ERMITTLUNGSMASSNAHMEN UND KYC IN ANONYMEN KRYPTOWÄHRUNGEN

Walter Hötzendorfer / Jan Hospes / Christof Tschohl / Markus Kastelitz

Senior Researcher, Research Institute AG & Co KG
Annagasse 8/1/8, 1010 Wien, AT
walter.hoetzendorfer@researchinstitute.at; http://www.researchinstitute.at

Junior Researcher, Research Institute AG & Co KG
jan.hospes@researchinstitute.at; http://www.researchinstitute.at

Wissenschaftlicher Leiter, Research Institute AG & Co KG
christof.tschohl@researchinstitute.at; http://www.researchinstitute.at

Senior Researcher, Research Institute AG & Co KG
markus.kastelitz@researchinstitute.at; https://www.researchinstitute.at

Schlagworte: ***Blockchain, Kryptowährungen, Know Your Customer, Datenschutz, Ermittlungsmaßnahmen, Sicherstellung***

Abstract: *Mit der fünften Geldwäscherichtlinie werden KYC-Pflichten auf Handelsplattformen für Kryptowährungen und Hot Wallet Provider ausgedehnt. Der Beitrag stellt diese neuen Regeln dar und behandelt die Frage, wie wirksam diese sein können. Darüber hinaus wird der rechtliche Rahmen polizeilicher Ermittlungsmaßnahmen in Bezug auf Handelsplattformen und Hot Wallet Provider untersucht. Ein besonderes Augenmerk legt der Beitrag auf die Besonderheiten anonymer Kryptowährungen.*

1. Anonyme Kryptowährungen

Anonyme Kryptowährungen bedienen sich neben gängiger Proof-of-Work-Konsensverfahren auch besonderer Verfahren, um die Identität der Nutzer zu schützen. Zu den gängigen gehören hierbei Ethereum, Monero und Zcash. Zcash und Ethereum[1] nutzen das Zero-Knowledge-Proof-Verfahren. Die Blockchain enthält nicht den Transaktionsinhalt, sondern lediglich Beweise dafür, dass die Transaktionsparteien bestimmte Voraussetzungen erfüllen (z.B. Absender A hat 100 Einheiten in seiner Wallet).

Monero nutzt das Ringsignaturverfahren, welches eine Spezialform des Zero-Knowledge-Proof-Verfahrens ist. Ziel des Verfahrens ist es, Währungseinheiten zu transferieren, ohne die Identität der Transaktionsparteien offenzulegen. Der Anonymisierungsgrad ist abhängig von der Anzahl an sog. Mixings (auch ringsize, RingCT genannt). Diese sind alternative Transaktionswege, welche einem potenziellen Angreifer die Bestimmung des Transaktionsflusses erschweren sollen. Der Anonymisierungsgrad kann wie folgt dargestellt werden:

$$p = \left(\frac{1}{k+1}\right)^n$$

Dabei ist *k* die Anzahl der Mixings, *n* die Anzahl der Transaktionen und k ist variabel und konnte bis zum Hardfork im April 2018 vom Nutzer frei gewählt werden. Diesem ging eine Debatte der Monero-Community

[1] Der Begriff Ethereum ist für die Zwecke dieses Beitrages als jene Version der virtuellen Währung zu verstehen, welche das zk-sNARKs-Update https://z.cash/blog/ethereum-snarks/ (aufgerufen am 14. Dezember 2018, alle weiteren in diesem Beitrag zitierten Internetquellen wurden am 7. Januar 2019 zuletzt aufgerufen) beinhaltet.

über die Höhe des obligatorischen Mixings voran, da ein höheres Mixing und die damit einhergehende höhere Anonymisierungsrate mit höheren Transaktionskosten verbunden ist. Ab dem Hardfork ist für Monerowallets ein Mixing k=7 obligatorisch, was die Nachverfolgbarkeit von Transaktionen nach derzeitigem Wissensstand[2] unmöglich macht.

