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 Vivian Lersch

I. Thematik, Kurzbeurteilung und Notenantrag

Ziel der Arbeit ist es, eine aktuelle Bestandesaufnahme vorzulegen der rechtlichen und technisch-praktischen Probleme der **strafprozessualen Beschlagnahme** von digitalen Vermögenswerten bzw. **Crypto-Assets** (Cryptos), insbesondere von Bitcoin. Darüber wurde zwar in jüngerer Zeit verschiedentlich geforscht und publiziert.[1] Auf diesem *anspruchsvollen* und zunehmend wichtigen Rechtsgebiet ist die technische und rechtspraktische Entwicklung jedoch von *grosser Dynamik* geprägt. Dies gilt nicht bloss für *technologische* Neuerungen, denen Strafverfolgung und Forensik regelmässig hinterherhinken, sondern auch für die ersten *Erfahrungen* der *Strafbehörden* im In- und Ausland und die ersten *Leitentscheide* der Gerichte.[2]

Methodisch konzentriert sich die Bearbeiterin (in den Kap. III-V) folgerichtig auf die Analyse der neueren einschlägigen *Literatur* und auf die Auswertung von selber durchgeführten **Interviews** über die *praktischen Erfahrungen* thematisch spezialisierter *Strafverfolger*.[3] Die Bearbeiterin entwickelt aufgrund der konstatierten rechtlichen und technologisch-forensischen Probleme **Empfehlungen** für eine *Effiziensteigerung* und verbesserte behördliche *Koordination* bei der Beschlagnahme und Einziehung von Cryptos (de lege lata) sowie auch (de lege ferenda) konkrete Vorschläge für *gesetzliche Präzisierungen* und verstärkte *internationale Zusammenarbeit* im Bereich entsprechender grenzüberschreitender Zwangsmassnahmen (Kap. VI).

Es handelt sich um eine fleissige, juristisch solide und arbeitstechnisch sorgfältige Masterarbeit, die nicht rein deskriptiv ausfällt, sondern (in den Kap. V-VI, namentlich

1 Etwa Diss. TSCHUDI (2020).
2 Z.B. BGE 148 IV 74.
3 Der Staatsanwaltschaften – je Kompetenzzentren Cyberkriminalität – der Kantone AG, BE, SG und ZH.

gestützt auf die Interviews) zum Teil eigenständige wissenschaftliche Überlegungen und Ideen beiträgt. Der Referent beantragt dafür die **Note 5,25** (gut bis sehr gut).

II. Arbeitstechnik

Die *Zitiertechnik* im Fussnotenapparat und die *Verzeichnisse* sind formal sauber.[4] Die *Literatur*auswahl ist thematisch fokussiert und aktuell.[5] Die publizierte *Rechtsprechung* des Bundesgerichtes (insbes. zur themennahen Einziehungsbeschlagnahme) fällt hingegen etwas knapp aus.[6] Die *Sprache* ist, von wenigen kleinen Ungenauigkeiten abgesehen, grossteils klar und unauffällig.[7] *Zielsetzung* und *Aufbau* der Arbeit erscheinen deutlich und konsequent (vgl. Kap. I/B, S. 2 f.).

III. Inhaltliche Bemerkungen

Im einleitenden **Kap. II** werden die technischen und rechtlichen *Prolegomena* der Crypto-Assets prägnant und konzise erarbeitet.[8] Etwas kursorisch fällt dabei die Beschreibung des *Public Key* (und dessen Abgrenzung vom Private Key) aus (S. 8).[9] Im Lichte der strafprozessualen Praxis erscheint dem Referenten die Diskussion um die *Beschlagnahmbarkeit* von *digitalen Daten* (S. 14 f. und 19 f.) zwar rechtsstaatlich nötig, aber eher akademischer Natur: Einerseits werden Daten in Art. 263 StPO nicht ausdrücklich genannt. Anderseits dürfen *Aufzeichnungen* auf sichergestellten *Datenträgern* und *EDV-Anlagen* nach ausdrücklicher gesetzlicher Vorschrift *durchsucht* werden (Art. 246-248 StPO). Das gilt etwa für Private Keys auf Crypto-Wallets. Da elektronische Aufzeichnungen regelmässig *ausgedruckt* oder ab Bildschirm *fotografiert* werden können, lassen sich entsprechende (analoge)

