oder Geldstrafe führen. Beim qualifizierten Tatbestand der Gewerbsmässigkeit darf die Freiheitsstrafe nicht unter einem Jahr betragen.[113]

2. Ausgewählte bedeutende Ermittlungserfolge im Darknet in der Schweiz

Als wohl berühmtester Fall gilt derjenige von Tobias Kuster, der sich nach der Tötung eines Unbeteiligten im Zürcher Seefeld im Jahr 2016 über ein halbes Jahr den Strafbehörden entziehen konnte. Anfangs 2017 konnte Kuster inhaftiert werden, als er im Darknet versuchte, illegal eine Waffe zu erwerben und am vermeintlichen Übergabeort am Bahnhof Burgdorf auf einen verdeckten Ermittler der Berner Strafverfolgungsbehörde traf. Der entscheidende Hinweis für dieses Geschäft kam dabei von einem verdeckten Ermittler der australischen Bundespolizei, der ein Scheinangebot für eine Waffe auf einer Darknet-Verkaufsplattform platziert hatte, worauf sich Kuster meldete. Diese Information ging dann wiederum via Europol zu den Schweizer Behörden und schlussendlich zur Kriminalpolizei Bern, wo ein verdeckter Ermittler mit dem Waffeninteressenten via Darknet in Kontakt trat und diesen zu einem Treffen bewegte. Erst nach diesem Treffen und einem Abgleich der Fingerabdrücke wurde bekannt, dass es sich um den gesuchten Gewaltstraftäter handelte.[114]

Auch im Fall eines pädophilen Kindertagesstätten-Betreuers in St. Gallen begannen die Ermittlungen ursprünglich bei der Kriminalpolizei Bern und wurden anschliessend an die St. Galler Strafbehörden weitergegeben.[115] Der Betreuer wurde im Jahr 2018 verhaftet, weil er verdächtigt wurde im Darknet kinderpornografisches Material verbreitet zu haben.[116] Im Zuge der Ermittlungen konnte u.a. festgestellt werden, dass der Beschuldigte sexuelle Handlungen an insgesamt drei Jungen unter sechs Jahren im

[108] Zum Ganzen SCHWARZENEGGER, 409 f.; Vgl. auch BIEMANN, 46 f.
[109] GYARMATI, 87 f.
[110] GERMANN/WICKI-BIRCHLER, 88 f.
[111] Verboten sind auch das Anfertigen, Erstellen, Verbreiten, Besitzen und das Konsumieren solcher Aufnahmen.
[112] Art. 33 Abs. 3 lit. a WG.
[113] Art. 19 Abs. 2 und Art. 20 Abs. 2 BetmG.
[114] Zum Ganzen BAUMGARTNER, Abschn. 1.; Anh. 1: Interview WERREN/ZAUGG, Frage 1.4 und 1.5; weitere Hinweise zur Anklage von Tobias Kuster in SCHOOP/BAUMGARTNER, Abschn. 1 ff.
[115] Anh. 1: Interview WERREN/ZAUGG, Frage 1.4 und 1.5.
[116] SRF, Abschn. 1.

privaten und beruflichen Umfeld vornahm, sich dabei filmte und die Videos im Darknet in Pädophilen-Foren stellte.[117]

Weitaus häufiger als Berichterstattungen über potenzielle Waffenkäufer oder Pädophile auf Darknet-Plattformen sind solche über Straftaten im Zusammenhang mit Betäubungsmitteldelikten. Dazu zählt bspw. die Verhaftung von drei Drogenhändlern im Jahr 2017 durch die Aargauer Strafbehörden, welche über Darknet-Verkaufsplattformen Drogen wie Amphetamin, Marihuana, Ecstasy, Kokain und LSD verkauft und anschliessend per Post an ihre Kunden versendet hatten.[118] Dabei gelang den Strafbehörden der Zugriff auf die Benutzerkonten dieser Drogenhändler und die anschliessende Beschlagnahme. Die Drogenhändler hatten Waren auf der Plattform Dream Market unter den Profilen «DrFeelWell» und «DerErsteAffe» angeboten und anschliessend per Post an ihre Käufer gesendet.[119] In einem sehr ähnlich gelagerten Fall, auf den sich auch die beiden einleitend und im zweiten Teil dieser Arbeit erwähnten Bundesgerichtsentscheide beziehen, gelang es den Zürcher Strafbehörden, im Jahr 2018 durch Fahndungsmassnahmen fünf Personen festzunehmen, die über ihre Benutzerkonten u.a. ebenfalls auf Dream Market in grossem Stil Drogen verkauften.[120] Wie im Falle der Aargauer Strafbehörden konnten auch die Zürcher die Benutzerkonten sperren, wobei es sich beim Konto von «Swiss Flakes» um das damals umsatzstärkste Verkaufsprofil des Schweizer Drogenhandels im Darknet handelte. Aber auch die weiteren gesperrten Konten von «Happy Olaf» und «CH-Koks» gehörten zu den Top-10-Shops.[121] Ein Jahr zuvor konnten die Luzerner Behörden in Zusammenarbeit mit der deutschen Polizei einen 34-jährigen Luzerner verhaften, der einerseits im Darknet grosse Mengen an Kokain und Amphetamin kaufte und andererseits selber Marihuana anbaute. Die aus dem Darknet gekauften Drogen liess er sich an Paketshops in Deutschland liefern und von dort aus in die Schweiz transportieren, wo er die Drogen weiterverkaufte, indem er diese in DVD-Hüllen verpackte und innerhalb der Schweiz versendete. Insgesamt soll er im Zeitraum von zwei Jahren rund 800 Drogendeals über das Darknet abgeschlossen haben.[122]

III. Herausforderungen bei der Strafverfolgung im Darknet

In den nachfolgenden Ausführungen werden die Herausforderungen im Zusammenhang mit der Strafverfolgung auf Darknet-Verkaufsplattformen für die Strafbehörden kurz dargelegt und auf rechtliche Problematiken verwiesen, welche im Rahmen der Arbeit detaillierter diskutiert werden.

A Straftaten im Darknet als Kontrollkriminalität und polizeiliche Vorermittlungen

Eine Eigenheit und gleichzeitig Schwierigkeit bezüglich der Aufklärung von Delikten auf Verkaufsplattformen im Darknet liegt darin, dass es allgemein keine Opfer gibt, wie das bei anderen Cybercrimes z.B. Hacker-Angriffen normalerweise der Fall ist.[123] Diese Delikte, bei deren Verfolgung die Polizei kaum auf Anzeigen und Verdachtsmeldungen aus der Öffentlichkeit setzen kann, werden als sog. Hol- resp. Kontrollkriminalität bezeichnet. Mithilfe von Aufklärungs- und Streifentätigkeit muss sich die Strafbehörde die Straftäter selbst «holen».[124]

[117] PAVLOVIC, Abschn. 1.
[118] Zum Ganzen Kantonspolizei Aargau, Abschn. 1; Anh. 4: Interview WALDMEIER, Frage 1.1 ff.
[119] Zum Ganzen Berner Zeitung, Abschn. 1 ff.
[120] SCHOOP, Dealer im Darknet, Abschn. 2 ff.; Vgl. Anh. 2: Interview WALDER, Frage 2.1.
[121] SCHOOP, Dealer im Darknet, Abschn. 6.
[122] Zum Ganzen KÜTTEL, Abschn. 1; KOPP, Abschn. 1.
[123] Vgl. VON HEIN, Abschn. 4.
[124] Zum Ganzen Stadt Bern, 288; Anh. 2: Interview WALDER, Frage 1.2.

Zusätzlich erschwerend kommt bei den Darknet-Ermittlungen hinzu, dass die Käufer und Verkäufer auf den Darknet-Plattformen voneinander abhängig sind und in einem engen Verhältnis zueinander stehen und dementsprechend kaum an einer staatlichen Strafverfolgung interessiert sind.[125] D.h. selbst bei Scams werden keine Strafanzeigen erstattet, da die Anzeige erstattende Person sich sonst vor der Polizei erkenntlich machen müsste und damit in Gefahr läuft, selbst bestraft zu werden.[126] Diese Gegebenheiten führen dazu, dass die Polizei im Rahmen von sog. Vorermittlungen «ihre Augen offen halten muss» und selbst ohne einen strafprozessualen Anfangsverdacht proaktiv tätig wird.[127] Unter «Vorermittlungen», die auch als kriminalpolitische Ermittlungsarbeit bezeichnet werden,[128] sind polizeiliche Massnahmen zu verstehen, die auf Verdachtsbegründung gerichtet sind und bloss auf unspezifischen, noch ungesicherten Anhaltspunkten, kriminalistischen Erfahrungswerten oder auf einer Hypothese gründen und für die Eröffnung eines Ermittlungsverfahrens gem. Art. 306 f. StPO nicht ausreichend sind und deshalb vor diesem Ermittlungsverfahren stattfinden.[129] Des Weiteren fallen darunter sog. Strukturermittlungen[130] und Methoden zur Aufklärung von bevorstehenden Straftaten für den Fall, dass diese begangen werden.[131] Vorermittlungen sind Informationsbeschaffungen, die in einer Grauzone zwischen sicherheits- und gerichtspolizeilichen Tätigkeiten und darum im Übergangsbereich zwischen Polizeigesetz (PolG) und Strafprozessrecht stattfinden.[132] Sie werden in polizeilicher Kompetenz und gestützt auf die unterschiedlichen kantonalen PolG betrieben,[133] die diese Tätigkeit jedoch häufig nur sehr rudimentär und unklar regeln.[134] Als polizeitaktische Instrumente im Rahmen der Vorermittlung dienen u.a. die Nutzung von Informationen, die polizeiliche Beobachtung und Observation, die Kontaktaufnahme sowie die verdeckte Vorermittlung auf Basis der PolG.[135]

Im Internet resp. Darknet finden die Vorermittlungen häufig als sog. «virtuelle Streifenfahrten» statt.[136] Dabei begeben sich die Strafverfolgungsbehörden auf «Streifenfahrten» im öffentlich zugänglichen Netz und halten Ausschau nach potenziellen Straftaten, ähnlich wie sie den öffentlichen Grund im Vorbeigehen in der realen Welt beobachten.[137] Da öffentlich zugängliche Websites und Kommunikationsräume nicht durch den Schutz der Privatsphäre von Art. 13 BV geschützt sind, darf die Polizei diese öffentlich zugänglichen Informationen im selben Umfang wie Private zur Kenntnis nehmen. Dies kann bspw. durch anlassunabhängige, systematische Recherchen und Auswertungen von Informationen[138] auf allgemein zugänglichen Internetplattformen wie bspw. Facebook geschehen.[139] Aber auch das reine Beobachten, als Vorstufe zur Observation, ist im Rahmen der Vorermittlung möglich. Kein Hindernis stellen dabei allenfalls notwendige Registrierungen dar, die sogar mit falschen Angaben erstellt werden

[125] Vgl. BOSCIANI, 19, der seine Aussagen jedoch auf den generellen Offline-Drogenhandel stützt.
[126] Siehe Kap. II. B 2.; Anh. 1: Interview WERREN/ZAUGG, Frage 1.6.
[127] MUGGLI, Diss., 162; BÜRGE, 70.
[128] BÜRGE, 68.
[129] BGE 140 I 353 E. 6.1 S. 365; BSK StPO-RHYNER, Art. 306, N 8; DEL GIUDICE, 121; BÜRGE, 68 f.
[130] Umfassendere polizeiliche Vorermittlungen befassen sich häufig mit der Erforschung von kriminellen Szenen (z.B. Prostitution, auch Darknet-Verkaufsplattformen), indem diese Milieus beobachtet sowie etwaige Strukturen (Organisationsformen) ermittelt und allfällige Sachverhalte festgestellt werden, die einen strafrechtlichen Tatverdacht begründen (BÜRGE, 69 f.).
[131] BSK StPO-RHYNER, Art. 306, N 8; DEL GIUDICE, 121; BÜRGE, 68 f.
[132] DEL GIUDICE, 121; BSK StPO-RHYNER, Art. 306, N 8.
[133] LANDSHUT/BOSSHARD, StPO-Kommentar, Art. 299 N 14; BSK StPO-RHYNER, Art. 306 N 8; BÜRGE, 71; DEL GIUDICE, 121.
[134] BSK StPO-RHYNER, Art. 306 N 8; BÜRGE, 71.
[135] BÜRGE, 70.
[136] MUGGLI, Diss., 162; Vgl. Anh. 2: Interview WALDER, Frage 3.1 und 3.2.
[137] MUGGLI, Diss., 162; GLESS, Strafverfolgung im Internet, 15; BISCHOFF/LANTER, N 45.
[138] Dazu kann sie auch automatische Suchprogramme beiziehen, die bspw. kinderpornografische Objekte identifizieren oder grosse Datenmengen nach strafbaren Inhalten durchsuchen können (HANSJAKOB, Überwachungsrecht, N 253).
[139] LENTJES MEILI, 422; GLESS, Strafverfolgung im Internet, 15; BISCHOFF/LANTER, N 45; HANSJAKOB Überwachungsrecht, N 252, weist daraufhin, dass solche Recherchen v.a. im Ausland mit immer grösserem Aufwand betrieben werden.

dürfen (bspw. Fake-Accounts), wenn keine materiellen Identitätsüberprüfungen erfolgen oder Zugangsbeschränkungen existieren.[140] Ziel dieser «digitalen Streifenfahrten» ist die Erhöhung des Verfolgungsrisikos für Straftäter und das zeitnahe Aufspüren von verdächtigen Inhalten.[141] Diese Methode stellt an sich – solange nicht aktiv in die Kommunikation eingewirkt wird – noch keine Ermittlungshandlung dar. Durch die Nutzung einer generell zugänglichen Informationsquelle soll eruiert werden, wo zu einem späteren Zeitpunkt evtl. Ermittlungen vorzunehmen sind.[142] Falls Bestimmungen der PolG dies vorsehen, kann aber auch die Interaktion mit Benutzern im Rahmen einer Kontaktaufnahme oder eine verdeckte Vorermittlung i.S. interaktiver Kontakte zum Aufbau eines Vertrauensverhältnisses noch im Zuge der polizeilichen Vorermittlungen erfolgen.[143] Ergibt sich jedoch durch das Monitoring im Internet, durch die Kontaktaufnahme oder eine verdeckte Vorermittlung ein strafprozessualer Tatverdacht (sog. Anfangsverdacht) auf insb. vergangene oder laufende Straftaten, so endet das Vorermittlungsverfahren, und das eigentliche Ermittlungs- resp. Vorverfahren nach den Regeln der StPO beginnt. Dieser Wechsel vom Polizei- ins Strafprozessrecht erfolgt aber auch dann, wenn zum Zwecke der Vorermittlung Zwangsmassnahmen oder andere formalisierte Ermittlungshandlungen eingesetzt werden müssen.[144] Ab diesem Zeitpunkt steht die Polizei unter der Aufsicht der StA.[145] Erkenntnisse, die aus den Vorermittlungen rechtmässig gewonnen werden konnten, sind im Strafverfahren dann prinzipiell verwertbar.[146] Trotzdem sollte das Ermittlungsverfahren frühzeitig eingeleitet werden, um kein Beweisverwertungsverbot (Art. 141 StPO) zu riskieren.[147]

In Bezug auf die Vorermittlungen bei möglichen Straftaten auf Darknet-Verkaufsplattformen bedient sich die Polizei verschiedener Ermittlungstaktiken. Einerseits bietet es sich an, aktiv mittels virtueller Streifenfahrten direkt auf den relevanten Darknet-Plattformen nach möglichen Straftaten zu suchen.[148] Andererseits kann eine Streifenfahrt aber auch im Clearnet beginnen, indem Beiträge in Foren oder Bewertungen angeschaut und analysiert werden, und bei Hinweisen auf Darknet-Plattformen diese dann im Darknet weitergeführt wird.[149] Ein mögliches Vorgehen zur Beobachtung und Recherche auf Darknet-Verkaufsplattformen kann bspw. darin bestehen, dass die Ratings, welche die meisten Plattformen haben, bezüglich Drogenverkäufen analysiert werden (vgl. Kap. II. B 2.). Dabei «filtert» der Polizeiangehörige innerhalb dieses Ratings nach Drogenhändlern, die mit «Freeshipping Switzerland» werben, weil es sich dabei um einen Täter handeln könnte, der in der Schweiz Drogen verkaufen möchte und allenfalls auch hier wohnhaft ist. So wird z.B. geprüft, ob solche Händler auf ihren Verkaufsprofilen einen innerkantonalen Lieferservice anbieten, was wiederum Rückschlüsse auf deren lokalen Bezug zulässt. Aufgrund der Rezensionen, welche die Plattformen umfassen, kann sich die Polizei aber auch ein Bild darüber machen, welche Menge und Zusammensetzung von Drogen der Händler bisher bereits umgesetzt hatte.[150] Die durch diese Streifenfahrten gewonnenen Informationen begründen häufig bereits

[140] LENTJES MEILI, 423; HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298a N 4; HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 4.
[141] MUGGLI, Diss., 162.
[142] MUGGLI, Diss., 162; GLESS, Strafverfolgung im Internet, 15.
[143] LENTJES MEILI, 424. Nennt als Beispiel für den Einsatz von verdeckten Vorermittlungen den Betrieb eines vermeintlich dubiosen Angebots in verschlüsselten Netzwerken wie dem Darknet.
[144] Zum Ganzen LANDSHUT/BOSSHARD, StPO-Kommentar, Art. 299 N 14; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 300 N 2; BSK StPO-RHYNER, Art. 306 N 8; BÜRGE, 71; DEL GIUDICE, 121.
[145] LANDSHUT/BOSSHARD, StPO-Kommentar, Art. 299 N 14.
[146] BSK StPO-RHYNER, Art. 306 N 8.
[147] DEL GIUDICE, 122; Anh. 3: Interview EUGSTER, Frage 1.4.
[148] Anh. 2: Interview WALDER, Frage 3.1 und 3.2.
[149] Anh. 3: Interview Eugster, Frage 1.1-1.3.
[150] Zum Ganzen Anh. 2: Interview WALDER, Frage 3.2.

einen ausreichenden Verdacht für begangene Straftaten, sodass ein Ermittlungsverfahren gegen Unbekannt nach StPO eröffnet und weitere Zwangsmassnahmen, wie der Einsatz von verdeckten Fahndern gestützt auf Art. 298a StPO, ergriffen werden können.[151]

B Strafanwendung und nationale Zuständigkeit

Eine weitere Problematik ergibt sich daraus, dass das Darknet als Teil des Internets nicht an Ländergrenzen gebunden ist. Server, Betreiber und Nutzer von Verkaufsplattformen befinden sich häufig mehrheitlich im Ausland. Bereits zu Beginn allfälliger Ermittlungen stellt sich deshalb die Frage, inwiefern das Schweizer Strafrecht auf den ermittelten Sachverhalt überhaupt anwendbar ist, und dementsprechend unter die Schweizer Gerichtsbarkeit resp. Strafhoheit fällt,[152] die in Art. 3 ff. StGB geregelt ist. Art. 3 Abs. 1 StGB hält den Grundsatz fest, dass dem Gesetz unterworfen ist, wer in der Schweiz ein Verbrechen oder Vergehen begeht.[153] Gem. Art. 8 StGB gilt ein Verbrechen bzw. ein Vergehen an jenem Ort als begangen, wo der Täter es ausführt oder pflichtwidrig untätig bleibt bzw. da, wo der tatbestandsmässige Erfolg eintritt. Dieses sog. Ubiquitätsprinzip definiert, dass Handlungs- und Erfolgsort bezüglich der Strafhoheit ebenso als Begehungsort gelten. Zudem gilt es auch Art. 5 Abs. 1 lit. c StGB zu beachten, wonach jemand dem StGB unterworfen ist, der sich in der Schweiz befindet, nicht ausgeliefert wird und im Ausland ein Delikt mit qualifizierter Pornografie[154] begangen hat.[155]

Da die grenzüberschreitenden Cybercrimes im Kontrast zum föderalistischen System der Schweiz stehen, welches die Zuständigkeit der Strafverfolgung kantonal regelt,[156] ist eine nationale Koordination unabdingbar.[157] Als solches Koordinationsgremium dient das «Cyberboard», dessen operativer Bereich «Cyber-CASE» sich aus Vertreter der kantonalen und nationalen Strafverfolgungsbehörden, dem Netzwerk digitaler Ermittlungsunterstützung Internetkriminalität (NEDIK)[158] und dem Nationalen Zentrum für Cybersicherheit (NCSC) zusammensetzt. In diesem Rahmen werden aktuelle Fallkomplexe im Zusammenhang mit Cybercrimes u.a. im Darknet offengelegt und analysiert, gemeinsame Vorgehensweisen definiert sowie Fragen der Zuständigkeit zwischen Bund und Kantonen geklärt, um auch mögliche Gerichtsstandkonflikte zu vermeiden.[159] Diese Koordination ist hinsichtlich der Strafverfolgung im Darknet von grosser Bedeutung.[160]

C Strafprozessuale Zwangsmassnahmen

Die Strafbehörden wissen bei der Hol-Kriminalität, dass gewisse Delikte an bestimmten Orten wie im Darknet wahrscheinlicher sind und sie deshalb durch sog. Vorermittlungen selbst aktiv werden müssen.[161] Ergibt sich aus den Vorermittlungen ein Tatverdacht gegenüber einer unbekannten Zielperson, soll ein Ermittlungsverfahren eingeleitet werden. Als Instrumente zur weiteren Aufklärung dieses Tatverdachts dienen den Strafbehörden vielfach Ermittlungsmassnahmen in Form von sog. geheimen Überwachungsmassnahmen (Art. 269 ff. StPO), wobei vorliegend v.a. die verdeckte Ermittlung (VE) und

[151] LANDSHUT/BOSSHARD, StPO-Kommentar, Art. 298b N 4; Anh. 2: Interview WALDER, Frage 3.2.
[152] Zum Ganzen RÜCKERT/SAFFERLING, 8.
[153] MUGGLI, Diss., 185.
[154] Art. 197 Abs. 3 und Abs. 4 StGB.
[155] Zum Ganzen MUGGLI, Diss., 186.
[156] Art. 22 StPO.
[157] Anh. 1: Interview WERREN/ZAUGG, Frage 2.2; Anh. 2: Interview WALDER, Frage 1.7.
[158] NEDIK ist als Netzwerk u.a. für die Sicherstellung des gegenseitigen Wissenstransfers, für die Zusammenstellung einer nationalen Fallübersicht und die Triage von interkantonalen Fällen verantwortlich (KKJPD, Abschn. 1).
[159] Zum Ganzen BURRI/EMMENEGGER/KOPP, 27 f.
[160] Anh. 1: Interview WERREN/ZAUGG, Frage 2.2; Anh. 2: Interview WALDER, Frage 1.7; m.w.H. zum Ganzen Interpellation BREGY (19.3288), Stellungnahme des Bundesrates.
[161] Anh. 2: Interview WALDER, Frage 1.2.

Fahndung (VF) sowie die Überwachung des Fernmeldeverkehrs von Bedeutung sind. Diese Überwachungsmassnahmen gelten in der Schweiz als Zwangsmassnahmen (Art. 196 ff StPO), d.h. als Verfahrenshandlungen einer Strafbehörde,[162] die *per definitionem* in Grundrechte der Betroffenen eingreifen und dem Zweck der Beweissicherung, der Sicherung der Anwesenheit von Personen sowie der Vollstreckung des Endentscheids dienen. Trotz dem allg. Wortlaut setzt eine Zwangsmassnahme nicht voraus, dass ein gegen die Massnahme gerichteter Widerstand gebrochen wird.

Wie der Name bereits sagt, bleiben die geheimen Überwachungsmassnahmen dem Betroffenen zumindest vorläufig verborgen, weshalb er sich dagegen gar nicht resp. erst im Nachhinein wehren kann.[163] Da sich die StPO jedoch grundsätzlich zu einem offenen Strafverfahren bekennt, sollen die «geheimen Überwachungsmassnahmen» nur subsidiär, d.h. ausnahmsweise, wenn die offenen Massnahmen nicht erfolgversprechend sind, zur Anwendung kommen.[164] Geheime Überwachungen dienen vielfach weniger der Beweissammlung, sondern eher als Fahndungsmittel,[165] so auch im Zusammenhang mit den Darknet-Ermittlungen. Zwangsmassnahmen unterstehen dem Zweck der Schrankenregelung von Art. 36 BV und dürfen gem. Art. 197 StPO nur ergriffen werden, wenn dafür eine gesetzliche Grundlage besteht (lit. a), wenn ein hinreichender Tatverdacht vorliegt (lit. b), keine milderen Mittel den gleichen Zweck ermöglichen (lit. c) und die Bedeutung der Straftat die Zwangsmassnahme rechtfertigt (lit. d).[166] Diese Voraussetzungen müssen kumulativ erfüllt sein.[167] Die gesetzliche Grundlage erfordert ein Gesetz im formellen Sinne. Sie findet sich dabei im Normalfall in der StPO oder in strafprozessualen Bestimmungen des Nebenstrafrechts, so im VStrR. Dies bedeutet, dass es keine strafprozessualen Zwangsmassnahmen gibt, die nicht in einem Gesetz festgelegt sind und folglich ein *numerus clausus* der Zwangsmassnahmen besteht.[168] In Bezug auf den Tatverdacht muss die Vermutung einer tatsächlich begangenen Straftat bestehen, die sich jedoch (noch) nicht gegen eine konkrete Person oder einen bestimmten Personenkreis richten muss.[169] Dies ist bezüglich den Ermittlungen im Darknet von grosser Relevanz, da sich diese gegen «Zielpersonen» richtet, deren Lokalität und Identität noch unbekannt sind.[170]

IV. Geheime Überwachungsmassnahmen

A Überwachung des Post- und Fernmeldeverkehrs (Art. 269-279 StPO)

Obwohl aus dem bisher Gesagten bereits herauszulesen ist, dass die Zwangsmassnahmen in Form von technischen Überwachungsmöglichkeiten im Rahmen der Darknet-Ermittlungen praktisch unmöglich sind, sollen diese m.E. vorliegend erklärt werden.

1. Sachlicher und örtlicher Geltungsbereich

Die Überwachungen nach Art. 269 ff. StPO können v.a. aufgrund zweier Charakteristiken von anderen Zwangsmassnahmen unterschieden werden: Es handelt sich dabei einerseits um geheime Massnahmen und andererseits, um solche, die ins Fernmeldegeheimnis eingreifen.[171] Mit Art. 269 ff. StPO wird die

[162] GLESS, Heimliche Ermittlungsmassnahmen, 442.
[163] BSK StPO-WEBER, Art. 196 N 2.
[164] GLESS, Heimliche Ermittlungsmassnahmen, 442.
[165] SCHMID/JOSITSCH, Praxiskommentar StPO, Vor Art. 269-279 N 1.
[166] Zum Ganzen siehe anstelle vieler BSK StPO-WEBER, Art. 197 N 1-3.
[167] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 197 N 1.
[168] Zum Ganzen BSK StPO-WEBER, Art. 197 N 4; VIREDAZ/JOHNER, Commentaire Romand, Art. 197 N. 4.
[169] BSK StPO-WEBER, Art. 196 N 4.
[170] Anh. 1: Interview WERREN/ZAUGG, Frage 2.4; Anh. 2: Interview WALDER, Frage 3.1; Anh. 3: Interview EUGSTER, Frage 2.1.
[171] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 12; BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 269 N 21.

Überwachung des sog. Post[172]- und Fernmeldeverkehrs bezweckt, wobei vorliegend Letzteres von Interesse ist. Als Fernmeldeverkehr werden die in Art. 2 und 3 lit. c FMG regulierten Tätigkeiten und somit die fernmeldetechnische Übertragung von Informationen verstanden.[173] D.h. das elektrische, magnetische und optische Senden und Empfangen von Informationen über Leitungen und Funk.[174] Unter den Fernmeldeverkehr fällt auch der Internetverkehr und die damit zusammenhängen Kommunikationsformen, wie E-Mail, Internet-Telefonie oder Messaging-Dienste.[175] Nach herrschender Meinung ist das Fernmeldegeheimnis das bedeutende Schutzobjekt von Art. 269-279 StPO, welches als Teilaspekt dem Grundrecht auf Schutz der Privatsphäre in Art. 13 Abs. 1 BV zuzurechnen[176] und in Art. 43 FMG verbrieft ist.[177] Art. 269 ff. StPO und das BÜPF stellen demnach die für Grundrechtseingriffe notwendige gesetzliche Grundlage für die Aufhebung des Fernmeldegeheimnisses dar.[178]

Dabei legt Art. 269 ff. StPO fest, wann eine Überwachung überhaupt zulässig ist und das BÜPF definiert, welche Akteure bei einer Überwachung zur Mitwirkung verpflichtet werden können.[179] Vom Fernmeldegeheimnis und damit vom Anwendungsbereich des Art. 269 ff. StPO bzw. dem BÜPF erfasst sind einerseits nur Informationen, die geheim und eben nicht öffentlich zugänglich sind. Nicht geschützt sind demnach z.B. Tweets auf Twitter,[180] Kommunikation sowie Posts auf einem öffentlichen Facebook-Profil und auch die Angebote auf Darknet-Verkaufsplattformen.[181] Andererseits gilt das Fernmeldegeheimnis nur während der Zeitdauer der fernmeldetechnischen Übertragung von Informationen.[182] Sobald der Kommunikationsvorgang abgeschlossen ist und m.a.W. sobald die Kommunikationsdaten im Zugriffsbereich des Empfängers liegen, müssen die Daten nach den Regeln der Durchsuchung (Art. 246 ff. StPO), Edition (Art. 265 StPO) bzw. Beschlagnahme (Art. 263 ff. StPO) erhoben werden.[183] Dabei ist nicht entscheidend, ob der Empfänger Kenntnis von den Daten genommen hat oder nicht; ausschlaggebend ist primär, ob sie sich in seinem Zugriffsbereich befinden und der Empfänger diese zur Kenntnis nehmen könnte (bspw. E-Mails etc.).[184] In örtlicher Hinsicht beschränken sich die Überwachungsmassnahmen auf die Schweiz. Überwachungen sind somit möglich, wenn der Fernmeldeverkehr über die Schweiz abgewickelt wird, sodass die Daten hierzulande anfallen und diese in der Schweiz ediert werden können.[185]

[172] Unter dem Postverkehr werden sämtliche Tätigkeiten, die unter den Geltungsbereich des Postgesetzes (PG) vom 17.12.2010, SR 783.0 fallen, verstanden. Darunter sind alle gewerbsmässigen Postdienste gem. Art 1 Abs. 1 lit. a PG, ausgenommen der Dienstleistungen des Zahlungsverkehrs gem. Art. 1 Abs. 1 lit. b PG, zu verstehen.
[173] Botschaft 2013 BÜPF, 2704.
[174] Botschaft 1998 BÜPF, 4255 f.
[175] Botschaft 2013 BÜPF, 2704., wie bereits im Kap. III. A angetönt wurde, fallen offen zugängliche Informationen, solange keine Kommunikation mit Menschen stattfinden nicht unter den Fernmeldeverkehr (HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 12 f.; BIEDERMANN, 78).
[176] BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 269, N 21.
[177] Art. 43 FMG: Wer mit fernmeldedienstlichen Aufgaben betraut ist oder betraut war, darf Dritten keine Angaben über den Fernmeldeverkehr von Teilnehmenden machen und niemandem Gelegenheit geben, solche Angaben weiterzugeben.
[178] Botschaft 2013 BÜPF, 2704.
[179] Botschaft 2013 BÜPF, 2750.
[180] Öffentlich abrufbare Tweets, d.h. solche ohne spezielle publikumsbegrenzende Einstellung, sind gem. BGer öffentlich (BGer 5A_195/2016); m.w.H. ZULAUF/SIEBER, 548 ff.
[181] Vgl. HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 13.
[182] BGE 140 IV 181 E. 2.4. S. 184; HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 13.
[183] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 16.
[184] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 16; HANSJAKOB, Überwachungsrecht, N 298 ff.
[185] HANSJAKOB, Überwachungsrecht N 389.