2. Personenbezug anonymer Kryptowährungen

An dieser Stelle soll kurz beleuchtet werden, wie dieser Umstand datenschutzrechtlich einzuordnen ist. Gem. Art. 4 Z. 1 DSGVO[3] sind alle Daten personenbezogen, «die sich auf eine identifizierte oder identifizierbare natürliche Person» beziehen. Dies ist in ErwGr. 26 der DSGVO näher umschrieben und wurde im Wesen unverändert aus der DSRL[4] übernommen. Im Ergebnis ist von einer Bestimmbarkeit der Identität des Betroffenen jedenfalls immer dann auszugehen, wenn der eigentliche Zweck der Verarbeitung die Identifizierung von Personen miteinschließt oder sogar in der Identifizierung von Personen besteht.[5] Ähnliches hat die DSK[6] ausgesprochen, anknüpfend an eine Entscheidung zu einer ähnlichen Auslegungsfrage im Erkenntnis des VfGH zur Section Control[7]: Es liege jedenfalls dann eine Ermittlung von Daten über Personen vor, deren Identität bestimmbar ist, wenn der einzige Sinn der Datenermittlung darin liege, diese Personen zu identifizieren, und sei es auch erst durch Heranziehung eines Dritten.[8] Das bedeutet, jede Form der Verarbeitung der Blockchain anonymer Kryptowährungen mit dem Ziel, Transaktionen nachzuvollziehen und diese mit natürlichen Personen in Verbindung zu bringen, insbesondere zu Ermittlungszwecken (siehe dazu Kapitel 4), ist eine Verarbeitung personenbezogener Daten und somit ein rechtfertigungsbedürftiger Grundrechtseingriff, der verhältnismäßig sein muss.

3. Die 5. Geldwäscherichtlinie

In Umsetzung der 4. Geldwäscherichtlinie (RL 2015/849)[9] ist in Österreich das FM-GwG[10] vom 1. Januar 2017 ergangen. Dieses regelt unmittelbare KYC-Pflichten für im Inland ansässige Institutionen, insbesondere für Finanz- und Kreditinstitute. Dienstleister im Bereich der Kryptowährungen sind von RL 2015/849 ihrem Wortlaut nach nicht erfasst, da Kryptowährungen ihrer Rechtsnatur nach keine bekannte Form des Geldes

---

2 Möser et al., An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies, Volume 2018, Issue 3, S. 143–163; Kumar et al., A Traceability Analysis of Monero's Blockchain, in: Foley/Gollmann/Snekkenes (Hrsg.). Computer Security – ESORICS 2017, 22nd European Symposium on Research in Computer Security 2017, Proceedings, Part II, Lecture Notes in Computer Science 10493, Springer, 2017, S. 153 ff.

3 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl L 2016/119, 1.

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 1995/281, 31.

5 Vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff «personenbezogene Daten», WP 136, 2007, S. 19 f.

6 Österr. Datenschutzkommission, ab 1. Januar 2014 von der österr. Datenschutzbehörde abgelöst.

7 VfGH G 147/06 vom 15. Juni 2007.

8 DSK K121.359/0016-DSK/2008 vom 11. Juli 2008.

9 Richtlinie (EU) 2015/849 vom 20. Mai 2015 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung, zur Änderung der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates und der Richtlinie 2006/70/EG der Kommission, ABl L 2015/141, 73.

10 Bundesgesetz zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung im Finanzmarkt (Finanzmarkt-Geldwäschegesetz – FM-GwG) BGBl I 118/2016.

darstellen[11] und daher nicht unter den Wortlaut des Art. 4 VO 2013/575,[12] auf welchen RL 2015/849 verweist, subsumierbar sind.

