MARC FORSTER
Prof. Dr. iur., Rechtsanwalt
Schweizerisches Bundesgericht
CH-1000 Lausanne 14

Tel.: +41 21 318 91 51
E-Mail: marc.forster@bger.ch
www.marc-forster-strafrecht.com

Gutachten zur Masterarbeit von Frau Tanja Niederer

I. Thematik, Kurzbeurteilung und Notenantrag

Die Bearbeiterin erforscht die **strafprozessualen Untersuchungsmethoden** (Überwachung, Durchsuchung, verdeckte Fahndung, Zwangsverwaltung von Accounts usw.), mit denen **illegale Geschäfte** über **Online-Verkaufsplattformen** im **Darknet**, ermittelt und verfolgt werden können. Dazu gehören (typischerweise) namentlich der Handel mit *Drogen, Waffen, Kinderpornografie, Ausweisen* oder illegaler *Software* (zu deliktischen Zwecken). Die Thematik ist von grosser **Aktualität** und rasant steigender *Bedeutung,* zumal insbesondere über den **TOR-Browser** globusübergreifend illegale Geschäfte in (jährlicher) Multi-*Milliardenhöhe* abgewickelt werden, – primär mittels *Cryptoasset*-Zahlungsmitteln wie **Bitcoin** – und sich eine *Strafverfolgung* der Verantwortlichen angesichts der angewendeten *Verschlüsselungstechniken* als aufwändig und *schwierig* erweist.

Die Bearbeiterin systematisiert die rechtliche Thematik primär anhand der Literatur und Urteilspraxis. Besonders wertvoll sind noch vier von der Bearbeiterin geführte **Interviews** zu **praktischen Emittlungserfahrungen** von kantonalen **Strafverfolger/innen** im Bereich *Darknet-Handelsplattformen.*[1] Wissenschaftliche Literatur und strafprozessuale Forschungsprojekte zu diesem Thema gab es bisher nur sehr spärlich. Die vorliegende Arbeit steuert eigene selbstständige Forschungsansätze bei.

1 Zu Interviews eingeladen wurden alle sechs vom BAKOM anerkannten Stellen für die Bekämpfung der Cyberkriminalität aus der Deutschschweiz (Art. 15 Abs. 3 VID), nämlich das Nationale Zentrum für Cybersicherheit, die Kantonspolizei Zürich, Abteilung Cybercrime, die Kantonspolizei Bern, Kriminalabteilung, das Bundesamt für Polizei fedpol, die Zuger Polizei, Fachbereich Cyberermittlung, und die Kantonspolizei Schwyz, Fachbereich Cybercrime; zusätzliche Anfragen gingen auch noch je an die Kompetenzzentren Cybercrime der Kantonspolizei St. Gallen und der Polizei Basel-Landschaft sowie an die Staatsanwaltschaft Brugg-Zurzach. Mit drei behördlichen Stellen kamen ausführlich dokumentierte persönliche Interviews zustande; eine Behörde beantwortete Fragen schriftlich. Rückmeldungen gaben erfreulicherweise alle angefragten Stellen. Das gegenseitige Interesse an einem Erfahrungsaustausch zwischen Praxis und Forschung ist offenbar gross. Aus Gründen des Amtsgeheimnisschutzes werden die Interviews (auf behördlichen Wunsch hin) nicht publiziert.

Es handelt sich um eine äusserst fleissige und engagierte, *inhaltlich reiche* und *präzise,* und auch *formal vorbildliche* Masterarbeit, die eine **hervorragende eigenständige Forschungsleistung** bildet und die **Höchstnote 6.0** verdient.

II. Aufbau der Arbeit

Nach der **Einleitung** (Kap. I), in der die *Ziele* und *Methodik* der Arbeit dargelegt werden, folgen **Prälegomena** (Kap. II) mit *technisch-normativen Definitionen* und *phänomenologischen* Hinweisen zum Thema TOR-basiertes Darknet. Einen **ersten Fokus** legt die Bearbeiterin auf die Schwierigkeiten und *Methoden* von *strafprozessualen* Ermittlungen und *Zwangsmassnahmen* (de lege lata) im *Darknet* (Kap. III-IV). Hier werden auch die *Erfahrungen* der *interviewten Praktiker* nutzbringend eingebaut. Einen **zweiten Forschungsschwerpunkt** widmet sie der Analyse und Kritik von ersten einschlägigen und themenverwandten *Urteilen* des *Bundesgerichtes,* wobei (neben Handelsplattformen) auch *Cloud-Speicherplätze* und *Social Media*-Benutzerkonten in den Fokus einbezogen werden (Kap. V). Dabei erfolgen auch *rechtsvergleichende* Darlegungen über entsprechende grenzüberschreitende Erfahrungen und Reformentwicklungen in Europa (insbes. gestützt auf deutsche Fachliteratur). Die Arbeit schliesst mit einer konzisen Zusammenfassung der wesentlichen Erkenntnisse (Kap. VI).