4 Hier sind höchstens Kleinigkeiten zu bemängeln. So wird die Publikation von SIMMLER/SELMAN/BURGERMEISTER (vgl. z.B. Fn. 142, 174) an verschiedenen Stellen mit einer anderen Abkürzung zitiert ("SIMMLER et al.", z.B. Fn. 6, 7, 80), die im Literaturverzeichnis nicht identifizierbar ist.

5 Erfasst wurden z.B. einzelne sehr aktuelle Aufsätze zu BGE 148 IV 74 oder auch noch Online-Artikel zum *FTX-Crash*. Diverse Internet-Beiträge werden in einem separaten Verzeichnis aufgeführt; die Datenquellen sind weit verstreut und nur schwer überschaubar, themenspezifisch wertvoll (und fachlich seriös) wäre z.B. noch der aktuelle Bericht von *Eurojust* (Cybercrime Judicial Monitor, Mai 2021).

6 Z.B. BGE 140 IV 57; 139 IV 250; 137 IV 145.

7 Selten finden sich etwas verunglückte Sätze wie z.B.: "Somit ist nicht zwingend vorausgesetzt, dass noch kein" (sic) "konkreter Tatverdächtiger vorhanden sein" (sic) (S. 21).

8 Funktionsweise des *Bitcoin-Netzwerks* und verwandter Cryptos (z.B. Ethereum, Monero usw.); Funktionsweisen des *Private Key* und von diversen *Wallets*; allgemeine *rechtliche* Einordnungen (zivilrechtlicher *Sach*begriff; strafprozessuale Definition beschlagnahmbarer *Gegenstände* und *Vermögenswerte*; *Inhaberschaft* bei Cryptos; *kriminalpolitische Relevanz,* vgl. S. 3-18).

9 *Public Keys* werden in der Praxis auch als Cryptowährungs-*Adresse* (cryptocurrency address) oder *Name* des Crypto-Assets bezeichnet; sie werden als *Verifikationsschlüssel* verwendet (Private Keys als notwendiger Signierschlüssel für die Transaktionen).

Dokumente und Fotos auch in den meisten Fällen nach Art. 263 StPO förmlich (als "Gegenstände") *beschlagnahmen* (etwa als Beweismittel).[10] Bei den *Crypto-Assets* selber (z.B. Bitcoin) bildet die **gesetzliche Grundlage** für eine Beschlagnahme und Einziehung von *Vermögen* (nach Art. 263 StPO bzw. Art. 70 StGB) schon gar kein Problem.[11] Die praktischen Schwierigkeiten liegen vielmehr auf der Ebene der **Ermittlung** deliktisch erworbener *Cryptos* und der *Identifizierung* ihrer Inhaber und wirtschaftlich Berechtigten.[12]

Bei der Darstellung der **Beschlagnahmearten** (in **Kap. III**) wird die Ausgleichs-("Vermögens")-*Einziehungsbeschlagnahme* angesichts der Thematik der Masterarbeit (Einziehungsbeschlagnahme von Cryptos) etwas gar knapp behandelt.[13] Nicht erkannt wird hier (und in Kap. IV) eine *weitere* gesetzlich geregelte strafprozessuale Beschlagnahmeart, nämlich die Vermögenssperre zur Sicherstellung einer staatlichen *Ersatzforderung* (Art. 71 Abs. 3 StGB).[14] Hier wirkt sich ungünstig aus, dass die Bearbeiterin der publizierten Bundesgerichtspraxis wenig Beachtung schenkt, in der die Themen Einziehungs- und Ersatzforderungsbeschlagnahme ausführlich behandelt werden.[15]