Diese Lücke soll durch die 5. Geldwäscherichtlinie (RL 2018/843)[13] geschlossen werden, die am 9. Juli 2018 in Kraft trat und gem. Art. 4 Abs. 1 der Richtlinie bis 10. Januar 2020 von den Mitgliedstaaten umzusetzen ist. Die Richtlinie sieht in Art. 1 die Ausweitung des Anwendungsbereichs der bestehenden RL 2015/849 auf Handelsplattformen und elektronischen Geldbörsen für virtuelle Währungen vor. Die Umsetzung wird voraussichtlich eine Novellierung des FM-GwG zur Folge haben. Wie die Erwägungen der anderen Geldwäscherichtlinien zuvor, beinhalten auch jene der 5. Geldwäscherichtlinie Bezüge zu Leitlinien der FATF.[14]

Methodisch erweitert die RL 2018/843 im Zusammenhang mit Kryptowährungen den Anwendungsbereich der RL 2015/849, indem sie den in Art. 2 RL 2015/849 abgesteckten Kreis der Verpflichteten, welche die von RL 2015/849 bereits aufgestellten Sorgfaltspflichten zu erfüllen haben, erweitert. Darüber hinaus führt sie aber keine wesentlichen inhaltlichen Änderungen der bestehenden Sorgfaltspflichten herbei. Die neuen Verpflichteten sind unter anderem Entitäten, welche Berührungspunkte mit virtuellen Währungen haben. Daher ist es begrüßenswert, dass RL 2018/843 eine Definition der «virtuellen Währungen» liefert.

3.1. Der Begriff der «Virtuellen Währungen» nach der 5. Geldwäscherichtlinie

Die Definition des Begriffs findet sich in Art. 1 Abs. 2 lit. d RL 2018/843 und enthält sowohl negative als auch positive Tatbestandsmerkmale. Zunächst stellt die Definition klar, dass es sich bei virtuellen Währungen um digitale Werteinheiten handelt, welche «auf elektronischem Wege übertragen, gespeichert und gehandelt» werden können und daher verschieden von Bargeld sind, welches körperlicher Natur ist. Danach wird festgehalten, dass virtuelle Währungen von «keiner Zentralbank oder öffentlichen Stelle» emittiert oder garantiert werden. Kryptowährungen werden stattdessen meist dezentral von einer Vielzahl an Einzelpersonen errechnet und damit von Fiatgeld abgegrenzt. Es wäre auch denkbar, dass Währungseinheiten von einer einzigen Stelle errechnet werden, was ihre Einstufung als virtuelle Währungseinheit jedoch nicht beeinflussen würde.

Darüber hinaus sind virtuelle Währungen «nicht zwangsläufig an eine gesetzlich festgelegte Währung angebunden». Aufgrund des Wortlautes «zwangsläufig» stellt dieser Passus kein Ausschlusskriterium dar. Somit gelten auch solche Kryptowährungen als virtuelle Währungen, welche an den Kurs einer Fiatwährung gebunden sind. Dies ist etwa bei der Kryptowährung Tether der Fall, welche an den Dollarkurs gebunden ist und als kursbeständige Währung auf Handelsplattformen, welche kein Fiatgeld entgegennehmen, Verwendung findet. Ausgenommen sind jene virtuellen Währungen, die «gesetzlichen Status einer Währung oder von Geld» besitzen. Damit wäre nach der Definition des Gesetzgebers etwa die Kryptowährung Petro, welche in Venezuela als gesetzliches Zahlungsmittel gilt, nicht von der Richtlinie erfasst. Die Voraussetzung der Gesetzmäßigkeit fügt sich nicht schlüssig in das System der Geldwäschebekämpfung ein, da dieses von Anbeginn bei gesetzlichen Zahlungsmitteln, angefangen mit Bargeld, angesetzt hat. Schließlich sind als virtuelle Währungen i.S.d. Richtlinie nur solche anzusehen, welche «von natürlichen oder juristischen Personen als Tauschmittel akzeptiert»

---

[11] Schimansky/Bunte/Lwowski, Bankrechts-Handbuch, 4. Aufl. 2011, § 123 Rz. 48; Kütük/Sorge, Bitcoin im deutschen Vollstreckungsrecht – Von der «Tulpenmanie» zur «Bitcoinmanie», MMR 2014, 643, S. 644; Beck, Bitcoins als Geld im Rechtssinne, NJW 2015, 580, S. 582; siehe auch BaFin Journal – Bitcoin, Januar 2014, S. 2.

[12] Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012, ABl L 2013/176, 1.