III. Arbeitstechnik

Die **wissenschaftliche Arbeitsmethodik** ist formal vorbildlich. Die Literatur und weitere wertvolle *Quellen* wurden gezielt und aufwändig recherchiert und ausgewertet, darunter auch viele englisch- und französischsprachige. Deren Dokumentation in den einschlägigen *Verzeichnissen* fällt sachgerecht und übersichtlich aus. Auch *sprachlich* liest sich die Arbeit flüssig; die Schreibfehlerquote ist erfreulich minim.[2]

IV. Inhaltliche Bemerkungen

Die Untersuchung ist ausserordentlich *dicht* und *reichhaltig recherchiert, themenfokussiert* und *praxisnah.* In den **Kap. I-IV** gilt dies namentlich für die Möglichkeiten, Grenzen und

2 An einer Stelle findet sich der Verschrieb "kriminalpolitische Ermittlungsarbeit" (gemeint: kriminalpräventive oder kriminalpolizeiliche).

Schwierigkeiten der **verdeckten Fahndung** im Darknet (S. 27-39).[3] Die Bearbeiterin leuchtet die Grauzonen aus zwischen *polizeilich-präventiven* Aktivitäten ("Vorermittlungen"), z.B. "virtuelle Streifenfahrten" (gestützt auf die kantonale Polizeigesetzgebung), und *gerichtspolizeilicher Ermittlung* (gestützt auf die StPO).[4] Wertvoll und hilfreich sind auch die "didaktische" Aufarbeitung des Stoffes und tabellarische Darstellungen von Zwischenergebnissen: Zur Darstellung der spezifischen Problematik von **Teilnehmeridentifikationen** im *Darknet* (Ermittlung von IP-Adressen), operiert die Bearbeiterin mit *Fallbeispielen* aus dem Clear- und Deepnet (Fall "Tutti.ch") bzw. dem TOR-basierten Darknet (Fall "Dream Market").[5] Auf den Seiten 24-26 werden wichtige *Definitionen* und *Analyseergebnisse*[6] **tabellarisch** dargestellt, aufgeschlüsselt auf *Darknet*-Verkaufsplattformen, *Clearnet*-Marktplätze, *Social Media* und *Cloud*anbieter.

Die Untersuchung geht den praxisrelevanten "neuralgischen" Punkten konsequent auf den Grund; etwa der Problematik der sogenannten *Kinderporno*-"**Keuschheitsprobe**" bei *verdeckten Fahndungen* in *pädosexuellen Netzwerken* sowie den dadurch ausgelösten Gesetzesreformen in Deutschland und der Schweiz (S. 35 f.).[7]

---

3 In den einleitenden Kapiteln finden sich nur wenige und sehr minime Ungenauigkeiten oder Lücken. So hätte für die Definition der überwachbaren *Randdaten* des Fernmeldeverkehrs auf die *Legaldefinition* im BÜPF hingewiesen werden können; auch wäre der Spezialfall des *Antennensuchlaufs* (mit Spezialregeln der bundesgerichtlichen Rechtsprechung) noch knapp erwähnenswert gewesen (vgl. S. 17 f.).