---

10 Von der Bearbeiterin zutreffend erkannt (S. 22), mit Hinweis auf die besondere Problematik des *beschränkten Zugriffes* (Grenzen des Territorialitätsprinzips) bei *Cloud Computing* bzw. im *Ausland* domizilierten Datenfarmen. Von solchen Fällen abgesehen, hat die "Beschlagnahmbarkeit" von Daten bzw. das betreffende Legalitätsprinzip (Art. 197 Abs. 1 lit. a StPO) in der Praxis kaum je Probleme bereitet. Dies dürfte auch der Grund sein, weshalb der Gesetzgeber bei der jüngst erfolgten *Teilrevision* der StPO (am 17. Juni 2022) noch keinen Anlass gesehen hat, die Gesetzgebung anzupassen.

11 Beim jüngsten Leitentscheid BGE 148 IV 74 wurde die Frage der ausreichenden gesetzlichen Grundlage weder von den Verfahrensbeteiligten bestritten, noch sonstwie in den Erwägungen thematisiert.

12 Von zentraler Bedeutung und häufig schwierig ist die *Identifizierung* des (in der Blockchain und in der verschlüsselten privaten Wallet regelmässig anonymisierten) *Inhabers* des betreffenden *Private Key* (und von am Crypto-Asset allfällig wirtschaftlich berechtigten Dritten). Teilweise *erleichtert* wird die Beschlagnahme und Einziehung von Cryptos hingegen infolge der besseren Nachvollziehbarkeit von *geldwäschereiverdächtigen Transaktionen* (samt dazugehörigen Public Keys/Adressen) auf der öffentlichen Blockchain. Falls sich der Geldwäschereiverdacht erhärtet, lässt das Gesetz die selbständige Einziehung von deliktisch erworbenen Cryptos auch *ohne Identifizierung* eines Beschuldigten bzw. des Inhabers zu.

13 Anstatt themenfernere Beschlagnahmearten (wie Sicherungseinziehungs-Beschlagnahme, Beweismittelbeschlagnahme oder Restitutionsbeschlagnahme) zu vertiefen, hätten hier besondere Probleme der *Ausgleichseinziehung* kurz genannt werden können (etwa Einziehung bei Dritten; Durchgriff auf "Strohleute"); die *Surrogats*problematik wird (in Kap. V) immerhin noch vertieft. Der auch in der Literatur teilweise anzutreffende Begriff "Vermögenseinziehungsbeschlagnahme" ist aus zwei Gründen unglücklich gewählt: Erstens geht es bei der Beschlagnahme nach Art. 263 Abs. 1 lit. d StPO i.V.m. Art. 70 StGB um eine *Ausgleichs*einziehung (im Gegensatz zur Sicherungseinziehung); zweitens erfolgt auch bei *anderen* Beschlagnahmearten (etwa Deckungs-, Restitutions- oder Ersatzforderungsbeschlagnahme) eine *Vermögens*sperre.

14 Keine Erwähnung findet auch der Umstand, dass der Gesetzgeber in der StPO-Revision vom 17.6.2022 die Ersatzforderungsbeschlagnahme (EFB) aus gesetzessystematischen und Gründen der Rechtssicherheit *in die StPO überführt* hat (nArt. 263 Abs. 1 lit. e StPO; vgl. BBl 2022 1560, 9 f.). Immerhin wird die EFB dann noch kurz in Kap. V/3 (S. 48) genannt.

15 Etwa BGE 140 IV 57.

Die **Kap. V-VI** bilden den Kern der Arbeit, der auch (über die rein deskriptiven Teile hinaus) einen selbstständigen *Forschungsbeitrag* enthält.