[13] Richtlinie (EU) 2018/843 vom 30. Mai 2018 zur Änderung der Richtlinie (EU) 2015/849 zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung und zur Änderung der Richtlinien 2009/138/EG und 2013/36/EU, ABl L 2018/156, 43.

[14] Insbesondere auf: FATF, Guidance for a Risk-Based Approach to Virtual Currencies, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf. Aus der Sicht des demokratischen Rechtsstaats ist der hohe faktische Stellenwert der FATF kritisch zu hinterfragen, da eine solche multinationale Arbeitsgruppe dem demokratisch legitimierten Gesetzgeber formell nicht übergeordnet sein kann.

werden, sohin jedenfalls alle Kryptowährungen, welche auf Handelsplattformen gehandelt werden, damit auch Ethereum, Monero und Zcash. Insgesamt handelt es sich um eine weite und technologieoffene Definition.

In den Erwägungsgründen des Vorschlages der Kommission findet sich die Überzeugung der Kommission, bei virtuellen Währungen käme die Distributed-Ledger-Technologie zum Einsatz[15], sodass der Anwendungsbereich auf Kryptowährungen einzuschränken wäre. Dieser Passus findet sich allerdings nicht in der verabschiedeten Fassung der RL 2018/843 wieder.

3.2. Kreis der Verpflichteten der 5. Geldwäscherichtlinie

Art. 1 Abs. 1 lit. c RL 2018/843 erweitert zunächst den persönlichen Anwendungsbereich der RL 2015/849 um «Dienstleister, die virtuelle Währungen in Fiatgeld und umgekehrt tauschen». Der Vorschlag[16] der europäischen Kommission sowie die FATF-Leitlinien[17] schränkten die Regelung auf beruflich ausgeübte Tauschbörsen ein und überließen es dem Rechtsanwender mangels eindeutiger Anhaltspunkte vollkommen, zu beurteilen, wann dies vorliegt. Insofern ist es im Sinne der Rechtssicherheit begrüßenswert, dass sich diese Einschränkung nicht in der Endfassung der Richtlinie wiederfindet. Erfasst sind alle Dienstleister, welche selbstständig einen diesbezüglichen Tauschvorgang durchführen. In den Erläuterungen des Kommissionsentwurfs finden sich in den Erwägungen zur Verhältnismäßigkeit sowie bei der Erläuterung einzelner Bestimmungen Verweise auf die Gatekeeper-Funktion.[18] Diese Funktion erfüllen nur jene Dienstleister, welche Primärzugang zu Kryptowährungen gewähren. Auch dieser Erwägungsgrund wurde zwar nicht in die Endfassung übernommen, dies ist aber ob des klaren Wortlautes des Art. 1 Abs. 1 lit. c RL 2018/843 nicht notwendig. Dem Wortlaut nach sind jene Dienstleister klar ausgenommen, welche virtuelle Währungen in andere virtuelle Währungen, also etwa Bitcoin in Monero, umwechseln (Krypto-zu-Krypto-Tauschbörsen). Ebenso sind an dieser Stelle Handelsplattformen ausgenommen, welche nicht selbstständig Tauschvorgänge durchführen, sondern bloß Kunden mit verschiedenen Währungen zusammenführen, da es in diesen Fällen die Nutzer selber sind, die Währungen untereinander tauschen, und nicht die Handelsplattform. Die Nutzer selber können nicht Verpflichtete i.S.d. Richtlinie sein, da sie keine Dienste anbieten, sondern den Tauschvorgang im eigenen Sinne durchführen.