2. Überwachungsformen und Auskünfte

a Echtzeitüberwachung der Inhaltsdaten

Bei einer aktiven Überwachung werden Kommunikationsinhalte, die dem Fernmeldegeheimnis unterliegen, geheim abgefangen resp. noch während des Kommunikationsvorgangs beim Provider ediert.[186] Abgefangen werden die sog. Inhaltsdaten (Call Content, CC),[187] d.h. der effektive Inhalt einer Information. Es wird somit bspw. der Inhalt eines Telefongesprächs mitgehört oder der Inhalt eines E-Mails mitgelesen.[188] Damit eine solche Überwachung vorgenommen werden kann, muss gem. Art. 269 Abs. 1 lit. a StPO ein dringender Tatverdacht in Bezug auf ein Delikt aus dem Straftatenkatalog von Art. 269 Abs. 2 StPO vorliegen,[189] womit die Anforderungen an den Tatverdacht höher sind als der allgemein bei Zwangsmassnahmen erforderliche hinreichende Verdacht.[190] Die Schwere des Delikts muss die Überwachung rechtfertigen und die Anforderungen an die Subsidiarität müssen gegeben sein.[191]

Für die Anordnung einer Überwachung ist die StA im Rahmen eines eröffneten Strafverfahrens zuständig, wobei sie den Dienst ÜPF[192] beauftragt, die Dienstanbieterin zur Umsetzung der Überwachung anzuweisen.[193] Nach erfolgter Anordnung muss die StA sowohl bei der aktiven Überwachung als auch bei der Randdatenerhebung gem. Art. 274 Abs. 1 StPO innert 24 Stunden einen Genehmigungsantrag beim Zwangsmassnahmengericht einreichen.[194] Das Fehlen einer Genehmigung würde zur absoluten Unverwertbarkeit der Ergebnisse aus der Überwachung führen.[195] Die nachträgliche richterliche Überprüfung dient gewissermassen als Korrektiv für den Betroffenen, dem aufgrund der Heimlichkeit der Massnahme kein rechtliches Gehör gewährt werden kann.[196]

b Aktive oder rückwirkende Randdatenerhebung

Viel häufiger als aktive Überwachungen kommen in der Schweiz jedoch sog. Randdatenerhebungen vor.[197] Von Interesse bei dieser Form der geheimen Überwachung sind nicht die Inhaltsdaten der Kommunikation,[198] sondern Daten, die über den Zeitpunkt, die Dauer und den Standort des Überwachten sowie über die Anschlussdaten und den Standort des Gesprächspartners Auskunft geben.[199] Vereinfacht gesagt, wer mit wem, wann und von wo aus kommuniziert (hat).[200] Art. 273 StPO regelt die in der Praxis relevanten bis zu sechs Monaten rückwirkenden Randdatenerhebungen (sog. Vorratsdatenspeicherung) sowie die äusserst selten angeordnete laufende Erhebung.[201] Da die Erhebung von Randdaten im Vergleich zu den Inhaltsdaten als weniger starker Eingriff in die Rechte des Betroffenen erachtet wird, muss keine Straftat aus einem Deliktskatalog erfüllt sein, sondern ein dringender Verdacht eines Verbrechens

---

[186] HANSJAKOB, Überwachungsrecht N 430 und 1677; FORSTER, Marksteine BGer-Praxis, 624.
[187] HANSJAKOB, Überwachungsrecht N 430 und 1677.
[188] BERANEK, 146; Dienst ÜPF, Statistik, Schweiz 2019; ROTH, grenzüberschreitende Edition, N 17.
[189] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 50.
[190] HANSJAKOB, Überwachungsrecht, N 444 ff.
[191] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 70 und 87.
[192] Überwachung des Post- und Fernmeldeverkehrs beim Informatik Service Center des Eidg. Justiz- und Polizeidepartements (ÜPF ISC-EJPD).
[193] HANSJAKOB, Überwachungsrecht, N 533 f.
[194] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 274 N 24.
[195] Art. 277 StPO i.V.m. Art. 141 Abs. 1 StPO; BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 277 N 3.
[196] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 272 N 4.
[197] Das Verhältnis zwischen den Randdatenerhebungen und den Echtzeitüberwachungen war 2018: 3.12, 2019: 3.34, 2020: 3.40 (Dienst ÜPF, Statistik, Anzahl Massnahmen im Jahresvergleich).
[198] HANSJAKOB, Überwachungsrecht, N 857 f.; BERANEK, 143 f.
[199] BGE 137 IV 340 E. 5.1-5.2 S. 346 f; BGE 142 IV 34 E. 4.3.2 S. 38 f.; HANSJAKOB, Überwachungsrecht, N 282.
[200] BGer 1C_598/2016 E. 6.2; ROTH, grenzüberschreitende Edition, N 17.
[201] Vgl. Art. 273 Abs. 1 und Abs. 3 StPO; HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 273 N 16.

oder Vergehens bestehen und die Voraussetzungen von Art. 269 Abs. 1 lit. b und c StPO erfüllt sein.[202] Trotzdem muss auch die Randdatenerhebung durch das Zwangsmassnahmengericht bewilligt werden.[203]

c Bestandesdatenauskünfte

Von den eben genannten geheimen Überwachungsmassnahmen muss die Auskunft über die sog. Bestandesdaten klar abgegrenzt werden.[204] Als Bestandesdaten werden Auskünfte verstanden, die nicht dem Fernmeldegeheimnis unterliegen und auch nicht vom Zwangsmassnahmengericht genehmigt werden müssen.[205] Unter dieser Kategorie von Daten werden solche über feststehende Abonnementsverhältnisse verstanden.[206] Dabei hat eine Bestandesdatenerhebung zum Ziel, den Teilnehmer eines bestimmten Anschlusses zu identifizieren und nicht die Daten zu einem spezifischen Gespräch zu erhalten.[207] Die Erhebung dieser Daten ist einerseits in Art. 21 BÜPF geregelt und umfasst bspw. Angaben wie Name und Adresse (Abs. 1 lit. a) sowie Adressierungselemente (Abs. 1 lit. b), wobei allfällige Straftäter wohl häufig falsche Adressen oder Personalien angeben und damit eine Identifikation verunmöglichen.[208] Andererseits sind die Auskunftsanfragen in Art. 22 BÜPF geregelt, der sich speziell auf die Internetkommunikation bezieht und eine Identifikation der Internetnutzer zum Ziel hat.[209]

Die Auskünfte von Art. 22 BÜPF sind v.a. zur Eruierung der Zuordnung von dynamisch vergebenen IP-Adressen zu einem bestimmten Kunden eines Access Providers von Relevanz.[210] Wie bereits in Kap. II. A 2. erklärt wurde, bedeutet dynamische Vergabe, dass jedem Kunden bei jedem Internetverkehr eine IP-Adresse zugewiesen wird,[211] wobei die Anbieterin eine Datenbank führt, welche die Zuteilung ihrer IP-Adressen an ihre Kunden zu jedem Zeitpunkt protokolliert.[212] Wenn die StA wissen möchte, wer eine bereits bekannte IP-Adresse zu einem gewissen Zeitpunkt für eine Kommunikation, deren Randdaten schon bekannt sind, verwendet hat, handelt es sich bei der betreffenden Anfrage an die Anbieterin grundsätzlich um eine Bestandesdatenabfrage.[213] Wenn die Strafverfolgungsbehörden jedoch nur von strafbarer Internet-Kommunikation erfahren haben und sie über die Randdaten der betreffenden Anbieterin die zugewiesenen IP-Adressen und Kunden eruieren möchte, sind gem. BGer bei Überwachungen die Vorschriften von Art. 273 StPO anwendbar.[214] Ob es sich bei der IP-Adresse um Bestandes- oder Verbindungsdaten handelt, ist von deren Verwendungszweck abhängig.[215]

3. Persönlicher Geltungsbereich des BÜPF

Im Unterschied zu anderen Zwangsmassnahmen gilt als Objekt der Überwachung nicht eine betroffene Person, sondern deren Fernmeldeverkehr und dementsprechend deren Anschluss (vgl. Art. 270 StPO)

---

[202] HANSJAKOB, Überwachungsrecht, N 894.
[203] Art. 273 Abs. 2 StPO; BGE 137 IV 340 E. 5.3 S 347.
[204] HANSJAKOB, Überwachungsrecht, N 1518.
[205] HANSJAKOB, Überwachungsrecht, N 888; HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 272 N 10.
[206] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 273 N 47.
[207] ROTH, grenzüberschreitende Edition, N 17; HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 273 N 47.
[208] Vgl. HANSJAKOB, Überwachungsrecht, N 1626 ff.
[209] HANSJAKOB, Überwachungsrecht, N 1637.
[210] ROTH, grenzüberschreitende Edition, N 17.
[211] BGE 136 II 508 E. 3.3 S. 514; HANSJAKOB, Überwachungsrecht, N 1638.
[212] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 273 N 50; BETSCHMANN, 360.
[213] BGer 6B_656/2015 E. 1.3.1; HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 273 N 50 f.; BETSCHMANN, 360; BÜHLMANN, Abschn. 3.
[214] BGer 6B_656/2015 E. 1.3.2; BÜHLMANN, Abschn. 3.
[215] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 45.

resp. Adressierungselemente[216] oder Fernmeldedienste.[217] Zentral ist, dass die Strafverfolgungsbehörden eine solche Überwachung nur unter Mitwirkung der jeweiligen Anbieter von Fernmeldediensten vornehmen können.[218] Wie bereits erwähnt, regelt der persönliche Geltungsbereich des BÜPF, wer dem Gesetz unterstellt ist und deshalb Pflichten hat.[219] Aufgrund der technologischen Entwicklungen der letzten Jahre wurde mit der Revision des BÜPF, die am 1. März 2018 in Kraft trat, der Geltungsbereich beträchtlich erweitert.[220] Das neue BÜPF umfasst gem. Art. 2 nun sechs Kategorien von Mitwirkungspflichtigen, denen verschiedene Pflichten auferlegt werden (vgl. Art. 19-34 BÜPF).[221] Nachfolgend wird v.a. auf die bereits im aBÜPF bestehende Kategorie der «Anbieterinnen von Fernmeldediensten», sog. FDA (Art. 2 lit. b BÜPF), sowie die mit der Revision eingeführten «Anbieterinnen abgeleiteter Kommunikationsdienste» sog. AAKD (Art. 2 lit. c BÜPF) eingegangen, da diese für die Arbeit von Relevanz sind.[222]

Als FDA wird eine nat. oder jur. Person verstanden «welche Informationen für Dritte fernmeldetechnisch selber überträgt oder übertragen lässt und diesen gegenüber im Rahmen eines privatrechtlichen Vertragsverhältnisses die Verantwortung für die Erbringung der versprochenen Dienstleistung übernimmt.»[223] Darunter fallen bspw. das Anbieten von Dienstleistungen wie Festnetz- oder Mobiltelefonie, Internet oder Fernsehen. Dies entspricht auch dem Angebot der bekanntesten FDAs, wozu bspw. die Swisscom zählt.[224] FDAs trifft einerseits die Pflicht Auskünfte über die Bestandesdaten gem. Art. 21 f. BÜPF zu erteilen und andererseits Echtzeit- und rückwirkende Überwachungen zuzulassen, indem der Inhalt- und/oder die Randdaten des Fernmeldeverkehrs der überwachten Person an den Dienst ÜPF weitergeleitet werden (Art. 26 BÜPF).[225]

Unter den sog. AAKD werden Service Provider verstanden, die weder ein FDA noch ein Access Provider sind, die aber Dienste im Zusammenhang mit dem Internetverkehr zur Verfügung stellen, welche nur in Verbindung mit der Tätigkeit eines FDA angeboten werden können.[226] Als Abgrenzungskriterium zu den FDA fungiert die fernmeldetechnische Übertragung von Informationen gem. Definition im FMG. Die von den AAKD angebotenen Dienste sind zwar auf eine solche Übertragung angewiesen, sie nehmen diese fernmeldetechnische Übertragung von Informationen aber nicht selbst vor.[227] Würden sie dies selbst vornehmen, so wären sie als FDA zu qualifizieren.[228] Erfasst werden als AAKD zum einen Anbieterinnen von Internetdiensten, die eine Einwegkommunikation gewährleisten, welche das Hochladen

[216] Adressierungselemente sind gem. Art. 3 lit. f FMG Kommunikationsparameter sowie Nummerierungselemente, wie Kennzahlen, Ruf- und Kurznummern. Unter Kommunikationsparametern werden Elemente zur Identifikation von Personen, Computerprozessen, Geräten etc. verstanden, die an einem fernmeldetechnischen Kommunikationsvorgang teilnehmen, worunter z.B. E-Mail-Adressen und Telefonnummern zu verstehen sind (HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 10).
[217] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 10; BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 270 N 5.
[218] Vgl. Art. 2 BÜPF.
[219] Botschaft 2013 BÜPF, 2694.
[220] Botschaft 2013 BÜPF, 2689 f. und 2694; Gemäss dem alten Recht umfasste der persönliche Geltungsbereich des BÜPF nur die Anbieter von Post- oder Fernmeldediensten, wozu die Internetzugangsanbieterinnen (auch Access Provider) sowie die Betreiber von internen Fernmeldenetzen und Hauszentralen zählten. Vom aBÜPF nicht erfasst waren, reine Dienste-Anbieter resp. Service Provider, welche Dienstleistungen im Internet anbieten (HANSJAKOB, Überwachungsrecht, N 1377).
[221] KLAUS/MATHYS, N 17.
[222] Botschaft 2013 BÜPF, 2694.
[223] Dienst ÜPF, Merkblatt «FDA - AAKD», 3.
[224] Dienst ÜPF, Statistik, Mitwirkungspflichtige.
[225] HANSJAKOB, Überwachungsrecht, N 1616, 1669 f. und 1677; Art. 22 Abs. 1 f. BÜPF.
[226] Botschaft 2013 BÜPF, 2707; KLAUS/MATHYS, N 20.
[227] Botschaft 2013 BÜPF, 2707 f.; KLAUS/MATHYS, N 20.
[228] Botschaft 2013 BÜPF, 2707 f.; Dienst ÜPF, Merkblatt «FDA - AAKD», 7.

von Dokumenten ermöglicht (z.B. Google Docs) und zum anderen solche, die eine Mehrwegkommunikation sicherstellen, welche die Kommunikation zwischen den Nutzern erlaubt (z.B. Facebook).[229] Dabei gilt es zu beachten, dass nur Anbieterinnen erfasst werden, die dem Schweizer Recht unterliegen resp. bei denen ein Bezug zur Schweiz besteht,[230] was für viele bekannte Anbieterinnen, wie Facebook und Google nicht gegeben sein dürfte.[231] Nach der Inkraftsetzung des neuen BÜPFs war es für die Unternehmen schwierig abzuschätzen,[232] unter welche Kategorie sie sich einordnen müssten. Deshalb hat der Dienst ÜPF ein Merkblatt als Orientierungshilfe herausgegeben.[233] Gemäss diesem fallen Online-Speicherdienste,[234] Dienste zum Hochladen und Teilen von Inhalten, Cloud Computing,[235] Online-Marktplätze,[236] Social Media und Location Based Services unter den Begriff AAKD.[237] Gemäss dem Merkblatt gilt es zu beachten, dass sich Kommunikationsdienste innerhalb von Online-Marktplätzen oder Social Media (z.B. Messenger von Facebook) als FDA qualifizieren.[238]

Die Mitwirkungspflichten der AAKD sind im Unterschied zu denjenigen der FDAs geringer und umfassen die Duldung der Überwachung der Kommunikation der über die von ihr angebotenen Dienste (Art. 27 Abs. 1 BÜPF) sowie die Lieferung der Randdaten, die ihnen zur überwachten Person zur Verfügung stehen (Art. 27 Abs. 2 BÜPF). Dasselbe gilt auch für die Lieferung der Bestandesdaten (Art. 22 Abs. 3 BÜPF).[239] Somit trifft sie im Allgemeinen keine aktive Überwachungspflicht oder eine Notwendigkeit zur Erhebung und Speicherung der Rand- bzw. Bestandesdaten.[240]

4. Probleme der Überwachungen des Fernmeldeverkehrs sowie den Datenerhebungen auf Darknet-Verkaufsplattformen

a Ermittlungsmöglichkeiten und Zwangsmassnahmen bei Darknet-Verkaufsplattformen

Es soll nun dargestellt werden, inwiefern die technikgestützten Zwangsmassnahmen der Überwachung resp. Datenerhebungsmöglichkeiten zur Identifikation der Verkäufer und Käufer illegaler Waren auf Darknet-Plattformen nicht zielführend sind.[241]

Da diese Erkenntnisse zum Verständnis der weiteren Arbeit von wichtiger Bedeutung sind, werden diese konkret anhand eines fiktiven Beispiels erklärt und ferner die Eigenheiten der Darknet-Verkaufsplattformen von den Herausforderungen und Spezifikationen, die sich im Zusammenhang mit der Strafverfolgung bei anderen Service Providern stellt, abgegrenzt. Dabei ist für Service Provider oftmals typisch, dass deren Anwender bei der erstmaligen Benutzung ein Benutzerkonto einrichten müssen. Der Zugang

[229] Botschaft 2013 BÜPF, 2708; HANSJAKOB, Überwachungsrecht, N 1685.
[230] Z.B. die Dienstanbieterin hat ihren Sitz in der Schweiz oder eine Niederlassung der Dienstanbieterin, welche die faktische oder rechtliche Kontrolle über die Kommunikation und/oder Datenspeicherung hat, befindet sich in der Schweiz (Dienst ÜPF, Merkblatt «FDA - AAKD», 7).
[231] HANSJAKOB, Überwachungsrecht, N 328; Dienst ÜPF, Merkblatt «FDA - AAKD», 6 f.
[232] KLAUS/MATHYS, N 21.
[233] Dienst ÜPF, Merkblatt «FDA - AAKD», 1 ff.
[234] Darunter wird Cloud Storage, File Hosting, Share Hoster, Online Storage und File Sharing verstanden.
[235] Vgl. Kap. IV. A 4.
[236] Da das Merkblatt «FDA – AAKD» keine Definition bezüglich Online-Marktplätze umfasst, wird hier auf eine generelle Definition zurückgegriffen. Als Online-Marktplätze gelten demnach elektronisch unterstützte Institutionen, die den Austausch von Leistungen ermöglichen. Sie fungieren als institutioneller Rahmen für Transaktionsprozesse und konkurrieren Distributions- und Kommunikationsmedien (Gabler Wirtschaftslexikon, E-Marketplace.).
[237] Dienst ÜPF, Merkblatt «FDA - AAKD», 5.
[238] Dienst ÜPF, Merkblatt «FDA - AAKD», 5; Beispiele selbst hinzugefügt.
[239] Zum Ganzen KLAUS/MATHYS, N 22; HANSJAKOB, Überwachungsrecht, N 1686 ff.
[240] KLAUS/MATHYS, N 22; BÜHLMANN/REINLE, Abschn. 9; Das BÜPF sieht Möglichkeiten vor, dass der Bundesrat Dienste einer Kategorie den Pflichten einer andere Kategorie unterstellen kann, insofern gewisse Voraussetzungen erfüllt sind (z.B. ein AAKD wird den Pflichten eines FDA unterstellt, vgl. Art. 22 Abs. 4, Art. 27 Abs. 3 BÜPF und Art. 52 VÜPF)
[241] Zum Ganzen KRAUSE, 679; ZÖLLER, 276.

zu diesem Konto wird über sog. Zugangsdaten gewährleistet, die sich meistens aus einem Benutzernamen und einem Passwort zusammensetzen und den unbefugten Zugriff auf vertrauliche Daten verhindern sollen. Stimmen die Zugangsdaten nicht mit dem Benutzerkonto überein, wird der Zugriff verweigert.[242] Dabei werden häufig nicht nur E-Mail-Konten, Benutzerkonten bei Social Medias, bei Cloud-Service Providern und bei Online-Marktplätzen sondern auch bei Darknet-Plattformen mittels Zugangsdaten geschützt,[243] resp. zur Authentifizierung des Benutzers verwendet.[244]

Als hypothetisches Beispiel wird angenommen, dass jemand anonym[245] und unter Verwendung eines «Nicknames» ein Benutzerkonto bei einer Verkaufsplattform wie tutti.ch eröffnet hat und dort ohne Bewilligung eine Waffe zum Verkauf anbietet.[246] Angenommen, jemand würde dieses illegale Angebot der Polizei melden,[247] würde diese wahrscheinlich in einem zweistufigen Verfahren vorgehen. Als erstes würde die Polizei versuchen, die IP-Adresse oder weitere Angaben zur Identität des Inhabers dieses Benutzerkontos beim Service Provider, in diesem Falle die Betreiberin von tutti.ch zu ermitteln.[248] Tutti.ch ist ein Schweizer Online-Marktplatz[249] und könnte gemäss Art. 2 lit. c BÜPF allenfalls als AAKD gelten.[250] Als AAKD könnte Tutti.ch zur Herausgabe der ihr zur Verfügung stehenden Rand- und Bestandesdaten der überwachten Person resp. der zu identifizierenden Täterschaft verpflichtet werden.[251] Die Polizei würde bspw. via Dienst ÜPF eine Anfrage an Tutti.ch stellen. Tutti.ch würde die IP-Adresse zum Waffeninserat ausfindig machen können und diese via Dienst ÜPF der Polizei zukommen lassen. Falls es sich um eine dynamische IP-Adresse handelt (vgl. Kap. II. A 2.), würde die Polizei in einem zweiten Schritt via Dienst ÜPF eine weitere Anfrage an den Access Provider veranlassen (bspw. Swisscom), der die IP-Adresse verwaltet.[252] Gemäss Art. 22 Abs. 1 BÜPF wäre die Swisscom als FDA[253] dann verpflichtet, alle (auch rückwirkende) Angaben zu machen, welche zur Identifikation der Zielperson beitragen. Dabei muss die Swisscom v.a. eruieren können, welchem Internetanschluss sie zum entsprechenden Zeitpunkt die fragliche IP-Adresse zugewiesen hat. Dazu führt sie eine Datenbank, welche die Zuteilung ihrer IP-Adressen an ihre Kunden zu jedem Zeitpunkt protokolliert.[254] Kann die Swisscom der Polizei mitteilen, wem sie die IP-Adresse zum fraglichen Zeitpunkt zugewiesen hat, muss die Strafverfolgungsbehörde anschliessend erheben, wer tatsächlich zu der Zeit vor dem Computer sass.[255]

Wird das Beispieldelikt auf das Darknet übertragen, würde jemand unter Verwendung eines Nicknames ein Benutzerkonto bei einer Verkaufsplattform wie Dream Market eröffnen und dort eine Waffe zum Verkauf anbieten. Stösst die Strafverfolgungsbehörde auf dieses Inserat und möchte sie Angaben zur Identität des Inhabers dieses Benutzerkontos oder die IP-Adresse des Sendegeräts herausfinden, wird

[242] Zum Ganzen CHRISTENSSON, Abschn. 1 ff.
[243] DALBY, 188; Vgl. BGer 1B_185/2019, Sachverhalt, lit. E.; BGer 1B_153/2019, Sachverhalt, lit. E.
[244] CHRISTENSSON, Abschn. 1.
[245] D.h. ohne weitere Angaben zur Identität, wie bspw. Name und E-Mail-Adresse.
[246] Beispiel in Anlehnung an Anh. 1: Interview WERREN/ZAUGG, Frage 1.9, es handelt sich dabei um ein hypothetisches Beispiel, da Online-Marktplätze wie tutti.ch oder ricardo.ch die Inserate entsprechend prüfen und bereits wegen Reputationsgründen keine illegalen Waffen-Inserate auf ihren Plattformen haben möchten.
[247] Von einer solchen Meldung ist bei einer Plattform wie ricardo.ch oder tutti.ch gemäss WERREN auszugehen (Interview WERREN/ZAUGG, Frage 1.9).
[248] Vgl. MUGGLI, Diss., 193.
[249] NZZ vom 13.2.2015, Abschn. 1.
[250] Dienst ÜPF, Merkblatt «FDA - AAKD», 5, Ziff. 4.1. Bei dieser Zuordnung handelt es sich um eine Annahme, da weder eine öffentlich publizierte Liste zu den AAKD, noch entsprechende Unternehmen als Beispiele für AAKD der Kategorie Online-Marktplätze gefunden wurden.
[251] Art. 27 Abs. 2 BÜPF und Art. 22 Abs. 3 BÜPF.
[252] Vgl. HANSJAKOB, Überwachungsrecht, N 1643.
[253] Vgl. Kap. IV. A 3.
[254] HANSJAKOB, Überwachungsrecht, N 1638; HANSJAKOB, Daten des Internetverkehrs, 254.
[255] Vgl. Anh. 1: Interview WERREN/ZAUGG, Frage 1.9; Vgl. MUGGLI, Diss., 192 f.

sowohl eine geheime Kommunikationsüberwachung (i.S. einer aktiven oder rückwirkenden Überwachung) genauso wie die Datenerhebung von bereits zugestellten Daten nach den Regeln der Durchsuchung, Edition resp. Beschlagnahme[256] aus nachfolgenden Gründen nicht zielführend sein und scheitern. Denn für beide Möglichkeiten ist die Strafverfolgungsbehörde auf die Mithilfe resp. die Auskünfte des Service Providers, in dem Falle des Plattformbetreibers angewiesen. Dabei ergibt sich erstens das Problem, dass die Plattformbetreiber grundsätzlich nicht bekannt sind und sich gerade selbst vor den Strafverfolgungsbehörden geheim halten.[257]

Zweitens ist deshalb auch unklar, wohin die Strafverfolgungsbehörde ihre Anfrage zur Kommunikationsüberwachung oder zur Edition von Daten richten müsste und welches Recht überhaupt zur Anwendung kommen würde. Da bisher sämtliche von internationalen Strafverfolgungsbehörden aufgedeckten Verkaufsplattformen einerseits nicht von Schweizern betrieben wurden und andererseits auch die Server-Standorte allesamt im Ausland lagen, ist anzunehmen, dass die Schweizer Strafverfolgungsbehörden rechtshilfeweise an die ausländischen Behörden gelangen müssten.[258]

Drittens wäre aufgrund ihres illegalen Geschäftsmodells sowieso keine Kooperation der Plattformbetreiber mit den Strafverfolgungsbehörden zu erwarten.[259] Und falls diese unerwarteterweise mit den Strafverfolgungsbehörden zusammenarbeiten würden, so könnten sie bspw. die IP-Adresse des Sendegeräts selbst nicht ausfindig machen, da die ursprüngliche Kommunikation vom Sendegerät über mindestens drei Tor Nodes umgeleitet wurde und der Plattformbetreiber nur die IP-Adresse des Exit Nodes kennt (vgl. Kap. II. A 3.). Da keiner der Serverstandorte innerhalb des Tor-Systems bekannt ist, könnten diese auch nicht beschlagnahmt und anschliessend ausgewertet werden.[260] Der Rückschluss auf den Inhaber eines Benutzerkontos einer Darknet-Verkaufsplattform wird nicht nur durch den Tor Browser und die anonyme Verkaufsplattform, sondern auch durch die Benutzung von Kryptowährungen, welche die Nachverfolgung von Zahlungsströmen praktisch verunmöglichen, weiter erschwert.[261]

b Abgrenzung der Darknet-Plattformen zu anderen Service Providern

Obwohl die Strafverfolgung bezüglich Daten- und Beweiserhebungen bei Service Providern u.a. wegen des Auslandbezugs im Zusammenhang mit Cybercrime typisch ist, verstärkt der Aufbau der Darknet-Verkaufsplattformen das Problem noch mehr. Inwiefern Darknet-Plattformen gewisse Gemeinsamkeiten oder eben Unterschiede zu anderen Service Providern, wie den Cloud Computing und den bedeutendsten Social Media, aufweisen, soll nachfolgend erläutert werden.

Charakteristisch für das Cloud Computing ist, dass der Cloud-Nutzer bei der Speicherung seiner Daten, diese nicht mehr lokal auf seinem Rechner abspeichert, sondern dafür einen gemieteten oder kostenlosen Datenspeicher eines Cloud Service Providers wie Dropbox nutzt.[262] Über einen sog. Fernzugriff kann

[256] Vgl. Kap. V.
[257] IHWAS, 146.
[258] Die Hauptinfrastruktur von Hansa befand sich bspw. in den Niederlanden, weitere Server waren in Deutschland und Litauen, die beiden Betreiber waren hingegen Deutsche. Beim Betreiber von AlphaBay handelte es sich wiederum um einen kanadischen Staatsbürger, der in Thailand gelebt hatte, die Server befanden sich u.a. in Kanada und den Niederlanden (Europol, Criminal Dark Web, Abschn. 6). Beim Betreiber von Silk Road handelte es sich um einen Amerikaner und die Server wurden in Island durch das FBI entdeckt (VINTON, Abschn. 4).
[259] KRAUSE, 679; RÜCKERT, 18; ZÖLLER, 276.
[260] RÜCKERT, 18; MEY, Darknet, N 133.
[261] HOSTETTLER, Hilflose Ermittler, 14.
[262] EDÖB, Abschn. 1; WICKER, 766; HANSJAKOB, Überwachungsrecht, N 336.

der Cloud-Nutzer seine in der Cloud gespeicherten Daten, wie Dokumente, Musik und Bilder von überall und von verschiedenen Geräten aus abrufen und auf diese zugreifen.[263] Der Cloud Service Provider stellt somit Datenspeicherplatz, Rechenkapazität und Programme auf Servern zur Verfügung, die über das Internet erreicht werden.[264] Typischerweise werden Daten in den Cloud-Speichern zur Gewährleistung der Datensicherheit aber auch zur besseren Auslastung der Rechnersysteme auf unterschiedlichen Servern, die zu einem Netzwerk zusammengeschlossen sind und sich in verschiedenen Ländern befinden, gespeichert.[265] Um eine hohe Verfügbarkeit sowie einen schnellen Zugriff von überall auf der Welt zu ermöglichen, werden die Daten gespiegelt, d.h. mehrfach abgespeichert, was dazu führt, dass der Cloud-Nutzer und meistens auch der Cloud Service Provider nicht wissen, wo bestimmte Daten zu einem gewissen Zeitpunkt gespeichert sind.[266]

Diese dezentralen und dynamischen Speichersysteme, sowie die rotierenden Speicherstandorte stellen die Strafverfolgungsbehörden v.a. bei der Anwendung von Zwangsmassnahmen bspw. zur Herausgabe von auf der Cloud gespeicherten Daten eines Verdächtigen vor grosse Herausforderungen.[267] Denn selbst wenn bei Cloud Service Providern der Standort des Unternehmens bekannt ist, ist für die Strafverfolgungsbehörden oft nicht erkennbar, wo sich die Daten effektiv befinden und unter welche Jurisdiktion diese fallen.[268] Die EU bezeichnet Situationen in denen die Strafverfolgungsbehörde den physischen Standort des Täters, der kriminellen Infrastruktur oder der digitalen Beweise nicht feststellen kann, als sog. «Verlust der Kenntnis über den Standort» oder «Standortverlust» (engl. «loss of knowledge of location» oder «loss of location»).[269] Bei gespeicherten Daten in Clouds beschränkt sich die Problematik des Standortverlusts primär auf den unbekannten Speicherort der Daten. Im Unterschied dazu ist die Problematik des Standortverlusts bei Darknet-Verkaufsplattformen bedeutend grösser, weil sowohl die Identität aber auch die Lokalisation einer verdächtigen Person im Darknet unbekannt ist. Ferner sind auch die eigentliche kriminelle Infrastruktur, d.h. der Plattformbetreiber, anonym und die Serverstandorte der jeweiligen Verkaufsplattform nicht bekannt.

Nachfolgend werden die Spezifika der einzelnen Service Provider übersichtshalber tabellarisch festgehalten.

[263] EDÖB, Abschn. 1; WICKER, 766.
[264] HANSJAKOB, Überwachungsrecht, N 336.
[265] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 19; GERCKE, Cloud Computing, 348; DALBY, 244. Google verfügt bspw. über 23 Server-Standorte verteilt in Nord- und Südamerika, Europa sowie Asien (Google, Rechenzentren).
[266] Council of Europe, Cloud Computing, 5. BÄR, EDV-Beweissicherung, Durchsuchungen mit Auslandsbezug, N 30.
[267] Council of Europe, Cloud Computing, 5; Council of Europe, Project on Cybercime, 9 f.; Ministers of Justice EU, 1.
[268] Council of Europe, Cloud Computing, 5 f.; Council of Europe, T-CY, N 16 und 40.
[269] Council of Europe, Cloud Computing, 5 f.; European Commission, Working Document, 3, 32 f. und 245; Council of Europe, T-CY, N 39 ff. und 51; vgl. auch KLEIJSSEN/PERRI, 162 f.

Definition	Darknet-Verkaufsplattformen	Vgl. Kap. II. B 2.
	Online-Marktplätze im Clearnet	Vgl. FN 236.
	Social Media	Dienen der vielfach profilbasierten Vernetzung von Benutzern und deren Kommunikation und Kooperation über das Internet.[270]
	Dark Social Media[271]	Bezeichnet den Datenverkehr auf Websites, der von nicht verfolgbaren, nicht messbaren Quellen ausgeht, bspw. über persönliche E-Mails und oder Messenger-Dienste.[272]
	Cloud Computing	Vgl. Kap. IV. A 4. b.
Jur. Person / Betreiber des Service Provider	Darknet-Verkaufsplattformen	Nicht bekannt, Betreiber möchten selbst anonym bleiben
	Online-Marktplätze im Clearnet	in- oder ausländische jur. Personen
	Social Media	in- oder ausländische jur. Personen
	Dark Social Media	in- oder ausländische jur. Personen
	Cloud Computing	in- oder ausländische jur. Personen
Beispiele	Darknet-Verkaufsplattformen	Dream Market, Hansa, AlphaBay (alle offline)
	Online-Marktplätze im Clearnet	Ebay, tutti.ch, ricardo.ch
	Social Media	Facebook, Twitter, Instagram
	Dark Social Media	Whatsapp, Telegram, Threema
	Cloud Computing	iCloud, Dropbox, OneDrive, Google Drive[273]

[270] Gabler Wirtschaftslexikon, soziale Medien.
[271] Wird auch als «geheimes soziales Netzwerk» oder «Dark Traffic» bezeichnet.
[272] VON GEHLEN, Abschn. 1 f.
[273] BURGERMEISTER, 4.