4 S. 12 f. Präventive Vorermittlungen bzw. digitale "Streifenfahrten" sind auch zulässig, wenn dabei Registrierungen auf Internetplattformen mit *Fake-Accounts* bzw. *anonymen Personalangaben* der Vorermittler erfolgen. Hier ist noch *kein konkreter Anfangsverdacht* gegeben, der die Einleitung eines Vorverfahrens nach den Regeln der StPO notwendig machen würde. Falls eine entsprechende *gesetzliche Grundlage* im Polizeigesetz besteht, kann der Vorermittler (bis zum Vorliegen eines Anfangsverdachtes) sogar "verdeckt" *mit Zielpersonen Kontakt aufnehmen,* z.B. auf Darknet-Plattformen, über die sowohl legale als auch illegale Geschäfte abgewickelt werden. Mit Recht empfiehlt die Bearbeiterin aber eine möglichst frühe Eröffnung des Strafverfahrens. Zwar können im genannten Rahmen auch Beweismittel aus den präventiven *Vorermittlungen* im Strafprozess *verwertet* werden; falls die Verfahrenseröffnung (und z.B. die Anordnung einer verdeckten Fahndung durch die Staatsanwaltschaft nach StPO) *zu spät* erfolgt, drohen jedoch Verwertungsverbote. Von hoher praktischer Tragweite sind die Erkenntnisse zur Bedeutung von *Ratings* sowie *Werbe-* und *Liefermassnahmen* im Clear- und Darknet.

5 S. 20-23. Dabei verweist die Bearbeiterin auch auf die (verwandte und zusätzlich heikle) Problematik des *Cloud Computing.*

6 Insbesondere betreffend Daten-*Speicherorte,* öffentliche *Zugänglichkeit* von Daten, Art der *Zugangsdaten* und *Kooperations*bereitschaft mit Strafbehörden. Gewisse Angaben zur "Kooperation" fallen etwas *vage* aus und basieren auf *Selbstdeklarationen* der IT-Konzerne: Wenn bei *Facebook* etwa angeführt wird, FB teile seine Daten mit den Strafbehörden "nach rechtmässiger Anfrage" (S. 26), wäre näher zu *definieren,* was FB unter "rechtmässiger Anfrage" versteht. – Bisher bestand FB gegenüber "ausländischen" (insbes. Schweizer) Strafbehörden oft auf *Rechtshilfeersuchen* am *Standort* der *Datenspeicherung*. Besonders "kooperativ" wäre das nicht. In der Praxis beantworten FB, Google usw. allerdings auch gewisse *direkte* Datenfragen von "ausländischen" Strafbehörden positiv. Dies wohl mit dem Ziel, grössere regulatorische Eingriffe der nationalen Gesetzgeber möglichst zu vermeiden.

7 Auch die Täter-"Szene" hat regelmässig gute Kenntnisse der sie betreffenden Vorschriften des Strafprozessrechts. Insbesondere ist unter Pädosexuellen und Kinderpornohändlern bekannt, dass die Polizeifahn-

Äusserst wertvoll, über weite Strecken eigenständig-kreativ und von *grossem praktischen Interesse* sind auch die thematischen Vertiefungen und Anwendungsbeispiele im abschliessenden **Kap. V**:

Ausgehend von *zwei Fällen,* bei denen es bereits zu *einschlägigen Bundesgerichtsurteilen* gekommen ist,[8] sondiert die Bearbeiterin akribisch mögliche **Ermittlungsstrategien im Darknet**. Eine erste zentrale Frage ist die, wie Fahnder das Manko kompensieren können, dass ihnen – mangels IP-Adressen, Identifizierbarkeit von Darknet-Providern und mangels Zugangsdaten auf Accounts – regelmässig *weder* ein *Fernzugriff* (auf Accounts und im Darknet verwendete Mailadressen) *noch* eine *Provider-Mitwirkung* (insbesondere durch die Betreiber von Handelsplattformen) zur Verfügung steht. Nebst *verdeckter Onlinefahndung* im Dark- und Clearnet (und Observationen bei analogen Vertriebsaktivitäten) kommt – nach einer *Lokalisierung* von Zielpersonen – auch der gezielte Einsatz von *technischen Überwachungsgeräten* in Frage. Nach den Recherchen der Bearbeiterin sind die Strafverfolger in den beiden genannten (Zürcher) Fällen offenbar auf solchen Wegen auf die *Mailadressen* und *Zugangsdaten* zu Drogen-Darknet-Accounts von Beschuldigten gestossen (vgl. S. 43 f.)[9]