Daneben nimmt Art. 1 Abs. 1 lit. c RL 2018/843 den «Anbieter von elektronischen Geldbörsen» in die Pflicht. Dieser ist nach Art. 1 Abs. 2 lit. d RL 2018/843 definiert als «Anbieter, der Dienste zur Sicherung privater kryptografischer Schlüssel im Namen seiner Kunden anbietet, um virtuelle Währungen zu halten, zu speichern und zu übertragen.» Es handelt sich also um Anbieter von Zugangsschlüsseln, welche es dem Nutzer ermöglichen, die Währungseinheiten zu verwalten und Dritte hiervon auszuschließen. Anknüpfungspunkt ist die Bereitstellung einer Dienstleistung, was eine kausale Beziehung zwischen dem Tätigwerden des Dienstleisters und der Möglichkeit des Konsumenten, die Währungseinheiten zu verwalten, erforderlich macht. An diesem Punkt ist zwischen Hot Wallets und Cold Wallets zu unterscheiden. Hot Wallets werden online verwaltet und von einem Anbieter bereitgestellt. Das macht sie anfälliger für Angreifer, sie sind aber einfacher zu handhaben. Cold Wallets sind nicht mit dem Internet verbunden.[19] Als Trägermaterial des kryptographischen Schlüssels dienen USB-Sticks oder Papier, welche bei sicherer Aufbewahrung keine Angriffsfläche bieten. Insbesondere sollten Cold Wallets nicht als Dienstleistung gelten, da sie direkt aus der Blockchain bezogen werden und vom Nutzer eigenständig und ohne Mithilfe von Dritten verwaltet werden. Zudem gibt es bei Cold Wallets keinen Dienstleister, welcher die Cold Wallet bereitstellt. Daher fallen nur Hot-Wallet-Anbieter in den Anwendungs-

15 COM (2016) 450 final, S. 14.

16 COM (2016) 450 final, Art. 1 Z. 1.

17 FATF, International standards on combating money laundering and the financing of terrorism & proliferation, (Stand: Oktober 2018), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, 2018, S. 125.

18 COM (2016) 450 final, S. 8, 14.

19 FATF, Guidance for a Risk-Based Approach to Virtual Currencies, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf, 2015, S. 29.

bereich der Richtlinie. Meist werden Hot Wallets von Handelsplattformen (siehe oben) bereitgestellt. Ist dies der Fall, sind diese zur Einhaltung der Geldwäschebestimmungen verpflichtet.

Nutzer und Miner sind nicht unmittelbar von den Sorgfaltspflichten der Richtlinie erfasst. Ihnen soll nach Art. 65 Abs. 1 RL 2018/843 eine freiwillige Registrierungsmöglichkeit in Formularform bereitgestellt werden. Gegen diese Ansätze spricht die fehlende Geeignetheit. Anwender, welche illegale Ziele verfolgen, werden sich nicht selber registrieren und selbst wenn, müsste die Richtigkeit der dabei gemachten Angaben in Zweifel gezogen werden.

3.3. Wann greifen die Sorgfaltspflichten?

Der sachliche Anwendungsbereich ist von mehreren Tatbeständen gekennzeichnet. Die Sorgfaltspflichten greifen gemäß § 5 FM-GwG insbesondere bei der Begründung einer Geschäftsbeziehung oder der Durchführung einer gelegentlichen Transaktion von mindestens 15 000 Euro. Nach § 2 Abs. 10 FM-GwG liegt eine Geschäftsbeziehung dann vor, wenn «bei Zustandekommen des Kontakts davon ausgegangen wird», dass die Geschäftsbeziehung von «gewisser Dauer» sein wird. Dabei wäre der Zeitpunkt des ersten Transaktionsauftrages als Zeitpunkt der Aufnahme der Geschäftsbeziehung denkbar. Dagegen spricht die eindeutige Absicht des Kunden, bei der Erstellung eines Nutzerkontos, welches rein dem Zweck des Erwerbs und der Verwaltung von Kryptowährungen dient, diese auch zu erwerben. Ist daher das Erstellen eines Nutzerkontos mit der Zuweisung einer Hot Wallet durch den Dienstleister verbunden, ist das als Begründung einer Geschäftsbeziehung zu werten, da dieser Vorgang gemäß § 1 Abs. 10 FM-GwG aus Ex-ante-Sicht eine geschäftliche Beziehung auf unbestimmte Zeit begründet. Die Kontoerstellung ist auch mit der gewerblichen Tätigkeit des Dienstleisters verbunden, da sie die Basis für die Inanspruchnahme der Dienstleistungen darstellt. Insgesamt greifen daher die Sorgfaltspflichten in diesem Fall bereits ab der Erstellung eines Kundenkontos.