Speicherort der Daten (bezüglich der aufgeführten Beispiele)	Darknet-Verkaufsplattformen	Wahrscheinlich in den meisten Fällen im Ausland[274]
	Online-Marktplätze im Clearnet	Bei ausländischen Providern liegen Daten im Ausland,[275] bei inländischen Providern (wahrscheinlich) im Inland.[276]
	Social Media	Bei den oben genannten Beispielen liegen die Daten auf Servern im Ausland.[277] Welche Daten, wo abgespeichert sind, ist den Providern grundsätzlich bekannt.
	Dark Social Media	-Daten von Whatsapp liegen auf Servern in den USA, welche Daten wo abgespeichert sind, ist bekannt.[278] -Daten von Telegram werden in mehreren Rechenzentren rund um den Globus gespeichert.[279]
	Cloud Computing	Daten liegen dezentral auf weltweit verstreuten Servern.[280]
Öffentlich zugängliche Daten	Darknet-Verkaufsplattformen	-Die Informationen auf digitalen Handelsplätzen sind grundsätzlich öffentlich zugänglich.[281] -Nachrichten in Chats sowie Angaben des Benutzerkontos sind hingegen privat.
	Online-Marktplätze im Clearnet	-Die Informationen auf digitalen Handelsplätzen sind grundsätzlich öffentlich zugänglich[282] -Nachrichten in Chats sowie Angaben des Benutzerkontos sind hingegen privat.
	Social Media	-Bei Twitter gibt es öffentliche und geschützte Profile, bei Facebook gibt es ebenfalls öffentliche und private. Dies ist von der jeweiligen Privatsphäre-Einstellung abhängig[283] -Nachrichten in Chats (z.B. Facebook Messenger) sind hingegen privat.
	Dark Social Media	-Chat-Nachrichten auf Whatsapp sind nicht öffentlich. -Bei Telegram können Nachricht in den Gruppen privat, aber auch öffentlich gestellt werden. Über Kanäle können öffentliche Nachrichten an unbegrenzt viele Leute gesendet werden.[284]
	Cloud Computing	-Es gibt öffentliche Daten in einer Cloud, die meistens als Ordner «public» oder «öffentlich» abrufbar sind[285] -Grundsätzlich sind die Daten aber privat.

[274] Vgl. FN 258.
[275] Bspw. bei Ebay liegen diese an verschiedenen Orten in den USA (SVERDLIK, Abschn. 10).
[276] Zu den Serverstandorten von Schweizer Online-Marktplätzen wie ricardo.ch und tutti.ch konnte leider keine Angabe gefunden werden.
[277] Gilt zumindest für die meistgenutzten Social Media in der Schweiz, welche allesamt im Ausland ihren Sitz haben. Facebook gibt bspw. an, dass sie global an 18 Standorten in Nordamerika, Europa und Asien Rechenzentren betreiben (PETERSON, Abschn. 1).
[278] Whatsapp, Unsere globalen Aktivitäten.
[279] Telegram, Frage: Reagiert ihr auf Datenabfragen?.
[280] EDÖB, Abschn. 5.
[281] IHWAS, 142.
[282] IHWAS, 142.
[283] HANSJAKOB, Überwachungsrecht N 430.
[284] Telegram, Frage: Was ist der Unterschied zwischen Gruppen und Kanälen?.
[285] Die öffentlich-zugänglichen Informationen sind nur von begrenztem Wert, da sie gerade bewusst geteilt werden. Zudem ist bspw. selbst der «Public-Ordner» der Dropbox nicht jedem einsehbar, da man dazu Kenntnisse über einen Link braucht (DALBY, 188).

Verwendung von Zugangsdaten	Darknet-Verkaufsplattformen	Benutzerkonten auf den Plattformen werden durch Zugangsdaten erreicht.
	Online-Marktplätze im Clearnet	Benutzerkonten auf den Plattformen werden durch Zugangsdaten erreicht.
	Social Media	Benutzerkonten auf Social Media werden häufig durch Zugangsdaten erreicht.[286]
	Dark Social Media	Benutzerkonten auf Whatsapp werden mithilfe der Mobiltelefonnummer des Nutzers erreicht.[287]
	Cloud Computing	Für den Zugriff auf die Cloud oder bestimmte Ordner wird meistens ein Link oder Passwort benötigt.[288]
Herausgabe von Daten an Behörden	Darknet-Verkaufsplattformen	Die anonymen Betreiber der Plattformen kooperieren nicht mit den Behörden.
	Online-Marktplätze im Clearnet	Keine Angaben gefunden
	Social Media	-Nicht öffentliche Informationen über Anwender von Twitter werden Strafbehörden im Rahmen eines rechtsgültigen Verfahrens mitgeteilt.[289] -Facebook teilt nach rechtmässiger Anfrage die Daten ihrer Nutzer mit den Strafverfolgungsbehörden.[290]
	Dark Social Media	-Whatsapp teilt Nutzerinformationen, um gem. anwendbaren Gesetzen, gerichtlichen Verfügungen oder auf Behördenanfragen zu reagieren.[291] -Gem. Angaben von Telegram wurden bisher noch keine Nutzerdaten an Dritte weitergegeben.[292]
	Cloud Computing	-Dropbox erteilt (Straf-)behörden bei rechtmässigen Anfragen Auskunft.[293] -Wenn die Auskunftsersuchen geltenden Gesetzen entsprechen gibt Google grundsätzlich über Daten ihrer Nutzer Auskunft.[294]

Tabelle 1: Abgrenzung der Darknet-Verkaufsplattformen zu anderen Service Providern.[295]

[286] Vgl. Kap. IV. A 4. a.
[287] Whatsapp, Informationen, die wir erheben.
[288] DALBY, 188.
[289] Twitter beantwortet jedoch Notfallanfragen auf Datenauskunft im Einzelfall unmittelbar unter Beachtung einschlägiger Gesetze. Zudem reagiert Twitter grundsätzlich umgehend auf Anträge, die im Rahmen eines Rechtshilfeabkommens oder -ersuchens gestellt werden (Twitter, Auskunftsanträge zu Twitter Accounts und Rechtshilfeabkommen).
[290] Facebook, Wie werden diese Informationen geteilt.
[291] Whatsapp, Gesetze, unsere Rechte und Schutz.
[292] Da die Daten von Telegram auf Servern in verschiedenen Ländern gespeichert sind, braucht es zur Datenherausgabe mehrere Gerichtsbeschlüsse aus verschiedenen Ländern. (Telegram, Frage: Reagiert ihr auf Datenanfragen?).
[293] Dropbox, Abschn. 1.
[294] Google, Datenschutzbestimmungen, Abschn. 1
[295] Selbst erstellte Tabelle.

B Verdeckte Ermittlungen und Fahndungen

Das eben Gesagte bedingt, dass neue Technologien wie das Darknet zu einer Rückkehr zu herkömmlichen personalen Ermittlungsmethoden führen, indem Ermittler versuchen, das Vertrauen von Einzelpersonen oder Gruppen zu gewinnen, um dadurch an Informationen zu gelangen, die man ansonsten über die IP-Adresse erhalten würde.[296] Die nachfolgenden Ausführungen beziehen sich auf die beiden Zwangsmassnahmen der VE und VF, wobei deren Bedeutung für die Ermittlungen im Darknet und die Herausforderungen dazu erklärt werden.

1. Begrifflichkeiten

a Die verdeckte Ermittlung (Art. 285a StPO)

Mit VE[297] sind Ermittlungsmethoden gemeint, bei der mithilfe einer falschen Identität (sog. urkundengestützter Legende) und durch täuschendes Verhalten Kontakte zu Zielpersonen geknüpft werden. Ziel der VE ist der Aufbau eines Vertrauensverhältnisses zur Zielperson und das Eindringen in ein kriminelles Umfeld, um besonders schwere Delikte aufzuklären.[298] Diese Delikte müssen im Straftatenkatalog von Art. 286 Abs. 2 StPO aufgeführt sein und zusätzlich muss dafür ein Tatverdacht bestehen.[299] Unter dem Begriff des kriminellen Umfelds wird allgemein die organisierte Delinquenz verstanden, wobei jedoch auch eine VE ausserhalb dieses Umfelds und bezogen auf einen Einzeltäter als Zielperson erlaubt ist.[300] Häufig richtet sich die VE jedoch gegen eine Personengruppe, da der verdeckte Ermittler nicht nur mit der Zielperson Geschäfte abwickeln, sondern darüber hinaus auch im Umfeld dieser Person zusätzliche Informationen über die Struktur der kriminellen Tätigkeit erhalten möchte.[301] Obwohl immer wieder betont wurde, dass die VE wegen des Aufbaus eines Vertrauensverhältnisses auf eine längere Dauer, i.d.R. mehrere Monate, ausgerichtet ist,[302] handelt es sich bei der Einsatzdauer nicht um ein Element von 285a StPO, weshalb unter Einhaltung aller Voraussetzungen auch kürzere Einsätze als VE gelten.[303] Als verdeckte Ermittler dürfen nur Angehörige der Polizei oder Personen, die vorübergehend für polizeiliche Aufgaben angestellt sind, tätig werden.[304]

b Die verdeckte Fahndung (Art. 298a StPO)

Bei der VF täuscht der verdeckte Fahnder, der zwingend ein Polizeiangehöriger sein muss,[305] über seine wahre Identität und Funktion und versucht, mit der Zielperson in Kontakt zu treten.[306] Obwohl die Regelungen der VF teilweise in Anlehnung an die Bestimmungen der Observation gem. 282 StPO entstanden sind, wird bei der Observation die Zielperson nur beobachtet, wohingegen diese bei der VF mittels Kommunikationsvorgängen getäuscht wird.[307] Für diese Täuschung dürfen verdeckte Fahnder im Un-

---

[296] HOSTETTLER, Darknet, 169; RÜCKERT/SAFFERLING, 9; IHWAS, 142; MEY, Darknet, N 133 f.; ZÖLLER, 276.
[297] Eine Legaldefinition der VE und VF wurde erst mit dem Bundesgesetz über die verdeckte Ermittlung und Fahndung und der damit verbundenen Änderung der StPO per 1.5.2013 eingeführt (BSK StPO-KNODEL, Art. 285a N 4 und 298a N 1.).
[298] Zum Ganzen KNODEL, StPO-Kommentar, Art. 285a N 5; Art. 285a StPO.
[299] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 285a N 8 und Art. 286 N 3 und 6.
[300] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 285a N 7a; Gl.M. KNODEL, StPO-Kommentar, Art. 285a N 14; HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 285a N 51; A.M. DONATSCH/SCHWARZENEGGER/WOHLERS, 241.
[301] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 285a N 51.
[302] RK-N, Bericht von 2012 zur VE, 5595; bereits im Grundsatz BGE 134 IV 266 E. 3.3 S. 273.
[303] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 285a N 9. A.M. BSK StPO-KNODEL, Art. 285a N 11; RIKLIN, Kommentar StPO, vor Art. 285a-298 N 5.
[304] BSK-StPO KNODEL, Art. 285a N 5; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 287 N 2 f.
[305] BSK StPO-KNODEL, Art. 298a N 3; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 298a N 3.
[306] Vgl. Art. 298a Abs. 1 StPO.
[307] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 298a N 2; BSK StPO-KNODEL, Art. 298b N 7.

terschied zu verdeckten Ermittlern keine mittels Urkunden abgesicherten falschen Identitäten (Legenden) gebrauchen.[308] Die verdeckten Fahnder dürfen sich jedoch einfacheren Lügen und Täuschungen bedienen.[309] Ein klassischer Anwendungsfall der VF stellt das Schein- oder Probegeschäft dar, welches explizit in Art. 298a Abs. 1 StPO vorgesehen ist.[310] Ihm kommt auch bezüglich den Ermittlungen im Darknet eine wichtige Rolle zu.[311] Mit der VF wird die Aufklärung von Vergehen oder Verbrechen bezweckt, für die wie bei der VE ein Tatverdacht bestehen muss.[312] Als Vergehen resp. Verbrechen gelten gem. Art. 10 StGB Straftatbestände, die mit einer Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe resp. Freiheitsstrafe von mehr als drei Jahren geahndet werden. Somit ist der Einsatz einer VF bei Übertretungen, welche mit Busse sanktioniert werden (vgl. Art. 103 StGB), nicht zulässig.[313] Im Unterschied zur VE wird die Identität des verdeckten Fahnders nach Beendigung eines Einsatzes im eröffneten Strafverfahren gegen die Zielperson immer preisgegeben. Eine Anonymitäts-Zusicherung ist nicht vorgesehen.[314] Ebenfalls gegensätzlich zur VE ist die VF auf eine kürzere Dauer ausgelegt. Falls ein Einsatz jedoch länger als einen Monat dauern sollte, kann dieser gem. Art. 298b Abs. 2 StPO mittels Genehmigung durch die StA verlängert werden.[315]

2. Abgrenzung zwischen der VE und der VF

Eine akkurate Abgrenzung zwischen der eingriffsschwächeren VF und der eingriffsstärkeren VE ist für die Strafrechtsbehörden von grosser Relevanz, weil deren korrekte Vorgehensweise - insb. die Einhaltung von Gültigkeitsvorschriften im Strafverfahren - die Verwertbarkeit der erlangten Beweise sicherstellt.[316]

a Legende

Die VE setzt zwingend voraus, dass die Kontaktaufnahme zur Zielperson unter Verwendung einer durch Urkunden abgesicherten falschen Identität (Legende) erfolgt.[317] Dagegen dürfen sich verdeckte Fahnder mittels einer raffinierten Legende milieugerecht und szenetypisch verhalten, jedoch keine urkundengestützte Legende einsetzen (vgl. Art. 298a Abs. 2 StPO).[318] Da sich der Urkundenbegriff nicht aus dem Gesetzestext ergibt, haben sich in der Lehre zwei Ansichten entwickelt.[319] Dabei geht die eine, von einem materiell-strafrechtlichen Urkundenbegriff (Art. 110 Ziff. 4 StGB bzw. 251 ff StGB) und die andere von einem strafprozessualen Begriff (Art. 192 Abs. 2 StPO) aus.[320] Als materiell-strafrechtliche Urkunden gelten Schriften, die bestimmt und geeignet sind, eine Tatsache von rechtlicher Bedeutung zu beweisen.[321] Der strafprozessuale Urkundenbegriff ist jedoch umfassender und versteht darunter ein

[308] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 298a N 1.
[309] RK-N, Bericht von 2012 zur VE, 5595; BSK StPO-KNODEL, Art. 298a N 5.
[310] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 298a N 10.
[311] Vgl. Anh. 2: Interview WALDER, Frage 3.2.
[312] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 298a N 4.
[313] RK-N, Bericht von 2012 zur VE, 5599.
[314] BSK StPO-KNODEL, Art. 288 N 5 ff.
[315] RK-N, Bericht von 2012 zur VE, 5598 f.
[316] Vgl. Art. 289 Abs. 6 StPO; RONC/VAN DER STROOM/MEYER, 302; GLESS, Beweisverwertungsverbote, 5
[317] BSK StPO-KNODEL, Art. 285a N 5 und 7.
[318] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 285a N 62.
[319] BSK StPO-KNODEL, Art. 285a N 8.
[320] Von einem materiell-strafrechtlichen Urkundenbegriff ausgehend: HANSJAKOB, Bestimmungen der VF und VE, 217; RONC/VAN DER STROOM/MEYER, 304 f.; MUGGLI, Diss., 273 f.; A.M. und von einem strafprozessualen Urkundenbegriff ausgehend: SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 285a N 4; BSK StPO-KNODEL, Art. 285a N 8; JOSITSCH/MULLE, 494.
[321] Art. 110 Abs. 4 StGB.

Schriftstück mit gedanklichem Informationsgehalt, das beweisbildend ist.[322] Obwohl somit beide Begriffe Ausweisschriften, wie Identitäts- oder Kreditkarten umfassen, fallen unter den strafprozessualen Urkundenbegriff auch E-Mail-Adressen, Facebook-Profile oder Websites mit falschen Identitäten.[323] Der Unterscheidung der Urkundenbegriffe kommt auch im Zusammenhang mit den Darknet-Ermittlungen eine zentrale Bedeutung zu, da die ermittelnden Polizisten wohl häufig z.B. «falsche» E-Mail-Adressen oder Darknet-Benutzerkonten einsetzen müssen. Würde für die Legende somit auf den strafprozessualen Urkundenbegriff abgestellt, müsste daher eine VE angeordnet werden.[324]

Mit dieser Legenden-Problematik musste sich auch das BGer am 28. September 2016 befassen und hatte zu entscheiden, ob die verdeckte Ermittlungstätigkeit eines Zürcher Polizisten in einem Chatroom[325] als nicht bewilligungspflichtige VF gem. Art. 298a StPO oder aber als bewilligungsbedürftige VE i.S.v. Art. 285a StPO zu behandeln war.[326] Dabei stellte das BGer auf den materiell-strafrechtlichen Urkundenbegriff ab.[327] Es kam deshalb konträr zu früheren Entscheiden[328] zum Schluss, dass «eine durch Urkunden abgesicherte Legende i.S.v. Art. 285a StPO […] bei Ermittlungen im Internet in der Regel […] gar nicht nötig [ist]. Wer sich im Chat unter einem Nickname registriert, über Namen, Wohnort, Alter und Aussehen unwahre Angaben macht, eine E-Mail-Adresse verwendet, die auf einen falschen Namen oder auf eine Fantasiebezeichnung lautet, und Fotos verschickt, braucht sich nicht mit Urkunden zu identifizieren.»[329] Solche Legendierungselemente würden auf jeden Fall keine durch Urkunden abgestützte Legende i.S.v. Art. 285a StPO schaffen.[330] Dieses Urteil wurde u.a. von RONC und VAN DER STROOM kritisiert, welche feststellten, dass aufgrund des gewählten Urkundenbegriffs für den Bereich der strafprozessualen Internetermittlungen (beinahe) keine Situationen mehr vorstellbar sind, in denen die verdeckte Massnahme in Chaträumen als VE i.S.v. Art. 285a StPO zu klassifizieren wäre. Die VF i.S.v. Art. 298a StPO würde als Generalnorm gelten.[331]

b Vertrauensverhältnis

Eng im Zusammenhang mit der Legende steht der Aufbau eines Vertrauensverhältnisses. Dabei versucht der verdeckte Ermittler unter Verwendung einer Legende das Vertrauen der Zielperson zu gewinnen, um ein kriminelles Geschäft abzuschliessen. D.h. der verdeckte Ermittler überwindet Barrieren, welche die Zielperson davon abhält, mit oder gegenüber jedem wahllosen Geschäftspartner straffällig zu werden. Für den verdeckten Ermittler ergibt sich daraus die Schwierigkeit, dass er zum einen das Vertrauen der Zielperson gewinnen und zum anderen beachten muss, dass er nicht als zu interessanter Geschäftspartner auftritt und die Zielperson zu strafbaren Handlungen verleitet, die sie ansonsten nicht begehen

[322] Botschaft StPO, 1213 f.; BSK StPO-BÜRGISSER, Art. 192 N 5.
[323] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 285a N 4; HANSJAKOB, Bestimmungen der VF und VE, 217; BSK StPO-KNODEL, Art. 285a N 8.
[324] Vgl. BSK StPO-KNODEL, Art. 285a N 8.
[325] W.H. zum Sachverhalt: Der Beschuldigte X lernte unter einem Pseudonym die mutmasslich 14-jährige «Sabrina» (Polizeiangehöriger) in einem Chatroom kennen. Die beiden schrieben über den Chatroom, wobei X offen zugab, dass er Sex suche. Anschliessend wurde ein Treffpunkt am Bahnhof Zürich vereinbart, wo X dann nicht auf «Sabrina», sondern auf einen Beamten der Stadtpolizei Zürich traf, der sich unmittelbar zu erkennen gab (BGE 143 IV 27 Sachverhalt, lit. A S. 28).
[326] BGE 143 IV 27 E. 3.2 S. 34.
[327] RONC/VAN DER STROOM, 347.
[328] Insb. BGE 134 IV 266. In diesem sog. «manuela_13» -Fall entschied das BGer, dass es sich nicht um eine VF handelte und erweiterte den Anwendungsbereich der VE massiv (JOSITSCH/MULLE, 492; RIKLIN, Kommentar StPO, Vor Art. 285a-298, N 2; RONC/VAN DER STROOM, 348).
[329] BGE 143 IV 27 E. 4.1.3 S. 35; m.w.H. HANSJAKOB, verdeckte polizeiliche Tätigkeit, 248.
[330] BGE 143 IV 27 E. 4.1.3 S. 36.
[331] RONC/VAN DER STROOM, 348.

würde.[332] Falls kein Aufbau eines Vertrauensverhältnisses notwendig ist, weil die Zielperson mit jedem Geschäftswilligen schnell und anonym ein Geschäft abwickeln will, besteht die vorgenannte Problematik einer möglichen Tatprovokation nicht, weshalb eher von einer VF auszugehen ist.[333]

Die Definition und das Vorliegen eins Vertrauensverhältnisses ist grundsätzlich eher schwierig.[334] Die Lehre scheint sich v.a. bezüglich der Bedeutung des Entstehungszeitpunkts eines Vertrauensverhältnisses einig zu sein, d.h. sobald ein solches vorliegt, ist von einer VE und keiner VF mehr auszugehen.[335] Diese evolutive Betrachtungsweise vertrat das BGer auch im vorhin angesprochenen Entscheid BGE 143 IV 27.[336] Es kam zum Schluss, dass der Austausch von 180 SMS zwischen dem Beschuldigten und dem Polizisten zur Vereinbarung eines Sexualkontakts zwar über eine nur flüchtige Begegnung hinausging, jedoch noch kein persönlich intensiver Kontakt vorlag. Auch das Zustellen von Fotos und die Mitteilung der E-Mail-Adresse sowie der Telefonnummer habe noch kein Vertrauensverhältnis begründet.[337] RONC ET AL., welche bereits grundsätzlich die evolutive Betrachtungsweise kritisieren, meinen, dass dadurch unvorhersehbar und unklar ist, wann ein Vertrauensverhältnis besteht.[338] Sie können deshalb dieser Entscheidung des BGer nicht beipflichten.[339]

c Relevanz der VF und VE bezüglich Ermittlungen im Darknet

Der eben erläuterte Entscheid hat bezüglich Ermittlungstätigkeiten im Internet resp. Darknet zur Rechtssicherheit für die Strafverfolgungsbehörden beigetragen. Da die Dauer des Einsatzes, sowie das Vertrauensverhältnis als Abgrenzungskriterium zwischen der VE und VF weniger praktikabel sind, gilt die urkundengestützte Legende als massgebliches Kriterium, das objektiv klar fassbar ist.[340] Eine urkundengestützte Legende ist im Zusammenhang mit dem Darknet mehrheitlich nicht notwendig, was einerseits daran liegt, dass üblicherweise bei der Registrierung auf einer Darknet-Verkaufsplattform nur ein fiktiver Benutzername angegeben werden muss und es kein eigentliches Identitätsmanagement gibt.[341] Somit können sich auch die Ermittler der Strafbehörde auf einer oder mehreren Verkaufsplattformen unter Verwendung eines beliebigen Nicknames registrieren, ein Benutzerkonto einrichten und anschliessend mit anderen Benutzern in Kontakt treten.[342] Andererseits sind urkundengestützte Legenden aber auch obsolet, weil im Darknet mit Kryptowährungen bezahlt wird, die sich nicht auf Personen zurückverfolgen lassen, und deshalb keine Bankkonten oder Kreditkarten für die Ermittler eröffnet resp. erstellt werden müssen.[343]

---

[332] Zum Ganzen HANSJAKOB, Bestimmungen der VF und VE, 216; BSK StPO-KNODEL, Art. 285a N 12. Es läge somit eine Tatprovokation vor.
[333] HANSJAKOB, Bestimmungen der VF und VE, 216.
[334] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 285a N 6.
[335] RONC/VAN DER STROOM/MEYER, 304.
[336] RONC/VAN DER STROOM, 349.
[337] BGE 143 IV 27 E. 4.2.3 S. 37 f.; m.w.H. RONC/VAN DER STROOM, 349.
[338] RONC/VAN DER STROOM/MEYER, 304.
[339] RONC/VAN DER STROOM, 349.
[340] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 285a N 40; Gl.M. RIKLIN, Kommentar StPO, Vor Art. 285a–298 N 5; SCHMID/JOSITSCH, Handbuch StPO, N 1204a; A.M. BSK StPO-KNODEL, Art. 285a N 10.
[341] Für die Registrierung auf einer Verkaufsplattform ist normalerweise lediglich ein fiktiver Benutzername anzugeben. Weitere Angaben zum Identitätsmanagement, wie es auf Social Media normal ist, sind bei der Anmeldung nicht notwendig (IHWAS, 143).
[342] Anh. 2: Interview WALDER, Frage 3.3; IHWAS, 144.
[343] Anh. 2: Interview WALDER, Frage 3.3.

Aber nicht nur die fehlende Notwendigkeit einer urkundengestützen Legendierung, sondern auch andere Spezifika der Darknet-Ermittlungen führen dazu, dass die Ermittlungen überwiegend als VF durchgeführt werden können.[344] So stehen im Fokus der Ermittler Zielpersonen, die an einem Kauf (z.B. Waffen) interessiert sind, oder Verkäufer, die über ihr eigenes Benutzerkonto Waren (wie bspw. Drogen) verkaufen möchten.[345] Da sowohl Käufer als auch Verkäufer grundsätzlich mit jedem Interessenten möglichst schnell und anonym ein Geschäft abschliessen möchten, muss eine weniger intensive Beziehung zur Zielperson aufgebaut werden,[346] was eher dem Charakteristikum der VF entspricht.[347] Wie die Experteninterviews aber verdeutlicht haben, werden trotzdem bei schwerwiegenden Delikten, die im Straftatenkatalog von Art. 286 Abs. 2 StPO enthalten sind, vereinzelt auch VE im Zusammenhang mit Darknet-Ermittlungen angeordnet.[348] Grundsätzlich sind VE, allgemein und nicht nur in Bezug auf das Darknet, in der Schweiz selten.[349] Obwohl keine Statistiken vorhanden sind, gehen HANSJAKOB und PAJAROLA davon aus, dass auch in den grossen Kantonen jährlich nicht mehr als eine Handvoll VEs angeordnet und bewilligt werden, wogegen in kleineren Kantonen häufig die notwendige Infrastruktur und die Ressourcen zur Durchführung solcher Einsätze noch fehlen.[350]

3. Voraussetzungen für die verdeckte Fahndung gem. Art. 298b StPO

Aufgrund ihrer wichtigeren Bedeutung im Zusammenhang mit Darknet-Ermittlungen sollen nachfolgend die Voraussetzungen gem. Art. 298b-298c StPO zur Anordnung einer VF erläutert werden.

a Personelle Voraussetzungen

Zu den personellen Voraussetzungen gehört, dass als verdeckte Fahnder gem. Art. 298c StPO ausschliesslich Angehörige von in- oder ausländischen Polizeicorps eingesetzt werden können.[351] Eine spezifische Ausbildung als verdeckter Fahnder wäre zwar begrüssenswert, ist aber nicht erforderlich.[352] Wie ZAUGG jedoch erklärt, sollten die verdeckten Fahnder, welche im Darknet eingesetzt werden, einerseits eine gewisse IT-Affinität besitzen, und andererseits müssen sie versierte Polizisten sein, die sich in die Straftäter hineinzuversetzen wissen. Da dies eine gewisse Erfahrung erfordert, verfügen Personen, welche in diesem Fachbereich der Kriminalpolizei Bern arbeiten über mindestens 15 Dienstjahre.[353] Zudem ist für die verdeckten Fahnder aber auch entscheidend, dass sie eingehende Kenntnisse der Szene sowie der bewährten Abläufe und der typischen Kommunikation innerhalb der Darknet-Plattformen und Foren kennen, damit sie mit den anderen Nutzern aktiv kommunizieren können.[354] Beaufsichtigt wird der verdeckte Fahnder durch eine Führungsperson, die Weisungen und Instruktionen erteilt sowie den Einsatz des verdeckten Fahnders überwacht und dokumentiert.[355]

---

[344] Anh.1: Interview WERREN/ZAUGG, Frage 3.4-3.6; Anh. 2: Interview WALDER, Frage 3.3; Anh. 3: Interview EUGSTER, Frage 2.8.
[345] Anh. 1: Interview WERREN/ZAUGG, Frage 2.7; Anh. 2: Interview WALDER, Frage 1.6.
[346] Vgl. HANSJAKOB bezieht seine Aussage auf Kleindealer, dies trifft m.E. aber auch auf Verkäufer und Käufer auf Darknet-Plattformen zu (HANSJAKOB, Bestimmungen der VF und VE, 216).
[347] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 285a N 62.
[348] Anh. 1: Interview WERREN/ZAUGG, Frage 3.4.
[349] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 285a N 59; ZAUGG weist daraufhin, dass die VE in der Schweiz nicht so präsent und ausgeweitet ist im Vergleich zu anderen Ländern wie bspw. Deutschland, USA oder Kanada (Anh. 1: Interview WERREN/ZAUGG, Frage 3.4).
[350] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 285a N 59; Gemäss ZAUGG haben viele Kantone keine verdeckten Ermittler, weder im Internet noch allgemein. Ob ein Kanton solche hat, ist eine Grössen- aber auch Ressourcenfrage bei den Polizeicorps (Anh. 1: Interview WERREN/ZAUGG, Frage 3.4).
[351] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298c N 1; BSK StPO-KNODEL, Art. 298c N 2.
[352] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298c N 1.
[353] Anh. 1: Interview WERREN/ZAUGG, Frage 3.4.
[354] KRAUSE, 679 f.
[355] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298c N 6; BSK StPO-KNODEL, Art. 298c N 5.

b Materielle Voraussetzungen

In materieller Hinsicht kann eine VF gem. Art. 298b Abs. 1 lit. a StPO bei hinreichendem Tatverdacht nur zur Aufklärung von Verbrechen und Vergehen, nicht aber für Übertretungen angeordnet werden. Da die VF häufig in einem Anfangsstadium der Ermittlungen eingesetzt wird, genügt ein «vager» Tatverdacht, der sich gegen eine bekannte oder unbekannte Täterschaft richten kann.[356] Gleichzeitig setzt eine VF aufgrund ihrer schwereren Eingriffsintensität aber eine erheblichere Verdachtslage voraus als bspw. die Observation, für welche gem. Art. 282 Abs. 1 lit. a StPO konkrete Anhaltspunkte ausreichend sind.[357] In Bezug auf die Ermittlungen auf Darknet-Plattformen sind verschiedene Konstellationen denkbar, wie ein hinreichender Tatverdacht gegenüber einer unbekannten Zielperson begründet werden kann. So kann dieser bspw. durch die gewonnenen Erkenntnisse aus den polizeilichen Vorermittlungen entstehen (vgl. Kap. III. A)[358] oder durch Hinweise von nationalen und internationalen Polizeibehörden.[359] Da sich der Tatverdacht zwingend gegen Vergehen oder Verbrechen richten muss, stehen im Fokus der Strafverfolger Zielpersonen, die auf Plattformen oder Foren illegale Pornografie austauschen oder handeln, sich auf solchen Plattformen Waffen kaufen oder solche verkaufen möchten, sowie Personen, die über ihr Benutzerprofil Drogen verkaufen (vgl. Kap. II. C 1.).[360] Wie bereits der Wortlaut[361] von Art. 298b Abs. 1 lit. a StPO verdeutlicht, steht die VF zur Aufklärung von begangenen Delikten zur Verfügung. Besteht ein konkreter Verdacht, dass die Zielperson bereits strafbare Handlungen beging, darf eine VF aber auch bei gegenwärtig stattfindenden Delikten angeordnet werden.[362] Bei den Darknet-Ermittlungen dürfte dies in den meisten Fällen gegeben sein: So zeigen bspw. die Rezensionen auf den Verkaufsplattformen, wie viele Drogen ein Verkäufer bereits abgesetzt hat, was ein wichtiger Hinweis auf bereits begangene strafbare Handlung darstellt.[363] Nicht zulässig sind gem. dem Geltungsbereich der StPO rein präventive Einsätze von verdeckten Fahndern,[364] welche im Rahmen der Vorermittlungen gemacht werden, wenn noch kein hinreichender Tatverdacht vorliegt.[365] Obwohl die Abgrenzung zwischen präventiven und repressiven VF teilweise schwierig ist, sind die praktischen Probleme gering, da die Voraussetzungen und das Verfahren in vielen PolG den Bestimmungen der StPO entsprechen.[366] Bezüglich Subsidiarität gilt es Art. 298b lit. b StPO zu beachten.