In **Kap V/B** werden die Möglichkeiten und Grenzen des strafprozessualen *Zugriffs* auf die verschiedenen *Wallet*-Varianten analysiert. Zur Auswertung gelangen hier (nebst Literatur) auch erste Erkenntnisse aus den **Interviews** mit den Experten (S. 29-31). Zum einen werden hier wertvolle Informationen – im Sinne einer aktuellen Auslegeordnung für Praktiker/-innen – zusammengetragen; anderseits zeigt sich auch, dass auf diesem Rechtsgebiet noch viel Forschungsarbeit zu leisten sein wird.[16] Bei der Problematik des gutgläubigen Erwerbs von Cryptos durch *Dritte* wären die einschlägigen *Gesetzes*bestimmungen (Art. 70 Abs. 2 StGB) nebst der konsultierten Literatur wenigstens kurz zu erwähnen (S. 32 f.). Die für die Praxis sehr wichtigen Themen **Territorialitätsprinzip** und **Zugriffsprinzip** (im Ausland verwaltete Wallet-Apps, Cloud Computing, abgeleitete Internetdienste, CCC, internationale Rechtshilfe usw.) werden etwas gar knapp abgehandelt (S. 33 f.).[17]

Bei der in **Kap. V/C** behandelten Problematik der "Übertragung" von Crypto-Assets von der *privaten* auf eine *staatliche Wallet*[18] wird ausgeführt, dass die Übertragung insbesondere dem Ziel diene, dass der Inhaber des Private Key keine Transaktionen durchführen könne mittels "Kopien des privaten Schlüssels", die sich noch "auf unbekannten Speicherorten befinden" können (S. 35). Diese Formulierung ruft nach einer gewissen Klärung: Bevor die Strafverfolgungsbehörde den aufgespürten Private Key nicht dazu verwendet hat, den Crypto-Asset *weiterzutransferieren* (mit Entstehung eines neuen Private Key), schlösse die blosse Verwahrung des *gefundenen* Private Key in einer staatlichen *Wallet* noch nicht aus, dass der Inhaber einer Kopie (des noch gültigen Schlüssels) den Asset erfolgreich weitertransferieren könnte.[19] Die Bearbeiterin *präzisiert* denn auch, dass

16 Welche "*geheimen* Zwangsmassnahmen" können wann "in Erwägung gezogen" werden? (S. 29). Inwiefern ist das *Hacken* von Software-Wallets "denkbar" bzw. "theoretisch mit der Govware möglich"? wann ist es legal? (S. 30). Könnte auf Anbieter von *Wallet-Apps* (S. 30 f.) das *neue BÜPF* (betreffend Anbieter von *abgeleiteten* Internetdiensten) direkt oder analog anwendbar sein? usw.

17 Das Zugriffsprinzip steht grundsätzlich nicht im Widerspruch zum Territorialitätsprinzip (TP): Eine Schweizer Strafverfolgungsbehörde, die z.B. von einem in der Schweiz gelegenen Rechner aus legal auf Daten zugreifen kann, die von einem im Ausland verwalteten System gespeichert werden (Datenfarmen, Clouds usw.), verletzt nach der Praxis des Bundesgerichtes das TP nicht. Dafür benötigt die Behörde allerdings in der Regel die Zugangsdaten zum betreffenden Nutzerkonto.

18 Als *zweiter* notwendiger Beschlagnahmeschritt *nach* dem Auffinden des *Private Key* (zur Auslösung einer Crypto-Transaktion).