Anders kann die Rechtslage bei Bitcoin-Automaten sein, welche nach Einwurf von Fiatgeld eine entsprechende Anzahl an Krypto-Währungseinheiten ausstellen. Hier ist die Ausgabe der virtuellen Währungseinheiten zwar meist nicht an die Erstellung einer elektronischen Geldbörse gebunden, jedoch vollzieht der Automat einen Tauschvorgang und ist daher innerhalb des Anwendungsbereiches der Richtlinie. Im sachlichen Anwendungsbereich wird eine längerfristige Beziehung oder eine Wertgrenze gefordert. Demnach würde der einmalige Wechselvorgang unter der Wertgrenze an einem Bitcoin-Automaten keine vorherige Registrierung voraussetzen. Freilich kann der wiederholte Besuch eines Bitcoin-Automaten durchaus eine längerfristige Beziehung begründen. Daneben treffen den Betreiber nach § 5 Abs. 2 FM-GwG Sorgfaltspflichten bei Transaktionen von mehr als 15 000 Euro und das auch dann, wenn diese Grenze erst durch mehrere Vorgänge überschritten wird, «zwischen denen eine Verbindung offenkundig gegeben ist». Es stellt sich also die Frage, ob der Betreiber des Automaten dazu verpflichtet ist, zu prüfen, ob seine Kunden den Automaten wiederholt nutzen. Da die Sorgfaltspflichten nach § 7 FM-GwG bereits vor der Begründung einer Geschäftsbeziehung bzw. der Durchführung einer gelegentlichen Transaktion greifen, ist davon auszugehen, dass den Betreiber eine solche Vorabprüfungspflicht trifft.

3.4. Kritische Würdigung und Ausblick

Im System der 5. Geldwäscherichtlinie ergeben sich insbesondere bei Tauschbörsen, welche keinen Tausch von und zu Fiatgeld anbieten, sowie bei der Verwendung von Cold Wallets Lücken bei der Nachverfolgbarkeit. Um diese Lücken zu schließen, enthalten die am 19. Oktober 2018 aktualisierten FATF-Leitlinien[20] auch einen Tatbestand für Tauschbörsen, welche den Umtausch zwischen einer oder mehreren virtuellen Währungen zum Gegenstand haben. Daneben findet sich an gleicher Stelle auch ein Tatbestand für Dienstleistungserbringer,

[20] FATF, International standards on combating money laundering and the financing of terrorism & proliferation (Stand: Oktober 2018), http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, 2018, S. 125.

welche den An-/Verkauf virtueller Währungen ermöglichen, was auch Anbieter von Tauschbörsen erfassen würde.

Allerdings würde selbst eine vollständige Umsetzung dieser Vorschläge zu keiner vollkommenen Nachverfolgbarkeit führen. Insbesondere bleibt die Möglichkeit einer Transaktion von einer Cold Wallet an eine andere Cold Wallet, was die Nachverfolgbarkeit der Zahlungsflüsse in anonymen Kryptowährungen – anders als etwa bei Bitcoin – ausschließt, vorausgesetzt das Transaktionsvolumen ist insgesamt groß genug, um eine verschleiernde Wirkung zu entfalten. Zwar muss der Anwender seine Währungseinheiten an einem gewissen Punkt wieder erfassten Systemen zuführen, um ihren Gegenwert zu lukrieren, doch bleiben mögliche illegale Zahlungsvorgänge mittels Cold Wallet unbemerkt.

Daneben ist der räumliche Geltungsbereich zu beachten. Zunächst ist der Kreis der Verpflichteten der Geldwäscherichtlinien auf jene mit Sitz in der EU beschränkt. Die G20 haben das Ziel bekundet, die FATF-Leitlinien umzusetzen,[21] jedoch eröffnet auch dieser Rahmen die Umgehung von KYC-Pflichten, indem Dienstleister ihren Sitz in eine andere Jurisdiktion verschieben, und weiterhin auch europäische Nutzer ansprechen. Im Sinne eines «Whitelistings» könnte etwa auf europäischer Ebene angedacht werden, dass nur solche Währungseinheiten gehandelt werden dürfen, welche aus Ländern stammen, die mit geeigneten KYC/AML-Regelungen ausgestattet sind, oder von Dienstleistern stammen, welche dem europäischen Dienstleister die Durchführung von KYC/AML vertraglich zusichern. Whitelisting stellt eine eingriffsintensive Maßnahme dar, da prinzipiell anlasslos gesamte Systeme unter Generalverdacht gestellt und überwacht werden. Dennoch ist Whitelisting nicht dazu geeignet, das Ziel vollkommener Nachverfolgbarkeit zu erreichen, da es keine Transaktionen von Cold Wallets an Cold Wallets zu erfassen vermag, weshalb es u.E. abzulehnen ist.