c Zuständigkeit und Verfahren

Für die Anordnung einer VF ist im Ermittlungsverfahren nach Art. 306 ff StPO die Polizei und nach Eröffnung der Untersuchung die StA nach Art. 309 StPO zuständig.[367] Dabei wird die VF häufig im Ermittlungsverfahren eingesetzt, weil abgeklärt werden muss, ob eine Straftat begangen wurde und um wen es sich beim Täter handelt.[368] Falls die StA eine VF zuhanden der Polizei anordnet, erfolgt diese

---

[356] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 298b N 3. HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 1 f.
[357] BSK StPO-KNODEL, Art. 298b N 7.
[358] Vgl. auch Anh. 2: Interview WALDER, Frage 3.2.
[359] Vgl. im Fall von Tobias Kuster (vgl. Kap. II. C 2.) wurden die Schweizer Strafbehörden von Europol über die Hinweise der australischen Behörden informiert.
[360] Anh. 1: Interview WERREN/ZAUGG, Frage 1.6; Anh. 2: Interview WALDER, Frage 1.3.
[361] «der Verdacht besteht, ein Verbrechen oder Vergehen **sei begangen worden»** (Hervorhebungen durch die Autorin hinzugefügt).
[362] Zum Ganzen HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 3.
[363] Anh. 2: Interview WALDER, Frage 3.1 und 3.2.
[364] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 4; Eine Minderheit der Kommission wollte auch eine Regelung für die präventiven Einsätze in der StPO, was jedoch abgelehnt wurde (RK-N, Bericht von 2012 zur VE, 5596 f. und 5599).
[365] TIEFENTHAL, 395 N 4.
[366] BGE 140 I 353 E. 5.2; BGE 143 IV 27 E. 2.5 und 3.2, HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 3; Nach der Einführung der StPO im Jahr 2011 bestand bei vielen Kantonen diesbezüglich eine Gesetzeslücke in den PolG, die mittlerweile jedoch in den meisten Kantonen geschlossen wurden (TIEFENTHAL, 406, N 19 und 416 N 3).
[367] BSK StPO-KNODEL, Art. 298b N 1; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 298b N 9.
[368] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 9.

normalerweise schriftlich unter Angabe des Verdachts, des Sachverhalts und der abzuklärenden Straftatbestände, den Ausführungen zur Zielperson sowie der Person, welche als verdeckter Fahnder eingesetzt werden soll.[369] Wird die VF durch die Polizei angeordnet, wäre grundsätzlich jeder Polizeiangehörige zur Anordnung berechtigt.[370] Eine Anordnung der VF durch die Polizei ist nur auf einen Monat befristet.[371] Soll die VF länger dauern, muss gem. Art. 298b Abs. 2 StPO eine Bewilligung zur Verlängerung durch die StA eingeholt werden.[372] Anschliessend muss die StA prüfen, ob die Voraussetzungen für eine VF erfüllt sind, oder ob diese als VE weiterzuführen ist, weil eine urkundengestützte Legende eingesetzt werden muss.[373] Die StA kann die VF damit um einen bis zu drei Monate verlängern.[374]

4. Verfolgung von Drogendelikten verglichen mit Straftaten bezüglich Kinderpornografie

Natürlich sind auch den verdeckten Ermittlern und Fahndern bei ihrer Tätigkeit gewisse Grenzen gesetzt. So hält Art. 293 StPO fest, dass verdeckte Ermittler und Fahnder (Verweisnorm in Art. 298c Abs. 2 StPO) vorbehältlich von Abs. 3 für begangene Delikte strafbar sind.[375] Deren Strafbarkeit ist unter Beachtung möglicher vorliegender Rechtfertigungsgründe stetig zu prüfen. Als solcher Rechtfertigungsgrund gelten Probe- und Scheinkäufe. Geht es um Probekäufe im Betäubungsmittelhandel, korrespondiert Art. 293 Abs. 3 StPO mit Art. 294 StPO, weshalb Art. 293 Abs. 3 StPO für den Bereich der Betäubungsmittelkriminalität überflüssig wäre. Daraus lässt sich schliessen, dass der Gesetzgeber auch Probekäufe aus anderen Bereichen z.B. aus verbotenem Waffenhandel oder Pornographie durch den Art. 293 Abs. 3 StPO erfassen wollte.[376] Sind die Probekäufe somit zur Anbahnung des Hauptgeschäfts erforderlich, bleiben sie für die verdeckten Ermittler und Fahnder straflos (Verweisnorm in Art. 298a Abs. 1 StPO).[377] Die Straflosigkeit für die Probekäufe wird durch den Umstand begründet, dass sich der Vorsatz der verdeckten Ermittler und Fahnder darauf fokussiert, die Ware aus dem Verkehr zu ziehen, wohingegen die einschlägigen Strafbestimmungen gerade die Inverkehrbringung bestrafen.[378]

a Verfolgung von Delikten gegen das BetmG und WG

Die StPO sieht in Art. 294 einen umfassenderen Rechtfertigungsgrund für Betäubungsmitteldelikte vor, der sich nicht nur auf Probekäufe bezieht, sondern für sämtliche Delikte gem. Art. 19 sowie 20-22 BetmG gilt.[379] Obwohl sich die Verweisungsnorm von Art. 298 Abs. 2 StPO auch auf Art. 294 bezieht, ist für KNODEL fraglich, ob dieser Artikel vollumfänglich für den verdeckten Fahnder Anwendung findet. Denn anders als die VE muss die VF nicht richterlich bewilligt werden, weshalb der verdeckte Fahnder praktisch keiner Kontrolle untersteht und er bei der Begehung von Straftaten zurückhaltend sein soll. Für KNODEL ist deshalb schwierig vorstellbar, dass ein verdeckter Fahnder im Rahmen seines

[369] In Ausnahmefällen können die Anordnungen auch mündlich sein, wobei sie entsprechend zu dokumentieren sind (HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 10); Gl.M. SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 298b N 2.
[370] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 298b N 2; Vgl. auch Art. 198 Abs. 1 lit. c StPO.
[371] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 13.
[372] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 13.
[373] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 14.
[374] KNODEL, SCHMID und JOSITSCH sprechen sich für eine Verlängerung um einen Monat aus, wohingegen HANSJAKOB und PAJAROLA eine solche von drei Monaten annehmen (BSK StPO-KNODEL, Art. 298b N 10; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 298b N 5; A.M. HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 298b N 17).
[375] BSK StPO-KNODEL, Art. 293 N 15.; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 293 N 9.
[376] Zum Ganzen BSK StPO-KNODEL, Art. 293 N 9 und N 15 und Art. 294 N 7; Gl.M. SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 293 N 5 f.; MUGGLI, Arbeitstagung, N 21.
[377] BSK StPO-KNODEL, Art. 293 N 9; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 293 N 6.
[378] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 293 N 31.
[379] BSK StPO-KNODEL, Art. 294 N 7, falls die VE zur Verfolgung einer Straftat gem. Art. 286 Abs. 2 lit. f stopp zum Einsatz kommt, geht für Probekäufe Art. 294 gegenüber Art. 293 Abs. 3 als lex specialis vor; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 294 N 2 ff.

Einsatzes i.S.v. Art. 19 Abs. 1 BetmG Betäubungsmittel vermittelt, den unerlaubten Verkehr finanziert oder gar öffentlich eine Gelegenheit zum Erwerb oder Konsum von Betäubungsmitteln bekannt gibt. KNODEL empfindet den Verweis in Art. 298c auf Art. 294 StPO als überbordend und verneint die komplette Anwendung von Art. 294 StPO auf die VF.[380] Generell beschränkt sich die Straflosigkeit der Ermittler gem. Art. 294 StPO nur auf die im Zusammenhang mit dem Auftrag begangenen Taten und somit auf solche, die auf Weisungen der Führungsperson beruhen.[381] Zusätzlich regelt auch das BetmG in Art. 23 Abs. 2 die Straflosigkeit von Beamten, die mit der Bekämpfung des unerlaubten Betäubungsmittelverkehrs beauftragt sind und zu Ermittlungszwecken selber ein Angebot von Betäubungsmitteln annehmen, auch wenn sie ihre Identität und Funktion nicht offenlegen.[382] Die eben genannten Bestimmungen in der StPO und dem BetmG beziehen sich sowohl auf verdeckte Ermittler als auch auf Fahnder (vgl. Art. 298c Abs. 2 StPO).[383]

Obwohl sich die Literatur bezüglich der Anwendbarkeit und den Möglichkeiten von Drogen-Scheingeschäften durch verdeckt ermittelnde Polizeiangehörige häufig nur mit dem offline Handel auf der Gasse auseinandersetzt,[384] werden solche Scheingeschäfte bezüglich Drogen und Waffen gestützt auf Art. 294 StPO resp. 293 Abs. 3 StPO bei Waffenkäufen auch von verdeckten Ermittlern und Fahndern bei Einsätzen im Darknet getätigt.[385] Dabei hoffen die Fahnder einerseits, dass sie von den Zielpersonen Angaben und Rückschlüsse zu deren Identifikation erhalten oder andererseits Anhaltspunkte für weitere Ermittlungen gewinnen können.[386] Falls die bestellten Waren tatsächlich geliefert werden, können auch «traditionelle» polizeiliche Ermittlungsmethoden wie daktyloskopische Untersuchungen[387] durchgeführt werden.[388] Lassen sich auf den Waren allenfalls Fingerabdrücke oder DNA-Spuren finden, liefern diese neue Ermittlungsansätze, wenn der Spurenleger bereits in den einschlägigen Datenbanksystemen bei der Polizei geführt ist.[389]

b Verfolgung von Delikten im Zusammenhang mit harter Pornografie

Im Unterschied zu den Scheinkäufen von Drogen und Waffen stellt sich die Situation für die Ermittlungstätigkeit im Zusammenhang mit harter Pornografie aus einer tatsächlichen und juristischen Perspektive schwieriger dar.[390] Aus tatsächlicher Sicht besteht die Herausforderung darin, dass sich der Austausch von Kinderpornografie im Vergleich zum Handel mit inkriminierten Gütern wie Drogen oder Waffen nicht in die reale Welt verschieben muss, und damit die für Ermittlungsansätze wichtige Offline-Komponente fehlt.[391] Aus einem juristischen Gesichtspunkt dürfen die verdeckten Ermittler resp. Fahnder zwar gestützt auf den vorhin erwähnten Rechtfertigungsgrund gem. Art. 293 Abs. 3 StPO kinderpornografisches Material annehmen,[392] resp. downloaden, um es als Beweis sicherzustellen und nach

[380] Zum Ganzen BSK StPO-KNODEL, Art. 298c N 9.
[381] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 294 N 3; Gl. M. BSK StPO-KNODEL, Art. 294 N 4 f.
[382] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 294 N 2.
[383] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 294 N 2.
[384] HOSTETTLER, nennt den einmaligen Scheinkauf von Betäubungsmitteln (etwa bei «Kügeli-Dealern») durch einen kurzfristigen Einsatz, der ohne besondere durch Urkunden gestützte Legende getätigt wird, als klassisches Beispiel für die VF (HOSTETTLER, zulässige Einwirkung bei VF und VE, 196).
[385] Anh. 2: Interview WALDER, Frage 3.2; KRAUSE, 680; SULIAK, Frage 2.
[386] MEY, Darknet, N 134.
[387] Die Daktyloskopie bezeichnet das Fingerabdruckverfahren, welches ein altbekanntes Verfahren zur Identifikation von Personen ist. Es nutzt den Umstand, dass die sog. Papillarlinien an Händen und Fingern bei jedem Menschen anders sind (Fedpol, Fingerabdrücke und AFIS).
[388] KRAUSE, 680; IHWAS, 147; VON HEIN, Abschn. 4.
[389] ZÖLLER, 277.
[390] SULIAK, Antwort 2 und 3; MEY, Darknet, N 134.
[391] RÜCKERT/GOGER, 374.
[392] MUGGLI, Arbeitstagung, N 21.

Hinweisen betreffend Ort und Zeit des Missbrauchs, den Identitäten der Opfer oder den Uploadern zu suchen.[393] Ihnen ist es jedoch untersagt, selber solche Bilder anzubieten, um ihre «Tarnung» aufrechtzuerhalten,[394] da sie sich gem. Art. 197 Abs. 4 StGB strafbar machen, wenn sie pornografische Ton- oder Bildaufnahmen sowie Abbildungen, die sexuelle Handlungen mit Minderjährigen zum Inhalt haben, zugänglich machen[395] oder überlassen.[396]

Da auch die Straftäter von dieser rechtlichen Schranke wissen, hat sich bereits vor der Erfindung des Darknets in der Kinderpornografie-Szene eine verwerfliche Methode namens «Keuschheitsprobe» entwickelt. Damals wurde bekannt, dass es den Polizeiangehörigen gelang, sich in Passwort-geschützte Foren einzuschleichen.[397] Die sog. Keuschheitsprobe gilt als Vertrauensbeweis,[398] indem man als Interessent auf einem Forum oder einer Plattform nur Einlass erhält, wenn man selbst kinderpornografisches Material in Form von Bild- oder Videodateien hochlädt,[399] oder dieses an einen Moderator sendet, der den Benutzer freischaltet.[400] Für diese moralisch fragwürdige Abgabe von kinderpornographischem Material hält die StPO momentan keinen gesetzlichen Strafausschlussgrund resp. Rechtfertigungsgrund bereit.[401] Die sich daraus ergebende beschränkte Straflosigkeit des Ermittlers kann zwar aus rechtsstaatlichen Gründen begrüsst werden, erschwert aber gleichzeitig die Anwendung des Ermittlungsinstruments.[402] Um dieses Problem in der Praxis zu umgehen und trotzdem Einlass in solche Foren oder auf Plattformen zu erhalten, ist die Kreativität der verdeckten Fahnder gefragt, welche die Begehung einer Straftat zumindest vortäuschen dürfen.[403] Sie deuten bspw. an, dass sie ein Bild gesendet haben, welches jedoch beim Empfänger nicht heruntergeladen werden kann, weil es einen Defekt hat. Eine weitere List stellt das Versenden eines fehlerhaften Videos mit sehr langer Download-Dauer dar. [404] Wie viele der Ermittlungen jedoch faktisch an einer Keuschheitsprobe scheitern, kann nicht eruiert werden, weil empirische Untersuchungen fehlen.[405]

Die Thematik der Keuschheitsproben und deren Erschwerung bei der Bekämpfung von Kinderpornografie wird jedoch sowohl im umliegenden Ausland als auch in der Schweiz diskutiert.[406] Auf nationaler Ebene haben sich zwölf Teilnehmende[407] im Rahmen des Vernehmlassungsverfahrens über den Bericht und den Vorentwurf zur Änderung der StPO, welche am 14. März 2018 endete, dafür ausgesprochen, dass verdeckte Ermittler und Fahnder von der Strafbarkeit ausgenommen werden, wenn diese fiktives[408]

---

[393] MEY, Darknet, N 134.
[394] MUGGLI, Arbeitstagung, N 22; Vgl. für das deutsche Recht: MEY, Darknet, N 134; KRAUSE, 680; SULIAK, Frage 2 und 3.
[395] Zugänglich-machen gem. Abs. 4 meint das bewusste Einräumen der Option der Kenntnisnahme aus eigenem Antrieb (BSK StGB-ISENRING/KESSLER, Art. 197 N 52i).
[396] Überlassen ist die Einräumung zumindest faktischer Herrschaftsmacht über die pornographischen Inhalte: Z.B. die Leihe eines pornographischen Videofilms. Durch Überlassen erfolgt zumindest eine vorübergehende Übertragung des Besitzes, sodass der neue Besitzer Verfügungsmacht über das Produkt erlangt (BSK StGB-ISENRING/KESSLER, Art. 197 N 52h).
[397] MEY, Darknet, N 134.
[398] MUGGLI, Arbeitstagung, N 19.
[399] Regierungsrat Kt. Zug, Vernehmlassung StPO, 14; Vorsteher des SJD des Kt. Obwalden, Stellungnahme StPO, 6.
[400] WITTMER/STEINEBACH, 382.
[401] MUGGLI, Arbeitstagung, N 22; vgl. hierzu ebenfalls: MUGGLI, Diss., 303 f.
[402] Vgl. SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 293 N 9.
[403] Anh. 1: Interview WERREN/ZAUGG, Frage 3.9; Anh. 2: Interview WALDER, Frage 3.4; KRAUSE, 678; Art. 298a StPO umfasst die Bestimmung, dass ein verdeckter Fahnder «insbesondere Scheingeschäfte abschliessen oder den **Willen zum Abschluss vortäuschen [darf]»** (Hervorhebungen durch die Autorin hinzugefügt).
[404] Anh. 2: Interview WALDER, Frage 3.4.
[405] GERCKE, Kinderpornographie, 481, die Aussage bezieht sich auf Deutschland, gilt m.E. aber auch für die Schweiz.
[406] An der 3. internationalen Arbeitstagung für Staatsanwälte und Ermittlungsleiter der Landeskriminalämter diskutierten Vertreter aus Österreich, Deutschland und der Schweiz im Jahr 2018 die Bekämpfung der Kinderpornografie und sexuellem Missbrauch Minderjähriger (MUGGLI, Arbeitstagung, N 1 f.).
[407] Die Kantone Aargau, Bern, Basel-Landschaft, Luzern, Obwalden, Solothurn, Schwyz, Thurgau, Zug, Zürich, sowie die KKPKS und die SVSP (BJ, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zur StPO, 31).
[408] Künstlich erstelltes Material, das keine real existierenden Personen zeigt.

kinderpornografisches Material einsetzen, um so den Zugang zu einschlägigen Foren zu erhalten.[409] Es wird eine Ergänzung von Art. 294 StPO um einen weiteren Absatz vorgeschlagen sowie die Aufhebung der Beschränkung dieses Artikels auf das BetmG.[410] Die Kommission für Rechtsfragen des Nationalrates hat im Sommer 2020 einstimmig beschlossen, dass die VE im Bereich der Kinderpornografie gem. dem oben angesprochenen Vorschlag zukünftig zu erleichtern ist.[411] Der Nationalrat befürwortete diesen Vorschlag in der Frühjahressession 2021 ebenfalls, weshalb sich als nächstes der Ständerat mit der Vorlage auseinanderzusetzen hat.[412] In Deutschland ist am 13.3.2020 die neue Gesetzesgrundlage im StGB und der StPO in Kraft getreten, welche es Polizeibeamten i.R.v. Ermittlungsverfahren zur Aufrechterhaltung ihrer Tarnung erlaubt, unter strikten Voraussetzungen selbst künstlich hergestellte Kinderpornografie zu veröffentlichen.[413]

Aus den Experteninterviews mit Schweizer Strafverfolgungsbehörden konnte die Erkenntnis gewonnen werden, dass die Praktiker eine definitive Einführung einer solchen Bestimmung als Chance sehen, um eine effektivere Strafverfolgung auf diesen Foren und Verkaufsplattformen zu gewährleisten.[414] Trotz der moralischen Bedenken, dass der Einsatz von solchem fiktivem kinderpornografischen Material durch die verdeckten Ermittler und Fahnder bei den Nutzern dieser Foren einen Anreiz zu neuen Produktionen liefern und damit den Kindesmissbrauch weiter fördern könnte,[415] ist die geplante Gesetzesänderung m.E. zu begrüssen. Ebenfalls beizupflichten ist dem Argument von WALDER, der vorbringt, dass geäusserte Bedenken ansonsten auch bezüglich der Scheinkäufe bei Drogen beachtet werden müssten, welche indirekt auch den Drogenhandel weiter fördern würde.[416] Auch RÜCKERT und GOGER ist zuzustimmen, dass einige wenige künstlich hergestellte kinderpornografische Dateien in Ermittlungsverfahren im Hinblick auf tausende solcher Dateien in den Foren und auf den Verkaufsplattformen im Darknet nicht wesentlich ins Gewicht fallen.[417]

C Identifikation der anonymen Zielperson in der Praxis

Der Einsatz einer VF (allenfalls auch VE) soll im Zusammenhang mit Darknet-Verkaufsplattformen zur Identifikation einer realen Person hinter der bisher anonymen Zielperson beitragen. Gemäss MÜLLER gelingt dies häufig nur, indem die Strafverfolgungsbehörden oftmals Unachtsamkeiten von Zielpersonen erkennen und zu ihren Gunsten ausnutzen.[418] Diese Fehlerquellen sind nahezu unbegrenzt und können ganz verschieden sein. Die Zielpersonen neigen jedoch gerade unter dem vermeintlichen Schutz der Anonymität zeitweise zur Leichtsinnigkeit.[419] Deswegen versuchen verdeckte Fahnder häufig, die Zielperson aus der Anonymität des Darknets zu locken und ein persönliches Treffen zu vereinbaren.[420] Wie

[409] BJ, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zur StPO, 31.
[410] Regierungsrat Kt. Zug, Vernehmlassung StPO, 14; Vorsteher des SJD des Kt. Obwalden, Stellungnahme StPO, 6; Der Kanton Zürich forderte beim Vernehmlassungsverfahren gar die Ausweitung auf einen allgemeinen Rechtfertigungsgrund für verdeckte Ermittler, wenn diese im Rahmen einer genehmigten Ermittlung tätig werden und die Verhältnismässigkeit gewahrt ist. Dies sei nötig, weil die VF immer mehr auch bei anderen Straftaten wie Geldwäscherei, Raub, Sexualdelikten, Hehlerei, Terrorismus und Cybercrime zur Anwendung komme und die verdeckten Ermittler z.B. auch Geldwäschereihandlungen oder gestohlene Waren kaufen können sollten. Dieser sehr weitgehende Vorschlag wurde bisher nicht in den parlamentarischen Diskussionen berücksichtigt (BJ, Zusammenfassung der Ergebnisse des Vernehmlassungsverfahrens zur StPO, 31).
[411] RK-N, Medienmitteilung vom 6.11.2020, Abschn. 7.
[412] Nationalrat, Frühjahressession 2021, Abschn. 1.
[413] RÜCKERT/GOGER, 373.
[414] Anh. 1: Interview WERREN/ZAUGG, Frage 3.9; Anh. 2: Interview WALDER, Frage 3.4.
[415] WITTMER/STEINEBACH, 390.
[416] Anh. 2: Interview WALDER, Frage 3.4.
[417] RÜCKERT/GOGER, 376.
[418] MÜLLER, 100.
[419] MÜLLER, 100.
[420] Anh. 2: Interview WALDER, Frage 3.4.

die vermeintliche «Waffenübergabe» im Fall Tobias Kuster zeigt (vgl. Kap. II. C 2.), bietet sich dies v.a. bei Scheingeschäften von Waren, die physisch ausgetauscht werden müssen, an.[421] Aber auch im Zusammenhang mit einer pädophilen «Zielperson» kann die Vereinbarung eines Treffens zielführend sein, da diese häufig sehr lustgetrieben ist und das eigene Schutzverhalten ausblendet.[422] So hat exemplarisch in einem Fall der Zürcher Kantonspolizei ein pädophiler Sexualstraftäter nicht nur kinderpornografische Bilder im Darknet angeboten, sondern dort auch sein Interesse für sexuelle Treffen mit erwachsenen Müttern und deren Kinder geäussert. Ein verdeckter Fahnder, der gegen diese pädophile Zielperson ermittelte, gab sich dieser gegenüber als «Frau» aus und vereinbarte ein Treffen, zu welchem die Person erschien und festgenommen werden konnte.[423] Gelingt somit ein reales Treffen, so kann die Zielperson unmittelbar identifiziert werden.

In vielen Konstellationen werden die Zielpersonen jedoch nicht zu einem physischen Treffen bereit sein, weshalb sich der verdeckte Fahnder anderer Taktiken bedienen muss. Eine dieser kann bspw. darin bestehen, dass er versucht, durch die Kommunikation mit der Zielperson private Details zu erhalten, die allenfalls Rückschlüsse auf eine bestimmte Person zulassen.[424] Er kann versuchen, die Zielperson zur Anbahnung eines angeblichen An- oder Verkaufsgesprächs zum Umstieg auf andere Kommunikationskanäle ausserhalb des Darknets zu bewegen[425] und dadurch bspw. eine E-Mail-Adresse, Handynummer oder sonstige Hinweise zu erhalten, die für weitere geheime Überwachungsmassnahmen genutzt werden können. Ergänzend werden auch klassische kriminalistische Ermittlungsmethoden, wie die Auswertung von Benutzerkonten auf mehreren Verkaufsplattformen und diesbezügliche Erwähnungen in Foren beigezogen,[426] sowie allfällige Spuren in Social Media gesucht.[427] Auch Suchanfragen im Clearnet können weitere Erkenntnisse liefern, wenn die Kriminellen ihre Fotos und Texte zur Präsentation ihres Angebots nicht nur auf Darknet-Verkaufsplattformen verwenden, sondern auch einen Underground-Economy-Shop des offenen Internets verwenden.[428] Ferner sind Ermittlungen an den Schnittstellen zwischen der digitalen und analogen Welt sehr wichtig.[429] Denn die Waren, wie bspw. Drogen, Medikamente oder auch Falschgeld müssen letztlich zum Käufer gelangen, was einem physischen Vorgang entspricht, der über das Darknet nicht vollzogen werden kann.[430] Stattdessen werden die Waren vom Verkäufer verpackt[431] und per Post versandt und vom Käufer am Bestimmungsort entgegengenommen.[432] Da Briefe und Pakete, welche die Schweizer im Ausland bestellen, im Briefpostzentrum durch die Zollbehörden auf verdächtige Sendungen untersucht werden,[433] können vom Zoll abgefangene Sendungen (häufig

[421] Anh. 1: Interview WERREN/ZAUGG, Frage 1.4; BAUMGARTNER, Abschn. 1.
[422] Anh. 2: Interview WALDER, Frage 3.4.
[423] FEUSI, Abschn. 9.
[424] MÜLLER, 99 f.
[425] KRAUSE, 679 f.
[426] HOSTETTLER, Hilflose Ermittler, 14 f.
[427] WHITE/KAKKAR/CHOU, 71.
[428] In einem ähnlichen Fall hat die Zürcher Polizei und StA lange einen Drogendealer im Darknet beobachtet, der nebst Drogen auch gefälschte Dokumente verkaufte. Als er auf seinem Benutzerkonto das Foto eines gefälschten amtlichen Stempels veröffentlichte, versuchten die Strafbehörden herauszufinden, woher er dieses hatte. Denn selbst aufgenommene Fotos können den Strafbehörden hilfreiche Informationen liefern, wie bspw. die Kamera, die benutzt wurde. In diesem Fall wurde das Foto aber heruntergeladen und die Strafbehörden konnten herausfinden, woher es stammte. Dies war nur möglich, da der Täter nachlässig handelte und das Foto nicht mittels Tor Browser, sondern über den normalen Internetanschluss herunterlud (EIHOLZER, Frage 2 und 3).
[429] BACHMANN/ARSLAN, 245.
[430] IHWAS, 147.
[431] Kleinere Mengen von Drogen werden häufig in DVD-Hüllen verpackt und in Briefumschlägen verschickt. Die sichere Tarnung der Ware, wird von den Verkäufern sehr ernst genommen, und auch in den Rezessionen auf den Verkaufsplattformen angegeben (MEY, Darknet, N 137).
[432] MEY, Darknet, 137.
[433] HANSJAKOB, Überwachungsrecht, N 364 ff.

Drogenlieferungen) ebenfalls wichtige Ermittlungshinweise liefern.[434] Solche Hinweise können aber auch direkt von der Post erfolgen, weil diese häufig nicht zustellbare Briefsendungen öffnet und beim Auffinden von Substanzen eine Meldung an die Polizei macht.[435]

Gesammelte und verdichtete Hinweise aus den Recherchen und der VF, wie Handynummern, IP- oder E-Mail-Adressen werden von den Strafverfolgungsbehörden häufig für weitere geheime Überwachungsmassnahmen eingesetzt.[436] Kann bspw. eine Handynummer oder eine IP-Adresse einer Zielperson zugeordnet werden, die von einem Schweizer Fernmeldedienst stammt und sind die weiteren Voraussetzungen gem. Art. 273 StPO, v.a. der dringende Verdacht auf ein Vergehen oder Verbrechen sowie die Genehmigung des ZMG gegeben, so wird die StA oft eine rückwirkende Randdatenerhebung anordnen.[437] Auskünfte zu Bestandesdaten gem. Art. 21 und 22 BÜPF kommen in der Praxis ebenfalls teilweise zum Einsatz, sie sind jedoch häufig nicht sehr aussagekräftig, da die wenigsten Straftäter die benutzten Geräte, resp. SIM-Karten oder E-Mail-Konten unter Verwendung ihrer echten Personalien registrieren lassen.[438] Wird hingegen eine rückwirkende Randdatenerhebung durchgeführt und bspw. die Daten des Internetverkehrs erhoben, so erhalten die Behörden u.U. auch Angaben zum E-Mail-Verkehr, d.h. wann und an wen von der überwachten E-Mail-Adresse E-Mails verschickt und empfangen wurden und welche Websites (URLs) die Person besucht hatte.[439] Lassen auch diese weiteren Informationen keinen Rückschluss auf die Identität und/oder den Standort der Zielperson zu und sind die strengeren Voraussetzungen für eine geheime aktive Überwachung gem. Art. 269 StPO gegeben, so wird in der Praxis als weiteres Vorgehen eine solche angeordnet.[440] Wie WALDER erläutert, fokussieren sich die Strafverfolgungsbehörden bei den Ergebnissen aus geheimen Überwachungen nicht nur auf Sachverhaltsdaten sondern auch auf Identifikationsdaten. Wenn z.B. die Zürcher Strafverfolgungsbehörde beim abgehörten Telefongespräch im Hintergrund ein Tram durchfahren hört, dann könnte sich die Zielperson evtl. gerade in der Stadt Zürich befinden. Bucht die Zielperson online ein Flugticket, muss sie allenfalls eine Kreditkarte oder die Angaben in ihrem Pass offenlegen. Macht die Zielperson mit ihrem Smartphone ein Foto mit einem «Geo-Catch» oder gibt einen Standort ein, dann wissen die Strafbehörden wo sich die Person aktuell aufhält, auch wenn dies nicht dem Wohnsitz der Zielperson entsprechen muss.[441]

Wichtig ist jedoch zu erwähnen, dass sowohl die aktive als auch rückwirkende Überwachung des Internetverkehrs einer Zielperson nur dann allenfalls zu neuen Erkenntnissen führt, wenn sie auch im Clearnet surft und nicht den gesamten Internetverkehr über den Tor Browser abwickelt. Denn würde die Ziel-

[434] GOTSCH/RENSCH, Abschn. 1 ff.; BGer 6B_504/2019 Sachverhalt, lit. Ba; FIOLKA/LAUPER, 663; Urteil 502 2019 297 Sachverhalt.
[435] BStGer BG.2019.31, Sachverhalt, lit. A: In diesem Fall wurden im Verteilzentrum der Schweizer Post (Centre Courrier Y. [VD]) in der «Clinique des lettres» sechs nicht zustellbare Briefsendungen geöffnet und wegen Auffinden von Substanzen die Polizei eingeschaltet. Dabei konnte die Polizei einen Adressaten (C.) ausfindig machen, den sie dann einvernahm. In der Einvernahme deuteten die Aussagen von C. darauf hin, dass er gegen Bitcoin Ketamin auf der Darknetseite «E.» gekauft habe.
[436] In Bezug auf den in FN 428 beschriebenen Falls hatte der Täter das WLAN eines Nachbarhauses mit 25 Wohnungen benutzt und war in diesem Netzwerk entsprechend gut getarnt. Die Strafbehörden gelang es jedoch die EDV-Anlage des Täters aus den rund 50 anderen Geräten, die dasselbe WLAN benutzten, herauszufiltern. Im Anschluss daran wurde der Täter überwacht und eine Drogenlieferung abgewartet. Bei der Verhaftung konnten dann ca. drei Kilogramm Kokain sichergestellt werden (EIHOLZER, Frage 4 und 5).
[437] Vgl. Anh. 2: Interview WALDER, Frage 3.7.
[438] Anh. 1: Interview WERREN/ZAUGG, Frage 3.8.
[439] HANSJAKOB, Überwachungsrecht, N 860 f.
[440] Vgl. Anh. 2: Interview WALDER, Frage 3.6.
[441] Zum Ganzen Anh. 2: Interview WALDER, Frage 3.6.

person nur mittels Tor Browser surfen, würde die gesamte überwachte Kommunikation resp. der Datenverkehr vorwiegend in verschlüsselter Form durchgeführt werden.[442] Für solche Fälle der verschlüsselten Kommunikation steht unter Einhaltung der strengen Voraussetzungen gem. Art. 269ter StPO grundsätzlich der Einsatz von Government Ware (GovWare) zur Verfügung. Eine solche Installation der GovWare auf dem Sendegerät wird in der Praxis jedoch scheitern, wenn jemand mit seinem Gerät nur über den Tor Browser surft, da beim Tor-Netzwerk das Sendegerät resp. dessen IP-Adresse, hinter mindestens drei Tor Nodes versteckt ist und man dieses eben gerade nicht kennt.[443]

WALDER vergleicht die Ermittlungstätigkeiten bezüglich Cybercrimes im Darknet mit einem Puzzle, bei dem die Strafverfolgungsbehörden einzelne noch wenig aussagekräftige Teilchen sammeln und versuchen, diese zu einem Gesamtbild zusammenzusetzen. Ist das Gesamtbild vollständig, so weiss die Strafverfolgungsbehörde, wer die Zielperson ist und wo sich diese befindet, sodass sie anschliessend verhaftet werden kann.[444] Zu einem solchen «Best Case-Szenario» kommt es gemäss WALDER bei rund 40% der vom Kompetenzzentrum Cybercrime der StA II des Kantons Zürich bearbeiteten Fälle, wobei sechs von zehn Fälle nicht erfolgreich enden und eingestellt werden müssen.[445]

V. Offene Zwangsmassnahmen – Sicherstellung von Daten im Zusammenhang mit Verkaufsplattformen im Darknet

Im Fokus dieses Teils der Arbeit steht nun die Frage, inwiefern die Strafverfolgungsbehörden zu Beweis- oder Sicherungszwecken v.a. Daten aber auch Gegenstände bei den verdächtigen Personen sicherstellen können. Dazu wird einerseits erläutert, wie die Behörden vorgehen und welche Daten oder beweisrelevanten Gegenstände bei Delikten im Zusammenhang mit Darknet-Verkaufsplattformen sichergestellt werden. Andererseits wird anhand der zwei nachfolgend aufgeführten Bundesgerichtsentscheide ein eher neuer international bei Cybercrime häufig vorkommender Ansatz zur Datenerhebung und Sicherung erläutert und dessen «Rechtmässigkeit» im schweizerischen und völkerrechtlichen Kontext reflektiert.