19 Entweder müssten *sämtlich Kopien* des Private Key gefunden und auf eine staatliche Wallet übertragen

nicht bloss der gefundene Private Key aus einer privaten auf eine staatliche *Wallet* zu verschieben sei, sondern ein "*Transfer* der *Crypto-Assets*" auf eine staatliche Wallet stattzufinden habe (S. 35).[20] Etwas verwirrend und unpräzise wirkt hier, wenn bei den generierten neuen Keys auf der staatlichen Wallet, mit denen "eine Übertragung" der Assets möglich ist, von "Public Keys" gesprochen wird (S. 36). Als **Public Keys** werden die Crypto-*Adressen* bezeichnet, die öffentlich sind und nur der *Verifikation* dienen; für *Transaktionen* hingegen verwenden auch Behörden die (neu generierten) *Private* Keys, die sie in der staatlichen *Wallet* verwahren. Wertvolle Informationen ergeben sich aus den Interviews zu den *Arten* der verwendeten *staatlichen Wallets* (Selbstverwaltung bzw. Drittverwahrung, S. 35 f.).

Zutreffend interpretiert und mit zielführenden Anmerkungen versehen hat die Bearbeiterin den neuesten *Leitentscheid* **BGE 148 IV 74** zur wichtigen Frage der **vorzeitigen Verwertung** (Art. 266 Abs. 5 StPO) von sichergestellten Crypto-Assets (**Kap. V/D**). Das BGer vertiefte die Frage, inwieweit es sich dabei grundsätzlich (und im beurteilten Fall der Verwertung und Beschlagnahme von diversen Crypto-"Währungs"-Arten) um eine Einziehungsbeschlagnahme von *Vermögenswerten* handelt, nicht, zumal diese Rechtsfrage unter den Verfahrensbeteiligten unbestritten war. Das BGer geht aber ausdrücklich von einzieh- und beschlagnahmbaren Vermögenswerten aus.[21] Der Entscheid konzentriert sich im Übrigen auf die (streitigen bzw. von den Zürcher Strafjustizbehörden in casu nicht ausreichend geregelten) **Modalitäten** der *werterhaltenden vorzeitigen Verwertung* der Cryptos und der anschliessende (Wieder-)*Beschlagnahme* des *Verwertungserlöses*.

Wie gerade der BGE 148 IV 74 verdeutlich, bedeutet *vorzeitige* Verwertung nicht zwangsläufig *sofortige* Verwertung.[22] Zentral ist dabei das Anliegen, dass die Staatsanwaltschaft – nötigenfalls unter Beizug von Fachleuten – in der Verwertungsverfügung

werden, oder die staatliche Wallet müsste technisch sicherstellen können, dass der gültige Private Key – atypischerweise – nur unter Verwendung der staatlichen Wallet benutzt werden könnte, oder die Behörde muss einen *neuen Private Key* generieren, indem sie den Asset *weitertransferiert* und den neuen Key in der staatlichen Wallet aufbewahrt.

20 Damit wird aber ein *neuer* Private Key generiert, der den bisherigen (samt allfälligen Kopien) nutzlos werden lässt.

21 Vgl. etwa E. 4.4.2 von BGE 148 IV 74.

22 Da sich selbst das Gesetz (Art. 266 Abs. 5 StPO) insofern *unpräzise* ausdrückt (bei teleologischer Auslegung), kann die betreffende Wortwahl in der MA (S. 37 und 38: "sofort verwerten"/"sofortige Verwertung") der Bearbeiterin nicht angelastet werden. BGE 148 IV 74 spricht insofern (schon in der Regeste) präziser von *vorzeitiger* Verwertung.

ausreichend präzise *Anordnungen* trifft, um bei Cryptos ein **möglichst günstiges Verwertungsergebnis** zu erzielen. Dabei ist (ähnlich wie beim Verkauf von Wertpapieren) u.a. zu prüfen, ob sich eine **gestaffelte** Veräusserung[23] aufdrängen könnte, um *Kursschwankungen* aufzufangen bzw. um unerwünschte Kursreduktionen zu vermeiden, insbesondere, wenn kurzfristig *sehr grosse Vermögenspositionen* auf den Markt geworfen werden. Gewisse ergänzende Hinweise der Interviewten (und der einschlägigen Literatur) werden sachgerecht eingebaut. Nur schwer nachvollziehbar ist für den Referenten die Aussage, es könne der beschuldigten Person (b. P.) "grundsätzlich gleichgültig sein, wie hoch der Erlös sein wird", wenn dieser "einer geschädigten Person zurückgegeben werden soll".[24] Etwas zu stark wird auch ein "Zustimmungserfordernis" der b. P. betont.[25]