Sehr sorgfältig fallen auch die themenspezifischen juristischen **Abgrenzungen** aus zwischen (Online-)*Durchsuchung* (inklusive Sicherstellung, Entsiegelung und Beschlagnahme von abgeschlossener Kommunikation) und (aktiver) *Fernmelde-Überwa-*

der hier *höhere rechtliche Hürden* haben, sich mit *Scheingeschäften* aktiv zu beteiligen, als das bei Drogen und Waffen der Fall ist. Insbesondere dürfen die Fahnder *keine Kinderpornos ins Netz stellen;* sonst droht ihnen selber eine Strafverfahren. Die Pädosexuellenszene nützt dies in der Weise aus, dass von unbekannten Interessenten eine sogenannte "Keuschheitsprobe" verlangt wird: Um zu vermeiden, dass Ermittler sich unerkannt einschleusen, werden neue Interessenten aufgefordert, zunächst *selber* Kinderpornos einzusenden. In *Deutschland* ist im März 2020 ein Gesetz in Kraft getreten, dass es Polizeifahndern neu erlaubt, unter gewissen Voraussetzungen sogenannte *Deepfake*-Kinderpornos zu teilen, also sehr echt aussehendes, aber in dem Sinne *künstliches* Material, als zu dessen Herstellung keine realen Personen missbraucht wurden. Im *Schweizer Parlament* steht derzeit eine ähnliche Vorlage zur Diskussion; der Nationalrat hat sie in der Frühlingssession 2021 bereits befürwortet.

8 1B_185/2019 und 1B_153/2019. Zwar handelt es sich um zwei *Nichteintretensentscheide* in Entsiegelungsfällen. Die Bearbeiterin filtert jedoch sorgfältig heraus, dass sich daraus bereits gewisse *Weichenstellungen* ablesen lassen: Zum einen wird deutlich, dass die *Durchsuchung* von abgerufener *E-Mail-Korrespondenz* und von sichergestellten *Chats* auf *Darknetplattformen* über den Weg des *Entsiegelungsverfahrens* zu erfolgen hat, soweit gesetzlich geschützte Geheimnisinteressen als verletzt angerufen werden. Anderseits deutet das Bundesgericht an, dass die *Zwangsverwaltung* von *Benutzerkonten* (mittels rechtmässig erhobenen Zugangsdaten) als *Sicherungs-Einziehungsbeschlagnahme* (ähnlich wie die Zwangsverwaltung analoger Drogen- oder Waffenverkaufseinrichtungen) einzustufen ist (S. 42).

9 Letztlich wohl mit koordinierten Hausdurchsuchungen und Sicherstellungen von Geräten bei "geöffneten" Benutzerkonten. Übertragen auf eine "analoge" Drogenplattform wären die Ermittler sozusagen an die "Schlüssel" zu einem Drogenlager und an Korrespondenz zwischen Drogenhändler und Kunden gelangt.

chung:

Die Bearbeiterin widerlegt – nach Ansicht des Referenten sehr überzeugend – die Kritik von HANSJAKOB, wonach BGE 143 IV 270 die **Online-Durchsuchung** von **Facebook**-(FB-)**Chatverläufen** zu Unrecht *nicht* als *Fernmeldeüberwachung* eingestuft habe.[10] Im *Beschlagnahme*- und *Einziehungsrecht* gelangt die Bearbeiterin zum Ergebnis, dass die **Zwangsverwaltung** von Accounts auf **Darknet-Handelsplattformen** grundsätzlich als *Sicherungs-Einziehungsbeschlagnahme*[11] zu qualifizieren ist (S. 52). Zur Verdeutlichung dieser (zutreffenden) These hätten auch Vergleiche mit "analogen" *Drogen*- oder *Waffenlagern* bzw- Handels-Infrastrukuren herangezogen werden können.[12]

Kriminologisch *rückwärtsgewandt* (und teilweise betont "akademisch") erscheinen gewisse (auf veraltete Bundesgerichtsurteile gestützte) Diskussionen in der *Lehre*, ob **elektronische Daten** und Dateien "**beschlagnahmefähig**" seien oder nur die betreffenden *Datenträger* bzw. *Serveranlagen*. Die Bearbeiterin lässt sich auch hier nicht auf dogmatisierende Nebengeleise manövrieren:

Dass in einem vernünftigen modernen Strafprozessrecht nötigenfalls auch elektromagnetisch gespeicherte "**Daten**" *sichergestellt* werden und grundsätzlich *beschlagnahmbar* sein müssen, ergibt sich nicht nur aus dem *Sinn und Zweck* und der *Systematik* des Gesetzes, sondern auch deutlich aus seinem *Wortlaut:* Gemäss Art. 246-248 StPO dürfen "**Datenträger** sowie **Anlagen** zur **Verarbeitung und Speicherung von Informationen**" (so wie "andere Aufzeichnungen" auf Schriftstücken, Ton- oder Bildträger) *durchsucht* und *entsiegelt* werden, "wenn zu vermuten ist, dass sich **darin Informationen** befinden, die **der Beschlagnahme** unterliegen". – Diese zentrale Bestimmung des Zwangsmassnahmenrechts wäre völlig *nutzlos* und *widersinnig,* wenn exakt das, was sich **in** bzw. auf den **Datenträgern** und **EDV-Anlagen** befindet, nämlich **Daten**, zum *Vornherein* "nicht beschlagnahmefähig" wäre.[13] – Eine völlig *andere Frag*e ist die, ob elektronische