A Überblick zur Bundesgerichtspraxis

Die bedeutsame Rechtsprechung bezüglich strafprozessualer Zwangsmassnahmen zur Beweiserhebung im Zusammenhang mit Verkaufsplattformen im Darknet ist bis anhin (noch) sehr überschaubar und bezieht sich vorwiegend auf das Urteil 1B_185/2019 vom 26. November 2019 und 1B_153/2019 vom 11. Dezember 2019, welche anschliessend überblicksmässig dargelegt werden. Wie bereits erwähnt, handelt es sich bei den Beschwerdeführern in den beiden Entscheiden um die in Kap. II. C 2. erläuterten Ermittlungserfolge der Zürcher Strafverfolgungsbehörden im Zusammenhang mit den Darknet-Benutzerkonten um die Pseudonyme «Swiss Flakes», «Happy Olaf» und «CH-Koks». Das Vorgehen der Zürcher Behörden entspricht bezüglich Durchsuchung und Beschlagnahme von Darknet-Benutzerkonten demjenigen der Aargauer Behörden in Bezug auf die Benutzerkonten mit den Nicknames «DrFeelWell» und «DerErsteAffe» (vgl. Kap. II. C 2.).

[442] Zum Ganzen KRAUSE, 679.
[443] Anh. 2: Interview WALDER, Frage 3.6.
[444] Zum Ganzen Anh. 2: Interview WALDER, Frage 3.7; EIHOLZER, Frage 1. vgl. auch MÜLLER, 100.
[445] Anh. 2: Interview WALDER, Frage 1.4.

1. Urteil 1B_185/2019 vom 26. November 2019

a Sachverhalt und Anträge

Die StA II des Kantons Zürich (nachfolgend StA II) führte eine Strafuntersuchung gegen A wegen des Verdachts der Begehung qualifizierter Drogendelikte. A wurde vorgeworfen, dass er seit etwa September 2016 im Darknet Verkaufsplattformen betrieben und grosse Mengen Drogen, darunter Kokain mit hohem Reinheitsgehalt, an in der Schweiz wohnhafte Kunden verkauft und per Post geliefert hatte. Am 2. August 2018 wurde A in Untersuchungshaft gebracht. Am selben Tag liess die StA II Hausdurchsuchungen und diverse Sicherstellungen in den von A gemieteten Räumlichkeiten durchführen.[446] Mittels zweier Verfügungen vom 7. und 22. August 2018 beschlagnahmte die StA II diverse elektronische Accounts, darunter auch E-Mail-Konten und Benutzerkonten für Verkaufsplattformen. In einer weiteren Verfügung wurden die in der Hausdurchsuchung sichergestellten Gegenstände beschlagnahmt. Am 24. August 2018 verlangte der amtliche Verteidiger von A die Siegelung für alle sichergestellten Daten oder Gegenstände, worauf die StA II am 7. September 2018 beim kantonalen ZMG das Entsiegelungsgesuch stellte.[447] Am 18. März 2019 wies das Bezirksgericht Zürich als ZMG,[448] das Entsiegelungsgesuch für bestimmte Daten der ersten Beschlagnahmeverfügung ab. Ansonsten hiess das ZMG das Gesuch gut, indem es zehn weitere E-Mail-Accounts, ein Benutzerkonto für eine Verkaufsplattform, drei weitere Accounts, alle Angebote eines anonymen Internet-Users auf vier Verkaufsplattformen sowie bei Hausdurchsuchungen sichergestellte Gegenstände (darunter auch Computer und Datenträger) zur Durchsuchung durch die StA II freigab.[449]

Gegen diesen Entscheid gelangte A mit Beschwerde in Strafsachen vom 17. April 2019 an das BGer, wobei er die Abweisung des Entsiegelungsgesuchs, ausgenommen der Gegenstände, welche in der Hausdurchsuchungen sichergestellt wurden, beantragte.[450] In einer weiteren Eingabe an das BGer machte er geltend, dass er an der Siegelung «einzig und allein» für jene Dateien festhalte, welche sich «nicht auf den (anlässlich der vier Hausdurchsuchungen) sichergestellten Datenträgern» befinden, also ihm persönlich «zugeordnet wurden».[451] Zudem wollte er feststellen lassen, dass die von der StA II angeordnete Verwaltung von elektronischen Accounts (inklusive Passwörterverwaltung) einen nicht wiederherstellbaren Eingriff in die Account-Grundeinstellungen bedeuteten und dass das BGer die Passwortzurücksetzung erneut vornehmen müsse.[452]

b Entscheid des BGer

Beim angefochtenen Entscheid handelt es sich um einen letztinstanzlichen Entsiegelungsentscheid, bei dem zu prüfen war, ob die gesetzlichen Sachverhaltsvoraussetzungen erfüllt sind, wobei das BGer diese Frage von Amtes wegen und mit freier Kognition beurteilt.[453] Das BGer anerkannte, dass das Feststellungsbegehren des Beschwerdeführers betreffend die Zwangsverwaltung von elektronischen Accounts

[446] Zum Ganzen BGer 1B_185/2019, Sachverhalt, lit. A.
[447] Zum Ganzen BGer 1B_185/2019, Sachverhalt, lit. B.
[448] Das vorinstanzliche Urteil des ZMG Zürich liegt nicht in anonymisierter Form vor. Da es sich um ein nicht-öffentliches Verfahren gem. Art. 225 Abs. 1 StPO handelt, wird das Urteil nur an die beteiligten Parteien abgegeben. Trotz Nachfrage beim ZMG Zürich konnte die Autorin dieses deshalb nicht einsehen.
[449] Zum Ganzen BGer 1B_185/2019, Sachverhalt, lit. D.
[450] Das Rechtsbegehren des Beschwerdeführers richtete sich somit gegen die Entsiegelung und Durchsuchung der zehn E-Mail-Accounts, dem Benutzerkonto für eine Verkaufsplattform, drei weiteren Accounts sowie allen Angeboten eines anonymisierten Internet-Users auf vier Darknet-Handelsplattformen (BGer 1B_185/2019, Sachverhalt lit. E und E. 1.2).
[451] BGer 1B_185/2019, E. 1.2.
[452] BGer 1B_185/2019, Sachverhalt, lit. E.
[453] BGer 1B_185/2019 E. 1.

sowie sein Antrag zur Passwortrücksetzung nicht Gegenstand des angefochtenen Entscheides (der Entsiegelung und Durchsuchung von Aufzeichnungen und Gegenständen gem. Art. 248 i.V.m. Art. 246 StPO) war, sondern weitere Untersuchungshandlungen bzw. strafprozessuale Sicherungsmassnahmen der StA (vgl. Art. 263 Abs. 1 lit. d StPO i.V.m. Art. 69 f. StGB) betrifft und trat darauf nicht ein (Art. 80 BGG).[454]

Die Beschwerde in Strafsachen gegen Entsiegelungsentscheide des ZMG setzt voraus, dass dem Betroffenen aufgrund eines Eingriffs in seine rechtlich geschützten Geheiminteressen ein nicht wieder gutzumachender Rechtsnachteil droht (Art. 93 Abs. 1 lit. a BGG i.V.m. Art. 248 Abs. 1 StPO). Tangierte Geheimnisinteressen sind kurz zu umschreiben und glaubhaft zu machen. Aufzeichnungen und Dateien, die dem Geheimnisschutz unterliegen sind zu benennen.[455] Der Beschwerdeführer begründete seinen nicht wieder gutzumachenden Rechtsnachteil wie folgt: Im Falle einer Entsiegelung würden «nicht gesetzeskonform erhobene Informationen und Daten in das Strafverfahren» einfliessen. Die vom Beschwerdeführer aufgebrachten materiellrechtlichen Fragen, insb. «die Kernfrage, ob Daten ohne deren Datenträger» strafprozessual beschlagnahmt werden könnten, seien «von grundsätzlicher Bedeutung».[456] Bezüglich seiner Beschwerdelegitimation machte der Beschuldigte geltend, er sei der «User» von vier betroffenen Darknet-Handelsplattformen und habe über zwei genannte E-Mail-Accounts «kommuniziert».[457] Das BGer kam zum Schluss, dass in der Beschwerdeschrift keine Nennung der bedrohten und gesetzlich geschützten Geheimnisinteressen gemacht wurde und das blosse prozesstaktische Parteiinteresse eines Beschuldigten zur Erschwerung der Beweiserhebung durch die Untersuchungsbehörde nicht unter die schutzwürdigen Geheimnisinteressen i.S.v. Art. 248 Abs. 1 StPO fiel. Darüber hinaus fehlte es dem Beschwerdeführer auch an seiner Beschwerdelegitimation, da ihm die elektronischen Accounts und Dateien, deren Entsiegelung er verhindern wollte, um Gegenstände handelte, die ihm noch nicht persönlich «zugeordnet» wurden.[458] Das BGer trat nicht auf die Beschwerde ein.[459]

2. Urteil 1B_153/2019 vom 11. Dezember 2019

Sowohl der Sachverhalt als auch die gerichtliche Würdigung im Bundesgerichtsentscheid 1B_153/2019 gestalten sich praktisch identisch mit demjenigen aus 1B_185/2019. Wiederum ermittelte die StA II gegen einen Beschuldigten, der unter Verdacht stand, über Verkaufsplattformen grosse Mengen Drogen an Schweizer Kunden verkauft zu haben. Die Verhaftung des Beschuldigten, die anschliessende Hausdurchsuchung und Sicherstellung von Geräten und Datenträger erfolgte einen Tag später als im obigen Entscheid.[460] Bezüglich der Sicherstellungen, resp. Beschlagnahmen reichte der Beschuldigte ebenfalls ein Siegelungsgesuch ein, worauf die StA II das Entsiegelungsgesuch beim ZMG stellte.[461] Das ZMG

[454] BGer 1B_185/2019 E. 1.1.
[455] Zum Ganzen BGer 1B_185/2019 E. 1.3.
[456] BGer 1B_185/2019 E. 1.4.
[457] BGer 1B_185/2019 E. 1.4.
[458] BGer 1B_185/2019, E. 1.4 f.
[459] BGer 1B_185/2019, E. 2.; Ergänzend ist zu erwähnen, dass das BGer in einem weiteren Urteil die Beschwerde desselben Beschuldigten gegen den Beschluss des Obergerichts in Bezug auf die angeordnete Untersuchungshaft zu beurteilen hatte. In diesem Urteil erläuterte es in den Erwägungen, dass das Urteil 1B_185/2019 am 9.12.2019 bei der StA II einging und diese am Tag darauf die Kantonspolizei mit der Auswertung der entsiegelten Daten beauftragte. Daraus wurden wesentliche Erkenntnisse über die Hintergründe des vom Beschwerdeführer betriebenen Drogenhandels erwartet, insb. Aufschlüsse über Lieferanten und Abnehmer sowie das Ausmass der Geschäfte (BGer 1B_164/2020 E. 2.3).
[460] Zum Ganzen BGer 1B_153/2019, Sachverhalt, lit. A.
[461] BGer 1B_153/2019, Sachverhalt, lit. B.

hiess das Gesuch teilweise gut und gab die Dateien zweier User auf Accounts von vier Darknet-Handelsplattformen sowie sichergestellte elektronische Geräte[462] zur Durchsuchung frei.[463] Der Beschuldigte gelangte mit Beschwerde vom 28. März 2019 ans BGer und beantragte die Aufhebung des angefochtenen Entscheids bezüglich den Freigaben zur Durchsuchung, was auch die Angebote von zwei Darknet-Usern betraf. Er verlangte die Feststellung durch das BGer, dass allfällige Änderungen der Strafbehörden an sichergestellten Benutzerkonten[464] sowie deren polizeiliche Verwaltung zu unterlassen seien.[465] Auf dieses Feststellungsbegehren trat das BGer wegen derselben Begründung wie im vorherigen Entscheid wiederum nicht ein.[466] Da der Beschwerdeführer nicht ausreichend darlegen konnte, inwiefern ihm durch einen Eingriff in seine rechtlich geschützten Geheimnisinteressen ein nicht wiedergutzumachender Rechtsnachteil drohte und sein rechtlich geschütztes Anfechtungsinteresse nicht ausreichend dargetan wurde, trat das BGer ebenfalls nicht auf die Beschwerde gegen den Entsiegelungsentscheid ein.[467]

3. Würdigung der Bundesgerichtspraxis

Da die Beschwerdeführer in beiden Entscheiden ihren nicht wiedergutzumachenden Rechtsnachteil sowie ihr rechtlich geschütztes Anfechtungsinteresse nicht genügend substantiierten, waren die Eintretensvoraussetzungen nicht gegeben. Aus diesem Grund konnte das BGer die Nichteintretensentscheide fällen und musste bedauerlicherweise auch keine materielle Prüfung der Begehren der Beschwerdeführer vornehmen. Die Entscheide verdeutlichen jedoch die materielle Beurteilung durch die Vorinstanz und bringen zum Ausdruck, dass elektronisch aufgeschaltete Angebote von Usern auf Verkaufsplattformen sowie diesbezügliche Korrespondenz via E-Mail über die Entsiegelung und Durchsuchung von Aufzeichnungen und Gegenständen gem. Art. 248 i.V.m. Art. 246 StPO zu erfolgen haben. Trotz des Nichteintretens auf die Feststellungsbegehren der Beschwerdeführer wird deutlich, dass die sog. Zwangsverwaltung der Benutzerkonten durch die Polizei als Beschlagnahme gem. Art. 263 Abs. 1 lit. d StPO i.V.m. Art. 69 f. StGB anzusehen ist.

Diese Praxis wirft jedoch drei wesentliche Fragestellungen auf, welche nachfolgend diskutiert werden. Dies umfasst erstens die Frage nach der Zulässigkeit von Durchsuchungen via Internetzugriff und die dafür notwendige Abgrenzung zwischen der Durchsuchung von Aufzeichnungen gem. Art. 246 StPO und der aktiven Kommunikationsüberwachung gem. Art. 269 ff. StPO. Zweitens soll erläutert werden, was unter der Beschlagnahme gem. Art. 263 StPO zu verstehen ist und inwiefern dezentral gespeicherte Daten, deren Speicherort unbekannt ist, beschlagnahmefähig sind. Letztlich gilt es zu untersuchen, inwiefern die Durchsuchung via Internetzugriff und die Beschlagnahme dieser Daten in Anbetracht des Territorialitätsprinzips zu werten sind und welche Ausnahmen davon diskutiert werden.

B Direkter Zugriff auf bei Service Providern gespeicherte Daten in der Praxis

Wie bereits in Kap. IV. A 4. ansatzweise angedeutet wurde, stehen den Strafverfolgungsbehörden unterschiedliche strafprozessuale Zwangsmassnahmen zur Beweiserhebung im Internet zur Verfügung, die teilweise auch im Darknet Anwendung finden. Die Strafverfolgungsbehörden können erstens die Daten

[462] Computer, Mobiltelefone, Kameras und weitere Datenträger.
[463] BGer 1B_153/2019, Sachverhalt, lit. D.
[464] Passwort des Accounts und E-Mail-Adresse zur Rücksetzung des Passwortes.
[465] Zum Ganzen BGer 1B_153/2019, Sachverhalt, lit. E: Ferner forderte er eine richterliche Triage der sichergestellten elektronischen Geräte zur Aussonderung von pornografischem Material, was vorliegend m.E. aber nicht von Relevanz ist.
[466] BGer 1B_153/2019 E. 1.1.
[467] Zum Ganzen BGer 1B_153/2019 E. 1.4, E. 1.6 und E. 2.

einer beschuldigten Person durch die Anordnung einer Editionsverfügung gem. Art. 265 StPO beim Provider anfordern und somit direkt mit diesem «zusammenarbeiten».[468] Liegen die Daten im Ausland, müssen die Daten vielfach über den Rechtshilfeweg eingefordert werden, womit zweitens eine justizielle Zusammenarbeit zwischen den Behörden begründet wird. Immer bedeutender wurde in den letzten Jahren aber die dritte Möglichkeit in Form des direkten Datenzugangs durch die Strafverfolgungsbehörden mittels Durchsuchung (Art. 246-248 StPO) und Beschlagnahme (Art. 263-268 StPO).[469] Unter den direkten Zugang fallen einerseits die Konstellationen, in denen Geräte bspw. im Rahmen einer Hausdurchsuchung beschlagnahmt und anschliessend durchsucht werden. Wie noch ausführlicher erläutert wird, fallen darunter auch Konstellationen, bei denen die Behörden mittels Fernzugriff unter Verwendung von rechtmässig erworbenen Zugangsdaten auf die Daten zugreifen.[470] Der direkte Datenzugang ist im Zusammenhang mit Untersuchungen im Darknet von besonderer Relevanz, da die Strafverfolgungsbehörden eben gerade nicht auf die Zusammenarbeit mit den Service Providern (den Plattformbetreibern) zählen können.[471]

Auch in BGer 1B_185/2019 und BGer 1B_153/2019 gelangten die Strafverfolgungsbehörden mittels direkten Zugriffes an die erforderlichen Daten. Dabei bedienten sie sich eines für Cybercrime typischen Vorgehens, bei dem versucht wird, einen Verdächtigen «auf frischer Tat» anzutreffen, was bedeutet, dass dieser während des polizeilichen Zugriffs aktiv an seinem Computer eingeloggt ist.[472] Nach der gelungenen Lokalisation und Identifikation der Beschuldigten in den beiden Entscheiden wurden die Personen nicht unmittelbar verhaftet, sondern deren (Nutzungs-)Verhalten bezüglich Tätigkeiten auf den Verkaufsplattformen mittels Einsatz von weiteren geheimen Überwachungsmassnahmen analysiert.[473] Dazu können die Strafverfolgungsbehörden bspw. VF, VE, Observationen oder technische Überwachungsgeräte einsetzen, wenn die gesetzlich normierten Voraussetzungen sowie die Subsidiarität und Verhältnismässigkeit den Einsatz dieser Zwangsmassnahmen zulassen. Dabei ermöglicht eine Observation gem. Art. 282 StPO die verdeckte Beobachtung sowie das Erstellen von Bild- oder Tonaufzeichnungen von Personen oder Sachen an allgemein zugänglichen Orten.[474] Der Einsatz von technischen Überwachungsgeräten gem. Art. 280 StPO ermöglicht hingegen die akustische Abhörung und Aufzeichnung des nicht öffentlichen Wortes, d.h. von Gesprächen, die nicht in einem allgemein zugänglichen Rahmen geführt werden.[475] Sowie die Beobachtung und Aufzeichnung an nicht öffentlichen und nicht allgemein zugänglichen Orten und Feststellung des Standortes der beschuldigten Person oder deren Gegenstände.[476]

Mithilfe des Einsatzes der eben genannten geheimen Überwachungsmassnahmen gewannen die Zürcher Strafverfolgungsbehörden wichtige Erkenntnisse über die Tätigkeiten und das Verhalten der Beschuldigten, was ihnen dabei half für die Durchführung der Hausdurchsuchung gem. Art. 244 f. StPO einen bestimmten Zeitpunkt festzulegen.[477] Es entsprach somit dem taktischen Ziel der Strafverfolger, die Beschuldigten «während der Arbeit» zu überraschen und deren Computer im laufenden Betrieb und mit

[468] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 18.
[469] Zum Ganzen European Commission, Working Document, 10 f.
[470] European Commission, Working Document, 11 und 33; HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 18.
[471] European Commission, Working Document, 11, 33 und 37.
[472] MÜLLER, 100.
[473] MÜLLER, 100; Anh. 2: Interview WALDER, Frage 2.2.
[474] Eine Observation ist zulässig, wenn es konkrete Anhaltspunkte gibt, dass ein Verbrechen oder Vergehen begangen worden ist und die Ermittlungen sonst aussichtslos wären oder unverhältnismässig erschwert würden (Art. 282 Abs. 1 lit. a und b StPO)
[475] BSK StPO-EUGSTER/KATZENSTEIN, Art. 280 N 23; HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 280 N 16.
[476] BSK StPO-EUGSTER/KATZENSTEIN, Art. 280 N 28 und 35; SCHMID/JOSITSCH, Praxiskommentar, Art. 280 N 23 und 29.
[477] Anh. 2: Interview WALDER, Frage 2.2, 2.3 und 4.4; EIHOLZER, Frage 5.

geöffneten Benutzerkonten sicherzustellen. Durch diesen Überraschungsmoment konnte verhindert werden, dass die Beschuldigten rechtzeitig den Computer schliessen resp. herunterfahren konnten und dadurch den Zugriff auf die Daten verhinderten.[478] Da die Beschuldigten zu diesem Zeitpunkt bei ihren Benutzerkonten eingeloggt waren, konnten die Strafverfolgungsbehörden die Zugangsdaten nachschauen und anschliessend verändern, sodass der Zugang zu den Konten den Beschuldigten mindestens vorübergehend entzogen werden konnte.[479] Dies funktioniert jedoch nur, wenn die Täter das Darknet auf «normale» Weise aufrufen und nicht zusätzlich bspw. Tails verwenden. Tails ist ein Life-Betriebssystem, das Nichts speichert und über einen USB-Stick betrieben wird.[480] Hätten die Beschuldigten Tails verwendet und den USB-Stick rechtzeitig herausgezogen, hätten die Strafbehörden nicht mehr nachvollziehen können, was diese gerade gemacht haben. Gemäss WALDER und WERREN wird Tails vermehrt von versierten Tätern genutzt.[481]

Um an verfahrensrelevante Daten zu gelangen, können die Strafbehörden die betroffene Person auch um eine freiwillige Datenherausgabe bitten.[482] Dabei kann die beschuldigte Person z.B. in einer Einvernahme nach den Benutzerdaten und nach der Einwilligung der Sichtung, Sicherung und Auswertung solcher Daten gefragt werden.[483] Dem Verhältnismässigkeitsprinzip entsprechend, kommt es nur zur Anwendung von Zwangsmassnahmen, wenn vorgängig keine freiwillige Herausgaben erfolgen.[484] Unabhängig davon, über welchen Weg die Strafbehörden an die Zugangsdaten gelangen, besteht ein weiteres Problem darin, dass die Strafbehörden häufig nicht sämtliche Benutzerkonten und Aktivitäten der beschuldigten Person kennen,[485] weil sich diese gerade durch Verwendung von Nicknames nicht zu erkennen geben möchte.[486]

C Durchsuchungen gem. Art. 241 ff. StPO

Durchsuchungen bezwecken das Auffinden von beschuldigten Personen, Beweismitteln oder delikts- bzw. einziehungsrelevanten Vermögenswerten und deren Sicherstellung für das Strafverfahren. Sie bilden häufig den Ausgangspunkt für die Anordnung weiterer Zwangsmassnahmen.[487] Durchsuchungsbefehle haben Verfügungscharakter und müssen schriftlich und begründet ergehen.[488] Wird die Durchsuchung unter Verletzung von Anordnungsvorschriften erhoben, unterliegen allfällig gefundene Beweismittel einem Verwertungsverbot.[489]

---

[478] Zum Ganzen Anh. 2: Interview WALDER, Frage 2.2; Anh. 4: Interview WALDMEIER, Frage 2.2; vgl. auch MÜLLER, 100.
[479] Zum Ganzen Anh. 2: Interview WALDER, Frage 2.2 und 2.4; Anh. 4: Fragebogen WALDMEIER, Frage 2.3.
[480] Tails ist ein tragbares Betriebssystem, das vor Überwachung und Zensur schützen sollte. Es kann auf dem USB-Stick installiert werden. Tails schreibt nichts auf die Festplatte und läuft nur im Arbeitsspeicher des Computers. Der Arbeitsspeicher wird komplett gelöscht, wenn Tails heruntergefahren wird, wodurch mögliche Spuren wie bspw. Websites, die man besucht hat, vernichtet werden (Tails, Abschn. 1 und 2).
[481] Anh. 1: Interview WERREN/ZAUGG, Frage 1.10; Anh. 2: Interview WALDER, Frage 4.2 und 4.3.
[482] BURGERMEISTER, 19.
[483] BURGERMEISTER, 19 sieht zudem das Recht auf Siegelung bei einer freiwilligen Datenherausgabe als verwirkt, denn durch die Zustimmung der betroffenen Person zur Durchsuchung und Auswertung, liege eine Willensäusserung vor, die einer Siegelung entgegenspricht. A.M. SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 246 N 1, sehen das Recht auf Siegelung auch in einem solchen Fall als gewahrt.
[484] SCHMID, Computerdelikte, 94.
[485] Es ist nicht ungewöhnlich, dass die Nutzer von Verkaufsplattformen mehrere Benutzerkonten haben (MUGGLI, Diss., 259).
[486] Anh. 1: Interview WERREN/ZAUGG, Frage 529.
[487] SCHMID/JOSITSCH, Praxiskommentar StPO, Vor Art. 241-259 N 1.
[488] BSK StPO-GFELLER, Art. 241 N 3.
[489] BSK StPO-GFELLER, Art. 241 N 4.

1. Durchsuchung von Aufzeichnungen gem. Art. 246 StPO

Die Durchsuchung gem. Art. 246 StPO verfolgt den Zweck, Schriftstücke, Ton-, Bild- und andere Aufzeichnungen, Datenträger sowie Anlagen zur Verarbeitung und Speicherung von Informationen auf ihre Beweiseignung hin zu prüfen, wenn die Vermutung besteht, dass darin Informationen zu finden sind, die der Beschlagnahme (Art. 263 ff. StPO) unterliegen.[490] Die Auslegung der in Art. 246 StPO statuierten Generalklausel umfasst sämtliche gegenwärtigen und zukünftigen Informationsträger, weshalb die Aufzählung nicht abschliessend zu verstehen ist. Erfasst werden nicht nur Urkunden gem. Art. 110 Abs. 4 StGB sondern insb. auch elektronische Aufzeichnungen auf Datenspeicherungs- und verarbeitungsanlagen sowie Festplatten und Mobiltelefonen.[491]

Nach herrschender Lehre bildet Art. 246 StPO keine gesetzliche Grundlage für eine für die betroffene Person *nicht* erkennbare Online-Durchsuchung.[492] Die Art. 246-248 StPO kommen demnach nur zur Anwendung, wenn es sich um eine offene Zwangsmassnahme handelt, welche der betroffenen Person bekannt ist. Mit der Revision des BÜPF im Jahre 2018 wurde, die bis dahin bestehende Unklarheit bezüglich Online-Durchsuchungen[493] behoben.[494] Mit dem revidierten BÜPF wurde der Art. 269ter StPO eingeführt, der den Einsatz von GovWare zur «geheimen» Echtzeit-Überwachung des Fernmeldeverkehrs regelt.[495] Obwohl die GovWare technisch fähig wäre, Online-Durchsuchungen eines Datenverarbeitungssystems zu ermöglichen,[496] wurde in Art. 269ter StPO darauf verzichtet, eine gesetzliche Grundlage dafür einzuführen.[497]

a Durchführung

Die Durchsuchung von Aufzeichnungen muss nicht mittels eines separaten Befehls angeordnet werden, wenn ein solcher bereits für die Hausdurchsuchung oder die Durchsuchung der betroffenen Person ausgestellt wurde und die Sicherstellung der Aufzeichnungen in diesem Zusammenhang erfolgt.[498] Gem. Art. 247 Abs. 1 StPO muss die zuständige Behörde dem Inhaber der zu durchsuchenden Aufzeichnungen vor deren Durchführung die Möglichkeit geben, sich zum Inhalt der Aufzeichnungen zu äussern.[499] Damit das Äusserungsrecht des Inhabers gewährleistet werden kann, muss die durchsuchende Behörde ihn in knapper Form und mittels Befehls über den Gegenstand des Verfahrens und die gesuchten Aufzeichnungen in Kenntnis setzen.[500] Der Betroffene muss in diesem Zusammenhang auch über seine Rechte zur Erwirkung der Siegelung gem. Art. 248 Abs. 1 StPO belehrt werden.[501] Der Betroffene ist in geeigneter Weise anzuhören, was nicht zwingendermassen eine Einvernahme voraussetzt. Bei zeitlicher Dringlichkeit ist eine informelle mündliche Befragung ausreichend, die dadurch gewonnen Erkenntnisse

---

[490] Die Durchsuchung erfolgt zeitlich somit vor der Beschlagnahme (KELLER, StPO-Kommentar, Art. 246 N 1).
[491] BSK StPO-THORMANN/BRECHBÜHL, Art. 246 N 2 f.; KELLER, StPO-Kommentar, Art. 246 N 6; BGE 137 IV 189 E. 4 S. 194.
[492] BSK StPO-THORMANN/BRECHBÜHL, Art. 246 N 5; AEPLI, 132 f.; HEIMGARTNER, 41; KELLER, StPO-Kommentar, Art. 246 N 8.
[493] Online-Durchsuchungen gehen über die gängige Überwachung des Fernmeldeverkehrs hinaus indem Daten auf einem Computer ohne Wissen des Betroffenen über das Internet durchsucht werden. Es könnten sehr wahrscheinlich auch Daten von Ermittlern gesichtet werden, die noch gar nicht übermittelt wurden (TEICHMANN, 430).
[494] BSK StPO-THORMANN/BRECHBÜHL, Art. 246 N 5.
[495] HANSJAKOB, Überwachungsrecht, N 582 ff.; Botschaft 2013 BÜPF, 2771.
[496] Botschaft 2013 BÜPF, 2702, 2772-2774, 2776 und 2779.
[497] TEICHMANN, 430.
[498] BSK StPO-THORMANN/BRECHBÜHL, Art. 246 N 6.
[499] Dies entspricht der Gewährung des Anspruchs auf rechtliches Gehör gem. Art. 29 Abs. 2 BV und Art. 3 Abs. 2 lit. c. StPO und wird dadurch begründet, dass bei der Durchsuchung von Aufzeichnungen private und geschäftliche Geheimnisse des Inhabers oder Dritter in besonderer Weise betroffen sein können (BSK StPO-THORMANN/BRECHBÜHL, Art. 247 N 1).
[500] Zum Ganzen BSK StPO-THORMANN/BRECHBÜHL, Art. 247 N 4.
[501] KELLER, StPO-Kommentar, Art. 247 N 1.