In Kap **V/E** werden noch einige **Spezialfragen** der Crypto-Beschlagnahme vertieft.[26] Das *zentrale Problem* der Strafverfolgung, die hinter den einsehbaren Crypto-Transaktionen stehenden konkreten *Personen* bzw. wirtschaftlich Berechtigten zu *identifizieren* (S. 47 f.), hätte noch etwas ausgeleuchtet werden können.[27] Bei *fehlendem Zugriff* auf Cryptos deliktischer Herkunft (z.B. Private Key nicht bekannt) kann zwar die Zusprechung einer *staatlichen Ersatzforderung* (st. EF) in Frage kommen (S. 48 f.); eine Ersatzlösung stellt dies jedoch nur dar, wenn *anderes* Vermögen als *Haftungssubstrat* für die st. EF beschlagnahmt werden kann.

Im abschliessenden **Kap. VI** werden **Handlungsempfehlungen** (de lege lata et ferenda) formuliert. Im Bereich *Wissenstransfer* und *Weiterbildung* für Strafverfolgungspersonal stützen sich diese Anregungen primär auf den bundesrätlichen Umsetzungsplan für eine

---

23 Das BGer spricht hier (gestützt auf Zitate aus den Akten) etwas untechnisch und unpräzise von einem "langsamen" Verkauf.

24 S. 39. Da die b. P. für den verursachten Schaden *über den Erlös von beschlagnahmtem Vermögen hinaus haftet,* hat sie durchaus ein erhebliches Interesse an einem möglichst hohen Verwertungserlös.

25 S. 44. Zwar ist im Rahmen der Verhältnismässigkeit möglichst auf einen Konsens bei den Verwertungsmodalitäten (zur Erhaltung von Haftungssubstrat) hinzuwirken; entscheidend ist nach der Praxis des BGer jedoch das Ziel eines möglichst *hohen Haftungssubstrates*, selbst gegen den Willen (bzw. gegen eine Selbstschädigungsabsicht) der b. P.

26 "Papertrail" bei *Surrogaten* von deliktischem Gewinn; *Spurenverwischung* u.a. mittels Crypto-"Mixern"; Rückverfolgbarkeit der Transaktionen auf der *Blockchain*; Thematik der *Ersatzforderungsbeschlagnahme*.

27 Hier sind die Strafverfolger teilweise noch stark auf klassische "analoge" Untersuchungsmethoden angewiesen (Kommunikations-*Überwachung* mit Teilnehmer-Identifikation; *Observationen*; *Hausdurchsuchungen*; *Sicherstellung* von *Zielgeräten*, möglichst mit geöffneter App, etwa von Krypto-Börsen oder von digitalen Wallets; usw.).

"Nationale Strategie gegen Cyber-Risiken (NCS)" und die diesbezüglichen Kommentare der interviewten Fachleute.[28] Mit Recht weist die Bearbeiterin darauf hin, dass im Lichte der Rechtsprechung des BGer die *Staatsanwaltschaften* in die Lage versetzt werden müssen, im Zusammenhang mit Verfügungen betreffend Cryptos die Berichte von IT- und Finanzfachleuten zu verstehen und in gerichtlichen Eingaben zu erläutern. Selbst in Kantonen mit spezialisierten Cybercrime-Abteilungen sei allgemein noch *zu wenig Fachwissen* vorhanden (S. 50 f.).[29]