10 S. 48 f. Die Bearbeiterin weist u.a. darauf hin, dass die Voraussetzungen einer einer Fernmelde-Überwachung nur für *noch nicht abgeschlossene* (aktive) Kommunikation gelten, dass im Zeitpunkt von BGE 143 IV 270 Chats über sogenannte *abgeleitete* Dienste wie FB gar noch nicht unter das damalige BÜPF bzw. unter den Begriff der *Fernmeldedienste* fielen, und dass selbst nach dem *neuen* BÜPF abgeleitete Dienste wie FB grundsätzlich nicht mitwirkungspflichtig wären, da sie die Daten ihrer (Schweizer) Kunden *im Ausland verwalten.*

11 Art. 263 Abs. 1 lit. d StPO i.V.m. Art. 69 StGB.

12 Nach ständiger Praxis fällt z.B. die polizeiliche Zwangsverwaltung von sichergestellten Cannabis-Plantagen oder Drogen-Warenlagern unter die Sicherungs-Einziehungsbeschlagnahme.

13 Die Beschlagnahme auf *Datenträger* zu beschränken, die aber *durchsucht* werden können, würde denn auch zu *absurden* und *grundrechtsgefährdenden* Ergebnissen führen: Die Staatsanwaltschaft dürfte – und

Daten (also in elektromagnetischer Form gespeicherte Aufzeichnungen) **prozessuale Beweiskraft** und **Urkundencharakter** haben, bzw. ob sie einen **einziehbaren Vermögenswert** darstellen. Diese Frage stellt sich speziell (und besonders dringlich) im Zusammenhang mit per *Blockchain* elektronisch aufgezeichneten und tokenisierten **Crypto-Assets** (wie "Bitcoin" usw.).

Wie die Bearbeiterin zutreffend erwähnt (vgl. S. 50), sind *Crypto-Assets* bzw. elektronische Dateien als *Vermögenswerte* **einziehbar** (insbes. Ausgleichseinziehung, Art. 70 StGB) und somit *beschlagnahmefähig.*[14] – Dass allenfalls nur *Ausdrucke* oder *Screenshots* von elektronisch gespeicherten Dateien und Dokumenten *prozessuale Beweiskraft* und *Urkundencharakter* haben und *förmlich beschlagnahmt* werden könnten (vgl. S. 54), ändert nichts daran, dass die betreffenden *Datenträger* zunächst *sichergestellt,* die darauf gespeicherten *Dateien entsiegelt* und *durchsucht* und dass die "**Daten**" dann nötigenfalls *ausgedruckt* (bzw. optisch lesbar festgehalten) und in dieser Form **auch als Beweismittel** (Art. 263 Abs. 1 lit. a StPO) **förmlich beschlagnahmt** werden können.[15] Bemerkenswert ist im übrigen noch der Befund, dass die Strafverfolgungsbehörden in der Praxis offenbar die *Zwangsverwaltung* von polizeilich "ausgehobenen" *Accounts* auf *Darknet-Handelsplattformen* **im Netz publik machen** und insofern *präventiven* Gesichtspunkten (gegenüber weiteren möglichen Ermittlungserfolgen) den *Vorrang* einräumen (vgl. S. 55 f.).

Abschliessend (S. 56-64) widmet sich die Arbeit noch der besonderen Problematik der **grenzüberschreitenden** Verfolgung von *Cyber-* und *Darknet*-Kriminalität (Territorialitäts- *vs*. Zugriffsprinzip, Cyber Crime Convention [CCC], Internationale Rechtshilfe).[16]

---

müsste dann zwangsläufig – ganze *Serveranlagen* und *Speicherzentren beschlagnahmen* und höchst aufwändig (in globo) *durchsuchen;* sie dürfte hingegen keine untersuchungsrelevanten *Dateien* gezielt durchsuchen und (nötigenfalls) förmlich beschlagnahmen. Eine solche "überschiessende" Auslegung contra legem läge im Interesse von niemandem.