sind wiederum zu protokollieren. Dem Betroffenen wird damit die Gelegenheit gegeben, um Argumente zur fehlenden Beweisrelevanz bestimmter Aufzeichnungen vorzubringen, die in der Folge nicht der Beschlagnahme unterliegen und auch nicht durchsucht werden dürfen.[502] Bei einer grösseren Menge von zu durchsuchenden Aufzeichnungen ist häufig eine Triage notwendig, um die verfahrensrelevanten von den irrelevanten und die schützenswerten von den nicht zu schützenden Aufzeichnungen zu trennen.[503] Es kann somit nicht verhindert werden, dass die Aufzeichnungen im Rahmen einer thematischen Grobtriage schnell gesichtet und begutachtet werden, um damit festzustellen, welche Akten detaillierter durchsucht und beschlagnahmt oder falls der Inhaber die Siegelung bereits verlangt hat, zu siegeln sind.[504] Gem. bundesgerichtlicher Rechtsprechung ist nur siegelungsfähig, was einer Durchsuchung i.S.v. Art. 246 StPO zugänglich ist.[505] Bei Hausdurchsuchungen im Zusammenhang mit Darknet-Ermittlungen werden nebst Daten häufig auch Drogen und Waffen sichergestellt.[506] Dabei sind diese Gegenstände nicht (nach Art. 246 StPO) zu «durchsuchen», sondern spurentechnisch zu analysieren und Drogen zusätzlich chemisch-toxikologisch zu untersuchen (vgl. Art. 182-191 StPO). Sie sind dementsprechend sicherzustellen und zu Einziehungs- und Beweiszwecken zu beschlagnahmen (Art. 263 Abs. 1 lit. a und lit. d StPO i.V.m. Art. 69 f. StGB).[507]

b Siegelung

Um ihre Geheimsphäre wirksam zu schützen, können der Inhaber von Aufzeichnungen oder eine daran rechtlich berechtigte Person einen sog. Siegelungsantrag stellen.[508] Dadurch wird der Entscheid über die Durchsuchung der Strafverfolgungsbehörde entzogen und auf ein Gericht übertragen, was ein suspensiv bedingtes Verwertungsverbot bewirkt.[509] Die Siegelung gem. Art. 248 StPO stellt einen Rechtsbehelf *sui generis* dar. Der Rechtsschutz wird dadurch gewährleistet, dass die Strafbehörde zumindest vorerst über die versiegelten Aufzeichnungen keine Kenntnis erhält, keine Auswertungen vornehmen und diese nicht für weiterführende Beweiserhebungen verwenden darf.[510]

Damit ein möglicher Beweisverlust verhindert und die Strafbehörden aufgrund eines Siegelungsantrags nicht sämtliche Akten oder Räume versiegeln müssen, ist eine Grobsichtung der zu versiegelnden Aufzeichnungen erlaubt.[511] Falls der Siegelungsantrag fristgemäss und ausreichend substantiiert erfolgt, müssen die Unterlagen und Dateien durch die Strafbehörden unmittelbar versiegelt werden.[512] Im Zusammenhang mit elektronischen Datenträgern werden angefertigte Kopien versiegelt, sodass der Inhaber seine Daten weiterhin nutzen kann und zugleich sichergestellt ist, dass die Strafbehörde deren Inhalt nicht erfährt.[513] Da die Siegelung als Sofortmassnahme ergriffen werden kann und zum Schutz des Geheimbereichs vor unbegründeten staatlichen Eingriffen dient, soll die Siegelung der Beschwerde gem. Art. 393 ff. StPO gegen den Durchsuchungs- oder den Beschlagnahmebefehl grundsätzlich vorgehen,

[502] Zum Ganzen BSK StPO-THORMANN/BRECHBÜHL, Art. 247 N 8.
[503] SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 247 N 4; KELLER, StPO-Kommentar, Art. 247 N 3.
[504] Zum Ganzen BSK StPO-THORMANN/BRECHBÜHL, Art. 247 N 13 f.; KELLER, StPO-Kommentar, Art. 247 N 3; BGE 106 IV 413 E. 7b S. 423. Wäre eine solche Sichtung/Prüfung durch die Strafbehörde nicht möglich und würde der Inhaber dieser Aufzeichnungen gegen die Durchsuchung opponieren, so müsste die Strafbehörde den gesamten Inhalt der durchsuchten Räume versiegeln, was unverhältnismässig wäre (BSK StPO-THORMANN/BRECHBÜHL, Art. 247 N 13).
[505] BGE 144 IV 74, E. 2.6 S. 79 f.
[506] Anh. 2: Interview WERREN/ZAUGG, Frage 2.5; Anh. 2: Interview WALDER, Frage 4.4.
[507] BGE 144 IV 74, E. 2.6 S. 79 f.
[508] BURCKHARDT/RYSER, 165.
[509] KELLER, StPO-Kommentar, Art. 248 N 3.
[510] Zum Ganzen BSK StPO-THORMANN/BRECHBÜHL, Art. 248 N 1; KELLER, StPO-Kommentar, Art. 248 N 3.
[511] BGE 106 IV 413 E. 7b S. 423.
[512] GRAF, Siegelung, 565.
[513] BSK StPO-THORMANN/BRECHBÜHL, Art. 248 N 14.

insofern die siegelungslegitimierte Person wesentliche Geheimnisinteressen vorbringt.[514] Dadurch können ineffiziente und ungerechtfertigte Doppelspurigkeiten verhindert werden.[515] Eine Beschwerde soll laut bundesgerichtlicher Rechtsprechung auch nicht möglich sein, wenn zusätzlich zum Geheimnisschutz weitere akzessorische Rügen, z.B. der fehlende Tatverdacht oder die Beweistauglichkeit der sichergestellten Aufzeichnungen, vorgebracht werden, da der Entsiegelungsrichter die zugrundeliegende Editionsverfügung resp. Zwangsmassnahme mit umfassender Kognition prüfen darf.[516]

2. Entsiegelung

Mit der Entsiegelung können die Strafbehörden auf die Siegelung reagieren. Gem. Art. 248 Abs. 2 StPO muss die Strafbehörde, d.h. die StA innerhalb von einer 20-tägigen Frist ein Entsiegelungsgesuch stellen, um die Herausgabe der versiegelten Aufzeichnungen und Gegenstände an die berechtigte Person verhindern zu können. Dieses Gesuch führt zur Einleitung des richterlichen Entsiegelungsverfahrens,[517] welches wiederum bezweckt, dass ein neutraler Richter über die Legitimität der Durchführung einer Durchsuchung entscheidet.[518] Im Vorverfahren hat das ZMG, in allen anderen Fällen der Sachrichter, innerhalb eines Monats den Entsiegelungsentscheid zu fällen (Art. 248 Abs. 3 StPO).[519] Als Parteien in diesem Entsiegelungsverfahren gelten die gesuchstellende StA und die zur Siegelung legitimierten Personen.[520] Die StA muss in ihrem Gesuch einen hinreichenden Tatverdacht geltend machen und mittels Beweismittel oder Indizien belegen, damit das Gericht eine Subsumtion unter einen oder mehrere Straftatbestände vornehmen kann.[521]

Die Gegenpartei, d.h. den Inhaber der versiegelten Aufzeichnungen, trifft hingegen eine prozessuale Begründungs- und Mitwirkungspflicht, da nur er den Inhalt seiner Aufzeichnungen kennt. Er muss beim Gericht die Geltendmachung von Geheimnissen genügend substantiieren und erklären, weshalb sein Geheimhaltungsinteresse das öffentliche Interesse zur Aufklärung der fraglichen Straftat überwiegt. Er hat die zu versiegelnden Akten und Datenträger zu bezeichnen und jene Dateien, die seiner Meinung nach der Geheimhaltung unterstehen deutlich zu benennen.[522] Da der Entsiegelungsrichter mit der Beurteilung einer ad-hoc-Beschwerde beauftragt ist, hat er nicht nur über das Bestehen und die Relevanz etwaiger Geheimnisse, sondern generell über die Rechtmässigkeit der Durchsuchung zu entscheiden.[523] Dabei kann er zum Ergebnis kommen, dass sämtliche, manche oder keine versiegelten Aufzeichnungen zur Durchsuchung durch die Strafbehörde freigegeben werden dürfen.[524] Gegen den Entsiegelungsentscheid des ZMG steht Betroffenen das Rechtsmittel der Beschwerde in Strafsachen gem. Art. 78 ff. BGG ans BGer zur Verfügung.[525]

---

[514] GRAF, Siegelung, 565; BSK StPO-THORMANN/BRECHBÜHL, Art. 248 N 61; SCHMID/JOSITSCH, Praxiskommentar StPO, Art. 248 N 6.
[515] GRAF, Siegelung, 565.
[516] BGer 1B_351/2016 E. 1.3; BGer 1B_360/2013 E. 2.2; BGer 1B_136/2012 E. 4.4.
[517] KELLER, StPO-Kommentar, Art. 248 N 39.
[518] BSK StPO-THORMANN/BRECHBÜHL, Art. 248 N 30.
[519] Die Frist von einem Monat entspricht einer reinen Ordnungsvorschrift, von der in komplexen Fällen abgewichen oder die durch Fristerstreckungsgesuche der Rechtvertreter verlängert werden kann (GRAF, Siegelung, 566).
[520] KELLER, StPO-Kommentar, Art. 248 N 43.
[521] KELLER, StPO-Kommentar, Art. 248 N 39.
[522] Zum Ganzen BGE 138 IV 225 E. 7.1 S. 229; BGE 137 IV 189 E. 4.2 S. 195; BGer 1B_233/2020 E. 1.3.
[523] BSK StPO-THORMANN/BRECHBÜHL, Art. 248 N 40.
[524] BSK StPO-THORMANN/BRECHBÜHL, Art. 248 N 40.
[525] BGer 1B_547/2020 E. 1.

3. Abgrenzung zwischen Durchsuchung von Aufzeichnungen und Überwachung

Inwiefern Durchsuchungen via Internetzugriff legitim und von der aktiven Kommunikationsüberwachung abzugrenzen sind, hatte das BGer in BGE 143 IV 270 zu beurteilen. Gemäss dessen Sachverhalt erhielt die Strafverfolgungsbehörde Kenntnis über die Zugangsdaten zu einem Facebook-Konto (Benutzername und Passwort) eines Untersuchungshäftlings, als der Häftling diese Daten als Kassiber aus dem Gefängnis schmuggeln wollte.[526] Der Zettel mit den Facebook-Zugangsdaten sollte eine in der Vollzugsanstalt arbeitende Sprachlehrerin erhalten und im Auftrag des Häftlings eine Facebook-Nachricht an dessen Lebenspartnerin senden. Die Nachricht richtete sich inhaltlich jedoch an zwei andere Personen, die als Mitbeschuldigte des Häftlings galten.[527] Das Personal des Untersuchungsgefängnisses stellte den Kassiber vor der Übergabe an die Lehrerin sicher, woraufhin die StA die Polizei mit der Sichtung des Facebook-Kontos (Onlinerecherche) und der vorläufigen Sicherstellung von beweisrelevanten Chat-Nachrichten unter Zuhilfenahme der ermittelten Zugangsdaten beauftragte.[528] Der besagte Häftling (Beschwerdeführer) brachte vor dem BGer u.a. vor, dass die StA ohne seine Zustimmung und ohne gesetzliche Grundlage seine Facebook-Zugangsdaten für eine Internet-Recherche und die Sicherstellung bzw. Durchsuchung der später gesiegelten Chat-Nachrichten verwendet hatte. Weder die Durchsuchung noch die Beschlagnahmung von elektronischen Daten sei zulässig gewesen. Chat-Nachrichten über Facebook würden wie E-Mails dem Schutz des Fernmeldegeheimnisses unterliegen, weshalb eine richterliche Fernmeldeüberwachung (nach Art. 269 ff. StPO) hätte angeordnet werden müssen.[529]

In seiner Beurteilung kam das BGer zum Schluss, dass das Vorgehen der Strafbehörde und deren gewählte Massnahmen bundesrechtskonform waren. Es legte fest, dass die Regeln zur Durchsuchung (Art. 246 StPO) nicht nur dann zur Anwendung kommen, wenn sich die Datenträger einer beschuldigten Person in der Hand der Polizei befinden, sondern auch, wenn die Strafverfolgungsbehörde durch fernmeldetechnischen Zugriff auf Daten bei Service Providern zugreifen kann, welche auf elektronischen Servern in diversen Ländern (sog. Clouds) gespeichert werden.[530] Das BGer argumentierte dabei wie folgt: Wenn die StA rechtmässig in den Besitz von Zugangsdaten zu einem Benutzerkonto gelange und sich dadurch Beweisunterlagen bzw. Chat-Nachrichten besorge, dann passiere dies übers Internet und nicht auf dem Weg einer Überwachung des Fernmeldeverkehrs.[531] Diese Vorgehensweise sei mit der Rechtslage im Falle der Erhebung von passwortgeschützter Fernmeldekommunikation gleichzusetzen (Art. 269 ff. StPO). Erlange die Untersuchungsbehörde (etwa über eine Beweisaussage oder eine erhobene Beweisurkunde) z.B. das Zugangspasswort zur Entsperrung eines sichergestellten und nicht gesiegelten Smartphones, so sei sie ermächtigt, die dort gespeicherte abgeschlossene Fernmeldekommunikation (vom Empfänger bereits abgerufene E-Mails oder SMS) zu sichten. Auch hier erfolge der Rechtschutz über die Siegelung.[532] Eine richterlich angeordnete Überwachung nach Art. 269 ff. StPO sei nur bei aktiver (vom Empfänger noch nicht abgerufener) Fernmeldekommunikation notwendig.[533]

HANSJAKOB erachtet den Entscheid des BGer u.a. als problematisch, weil dieser die Sicherstellung und Durchsuchung auf einen Sachverhalt anwendet, bei dem Daten mittels fernmeldetechnischen Zugriffes übers Internet, anstatt durch Beschlagnahme eines Datenträgers erhoben wurden. Seiner Meinung nach

[526] BGE 143 IV 270, Sachverhalt, lit. A S. 271 f.
[527] BGE 143 IV 270, Sachverhalt, lit. A und E. 5.2. S. 271 ff.; HANSJAKOB, Überwachungsrecht, N 328.
[528] BGE 143 IV 270, Sachverhalt, lit. A S. 271 f.; HANSJAKOB, Überwachungsrecht, N 328.
[529] BGE 143 IV 270, Sachverhalt, lit. A und E. 6.2. S. 271 ff.
[530] Zum Ganzen BGE 143 IV 270, Sachverhalt, lit. A S. 271 f.; HANSJAKOB, Überwachungsrecht N 328.
[531] BGE 143 IV 270 E. 7.1 S. 279 f.
[532] Zum Ganzen BGE 143 IV 270 E. 7.7 S. 285 f.
[533] BGE 143 IV 270 E. 7.7; m.w.H. BGE 140 IV 181 E. 2.6 f. S. 186 f.

müsste dieses Vorgehen der Strafbehörden unter die Bestimmungen der Überwachung gem. Art. 269 ff. StPO fallen.[534] Er argumentiert, dass die Kommunikation über den Facebook-Messenger mit dem E-Mail-Verkehr vergleichbar und deshalb vom Fernmeldegeheimnis geschützt sei. Solche Messenger-Nachrichten würden als Inhaltsdaten der Kommunikation gelten und müssten mittels Durchsuchung bei der beschuldigten Person, jedoch nicht auf dem Weg der Fernmeldekommunikation gegen den Willen des Beschuldigten, abgerufen werden.[535] Dieser Kritik von HANSJAKOB ist m.E. nicht beizupflichten, weil er verkannte, dass der Aufruf des Facebook-Kontos und dessen Kommunikationsinhalte über die Zugangsdaten gerade keinen Kommunikationsvorgang auslöste. Ferner gilt es zu bemerken, dass auch der tatsächliche Messenger-Verkehr nicht mehr vom Fernmeldegeheimnis geschützt war, sobald die Nachrichten abgerufen wurden.[536]

Unabhängig davon, dass eine Überwachung gemäss der damals geltenden Rechtslage gar nicht möglich gewesen wäre,[537] ist m.E. die bundesgerichtliche Qualifikation des Internetzugriffs mittels Zugangsdaten als Sicherstellung und Durchsuchung richtig. Zugleich war und ist dieser Entscheid aber auch wegweisend für die Modalitäten, wie eine Durchsuchung von Benutzerkonten stattfinden kann und darf.[538] Aufgrund dieses Entscheids scheint es m.E. somit gerechtfertigt, dass die elektronisch aufgeschalteten Angebote von Nutzern auf Verkaufsplattformen in den beiden Darknet-Entscheiden mithilfe der Zwangsmassnahme der «Durchsuchung von Aufzeichnungen» durchsucht werden durften. Die betroffenen Nutzer werden zudem bei solchen Konstellationen mit dem Rechtsbehelf der Siegelung ausreichend gegen den staatlichen Grundrechtseingriff geschützt.

D Beschlagnahme nach Art. 263 ff. StPO

Die Zwangsmassnahme der Beschlagnahme dient dazu, deliktsrelevante Gegenstände oder Vermögenswerte ohne Zustimmung der betroffenen Person im Rahmen des Strafverfahrens zu entziehen bzw. einer Verfügungsbeschränkung zu unterwerfen.[539] Die Beschlagnahme ist zu differenzieren zwischen den Durchsuchungen und Untersuchungen gem. Art. 241 ff. StPO, die nur vorbereitenden, und der Einziehung gem. Art. 69 ff. StGB, die definitiven Charakter hat.[540] Gem. Art. 263 Abs. 1 StPO können Gegenstände und Vermögenswerte beschlagnahmt werden, wenn diese wahrscheinlich als Beweismittel verwendet, zur Sicherstellung von Verfahrenskosten, Geldstrafen oder Bussen dienen sowie den Geschädigten wiederzugeben oder einzuziehen sind. Somit differenziert Art. 263 Abs. 1 StPO folgende vier Beschlagnahmearten: die Beweismittel- (lit. a), die Kostendeckungs- (lit. b), die Restitutions- (lit. c) und die Einziehungsbeschlagnahme[541] (lit. d), wobei erstere und letztere im Zusammenhang mit der Beschlagnahme von Benutzerkonten auf Darknet-Verkaufsplattformen von grösster Bedeutung sind.[542]

[534] Zum Ganzen HANSJAKOB, Überwachungsrecht, N 330 und 332.
[535] Zum Ganzen HANSJAKOB, Überwachungsrecht, N 330.
[536] Gl.M. DUSANEK, 34.
[537] Nach der damaligen Rechtslage waren Art. 269 ff. StPO auf abgeleitete Internetdienste wie Facebook (FB) gar nicht anwendbar (BGE 143 IV 270 E. 7.1 S. 279 f.); HANSJAKOB, Überwachungsrecht, N 328: bemerkt richtig, dass dies nach heutigem Recht anders ist und das BÜPF nun grundsätzlich auch AAKD erfasst, jedoch nur solche, welche dem Schweizerischen Recht unterliegen.
[538] Anh. 4: Fragebogen WALDMEIER, Frage 2.11.
[539] SCHMID/JOSITSCH, Praxiskommentar StPO, vor Art. 263-268 N 1; RIKLIN, Kommentar StPO, Art. 263 N 1.
[540] SCHMID/JOSITSCH, Praxiskommentar StPO, vor Art. 263-268 N 1.
[541] Wird auch als Konfiskationsbeschlagnahme bezeichnet.
[542] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 9, 32, 48 und 53.

1. Vorliegend relevante Beschlagnahmearten

Die Beweismittelbeschlagnahme hat zum Zweck, im Rahmen des Strafprozesses wesentliche Abklärungen in tatsächlicher Hinsicht vorzunehmen und dadurch den grundlegenden Sachverhalt für die materielle Strafrechtsanwendung zu ermitteln. Es werden insofern diejenigen sachlichen Beweismittel provisorisch sichergestellt, die der Ermittlung der materiellen Wahrheit dienen.[543] Voraussetzung für eine Beweismittelbeschlagnahme ist ein laufendes Strafverfahren, die Beweisbedeutung des zu beschlagnahmenden Gegenstands sowie das Fehlen eines Beschlagnahmeverbots.[544] Hinsichtlich der Anwendbarkeit auf Benutzerkonten auf Darknet-Verkaufsplattformen wird noch zu erläutern sein, ob diese ein geeignetes Beweisobjekt darstellen, da die Beweismittelbeschlagnahme nur «Gegenstände» umfasst.[545] Die Einziehungsbeschlagnahme beabsichtigt indessen den Einzug von vorläufig sichergestellten und gegebenenfalls rechtsgutgefährdenden Gegenständen (Sicherungseinziehungsbeschlagnahme) oder inkriminierten Vermögenswerten (Vermögenseinziehungsbeschlagnahme).[546] Beide Beschlagnahmen erfolgen entweder im Zuge eines laufenden Strafverfahrens oder als selbständiges Massnahmeverfahren (i.S. eines Einziehungsverfahrens gem. Art. 377 Abs. 1 StPO).[547]

a Vermögenseinziehungsbeschlagnahme

Die rechtmässige Vermögenseinziehungsbeschlagnahme richtet sich nach dem Umfang der zulässigen Vermögenseinziehung gem. Art. 70 ff. StGB.[548] Demnach unterliegen Vermögenswerte der Beschlagnahme, wenn sie durch eine Straftat erlangt worden sind (Tatgewinn) oder zu deren Veranlassung oder Belohnung (Tatlohn) bestimmt waren und die Vermögenswerte nicht zur Wiederherstellung des rechtmässigen Zustandes dem Verletzten ausgehändigt werden müssen.[549] Hauptsächlich eingezogen werden Vermögenswerte, die mutmasslich durch eine Straftat erlangt worden sind, wie bspw. Diebesbeute oder Erträge aus Straftaten ohne individuellen Geschädigten, etwa aus unerlaubtem Handel mit Betäubungsmitteln.[550]

Unter Vermögenswerte wird im Sinne des Vermögensstrafrechts *jeder konkrete spezifische Vermögensbestandteil* verstanden.[551] Auch i.S.v. Art. 70 StGB wird der Begriff des Vermögenswerts eher weit gefasst, in dem alle Güter in Frage kommen, denen ein abstrakter Tauschwert zukommt, *d.h. all jene Güter, die Gegenstand eines Rechtsgeschäftes «Tausch gegen Geld»* sein können.[552] Als Vermögenswerte gelten somit u.a. Gegenstände bzw. Sachen (Bargeld und Wertpapiere), Forderungen bzw. allgemeine Rechte, insb. Bankguthaben, immaterielle[553] und andere Rechte, d.h. auch Daten.[554] Letzt-genannte bilden dann einen Vermögenswert, wenn sie verkäuflich sind.[555] BOMMER überträgt diese Überlegungen auf Daten, welche strafbare Gewaltdarstellungen sowie pornografische oder rassendiskriminierende Aufzeichnungen umfassen. Er kommt zum Schluss, dass diese Aufzeichnungen als *producta sceleris* eher das Substrat der Straftat darstellen und weniger «durch die strafbare Handlung erlangt»

[543] AEPLI, 5; HEIMGARTNER, 73.
[544] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 10.
[545] Vgl. SIMMLER ET AL., 970, ihr Aufsatz bezieht sich auf die Beschlagnahme von Kryptowährungen.
[546] HEIMGARTNER, 80 ff.; BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 33 und 41; BSK StGB-BAUMANN, Art. 69 N 2.
[547] HEIMGARTNER, 81; BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 35 und 40.
[548] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 41.
[549] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 41 f.; BSK StGB II-BAUMANN, Art. 70/71 N 12.
[550] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 43.
[551] BSK StGB-NIGGLI/RIEDO, Vor Art. 137 N 62.
[552] NIGGLI, 262 und 280.
[553] BSK StGB-BAUMANN, Art. 70/71 N 44.
[554] RYSER, 560; AEPLI, 37.
[555] BOMMER, 174 f.

wurden und lehnt deshalb eine Einziehung von Daten als Vermögenseinziehung ab.[556] Diese scheide ohnehin aus, wenn solche pornografischen oder rassendiskriminierenden Daten ohne Vermögenswert seien oder der Feststellung dieser Vermögenswerte praktische Hindernisse[557] im Wege stehen.[558] Er schlussfolgert, dass die Einziehung dieser Daten entweder im Rahmen einer Sicherungseinziehung (Art. 69 StGB) oder gem. den entsprechenden Sonderbestimmungen[559] zu erfolgen hat.[560] Werden die eben gemachten Ausführungen nun auf Benutzerkonten von Darknet-Plattformen angewendet, ergibt sich m.E. bereits das Problem, dass die «Vermögenswerte» (i.c. Zugangsdaten) nicht durch eine Straftat erlangt oder dazu bestimmt waren, eine solche zu veranlassen resp. zu belohnen (vgl. Art. 70 Abs. 1 StPO). Die Benutzerkonten dienten eher als Hilfsmittel zur eigentlichen Straftat, da sie den Verkäufern dazu dienten, ihre Drogen einem interessierten Abnehmerkreis zu präsentieren und Verkäufe abzuwickeln. Ebenfalls fraglich ist m.E., ob die Zugangsdaten überhaupt einen Vermögenswert darstellen und wie sich ein Entgelt dafür festlegen liesse. Eine Deklaration der Zwangsverwaltung resp. Beschlagnahme von Darknet-Benutzerkonten unter die Vermögenseinziehungsbeschlagnahme gem. Art. 263 Abs. 1 lit. d StPO scheint m.E. nicht zielführend.

b Sicherungseinziehungsbeschlagnahme

Anhand der Sicherungseinziehungsbeschlagnahme sollen einerseits weitere Rechtsgutgefährdungen verhindert und andererseits die wichtigen Polizeigüter wie Sittlichkeit, Sicherheit und öffentliche Ordnung geschützt werden.[561] Fehlen Spezialbestimmungen im StGB oder den Nebengesetzen, so richten sich die Grenzen der rechtmässigen Beschlagnahme nach Art. 69 StGB.[562] Die Beschlagnahme zur Sicherungseinziehung ohne gleichzeitige Beweismittelbeschlagnahme des Gegenstands scheint eher selten. Denn die Sicherungseinziehung bedingt, dass der Gegenstand i.S.v. Art. 69 StGB gefährlich ist, was wiederum dessen Verfügbarkeit als Beweisgegenstand erfordert.[563] Die Beschlagnahme richtet sich gegen den Inhaber des einzuziehenden Gegenstands und ist nur zulässig, wenn:

- eine Straftat begangen oder eine solche ernsthaft vorbereitet wurde,
- Gegenstände sichergestellt wurden, die zur strafbaren Handlung einen Bezug aufweisen, indem sie zur Realisation der strafbaren Handlung genutzt wurden oder bestimmt waren (Tatinstrument) oder durch die Straftat entstanden (Tatprodukt),
- die Gegenstände eine konkrete Gefahr für (eben genannte) Polizeigüter darstellen
- die Einziehung als verhältnismässig erscheint.[564]

Als Straftat gem. Art. 69 StGB kommt jede Straftat nach Bundesrecht (inkl. Nebenstrafgesetzgebung) in Frage.[565] Dabei müssen die einzuziehenden Gegenstände einen zwingenden Bezug zu dieser Straftat aufweisen. Unter Tatinstrumente fallen bspw. Waffen und Munition sowie Kopiergeräte für das Herstellen von Pornofilmen. Als Tatprodukte werden z.B. Fälschungen von Geld, gefälschte Urkunden,

[556] MwH. BOMMER, 174 ff.
[557] Bspw. die Eruierung eines allfälligen Wertes auf dem Schwarzmarkt.
[558] BOMMER, 177.
[559] Z.B. im Falle von harter Pornografie gem. Art. 197 Abs. 4 und 5 StGB erfolgt die Einziehung nach Art. 197 Abs. 6 StGB, dasselbe gilt für Gewaltdarstellungen gem. Art. 135 Abs. 2 StGB.
[560] BOMMER, 176 f.; Sämtliche Ausführungen von BOMMER beziehen sich auf die Art. 58 und 59 aStGB, welche den heutigen Art. 69 und 70 StGB entsprechen.
[561] HEIMGARTNER, Beschlagnahme, 81; BSK StGB-BAUMANN, Art. 69 N 2.
[562] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 36.
[563] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 2.
[564] Zum Ganzen Art. 69 Abs. 1 StPO; BSK StGB-BAUMANN, Art. 69 N 2 und 5.
[565] BSK StGB-BAUMANN, Art. 69 N 6.

Pornographie i.S.v. Art. 197 StGB, Betäubungsmittel und deliktisch hervorgebrachte Daten gem. Art. 4 ff. DSG deklariert.[566]

Neben dem Deliktskonnex muss vom Gegenstand auch eine bestehende und zukünftige Gefährdung ausgehen. An diese sind keine übertrieben hohen Anforderungen zu stellen: Es genügt, dass die Gefährdung wahrscheinlich ist, falls der betreffende Gegenstand nicht eingezogen wird.[567] Auf die Benutzerkonten für Darknet-Plattformen scheinen die Voraussetzungen, unabhängig von der fraglichen Qualifikation als «Gegenstand», erfüllt zu sein. Die Benutzerkonten könnten als Tatinstrument klassifiziert werden, da sie den Beschuldigten in den Bundesgerichtsentscheiden zur Abwicklung des Verkaufs von grossen Mengen an Betäubungsmitteln dienten, was gem. Art. 19 Abs. 2 lit. c BetmG strafbar ist.[568] Die von diesen Benutzerkonten ausgehende Gefährdung kann wiederum dadurch begründet werden, dass das darüber ermöglichte Inverkehrbringen von Betäubungsmitteln eine Gefahr für die Gesundheit Einzelner darstellt. Gleichzeitig haben suchtbedingte Störungen Einzelner jedoch beträchtliche weitere Folgen für die Bevölkerung und können die öffentliche Ordnung und Sicherheit gefährden.[569]

2. Eignung von Daten als Beschlagnahmeobjekt

a Lehrmeinungen bezüglich Daten als Gegenstand

Wie bereits kurz ausgeführt wurde, können generell «Gegenstände» beschlagnahmt werden, worunter bewegliche körperliche Sachen zu verstehen sind.[570] Daten werden aufgrund ihrer mangelnden Körperlichkeit eben gerade nicht als Sache betrachtet.[571] Obwohl unter dem Sachbegriff nach h.L. und Rechtsprechung nur körperliche Gegenstände verstanden werden, ist beim Gegenstandsbegriff nach Art. 263 Abs. 1 StPO unklar, ob auch unkörperliche Objekte, wie elektronische Daten darunter fallen.[572] Gemäss BOMMER und GOLDSCHMID gelten als körperliche Gegenstände auch solche, die nicht wegen ihrer eigenen originären Beschaffenheit beweistauglich sind, sondern im Zusammenhang mit ihrer Funktion als Informationsträger tauglich sind.[573] Die h.L. vertrat bislang die Auffassung, dass deshalb nur auf einem physischen Datenträger (USB-Stick, Speicherplatte etc.) gespeicherte elektronische Daten, die gewissermassen «fassbar» sind,[574] der Beschlagnahme unterliegen.[575]

Eine Beschlagnahme von Datenträgern, auf denen sich die massgeblichen Zugangsdaten zu einem Benutzerkonto befinden, wäre somit zulässig. Dies erfüllt aber den Zweck der Zwangsmassnahme, nämlich einer effektiven Sicherstellung, nicht, da die beschuldigte Person weiterhin die Verfügungsgewalt behält, indem sie anhand der Zugangsdaten das Benutzerkonto ohne Weiteres auf einem anderen Speichermedium aufrufen kann. Es stellt sich deshalb die Frage, ob die Subsumption von nicht fassbaren Daten, resp. dezentral gespeicherten Daten unter den Gegenstandsbegriff erfolgen kann. Eine geeignete

[566] Zum Ganzen BSK StGB-BAUMANN, Art. 69 N 9 ff.
[567] BSK StGB-BAUMANN, Art. 69 N 13.
[568] Vgl. Kap. II. C 1.
[569] Botschaft 2001 BetmG, 3733 und 3754; Botschaft 2019 BetmG, 2530; HUG-BEELI, Art. 1 N 5 f.
[570] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 26 ff.; HEIMGARTNER, Beschlagnahme, 76.
[571] BSK StGB-NIGGLI/RIEDO, Vor Art. 137 N 37 und 68.
[572] SIMMLER ET AL., 971.
[573] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 27.
[574] HEIMGARTNER, StPO-Kommentar, Art. 263 N 1a; HEIMGARTNER, Beschlagnahme, 87.
[575] SCHMID, Strafprozessrecht, N 755; SCHMID, Computerdelikte, 96; AEPLI, 45 f.; BANGERTER, 245 f. und 280 ff.; DONATSCH/SCHMID, 162 f.; HEIMGARTNER, Beschlagnahme, 89; RYSER, 561; BOMMER, 178 f., äussert sich bezüglich der Beschlagnahme der Träger von Daten im Zusammenhang mit der Sicherungseinziehung.