De **lege ferenda** werden folgende Vorschläge unterbreitet: Im Bereich des *nationalen* Rechts wird (gestützt auf Meinungsäusserungen in der Literatur) eine *ausdrückliche* und *spezifischere Regelun*g der Beschlagnahme von *Cryptos* in der StPO empfohlen. Insbesondere wird eine Norm vorgeschlagen, die zu Beschlagnahmezwecken die *Übertragung* von Crypto-Assets auf eine *staatliche Wallet* ausdrücklich erlaubt. Auch wird die Einrichtung eines zentralen Expertengremiums angeregt.[30] Hier hätte ergänzend noch auf gewisse *ausländische* Regelungen hingewiesen werden können, die bereits legiferiert wurden.[31]

Zur Bewältigung der spezifischen Probleme beim Zugriff auf *im Ausland* (bzw. international verstreut) *verwaltete Daten* werden schliesslich noch weitere, **völkerrechtliche** Bemühungen (etwa im Rahmen der hängigen Reform der CCC) für einen *vereinfachten internationalen Datenaustausch* über eine zentrale *Koordinationsbehörde* verlangt.[32] Auch wird die in der Literatur (insbes. Diss. TSCHUDI) entwickelte Idee eines *internationalen Registers* ("Blacklist" nach dem Muster des in den USA eingeführten Registers) für *deliktsverdächtige* Crypto-Assets vorgestellt, deren *Adressen* (Public Keys) zwar *identifiziert* werden konnten, deren Beschlagnahme (Transfer auf eine staatliche Wallet) jedoch

28 Diese bewerten das nationale "Gremium Cyber Case" zwar als hilfreich im Bereich Informationsaustausch und Networking. Für eine zufriedenstellende Wissensvermittlung über Cryptos werden die Angebote des Gremiums aber als ungenügend beurteilt. Im Vordergrund stehen für spezialisierte Strafverfolger/-innen daher primär Selbststudium und Eigeninitiative. Im Rahmen der Cyberboard-Zusammenarbeit sei das Ausbildungsangebot auszubauen und – nebst Polizeiangehörigen – auch den Staatsanwält/-innen anzubieten (S. 50).

29 Verbesserungsmöglichkeiten de lege lata bestehen auch in den Bereichen *Koordination* und *Erfahrungsaustausch* sowie Verfahrenseffizienz bei der *interkantonalen* Zusammenarbeit (S. 51).

30 S. 52 f. Zu den gesetzgeberischen Bemühungen für eine Regelung des *interkantonalen Datenaustauschs* s. S. 53.

31 Etwa die neuen Gesetzesnormen der *Slowakei* (vgl. dazu Eurojust, Cybercrime Judicial Monitor, Nr. 6 Mai 2022, S. 7).

32 S. 53 f., mit Hinweis auf die Experteninterviews.

am fehlenden Zugriff auf die privaten Wallets bzw. die Private Keys scheitert.[33]

Prof. Dr. Marc Forster/11. Januar 2023

33 S. 54. Die öffentliche Registrierung auf einer "Schwarzen Liste" mindert die *Verkehrsfähigkeit* der adressierten Crypto-Assets und tangiert zudem die Einrede des *gutgläubigen Erwerbs* von *Drittkäufern* (vgl. Art. 70 Abs. 2 StGB). Dennoch bezweifeln einige interviewte Fachleute die Wirksamkeit von solchen Registern und "Warnlisten". – Der dabei erhobene Einwand, dass die Auflistung von verdächtigen Crypto-Adressen bzw. Public Keys eine *Übertragung* (mittels Private Keys) nicht verhindern könne, überzeugt allerdings nur teilweise: Auch bei analogen Vermögenswerten, z.B. gestohlenem Schmuck oder Kunstwerken, kann eine polizeiliche Identifizierung und *öffentliche Fahndungsausschreibung* (etwa mittels Fotos oder Registriernummern) einen Weiterverkauf an Hehler zwar nicht verhindern, trotzdem macht die öffentliche Ausschreibung durchaus Sinn.