14 Die *Beschlagnahme* (Art. 263 Abs. 1 lit. d StPO) wird in der Praxis *vollzogen* durch *Übertragung* der Kryptowerte (Subject Funds), unter Nennung ihrer Kryptowährungs-Adresse (Subject Address), vom sichergestellten *privaten* auf einen *staatlichen* elektronischen *Wallet*.

15 In der *Praxis* besteht denn auch nur *selten* die Notwendigkeit, elektronische *Dateien* als Beweismittel *förmlich* zu beschlagnahmen, wenn sie in "analoger" Form (z.B. ausgedruckt oder als optisch lesbare Datei) verlässlich reproduziert, gelesen und beschlagnahmt werden können (vgl. auch S. 54 f.).

16 Die Bearbeiterin legt u.a. zutreffend dar, dass *Angebote* und *Postings* im *Darknet,* die sich an *unbestimmte* Kundschaft auf *nicht passwortgeschützten* Sites richten, direkt "transnational" *online* erhoben werden dürfen, z.B. per Screenshot auf einem PC in der Schweiz mit Schweizer Internetanschluss (Art. 32 *lit. a* CCC). Es gibt somit *internationalstrafrechtlich* auch "öffentlich zugängliche" Bereiche des Darknets. Für

De lege ferenda verweist sie dabei u.a. auf die hängigen **Reformen** der *CCC*[17] und des *EU-Rechtes*[18] Auch die internationale Zusammenarbeit von Cyberspezialisten bei *Europol*[19] und *Interpol*[20] wird erwähnt. Die Bearbeiterin weist nach, dass sich in *Praxis* und *Doktrin* (zunächst vor allem in Deutschland, neuerdings auch in der Schweiz[21]) das sogenannte **Zugriffsprinzip**[22] allmählich durchsetzt.[23] – Einen der wichtigsten *Leitentscheide,* die auf diesem Prinzip basieren, bildet *BGE 143 IV 270*.

Die Arbeit schliesst mit einem überzeugenden Plädoyer für eine *Modernisierung* des Territorialitätsprinzips bzw. eine *völkerrechtliche Implementierung* und grundrechtskonform-*sachorientierte* Anwendung des Zugriffsprinzips (vgl. S. 63 f.).

Prof. Dr. Marc Forster/26. Juli 2021

---

den Zugang wird zwar technisch eine spezielle Browser-Software (z.B. TOR-Bundle) benötigt; diese steht jedoch grundsätzlich *jedermann* zur Verfügung. Hingegen fallen *passwortgeschützte* Kommunikationen oder Zahlungsvorgänge über Darknet-*Benutzerkonten* unter Art. 32 *lit. b* CCC, was eine transnationale Online-Datenerhebung derzeit (schon rechtlich) praktisch verunmöglicht.

17 Vorschläge der vom *Europarat* eingesetzten "Cloud Evidence Group".

18 "E-Evidence-Paket" der EU, gemäss Richtlinienvorschlag der EU-Kommission.

19 "European Cybercenter" und "Joint Cybercrime Action Taskforce" mit Beteiligung der *Schweiz*.

20 Z.B. globale Cryptoasset-Taxonomie im Rahmen der Interpol-Taskforce "Darknet und Kryptowährungen".

21 Z.B. BÄR, BANGERTER, HANSJAKOB/PAJAROLA; s.a FORSTER <www.marc-forster-strafrecht.com/2019/09/02/territorialitätsgrundsatz-und-internationalstrafrechtliches-zugriffsprinzip-bei-facebook-whatsapp-google-und-co-gefährliche-postkutschenromantik-im-21-jahrhundert/> (Blogbeitrag vom 9. September 2019).

22 Gegenüber einem veralteten bzw. formalistisch-nationalstaatlich ausgelegten Territorialitätsprinzip.

23 Das *Zugriffsprinzip* ("Power of Disposal") erlaubt es, *im Ausland gespeicherte* Daten von *Accounts* (z.B. Facebook-Chatverläufe oder Dateien von Clouddiensten) *sicherzustellen* (und nach inländischem Recht zu durchsuchen), wenn die Strafbehörde sich (nach ihrem inländischen Recht) *rechtmässigen Zugang* auf den Account verschafft hat (vgl. BGE 143 IV 270). Auch die *Reform der CCC* geht u.a. in diese Richtung (vgl. S. 61).