Beschlagnahme von Benutzerkonten auf Darknet-Verkaufsplattformen bedingt einen Zugriff auf die immaterielle Information an sich.[576]

b Lehrmeinungen bezüglich der Beschlagnahmefähigkeit von Daten

In der Botschaft zur StPO werden Daten oder Datenträger im Zusammenhang mit den Bestimmungen zur Beschlagnahme nicht ausdrücklich erwähnt.[577] Inwiefern Daten, unabhängig von ihrem Datenträger und damit auch ein Benutzerkonto auf einer Darknet-Plattform, in weiterer Auslegung des Gegenstandsbegriffs der Beschlagnahme unterliegen könnten, ist gemäss den verschiedenen Lehrmeinungen nicht eindeutig zu beurteilen.[578] Laut HEIMGARTNER impliziert die Anwendung der grammatikalischen Auslegung, dass der Gegenstandsbegriff weiter zu fassen ist, als der Sachbegriff. So kann ein Gegenstand i.w.S. «als Synonym für ein abgeschlossenes, reales oder ideales Objekt, das dem Betrachter gegenübersteht» aufgefasst werden, was somit auch mit dem Sinn und Zweck der Beschlagnahme übereinstimmt.[579] Ähnlich argumentiert auch BANGERTER, für den sich eine Beschränkung auf körperliche Objekte einzig aus der historischen Auslegung ergibt und es deshalb angezeigt ist, den Gegenstandsbegriff auch auf unkörperliche Objekte auszuweiten.[580] Insb. die systematische Auslegung zeige, dass mit der Einführung des Art. 246 StPO zur Durchsuchung von Aufzeichnungen, festgelegt wird: «[Dass] Datenträger sowie Anlagen zur Verarbeitung und Speicherung von Informationen […] durchsucht [werden dürfen], wenn zu vermuten ist, dass sich darin Informationen befinden, die der Beschlagnahme unterliegen.» Damit statuiere die StPO, dass Informationen losgelöst vom Datenträger beschlagnahmt werden können.[581] BURGERMEISTER spricht sich ebenfalls für eine Beschlagnahme von elektronischen Daten unabhängig von einem Datenträger aus und beruft sich dabei aber nicht auf die Auslegung der Rechtsnorm. Er argumentiert damit, dass das BGer bei mehreren Entsiegelungsverfahren[582] bei fraglichen Datenträgern, welche Daten enthielten, die dem Anwaltsgeheimnis unterstanden, entschied, dass einzelne Daten auszusondern seien und versiegelt bleiben müssen. Müssen diese Daten ausgeschieden werden, bedingt dies für BURGERMEISTER, dass elektronische Daten unabhängig von ihrem Datenträger gem. Art. 263 StPO beschlagnahmt werden können.[583] SCHMID erläutert, dass Zwangsmassnahmen nach dem Grundsatz a *maiore ad minus*[584] auch auf immaterielle Informationen Anwendung finden könnte und dadurch eine Ausweitung auf die Einziehung von unkörperlichen, dezentral gespeicherten Daten gerechtfertigt sei.[585]

[576] Vgl. zum Ganzen SIMMLER ET AL., 963 ff., ihre Ausführungen beziehen sich auf Kryptowährungen. Die Beschlagnahme von Kryptowährungen stellt die Strafbehörden vor ähnliche Herausforderungen, wie diejenige von Benutzerkonten auf Darknet-Plattformen.
[577] Botschaft StPO, 1245 ff.; SIMMLER ET AL., 972.
[578] Vgl. SIMMLER ET AL., 972.
[579] HEIMGARTNER führt weiter aus, dass es inkonsistent wäre, wenn die Beschlagnahme von Vermögenswerten in Form von unverbrieften Forderungen explizit vorgesehen (vgl. Art. 266 Abs. 4 StPO) und demgegenüber andere immaterielle Objekte als nicht beschlagnahmefähig klassifiziert werden (HEIMGARTNER, Beschlagnahme, 89 f.).
[580] BANGERTER, 246 ff.
[581] BANGERTER, 247.
[582] BURGERMEISTER stützt seine Argumentation auf nachfolgende Entscheide: BGE 126 II 495, E. 5e/aa S. 501 f.; BGE 130 II 193 E. 2.1 S. 195; BGE 137 IV 189 E. 4 S. 194.
[583] Zum Ganzen BURGERMEISTER, 8 f.
[584] In der Lehre und Praxis werden nach dieser Maxime teilweise nicht explizit im Gesetz vorgesehene Massnahmen als rechtmässig erachtet, wenn sie weniger weit gehen als die gesetzlich definierten Massnahmen (HEIMGARTNER, Beschlagnahme, 64).
[585] SCHMID, Computerdelikte, 96.

Anderer Meinung ist u.a. AEPLI, der schlussfolgert, dass Daten keine Gegenstände sind und folglich nur in verkörperlichter Form, mittels dem Speichermedium oder als Ausdruck auf Papier der Beweismittelbeschlagnahme unterliegen.[586] Ebenfalls dieser Meinung ist RYSER.[587] Gemäss BOMMER können Daten als unkörperliche Objekte auch bezüglich der Einziehung nicht als Gegenstände verstanden werden.[588]

c Gerichtspraxis bezüglich Beschlagnahmefähigkeit von Daten

Die Beschränkung des Gegenstandbegriffs auf körperliche Objekte wird in der Lehre[589] auf BGE 126 I 50 zurückgeführt.[590] Dabei hat das BGer dem Einwand der Beschwerdeführerin zugestimmt, dass Gegenstände als Objekte verstanden werden, die «gewissermassen aus der Schublade herausgenommen werden könnten».[591] BANGERTER vertritt jedoch die Auffassung, dass dieser Satzteil einzig bedeutet, dass die Herausgabepflicht und Beschlagnahme nur Gegenstände umfassen, welche schon existieren und dementsprechend aus der Schublade genommen werden können. *E contrario* sei die Metapher so zu verstehen, dass Gegenstände, die erst noch erstellt werden müssen, den eben erwähnten Pflichten nicht unterstehen. Somit stehe die bundesgerichtliche Rechtsprechung einer weiten Auslegung des Gegenstandsbegriffs nicht entgegen. [592]

Im bereits erwähnten Facebook-Entscheid BGE 143 IV 270 finden sich ebenfalls Hinweise zur vorliegend diskutierten Thematik. Gemäss dem BGer bestand in diesem Falle eine grosse Verdunkelungsgefahr, da ernsthaft zu befürchten war, dass der Häftling die per Internet zugänglichen untersuchungsrelevanten Beweismittel noch vor dem behördlichen Zugriff hätte löschen oder manipulieren können.[593] Da für solche Fälle von «Gefahr in Verzug» eine vorläufige Sicherstellung von Aufzeichnungen ausdrücklich im Gesetz vorgesehen ist, durfte die Polizei gemäss dem BGer mittels der rechtmässig erlangten Zugangsdaten die elektronischen Dateien (Chat-Nachrichten) auf dem Facebook-Konto des Häftlings vorläufig nach den Regeln der Durchsuchung von Datenträgern sicherstellen lassen (Art. 246 und Art. 263 Abs. 3 und Art. 265 Abs. 4 StPO).[594] Dabei waren die von der Polizei sichergestellten Chat-Nachrichten bei Facebook auf elektronischen Servern in diversen Ländern in Internet-Clouds gespeichert und konnten online sichergestellt werden.[595] Durch Erstellung von elektronischen Kopien wurden die sichergestellten Nachrichten von der Untersuchungsbehörde zu den Akten genommen (Art. 192 Abs. 2 i.V.m. Art. 263 Abs. 3 StPO),[596] d.h. die Daten wurden, losgelöst von einem physischen Datenträger, als Beweismittel vorläufig durch die Polizei sichergestellt. Eine solche vorläufige Sicherstellung überträgt der Polizei und auch Privatpersonen die Notkompetenz zur Sicherstellung von Gegenständen und Vermögenswerten zuhanden der StA oder der Gerichte.[597] Bei einer vorläufigen Sicherstellung handelt es sich in sachlicher Hinsicht nicht um eine Beschlagnahme im technischen Sinne, weil sie nicht von der dafür zuständigen Behörde (StA oder Gericht, gem. Art. 198 Abs. 1 StPO) angeordnet wird.[598] Die vorläufige

[586] AEPLI, 44 ff, 123, insb. 59 f. Seine Meinung basiert v.a. auf der grammatikalischen, historischen, systematischen, zeitgemässen und teleologischen Auslegung von §§ 96 Abs. 1 ZH-StPO (dieser Paragraf entspricht grösstenteils dem heutigen Art. 263 StPO).
[587] Nur die teleologische Auslegung liess den Schluss zu, auch unkörperliche Objekte zu erfassen (RYSER, 561).
[588] BOMMER, 178.
[589] AEPLI, 45; BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 28; SIMMLER ET AL., 972; JOSITSCH/POULIKAKOS, 152.
[590] BANGERTER, 248.
[591] BGE 126 I 50 E. 4c S. 58 f.
[592] Zum Ganzen BANGERTER, 248.
[593] BGE 143 IV 270 E. 7.6 S. 283 f.
[594] BGE 143 IV 270 E. 7.5 f. S. 282 ff.
[595] BGE 143 IV 270 E. 7.5 S. 282.
[596] BGE 143 IV 270 E. 7.6 S. 283 f.
[597] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 7.
[598] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 7.

Sicherstellung erfüllt aber dieselben Ziele wie eine Beschlagnahme.[599] Die Sicherstellungsbefugnis ist vom Umfang her deckungsgleich mit derjenigen einer ordentlichen Beschlagnahme.[600] Zusammenfassend kann daraus geschlossen werden, dass das BGer im eben erwähnten Facebook-Entscheid eine implizite Beschlagnahmefähigkeit von elektronischen Daten ohne Speichermedium annahm.

3. Durchführung der Beschlagnahme / Zwangsverwaltung in der Praxis

Mit der Beschlagnahme werden der Entzug und die Übertragung der Verfügungsgewalt über Gegenstände oder Vermögenswerte von dessen Inhaber auf eine Behörde bezweckt.[601] Wie eine solche Beschlagnahme zu erfolgen hat, ist von ihrem Gegenstand abhängig, wobei bspw. bewegliche Sachen typischerweise mittels physischer Ergreifung und Grundstücke mittels Verfügungssperre im Grundbuch beschlagnahmt werden.[602] Daten können grundsätzlich entweder durch die Einziehung des Datenträgers, auf denen sie sich befinden oder durch eine Kopie der Festplatte (sog. Spiegelung) sichergestellt werden.[603] Obwohl die Benutzerkonten auch in der Praxis gespiegelt, d.h. ein forensisches Image zur Sicherstellung des Inventars angefertigt wird, muss die Strafbehörde zu Beweiszwecken auch das Original sicherstellen, da der Beschuldigte bspw. behaupten könnte, dass gewisse Daten nur auf der Kopie gespeichert sind. Um beim Original-Benutzerkonto den unerwünschten Zugriff durch den Inhaber oder Dritte zu verhindern, ändert die Strafbehörde erstens das vom Inhaber gesetzte Passwort und setzt zweitens die E-Mail-Adresse zurück. Dadurch wird verhindert, dass der Inhaber des Benutzerkontos ein neues Passwort beantragen und sich erneut einloggen kann.[604]

Obwohl die StPO in Art. 266 für diese konkrete Methode keine spezifische rechtliche Grundlage bereithält, scheint eine solche Zwangsverwaltung einerseits dem Zweck der Beschlagnahmebestimmung zu entsprechen, weil nur damit die Verfügungsmacht des Beschuldigten über sein Konto verunmöglicht und dieses wirklich in die Verfügungsgewalt des Staates übertragen werden kann.[605] Andererseits werden die Behörden gem. Art. 266 Abs. 2 StPO dazu angehalten, die beschlagnahmten Gegenstände «sachgemäss» aufzubewahren, woraus SIMMLER ET AL. ableiten, dass die Behörden gefordert sind, in der Verfolgung des Sicherstellungszwecks eine adäquate Vorgehensweise zu finden.[606] Wie die Befragungen der Zürcher und Aargauer Staatsanwälte gezeigt haben, scheint diese Form der Zwangsverwaltung momentan auch die einzige praktikable und adäquate Lösung zu sein, um dem Beschlagnahmezweck im Zusammenhang mit Darknet-Benutzerkonten gerecht zu werden.[607] Obwohl die Aargauer und Zürcher Strafbehörden die Kontrolle über die Benutzerkonten übernahmen, liessen sie die Angebote weiterhin bestehen. Die ursprünglichen Bilder zu den jeweiligen Drogenangeboten wurden jedoch durch Mitteilungen wie «beschlagnahmt durch StA II, Zürich» auf Englisch ersetzt. Gemäss WALDER führte dies in den einschlägigen Darknet-Foren zur gewaltigen Aufruhr und zur Verunsicherung von Drogenkäufern. Die Zürcher Strafbehörde konnte gar in den Kommunikationsdaten einer anderen Tätergruppe lesen, dass diese aufgrund des erhöhten Risikos von den Strafbehörden identifiziert zu werden, keine Delikte mehr in der Schweiz verüben wollte.[608] Dies lässt den Schluss zu, dass die Zwangsverwaltung

[599] HEIMGARTNER, Beschlagnahme, 34.
[600] BSK StPO-BOMMER/GOLDSCHMID, Art. 263 N 7.
[601] RIEDO/FIOLKA/NIGGLI, N 1933; BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 1.
[602] BSK StPO-BOMMER/GOLDSCHMID, Vor Art. 263-268 N 8; Vgl. 266 Abs. 3 StPO.
[603] HEIMGARTNER, Beschlagnahme, 90; m.w.H. RYSER, 567.
[604] Zum Ganzen Anh. 2: Interview WALDER, Frage 2.2 und 2.4.
[605] Vgl. SIMMLER ET AL., 974.
[606] Vgl. SIMMLER ET AL., 975.
[607] Anh. 2: Interview WALDER, Frage 2.2 und 2.4; Anh. 4: Fragebogen WALDMEIER, Frage 2.3 f.
[608] EIHOLZER, Frage 21.

von Benutzerkonten durch die Strafbehörden allenfalls eine präventive Wirkung auf andere Nutzer von Darknet-Plattformen haben kann.

Zusammenfassend lässt sich sagen, dass es spannend und wünschenswert gewesen wäre, wenn sich das BGer in den beiden Entscheiden konkret zur Rechtmässigkeit der Zwangsverwaltung von Benutzerkonten durch die Strafbehörden geäussert hätte. Gleichzeitig scheint m.E. die in den Entscheiden angetönte Klassifizierung als Einziehungsbeschlagnahme gerechtfertigt, da sie einerseits im Einklang mit den jüngeren Lehrmeinungen steht, die den Gegenstandsbegriffs von Art. 263 Abs. 1 StPO weit auslegen und andererseits auch der jüngeren Rechtsprechung von BGE 143 IV 270 folgt.

E Grenzüberschreitende Zwangsmassnahmen zur Datensicherung

Obwohl die diskutierten Urteile sich nicht zur Problematik von im Ausland gelegenen Daten äussern mussten, da dies vom Beschuldigten nicht direkt gerügt wurde, ist dies bezüglich Darknet-Plattformen von grosser Wichtigkeit.

1. Das Territorialitätsprinzip

Das Territorialitätsprinzip gilt als «die primäre Grundlage des sog. internationalen Strafrechts» und ist im Schweizerischen Strafrecht in Art. 3 StGB verankert.[609] Es beschränkt die Anwendbarkeit des nationalen Strafrechts auf ausländische Sachverhalte und begrenzt staatliches Handeln auf das eigene Staatsgebiet.[610] Ein Staat, der auf fremdem Hoheitsgebiet eigenmächtige Handlungen mit Zwangs- und Eingriffscharakter begeht, verletzt grundsätzlich die Souveränität des anderen Staates und das Völkerrecht,[611] wenn diese Handlungen nicht durch internationale Rechtshilfeabkommen, bi- oder multilaterale Verträge oder Genehmigungen legitimiert sind.[612] Zu den Amtshandlungen, die das Territorialitätsprinzip zu berücksichtigen haben, zählt das BGer explizit die Zwangsmassnahmen und im Bereich der Rechtshilfe besonders die Beweismittelbeschlagnahmungen, Fernmeldeüberwachungen[613] und Datenerhebungen bei im Ausland ansässigen Access und Service Provider.[614]

2. Internationale Rechtshilfe und Übereinkommen über Cyberkriminalität

Die Rechtshilfe gründet auf der Tatsache, dass ein Staat nur innerhalb seines Territoriums tätig werden darf und deshalb zwingend auf die Zusammenarbeit mit anderen Staaten angewiesen ist. Als Rechtshilfe wird somit die materielle Unterstützung des ersuchten Staates an den ersuchenden Staat bezeichnet.[615] Die Rechtsgrundlagen für die Rechtshilfe befinden sich im Bundesgesetz über internationale Rechtshilfe in Strafsachen (IRSG) sowie in verschiedenen bi- oder multilateralen Verträgen.[616] Da förmliche Rechtshilfeverfahren von übergeordneten Stellen auf dem behördlichen oder diplomatischen Weg weitergeleitet werden müssen, dauern diese häufig sehr lange und gestalten sich sehr aufwändig. Sie sind deshalb bereits bei der Verfolgung von «normaler» Kriminalität regelmässig nicht erfolgversprechend.[617] Bei

[609] BGE 108 IV 145 E. 3 S. 146 f.
[610] BGE 140 IV 86 E. 2.4 S. 89 f.
[611] GLESS, Beweisverbote, 322.
[612] GRAF, Strafverfolgung 2.0, N 21.
[613] BGE 141 IV 108 E. 5.3 S. 121.
[614] BGE 143 IV 270 E. 4.7 S. 275; BGE 143 IV 21 E. 3.2 S. 24.
[615] BSK ISTR-HEIMGARTNER/NIGGLI, Einführung N 11 und 19.
[616] HEIMGARTNER, Internetstraffälle, 136.
[617] SCHWEINGRUBER, N 4 ff.

Cybercrimes ergibt sich zudem häufig das Problem, dass der Zeitraum zur verpflichtenden Datenspeicherung der Provider bereits abgelaufen ist, bevor das Rechtshilfeersuchen bearbeitet wurde.[618] Damit eine Vielzahl von Delikten im Internet nicht straffrei bleiben, braucht es pragmatische Lösungen zum grenzüberschreitenden Datenzugriff, wobei die CCC[619] eine mögliche Lösung darstellt.[620] Die CCC, die am 1.1.2012 durch die Schweiz in Kraft gesetzt wurde,[621] möchte die effiziente Bekämpfung der Computerkriminalität bezwecken, indem sie die geltenden bi- oder multilateralen Verträge zwischen den Mitgliedsstaaten insofern ergänzt, als dass eine gut funktionierende und schnelle internationale Kooperation in Strafsachen sichergestellt wird.[622]

Grundsätzlich sieht auch die CCC für ihre Vertragsparteien den Rechtshilfeweg vor (in Art. 31), wenn Daten, die auf Computersystemen gespeichert sind, welche sich im Hoheitsgebiet einer anderen Vertragspartei befinden, durchsucht, sichergestellt und beschlagnahmt sowie weitergegeben werden sollen.[623] Gleichzeitig werden in Art. 32 CCC aber auch Ausnahmen vom Rechtshilfeweg vorgesehen, wonach eine Vertragspartei ohne die Genehmigung einer anderen Vertragspartei auf öffentlich erhältliche gespeicherte Computerdaten zugreifen darf, unabhängig davon, wo sich die Daten geografisch befinden (lit. a). Überdies darf sie auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mithilfe eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die rechtmässige und freiwillige Zustimmung der Person einholt, die legitimiert ist, die Daten dieses Computersystems an sie weiterzugeben (lit. b).[624] Unter öffentlich zugänglichen Daten (lit. a) werden bspw. öffentliche Postings auf Facebook oder auch Angebote auf Verkaufsplattformen im Darknet verstanden. Lit b bezieht sich demgegenüber auf nicht öffentliche, insb. passwortgeschützte Daten, wozu Daten eines Darknet-Benutzerkontos zählen. Letzt genannte Daten können dementsprechend mittels freiwilliger Zustimmung des rechtmässigen Inhabers der Daten[625] via Online-Zugriff oder Empfang beschafft werden.[626] Die Zustimmungsberechtigung hängt von den konkreten Umständen, der Art der Person und dem anwendbaren Recht ab.[627] Gemäss der Botschaft des Bundesrats ist Art. 32 lit. b CCC eng auszulegen, was bedingt, dass eine freiwillige Zustimmung einer Person *im Inland* nötig ist.[628]

Im BGE 141 IV 108 widerspricht hingegen das BGer der Ansicht des Bundesrates, und hält fest, dass keine Zustimmung einer rechtmässig zur Herausgabe befugten *Person im Inland* erforderlich ist, da eine solche Zustimmung ansonsten die primären Ziele des Übereinkommens[629] unterlaufen würde.[630] Inwiefern eine konkrete Person über gewisse Daten verfügen und diese herausgeben darf, bestimmt sich nach dem innerstaatlichen Recht des Staates, in dem die betroffene Person agiert.[631] Deshalb kommen gemäss

[618] Viele Länder, in welchen die ISP ihren Sitz haben, kennen keine oder nur eine sehr kurze Vorratsdatenspeicherung, sodass z.B. die angeforderten IP-Adressen in der Regel nicht mehr vorhanden sind, bis das Rechtshilfeersuchen in diesen Ländern bearbeitet wird (SCHWEINGRUBER, N 5 f.); BÄR, EDV-Beweissicherung, Durchsuchungen mit Auslandsbezug, N 26.
[619] Aktuell haben 64 Staaten die CCC ratifiziert, während wichtige Länder wie Brasilien, Indien und Russland die Annahme der Konvention bislang ablehnen (Europarat, Ratifikationsstand der CCC, Abschn. 1.).
[620] FORSTER, Marksteine BGer-Praxis 617 f.; HEIMGARTNER, Internetstraffälle, 144 f. SCHWEINGRUBER, N 7 ff.
[621] Europarat, Ratifikationsstand der CCC, Abschn. 1.
[622] FORSTER, Marksteine BGer-Praxis, 615 f.; GERCKE, Internetkriminalität, 297.
[623] GRAF, N 34.
[624] Art. 32 lit. a und b CCC.
[625] Eine konkludente freiwillige Zustimmung liegt vor, wenn die berechtigte Person die Daten ohne Weiteres herausgibt.
[626] Zum Ganzen HEIMGARTNER, Internetstraffälle, 146; SCHWEINGRUBER, N 10 ff.; GRAF, N 29 f. Ergänzungen bezüglich des Darknets wurden durch die Autorin hinzugefügt.
[627] Council of Europe, Explanatory Report, 53 N 294.
[628] Botschaft 2010 CCC, 4738.
[629] U.a. die Verbesserung der Bekämpfung der grenzüberschreitenden Cyberkriminalität.
[630] BGE 141 IV 108, E. 5.9 f. S. 124 ff.; FORSTER, Marksteine BGer-Praxis, 618 f.
[631] Botschaft 2010 CCC, 4738.

dem BGer somit auch ausländische Personen und Unternehmen (Internetprovider bzw. Service Provider) als Zustimmungsberechtigte i.S.v. lit. b in Frage, wenn diese in ihren Allgemeinen Nutzungsbedingungen bzw. Datenverwendungsrichtlinien das Recht auf Datenweiterleitung an in- und ausländische Strafbehörden gegenüber ihren Kunden ausbedungen haben.[632]

3. Rechtshilfe und die CCC im Zusammenhang mit Darknet-Verkaufsplattformen

Bezüglich des Zugriffes durch die Schweizer Strafbehörden auf nicht öffentliche Daten einer Darknet-Verkaufsplattform, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, schafft Art. 32 lit. b CCC keine Abhilfe. Ein solcher Zugriff ohne vorgängiges Rechtshilfeverfahren wäre nur möglich, wenn der Inhaber der Daten freiwillig seine Zustimmung geben würde. Dies ist in zweierlei Hinsicht schwierig: Einerseits muss es den Strafbehörden zuerst gelingen, den Inhaber eines anonymen Darknet-Benutzerkontos zu identifizieren, und andererseits muss dieser der Datenerhebung noch zustimmen, was in der Praxis[633] eher selten der Fall sein wird. Selbst unter der Annahme, dass die ausländischen Plattformbetreiber als Service Provider zu klassifizieren und zur Datenherausgabe gem. Art. 32 lit. b CCC berechtigt wären, ist eine solche aber aus den bereits genannten Gründen nicht zu erwarten.[634] Da aber gem. den Ausführungen in Kap. IV. A 4. schon grundsätzlich unklar ist, wo sich die Plattformbetreiber und deren Server befinden, kann auch nicht eruiert werden, ob der Datenzugriff überhaupt in einem CCC-Vertragsstaat erfolgt.[635] Läge kein CCC-Vertragsstaat vor, müsste die Strafbehörde über den normalen Rechtshilfeweg gehen, doch auch dieser scheitert *per se* aus den mehrfach genannten Gründen.

Trotzdem könnten die europäischen Bestrebungen zum verbesserten Zugang zur grenzüberschreitenden elektronischen Beweismittelerhebung, v.a. die geplanten Anpassungen der CCC[636] gewisse Erleichterungen bringen, die auch für Darknet-Ermittlungen von Vorteil wären. Eine indirekte Auswirkung auf die Darknet-Ermittlungen in der Schweiz könnte zukünftig auch die geplante Massnahme zur Einführung des neuen E-Evidence-Pakets in der EU, bestehend aus der Verordnung über Herausgabe- und Sicherungsanordnungen für elektronische Beweismittel[637] sowie der Richtline zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren,[638] haben.[639]

Aufgrund der Aussichtslosigkeit des Rechtshilfewegs oder der direkten Datenabfrage bei den Providern empfehlen RÜCKERT und SAFFERLING die Bildung von internationalen Ermittlungsgruppen, in denen die Behörden der einzelnen Länder über Ermittlungsbefugnisse in ihrem jeweiligen Land besitzen.[640]

---

[632] BGE 141 IV 108, E. 5.9 f. S. 124 ff.; FORSTER, Marksteine BGer-Praxis, 618 f.; DERSELBE, Territorialitätsgrundsatz, Abschn. 10, weist daraufhin, dass die Internetprovider aus Geheimnisschutz oder Marketinggründen an einer freiwilligen Zusammenarbeit häufig nicht interessiert sind; SCHWEINGRUBER, N 13 ff.; ROTH, grenzüberschreitende Edition, N 39 f.

[633] Im Falle der StA Brugg-Zurzach waren einzelne Beschuldigte kooperativ, sodass sie ihre Zugangsdaten den Strafbehörden zur Verfügung stellten (Anh. 4: Fragebogen WALDMEIER, Frage 2.2).

[634] Vgl. IHWAS, 146.

[635] Wegen denselben Gründen scheinen auch andere Artikel der CCC (wie Art. 18 Abs. 1 lit. a CCC zur Anordnung der Herausgabe von Daten) nicht anwendbar.

[636] Die vom Europarat eingesetzte Cloud-Evidence-Group hat Vorschläge zu einer Anpassung der CCC erarbeitet und veröffentlicht, konkrete Anpassungen gab es bisher noch nicht (Council of Europe, T-CY, N 1 ff.).

[637] Die E-Evidence Verordnung hat zum Ziel gegen Probleme der Strafverfolgung im Zusammenhang mit der Volatilität von elektronischen Beweismitteln und der internationale Dimension vorzugehen, wobei Kooperationsverfahren an das digitale Zeitalter angepasst und der Justiz sowie Strafverfolgung geeignete Instrumente für den Umgang mit den heutigen Kommunikationsmethoden von Straftätern zu geben (Europäische Kommission, Vorschlag für Verordnung).

[638] Europäische Kommission, Vorschlag für Richtlinie.

[639] M.w.H. BÄR, EDV-Beweissicherung, Durchsuchungen mit Auslandsbezug, N 30; MÜLLER, 98 f.

[640] RÜCKERT/SAFFERLING, 8.

Internationale Zusammenarbeit der Justiz und Polizei gilt demnach als wichtigstes Instrument zur Bekämpfung von kriminellen Handlungen auf Darknet-Plattformen.[641] Dabei spielen v.a. die International Criminal Police Organisation (Interpol),[642] und im europäischen Rechtsraum Europol[643] eine wichtige Rolle.[644] Mithilfe solcher international koordinierten Ermittlungen konnten die Strafverfolgungsbehörden in jüngster Vergangenheit auch einige bedeutende Erfolge erzielen. Als Vorreiter der internationalen Kooperation zur Bekämpfung von Cybercrime gilt Europol und deren Spezialeinheit European Cybercrime Center (EC3), welche seit 2014 die Joint Cybercrime Action Taskforce (J-CAT) unterhält, der die Schweiz ebenfalls angehört.[645] Die J-CAT dient u.a. zum Austausch zwischen Spezialisten aus verschiedenen Ländern sowie zur Initiierung von länderübergreifenden Aktionen.[646] Europol konnte in der Vergangenheit durch sog. Joint Investigation Teams denn auch wichtige Ermittlungserfolge feiern: In Kooperation mit der amerikanischen Drogenbehörde DEA, dem FBI und der niederländischen Polizei gelang es Europol bspw. Mitte 2017 die damals grösste Verkaufsplattform «Alphabay»[647] stillzulegen. Gleichzeitig konnte auch die zu dieser Zeit drittgrösste Plattform «Hansa» vom Netz genommen werden.[648]

4. Das Territorialitätsprinzip und die Datenerhebung im Ausland

Inwiefern Datenerhebungen im Ausland, wie sie in den beiden Bundesgerichtsentscheiden ebenfalls vorgenommen wurden, in Anbetracht des Territorialitätsprinzips zu beurteilen sind, soll nun geklärt werden.

a Lehrmeinungen und internationale Entwicklungstendenzen

Gemäss GRAF können die Strafbehörden ohne Verletzung des Territorialitätsprinzips auf Daten zugreifen, die zwar im Ausland liegen aber, öffentlich zugänglich[649] sind, da es dabei nicht zur Anwendung einer Zwangsmassnahme kommt.[650] Hingegen kommt es bei nicht-öffentlich zugänglichen[651] ausländischen Daten aufgrund des Zugriffs unter Überwindung der Zugangssicherung, der Durchsuchung sowie der nachfolgenden Sicherstellung und Beschlagnahme zur Anwendung von Zwangsmassnahmen, welche mit grosser Intensität auf das ausländische (digitale) Hoheitsgebiet wirken.[652] Genau wie GRAF befürwortet ein grosser Teil der Schweizer aber auch der Deutschen Lehre das Territorialitätsprinzip und

[641] RÜCKERT, 20; HOSTETTLER, Darknet, 183 f.
[642] Die Interpol-Task Force «Darknet und Kryptowährungen» arbeitet u.a. an einer globalen Kryptowährungs-Taxonomie, die festlegt, welche Kategorien von Daten aus verdächtigen Kryptowährungstransaktionen gesammelt werden sollen. Die Taxonomie konzentriert sich dabei auf drei Kategorien von Informationen: auf erstens auf Entitäten, Einzelpersonen und Organisationen, zweitens auf Dienste, Darknet-Märkte, Austausch von Kryptowährungen und drittens mit welchen Straftaten die Transaktion in Zusammenhang steht, wie z.B. illegaler Online-Verkauf von Drogen oder Waffen etc. (Interpol, Abschn. 2).
[643] Die Zusammenarbeit der Schweiz und Europol ist im Kooperationsabkommen vom Jahr 2006 vereinbart. Das Abkommen ermöglicht den Austausch von strategischen und operativen Informationen sowie Spezialkenntnissen (Fedpol, Die Schweiz und Europol, Abschn. 1).
[644] RÜCKERT, 20.
[645] HOSTETTLER, Darknet, 183 f.; Europol, J-CAT, Abschn. 1.
[646] HOSTETTLER, Darknet, 183 f.
[647] Vor der Übernahme erreichte AlphaBay über 200 000 Benutzer und 40 000 Anbieter. Es gab über 250 000 Einträge für illegale Drogen und giftige Chemikalien und über 100 000 Einträge für gestohlene und gefälschte Ausweisdokumente, gefälschte Waren, Malware, Schusswaffen etc. (Europol, Criminal Dark Web, Abschn. 2 f.).
[648] Zum Ganzen Europol, Criminal Dark Web, Abschn. 2 f.; Vgl. auch BACHMANN/ARSLAN, 245.
[649] Z.B. öffentliches Facebook-Profil, Informationen aus der Website einer Firma, Ermittlung von Domaininformationen über «WhoIs»-Datenbanken, Angebote auf einer Verkaufsplattform im Darknet (GRAF, N 29).
[650] GRAF, N 29; m.w.H. HEIMGARTNER, Beschlagnahme, 93 und 267; Botschaft 2010 CCC, 4737 f.
[651] passwort- oder durch sonstige Barrieren geschützte Daten.
[652] GRAF, N 30.

wertet dementsprechend einen Zugriff von Ermittlungsbehörden auf im Ausland gespeicherte nicht-öffentliche Daten als Eingriff in fremdes Hoheitsgebiet.[653] An derartige Beweismittel können die Behörden nur durch internationale Rechtshilfe oder allenfalls direkt gelangen, wenn dies in einem internationalen Übereinkommen, wie bspw. der CCC konkret vorgesehen ist.[654] Werden Beweise unter Verletzung des Territorialitätsprinzips[655] erhoben, so kann dies womöglich für die Strafbehörden zum Beweisverlust zufolge Unverwertbarkeit führen und im innerstaatlichen Strafprozess gerügt werden.[656]

Gegensätzlich zur eben erläuterten strengen Auslegung des Territorialitätsprinzips spricht sich eine Minderheitsmeinung der Schweizer und der Deutschen Lehre für eine weniger strikte Auslegung, resp. Geltung des Territorialitätsprinzips aus und erlaubt unter gewissen Voraussetzungen einen länderübergreifenden direkten Zugriff[657] auf Datenverarbeitungs- und Speicherungsanlagen im Ausland.[658] Gemäss den Vertretern dieses sog. Zugriffsprinzips wird bei Computerdaten nicht auf geografische Konzepte wie das Territorialitätsprinzip und den Standort des Datenträgers abgestellt, auf dem die Informationen gespeichert sind, sondern auf die Tatsache, wer von wo aus Zugriff auf die verfahrensrelevanten Daten hat, unabhängig davon, wo sich diese effektiv befinden. D.h. die Datenherrschaft liegt bei derjenigen Person, welche über die Zugriffsberechtigung verfügt, und nicht bei derjenigen, die im physischen Besitze des Datenträgers ist,[659] was auf die Unkörperlichkeit von Daten zurückzuführen ist.[660] Dies bringen einzelne Autoren, wie BANGERTER, als Begründung vor, weshalb die Durchsuchung und Sicherstellung von im Ausland befindlichen Daten durch Schweizer Behörden keine Souveränitätsverletzung darstellen.[661] Anders ausgedrückt, soll die Zulässigkeit des Online-Zugriffs einzig von der Legitimität der inländischen Ermittlungshandlung abhängig sein, indem diese eben im Inland erfolgt.[662] Gemäss BANGERTER, der seine Aussagen auf Durchsuchungen im Rahmen des Kartellgesetzes bezieht (Art. 42 Abs. 2 KG) heisst das jedoch auch, dass ein Zugriff durch die Strafverfolgungsbehörden auf diese Daten nur innerhalb der Räumlichkeiten gemacht werden darf, die vom Hausdurchsuchungsbefehl abgedeckt sind. Ausgeschlossen sind für ihn heimliche Zugriffe auf Daten (sog. Online-Durchsuchungen), bei denen sich der Zugriff nicht in körperlicher Präsenz der Behörde manifestiert und der Dateninhaber seine Rechte nicht ausüben kann.[663] HANSJAKOB und PAJAROLA sprechen sich ebenfalls v.a. im Hinblick auf

---

[653] Die Schweizer Lehre: GRAF, N 30; HEIMGARTNER, Beschlagnahme, 93; DERSELBE, Internetstraffälle, 136; RYSER, 575 ff.; ferner AEPLI, 130 f.; die Deutsche Lehre: DOMBROWSKI, 159 ff.; GERCKE, Internetkriminalität, 295; BURCHARD, 263; DALBY, 248.

[654] GRAF, N 30; YOUSSEF, 105 f.; BÄR, transnationaler Zugriff, 54 f.; OBENHAUS, 654; SINGELNSTEIN, 597; vgl. SCHWEINGRUBER, N 4.

[655] Verletzung des Territorialitätsprinzips entsteht durch direkten Zugriff auf ausländische Datenträger unter Umgehung der Rechtshilfe in Strafsachen bzw. Überschreitung der Befugnisse der CCC.

[656] GRAF, N 21 und 42; siehe auch GLESS, Beweisverbote, 322 ff.

[657] Der Zugriff erfolgt nicht via Rechtshilfeweg und ist nicht in einem internationalen Übereinkommen konkret vorgesehen.

[658] Für die Schweizer Lehre: BANGERTER, 280 ff., der sich auf den Grundgedanken von SCHMID, Computerdelikte, 108 f., bezieht; BSK KG-BANGERTER, Art. 42 N 131; BURGERMEISTER, 22 f. HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 18 f.; Für die deutsche Lehre: WICKER, 768 f. argumentiert, dass die Durchsicht von Papieren und elektronischen Speichermedien (§ 110 StPO) dies wegen Absatz 3 zulasse «der Zugriff auf räumlich getrennte Speichermedien ist möglich, soweit auf diese Speichermedien von dem Speichermedium bei dem von der Durchsuchung Betroffenen aus zugegriffen werden kann.»

[659] BURGERMEISTER, 22 f.; BSK KG-BANGERTER, Art. 42 N 131; ebenfalls angetönt bei BOTTINELLI 1333; für das deutsche Recht, WICKER, 768 f.;

[660] Gemäss BANGERTER berücksichtigen die Lehrmeinungen zum Territorialitätsprinzip die Besonderheiten bei der Beschlagnahme von elektronischen Daten sowie die Rechtswirklichkeit nicht angemessen (BSK KG-BANGERTER, Art. 42 N 131).

[661] BANGERTER, 281 f., argumentiert, dass verschiedene Wettbewerbsbehörden, darunter auch die EU-Kommission, bei ihren Durchsuchungen und Beschlagnahmen gem. dem Anti-Cartel Enforcement Manual des International Competition Network den «Access Approach» anwenden und darin keine Souveränitätsverletzung sehen.; BURGERMEISTER, 22 f.; vgl. zu selbiger Thematik in der EU GRAVE/BARTH, 373.

[662] GRAF, N 31; WICKER, 768 f.

[663] BANGERTER, 280 f.

Daten in Clouds[664] für das Zugriffsprinzip aus und begründen dies damit, dass meistens weder der Benutzer noch der Anbieter des Cloud-Dienstes weiss, wo sich gewisse Daten zu einem bestimmten Zeitpunkt befinden.[665] In Anbetracht dieser undurchsichtigen Speichermethoden kann gem. HANSJAKOB und PAJAROLA nicht verlangt werden, dass die Strafverfolgungsbehörden abzuklären haben, wo die Daten aktuell gespeichert sind, um dann im entsprechenden Land rechtshilfeweise um Zugriff zu ersuchen.[666] Aus diesem Grund sollen die Strafverfolgungsbehörden berechtigt sein, von der Schweiz aus via Internet auf Daten zuzugreifen, zu sichern und diese zu verwerten, unabhängig davon, wo sich diese wirklich befinden.[667] Auch in der Deutschen Lehre wird eine grenzüberschreitende vorläufige Sicherung von zugangsgeschützten Daten in einer Cloud zur Vermeidung eines Datenverlusts nach nunmehr vorherrschender Meinung als zulässig erachtet.[668] BÄR weist jedoch darauf hin, dass ein Rechtshilfeersuchen auch noch nachträglich gestellt werden kann, falls sich herausstellt, dass bereits gesicherte Daten in der Cloud wirklich im Ausland lagen.[669] Inwiefern die Ergebnisse solcher Datenerhebungen einem Beweisverwertungsverbot unterliegen, ist jedoch umstritten.[670]

Auch die T-CY, ein Gremium des Europarates, welche u.a. Lösungen für den Zugang zu Beweismitteln in Clouds ausarbeiten sollte, hat in ihrem Bericht im Jahr 2016 erkannt, dass sich aufgrund der limitierten völkerrechtlichen Möglichkeiten die eben genannte weit verbreitete Praxis etabliert hat, bei der die Strafverfolger durch rechtmässig erhaltene Zugangsdaten auf E-Mail- oder Cloud-Service-Konten von Verdächtigten zugreifen, auch wenn sie wissen, dass die Daten sehr wahrscheinlich im Ausland liegen.[671] Um die Rechtsunsicherheit zu verringern und die Individualrechte der Einzelnen zu stärken, forderte die T-CY deshalb eine gemeinsame internationale Lösung.[672] Sie schlug vor, dass im Rahmen der Aushandlungen zum zweiten Zusatzprotokoll der CCC geprüft wird, ob nachfolgende Änderungen in das Protokoll aufzunehmen sind. Dabei handelt es sich erstens um den grenzüberschreitenden Datenzugang ohne Zustimmung aber mit rechtmässig erworbenen Zugangsdaten. Zweitens um einen solchen Datenzugang in gutem Glauben oder unter dringenden oder anderen Umständen, bspw. in Fällen, bei denen die Strafverfolgungsbehörde nicht wissen konnte, wo sich die Daten genau befinden.[673] Und drittens die Einführung einer Alternative zum Territorialitätsprinzip durch neue rechtliche Anknüpfungspunkte, wie die «Verfügungsgewalt» (engl. «power of disposal») oder «die Person im Besitz oder unter Kontrolle» (engl. «person in possession or control»).[674] Diese von der T-CY vorgeschlagenen Änderungen wurden jedoch im aktuellsten Entwurf des zweiten Zusatzprotokolls der CCC, der sich in der Vernehmlassung befindet, nicht berücksichtigt.[675]

---

[664] Siehe Kap. IV. A 4.
[665] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 19.
[666] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 19.
[667] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 19.
[668] BÄR verweist auf 5 weitere deutsche Lehrmeinungen, die dies als zulässig erachten (BÄR, EDV-Beweissicherung, Durchsuchungen mit Auslandsbezug, N 30).
[669] BÄR, EDV-Beweissicherung, Durchsuchungen mit Auslandsbezug, N 30.
[670] BÄR, EDV-Beweissicherung, Durchsuchungen mit Auslandsbezug, N 30.
[671] Council of Europe, T-CY, N 1 und N 45.
[672] Council of Europe, T-CY, N 46.
[673] Zum Ganzen Council of Europe, T-CY, N 144.
[674] Council of Europe, T-CY, N 144; Council of Europe, Cloud Computing, 10 f.; Diese Vorschläge sind teilweise ähnlich wie die von SUSSMANN bereits 1999 vorgebrachten Ausnahmegründe vom Territorialitätsprinzip. Als solche sah er die Gefahr in Verzug (engl.: exigent circumstances), worunter er eine Situation verstand bei der allenfalls Beweismittel vernichtet werden, wenn sie nicht vorgängig beschlagnahmt würden und die unwissentliche grenzüberschreitende Datenerhebung durch die Strafbehörde, welche bei der Durchsuchung nicht wissen konnte, wo die Daten liegen (SUSSMANN, 471)
[675] Vgl. Council of Europe, Draft Protocol Version April 12, 2021; Council of Europe, T-CY News, Abschn. 1 ff.

b Rechtsprechung des BGer

Die strafprozessuale Erhebung von sich im Ausland befindlichen Daten durch Schweizer Strafbehörden war in der jüngeren Vergangenheit auch mehrfach Gegenstand bundesgerichtlicher Rechtsprechung, wobei v.a. die sog. Facebook-Entscheide von Relevanz sind.[676] Gegenstand des ersten Entscheids aus dem Jahr 2015 war der Erlass einer Verfügung zur grenzüberschreitenden Herausgabe von Randdaten an den Facebook-Sitz in Kalifornien (BGE 141 IV 108, Facebook I)[677] und beim zweiten Entscheid im Jahr 2016 ein Editionsbefehl an die schweizerische Zweigniederlassung von Facebook mit dem Zweck, eine Datenherausgabe bei Facebook Irland zu bewirken (BGE 143 IV 21, Facebook II).[678] Im Zentrum beider Entscheide stand die Herausgabe von nicht-öffentlich zugänglichen Daten (bezüglich Facebook-Konten) auf ausländischen Servern derselben Social Media Unternehmung. Da sich die fraglichen Daten im Ausland befanden und deren Erhebung nicht in einem internationalen Übereinkommen vorgesehen waren,[679] kam das BGer unter Beachtung des Territorialitätsprinzips zum Schluss, dass die Strafbehörden in beiden Entscheiden den förmlichen Weg der internationalen Rechtshilfe in Strafsachen hätten beschreiten müssen.[680]

Im dritten bereits mehrfach diskutierten Entscheid (BGE 143 IV 270, Facebook III) ist das BGer wegen dem impliziten Rückgriff[681] auf das Zugriffsprinzip in Anlehnung an BANGERTER jedoch der konträren Ansicht gefolgt.[682] Es musste sich bei diesem Entscheid mit der Frage befassen, ob schweizerische Strafverfolgungsbehörden im Rahmen eines inländischen Strafverfahrens, als Ausfluss ihrer strafprozessualen Befugnisse, direkt auf Benutzerkonten bei Facebook zugreifen, beweisrelevante Daten sicherstellen und diese im inländischen Strafverfahren verwerten dürfen. Der direkte Zugriff erfolgte dabei nicht als Aufforderung an ausländische Provider zur Herausgabe von Daten, sondern mittels Einloggens auf Benutzerkonten durch die Strafbehörde unter Verwendung der ihr bekannten Zugangsdaten.[683] Das BGer entschied, dass die Durchsuchung und Beschlagnahme von im Ausland befindlichen Daten durch die Schweizer Behörden zulässig war. Es begründete seinen Entscheid folgendermassen: «Wer über einen Internetzugang im Inland einen abgeleiteten Internetdienst benutzt, der von einer ausländischen Firma angeboten wird, handelt nicht im «Ausland». Auch der blosse Umstand, dass die elektronischen Daten des betreffenden abgeleiteten Internetdienstes auf Servern (bzw. Cloud-Speichermedien) im Ausland verwaltet werden, lässt eine von der Schweiz aus erfolgte gesetzeskonforme Online-Recherche nicht als unzulässige Untersuchungshandlung auf ausländischem Territorium (im Sinne der dargelegten Praxis) erscheinen.»[684]

In seinen Erwägung ging das BGer denn auch nicht mehr konkreter auf den vom Beschuldigten vorgebrachten Einwand ein, dass die erhobenen Chat-Nachrichten nicht verwertet werden dürfen, da diese auf Servern im Ausland und unter Verletzung des Territorialitätsprinzips erhoben wurden.[685] Genau dieser Vorwand des Beschuldigten wurde auch von der Lehre teilweise als kritisch betrachtet und kontrovers diskutiert. GRAF erachtet in seiner Besprechung zu diesem Entscheid insb. als kritisch, dass ein

[676] ROTH, Territorialitätsprinzip, Abschn. 1.
[677] BGE 141 IV 108, Sachverhalt, lit. A. S. 111.
[678] BGE 143 IV 21, Sachverhalt, lit. A. S. 21.
[679] BGE 141 IV 108 E. 5.7 ff. S. 124 ff.; BGE 143 IV 21, E. 3.2 S. 24.
[680] BGE 141 IV 108 E. 6.5 f. S. 130 f.; BGE 143 IV 21 E. 3.4.3 S. 26.
[681] Ein solcher impliziter Rückgriff auf das Zugriffsprinzip zeichnete sich bereits im Urteil des BGer 1B_142/2016 E. 3.6 bezüglich Google ab; siehe auch BGE 143 IV 21 E. 3.4.2 S. 26 (GRAF, N 31).
[682] HUSMANN, 369; GRAF, N 13 und N 31.
[683] Zum Ganzen GRAF, N 2.
[684] Zum Ganzen BGE 143 IV 270 E. 7.10 S. 287 f.; wobei das BGer auf BANGERTER, 280 ff. verwies.
[685] BGE 143 IV 270 E. 6.2 S. 279.

solcher Online-Zugriff auf im Ausland liegende Daten zwar kein physisches Tätigwerden auf fremdem Staatsgebiet darstellt, jedoch die Eingriffsintensität nicht merklich geringer ist als bei äquivalenten physischen Tätigkeiten,[686] die unzulässig sind.[687] Er weist auch darauf hin, dass durch den Online-Abruf Datenverarbeitungsvorgänge im Ausland erzeugt und evidente Spuren im Zielstaat hinterlassen werden, weshalb sogar die Gefahr besteht, dass sich der Beamte je nach nationaler Gesetzgebung bspw. des Hackings strafbar macht.[688] Er begründet, dass die CCC einen solchen Zugriff bereits in begrenztem Masse erlaubt und damit, *e contrario* jede darüberhinausgehende Beweisbeschaffung als Eingriff in die staatliche Souveränität zu verstehen und somit das Territorialitätsprinzip verletzt sei.[689] Auch HUSMANN beanstandet in Bezug auf BGE 143 IV 270 bspw., dass ein solcher Zugriff dem Prinzip von Treu und Glauben widerspricht, weil damit offensichtlich der Rechtshilfeweg umgangen wird.[690] Anderer Meinung sind HANSJAKOB und PAJAROLA, welche als Befürworter des Zugriffsprinzips den Entscheid des BGer als richtig erachten, da es eben nicht massgebend ist, wo die Daten gespeichert sind, sondern woher der Berechtigte auf sie zugreifen kann.[691] WALDER sieht die fremde Territorialität ebenfalls nicht als verletzt, denn obwohl Datenbankinhalte von einem Server geladen wurden, der mutmasslich im Ausland ist, wurde die Website im Arbeitsspeicher auf einem Computer lokal in der Schweiz nicht im Ausland «aufgebaut».[692]

Im neusten Entscheid BGE 146 IV 36 betreffend vorgenannte Thematik, musste das BGer erneut die Verwertbarkeit von Daten beurteilen, wobei es um Daten ging, welche durch technische Überwachungsgeräte im Ausland aufgezeichnet wurden. Laut dem zugrundeliegenden Sachverhalt wurden im Fahrzeug der beschuldigten Person GPS-Tracker und Mikrofone auf Grundlage von Art. 280 StPO angebracht. Da sich die Person während der Überwachungsdauer mehrfach mit dem Fahrzeug ins Ausland begab, fanden im Strafverfahren auch Daten Eingang, welche die Überwachungsgeräte im Ausland aufgezeichnet hatten.[693] Dagegen wehrte sich der Beschuldigte erfolgreich vor BGer. Dieses kam zum Schluss, dass keine völkerrechtliche Grundlage die Vornahme dieser technischen Überwachungsmassnahmen im Ausland gestattet habe und das Territorialitätsprinzip verletzt wurde. Für eine Verwertbarkeit dieser Aufzeichnungen hätte der Rechtshilfeweg beschritten werden müssen.[694] Das BGer grenzt dabei den Sachverhalt insb. zum vorher erwähnten Facebook III-Entscheid ab. Vorliegend habe die StA aktiv technische Mittel eingesetzt, wobei sie im Facebook III-Entscheid die bewährten, von der Website angebotenen Verbindungsmöglichkeiten von einem unbestimmten Ort – einschliesslich der Schweiz – lediglich genutzt und gerade nicht für diesen Zweck eingerichtet habe.[695] Als einzige Ausnahme vom Territorialitätsprinzip scheint das BGer somit die Konstellation aus dem Facebook III-Entscheid anzuerkennen, indem die Strafbehörden das Internet nur so genutzt haben, wie es jeder Person zusteht, und im Rahmen dieser Nutzung Daten aus dem Ausland in die Schweiz auf ihre Systeme übermittelt haben.[696]

---

[686] Eine physische Ermittlungstätigkeit wäre bspw. die Durchsuchung des Speicherträgers im Ausland durch schweizerische Beamten.
[687] GRAF, N 32.
[688] GRAF, N 32.
[689] Digitale Beweisaufnahmen erfolgen gem. GRAF von der Schweiz aus für den ausländischen Staat heimlich, weshalb diese Ermittlungshandlungen durch das Rechtshilferecht abgesichert sein sollen (GRAF, N 32).
[690] HUSMANN, 369.
[691] HANSJAKOB/PAJAROLA, StPO-Kommentar, Art. 269 N 18.
[692] Anh. 2: Interview WALDER, Frage 2.5.
[693] Zum Ganzen BGE 146 IV 36, Sachverhalt, lit. A. S. 37.
[694] Zum Ganzen BGE 146 IV 36 E. 2.3 S. 46 f.
[695] BGE 146 IV 36 E. 2.3 S. 46 f.; HUSMANN, 366; ROTH, Territorialitätsprinzip, Abschn. 2.
[696] ROTH, Territorialitätsprinzip, Abschn. 3.

c Das Territorialitätsprinzip im Zusammenhang mit Darknet-Plattformen

Gem. WALDMEIER leistet das bundesgerichtliche Verdikt in BGE 143 IV 270 (Facebook III) einen wichtigen Beitrag zur Rechtssicherheit bezüglich der Durchsuchung von im Ausland gespeicherten Daten von Benutzerkonten.[697] Das Urteil wirkt sich laut GRAF auch dahingehend massiv auf die Praxis aus, indem die Strafbehörden vermehrt etwa durch Sichtung von beschlagnahmten Unterlagen oder mittels Nachforschungen auf sichergestellten Geräten versuchen werden, an die Zugangsdaten solcher Internetdienste zu gelangen, falls sie diese von der betroffenen Person nicht freiwillig erhalten.[698] Dass GRAF recht haben sollte wird auch aus den beiden diskutierten Urteilen im Zusammenhang mit Benutzerkonten bei Darknet-Plattformen ersichtlich, bei denen die Strafbehörden mithilfe der Zugangsdaten Zugriff auf die nicht öffentlich zugänglichen Daten der Darknet-Benutzerkonten erhielten. Obwohl sich das BGer in diesen Urteilen weder dazu äussern musste, ob sich die zu durchsuchenden Daten überhaupt im Ausland befanden, noch inwiefern das Territorialitätsprinzip tangiert war, betreffen sie gewissermassen dieselbe Problematik wie BGE 143 IV 270.[699] Deshalb kann m.E. bei den Darknet-Entscheiden ebenfalls eine Ausnahme vom Territorialitätsprinzip zugunsten des Zugriffsprinzips angenommen werden.

Wie diverse Ausführungen in dieser Arbeit verdeutlicht haben, stellen die Internationalisierung der Datenspeicherung, die vermehrte Nutzung von dezentralen und dynamischen Speichersystemen, die rotierenden Speicherstandorte von Daten sowie immer bessere Anonymisierungstechnologien die Strafbehörden vor immer grössere Herausforderungen. Um diesen Entwicklungstendenzen entgegenzuhalten und Cybercrimes weiterhin verfolgen zu können, scheint es m.E. unumgänglich, dass das konventionelle Territorialitätsprinzip, welches auf der althergebrachten Souveränität von Nationalstaaten basiert,[700] überdacht und nötigenfalls einer ergebnisorientierteren und weniger prinzipienbasierten Strafverfolgung weichen muss. Dabei stellt das Zugriffsprinzip für mich eine mögliche Lösung dar. Um jedoch die Rechtssicherheit zu erhöhen, einen international abgestimmten Konsens zu finden und einheitliche, länderübergreifende Kriterien als Ausnahmen vom Territorialitätsprinzip festzulegen, muss die Diskussion m.E. unbedingt auf internationaler und völkerrechtlicher Ebene stattfinden. Aus diesem Grund begrüsse ich den Diskurs, der im Rahmen der Aushandlungen zum zweiten Zusatzprotokoll der CCC erfolgt.

VI. Zusammenfassung und Ausblick

Zentral für die vorliegende Arbeit ist der Begriff des Darknets. Auf Verkaufsplattformen, die den konventionellen Plattformen wie Ebay und Amazon gleichen, werden im Darknet u.a. Drogen, Waffen und illegale Pornografie angeboten. Diese Plattformen zeichnen sich durch zwei wesentliche Merkmale aus. Einerseits können die Plattformen nur über den Tor Browser erreicht werden, was dazu führt, dass eine Identifikation über IP-Adressen wie sie im Clearnet erfolgt, unmöglich ist. Andererseits dienen Kryptowährungen als Zahlungsmittel, die Zahlungen ausserhalb überwachter Finanzmarktarchitekturen ermöglichen. Somit gewährleisten die Tor- und Krypto-Technologie eine fast vollständige Anonymität für illegale Geschäfte. Diese Umstände stellen die Strafverfolgungsbehörden vor zahlreiche rechtliche und faktische Herausforderungen bei der Überwachung von Verkaufsplattformen im Darknet und bei der Aufklärung allfälliger Straftaten. Der rechtliche Rahmen stützt sich hierbei primär auf Instrumente der althergebrachten polizeigestützten Ermittlungsarbeit.

[697] Anh. 4: Fragebogen WALDMEIER, Frage 2.11.
[698] GRAF, N 9 f.
[699] Anh. 2: Interview WALDER, Frage 2.1.
[700] M.w.H. BURCHARD, 251.

Stossen die Strafverfolgungsbehörden im Rahmen von Vorermittlungen oder aufgrund von Hinweisen auf widerrechtliche Inhalte, stehen grundsätzlich Ermittlungsmassnahmen in Form von geheimen Überwachungsmassnahmen gem. Art. 269 ff. StPO zur Verfügung. Solche Massnahmen sind aufgrund der Konzeption der Darknet-Verkaufsplattformen bei reinen Darknet-Ermittlungen nicht zielführend und bedingen, dass im Zusammenhang mit dem Darknet v.a. personengestützte Ermittlungsmethoden zur Anwendung kommen. Die Ermittler versuchen primär anhand von VE oder VF das Vertrauen der Zielperson zu gewinnen, um dadurch an Informationen zu gelangen.

Dabei kommt der VF eine wichtigere Bedeutung zu als der VE, deren Anordnungsvoraussetzungen strenger sind und die Verwendung einer durch Urkunden abgesicherten falschen Identität (Legende) voraussetzt. Bei Ermittlungen auf Darknet-Verkaufsplattformen benötigen die Polizeiangehörigen meistens keine solche Legende. Damit stehen den Strafverfolgungsbehörden insb. bei der Aufklärung von Drogendelikten grundsätzlich strafprozessuale Mittel zur Verfügung. Eine Ausnahme ergibt sich *de lege lata* im Bereich der Kinderpornographie. Aufgrund der Praxis der «Keuschheitsprobe» wird für die erfolgreiche Durchführung einer VE und VF *de lege ferenda* eine rechtliche Grundlage zum Versand von (virtuell produziertem) kinderpornografischen Material verlangt.

Ist ein Verdächtiger im Darknet identifiziert, gilt es in einem nächsten Schritt die Erhebung und -sicherung von Benutzerkontendaten innerhalb des vorgegeben Rechtsrahmens zu vollziehen. Hier zeigen sich Parallelen mit der Datenerhebung bei Social Media Benutzerkonten oder Daten auf Cloud-Speichern auf. Die Daten sind nicht lokal auf einem Gerät, sondern auf dezentralen Servern abgespeichert. Im Unterschied zu eben genannten Service Providern ist bei den Darknet-Verkaufsplattformen unbekannt, wo sich die Server mit den gespeicherten Daten befinden. Gleichzeitig sind auch die Betreiber der Darknet-Verkaufsplattformen unbekannt, und es handelt sich dabei konträr zu Social Media Unternehmen oder Cloud-Anbietern nicht um rechtmässige Unternehmen, die Daten an Strafverfolgungsbehörden herausgeben würden. Das führt dazu, dass Editionen oder Rechtshilfeverfahren zur Datenherausgabe bereits im Vorfeld scheitern. Aus diesem Grund versuchen die Strafverfolgungsbehörden mittels Fernzugriff unter Verwendung von rechtmässig erworbenen Zugangscodes auf die Daten zuzugreifen. Dieses Vorgehen wurde in BGer 1B_153/2019 und BGer 1B_185/2019 diskutiert.

Das BGer qualifizierte die Erhebung von Daten auf einem Darknet-Benutzerkonto trotz des Fernzugriffs via Internet richtigerweise als Durchsuchung von Aufzeichnungen gem. Art. 246 StPO und nicht als Kommunikationsüberwachung gem. Art. 269 ff. StPO. Es wurde aufgezeigt, dass der Betroffene mit dem Rechtsbehelf der Siegelung gem. Art. 248 StPO und dem Rechtsmittel der Beschwerde nach Art. 393 f. StPO einen entsprechenden Schutz gegen den staatlichen Grundrechtseingriff erhält. Obwohl das BGer in den genannten Urteilen diesbezüglich keinen materiellen Entscheid fällen musste, wurde zweitens die Frage diskutiert, inwiefern Daten, die nicht auf einem Datenträger gespeichert sind und deren Speicherort unbekannt ist, gem. Art. 263 ff. StPO beschlagnahmefähig sind. M.E. ist hinsichtlich der Auslegung des Begriffes «Gegenstände» der Minderheitsmeinung zu folgen, die «Gegenstände» weit auslegt und auch Daten unabhängig von ihrem Datenträger als beschlagnahmefähig erachtet. In einem dritten Aspekt wurde das von den Strafbehörden angewandte Vorgehen in Anbetracht des international anerkannten Grundsatzes des Territorialitätsprinzips beurteilt. Entgegen dem aus der physischen Verbrechenslehre des 19. und 20. Jahrhunderts stammenden Territorialitätsprinzips, stellen Vertreter des sog. Zugriffsprinzips bei Computerdaten nicht auf geografische Konzepte und den Standort des Datenträgers ab, sondern auf die Tatsache, wer von wo aus Zugriff auf die verfahrensrelevanten Daten hat,

unabhängig davon wo sich diese effektiv befinden. Aufgrund der zunehmenden dezentralen Datenspeicherung u.a. in sog. Clouds findet dieses Prinzip nicht nur in der Schweizer Lehre und Rechtsprechung, sondern auch auf internationaler Ebene immer mehr Zustimmung. Eine zu enge Auslegung des Territorialitätsprinzips im Zusammenhang mit Cybercrimes könnte u.a. bedingen, dass Daten von Darknet-Benutzerkonten im Strafprozess einem Beweisverwertungsverbot unterliegen und damit die ohnehin herausfordernde Strafverfolgung im Darknet noch weiter erschwert würde. Um dies zu verhindern und eine effiziente Strafverfolgung zu ermöglichen, soll m.E. das Zugriffsprinzip im Zusammenhang mit Darknet-Ermittlungen zulässig sein. Die Analyse der Bundesgerichtsentscheide verdeutlichte, dass eine Einordnung von digitalen Thematiken, in die bestehende strafprozessuale Systematik nicht einfach ist und dadurch gleichzeitig einen Raum für Interpretation resp. Auslegung bietet.[701]

Die vorliegend bearbeitete technisch komplexe Materie hat zum Ausdruck gebracht, welche Schwierigkeiten und Herausforderungen die Anonymisierungstechnologie Tor zur effektiven Strafverfolgung mit sich bringt. Nebst dem Tor Browser gibt es aber zahlreiche weitere Software und Apps, welche anonyme und/oder verschlüsselte Kommunikation zulassen. Dass sich sämtliche dieser Kommunikationsmittel für die Abwicklung von illegalen Geschäften über Verkaufsplattformen eignen, zeigen bspw. Medienberichte aus Deutschland vom Oktober 2020, die vermeldeten, dass die Behörden neun Drogen-Kanäle beim Messengerdienst «Telegram» zuerst übernommen und dann geschlossen haben.[702] Bezüglich Verschlüsselung und Anonymisierung kollidieren somit zwei gegensätzliche Ansprüche: Einerseits der Anspruch der Bevölkerung auf den Schutz der Privatsphäre und andererseits die Forderung des Staates, bei der Verbrechensbekämpfung alle Möglichkeiten ausschöpfen zu können.[703] Die Politik und die Rechtslehre werden auch in den kommenden Jahren gefordert sein, einen Kompromiss zwischen diesen Ansprüchen zu finden.

[701] Vgl. Anh. 4: Fragebogen, WALDMEIER, Frage 2.8.
[702] MUTH, Abschn. 1.
[703] TSCHIRREN, Abschn. 2.

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 ich sämtliche immateriellen Rechte an von mir allfällig verwendeten Materialien wie Bilder oder Grafiken erworben habe oder dass diese Materialien von mir selbst erstellt wurden;
- dass das Thema, die Arbeit oder Teile davon nicht bereits Gegenstand eines Leistungsnachweises einer anderen Veranstaltung oder Kurses waren, sofern dies nicht ausdrücklich mit dem Referenten /der Referentin im Voraus vereinbart wurde und in der Arbeit ausgewiesen wird;
- dass ich ohne schriftliche Zustimmung der Universität keine Kopien dieser Arbeit an Dritte aushändigen oder veröffentlichen werde, wenn ein direkter Bezug zur Universität St.Gallen oder ihrer Dozierenden hergestellt werden kann;
- dass ich mir bewusst bin, dass meine Arbeit elektronisch auf Plagiate überprüft werden kann und ich hiermit der Universität St.Gallen laut Prüfungsordnung das Urheberrecht soweit einräume, wie es für die Verwaltungshandlungen notwendig ist;
- dass ich mir bewusst bin, dass die Universität einen Verstoss gegen diese Eigenständigkeitserklärung sowie insbesondere die Inanspruchnahme eines Ghostwriter-Service verfolgt und dass daraus disziplinarische wie auch strafrechtliche Folgen resultieren können, welche zum Ausschluss von der Universität resp. zur Titelaberkennung führen können.»

Datum und Unterschrift

Zürich, 25. Mai 2021

Mit Einreichung der schriftlichen Arbeit stimme ich mit konkludentem Handeln zu, die Eigenständigkeitserklärung abzugeben, diese gelesen sowie verstanden zu haben und, dass sie der Wahrheit entspricht.

Diskretionserklärung

Die Unterzeichnende verpflichtet sich, die von der befragten Unternehmung/Verwaltung erhaltenen Informationen streng vertraulich zu behandeln. Insbesondere darf nur mit ausdrücklicher Einwilligung sämtlicher Auskunftgeber anderen Personen als den Referenten Einblick in die schriftliche Arbeit gewährt werden.

Sie nimmt zur Kenntnis, dass ihre Arbeit von der Universität St. Gallen mittels einer Plagiatssoftware auf allfällige Plagiate überprüft werden kann und dass die befragte Unternehmung/Verwaltung entsprechend zu orientieren ist.

Datum und Unterschrift

Zürich, 25. Mai 2021