Bei der Bekämpfung illegaler Aktivitäten innerhalb der Blockchain wird auch an bestehenden Sanktionslisten angeknüpft, welche Daten von Personen enthalten, bei denen Verdacht auf illegales Handeln besteht. Das amerikanische Office of Foreign Assets Control (OFAC) hat in diesem Sinne angekündigt, ihrer Sanktionsliste auch Walletadressen hinzuzufügen.[22] Anknüpfungspunkt können Wallets oder einzelne Transaktionen sein. Beim Walletblacklisting werden Public Keys der Wallets in einer Liste markiert, wodurch Transaktionen ab und an eine Adresse vom Mining Pool, welcher automatisiert eine Blacklisting-API verwendet, nicht durchgeführt werden. Beim Transaktionsblacklisting wird der Wert der Transaktion in jene Liste aufgenommen. Blockchains gängiger anonymer Kryptowährungen können nur Walletadressen, nicht jedoch die Transaktionswerte entnommen werden. Währungseinheiten anonymer Kryptowährungen sind demnach meist fungibel, was bedeutet, dass eine Einheit nicht in unterscheidbarer Weise markiert werden kann. Zwar können so mittels Blacklisting einzelne Walletadressen aus dem Verkehr gezogen werden, doch ist diese Methode, aufgrund des fehlenden Transaktionsbezuges, nicht dazu geeignet, Geldflüsse aus illegalen Aktivitäten zu markieren. Das bedeutet auch, dass der anonymen Blockchain prinzipiell kein Verdachtsmoment zu entnehmen ist, da keine Beziehung zwischen zwei Walletadressen hergestellt werden kann. Ein Verdacht muss sich viel mehr aus anderen Quellen, etwa der Sicherstellung einer Paper Wallet (siehe unten), ergeben und kann daraufhin erst mittels Walletblacklisting auch innerhalb der Blockchain Niederschlag finden. Zu diesem Zeitpunkt kann der Nutzer jedoch bereits eine neue Adresse angelegt haben.

4. Ermittlungsmaßnahmen

Nachdem nun die Regulierungsmaßnahmen behandelt wurden, denen Handelsplattformen und Hot Wallet Provider künftig ausgesetzt sind, soll hier noch untersucht werden, ob diese auch von polizeilichen Ermittlungsmaßnahmen betroffen sein können.

---

[21] G20 Leaders' declaration Building consensus for fair and sustainable development. https://www.consilium.europa.eu/media/37247/buenos_aires_leaders_declaration.pdf, Punkt 25, 2018.

[22] U.S. Department of the Treasury, OFAC FAQs: Sanctions Compliance, Questions on Virtual Currency, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#vc_faqs, 2018.

4.1. Sicherstellung von Währungseinheiten bei einem Hot Wallet Provider

Eine Betroffenheit von Ermittlungsmaßnahmen kann sich insbesondere für Hot Wallet Provider bei der Sicherstellung von Währungseinheiten nach § 109 Abs. 1 StPO[23] ergeben. Gemäß § 109 Abs. 1 lit. b StPO kann die Kriminalpolizei Dritte dazu verpflichten, die Herausgabe von «Gegenständen oder anderen Vermögenswerten» zu verweigern. Aus der nicht abschließenden Aufzählung zum Begriff der «anderen Vermögenswerte» in den Materialien[24] zu § 109 StPO ist ein weites Begriffsverständnis auszuleiten, das auch virtuelle Währungseinheiten umfasst. Dieser Auslegung folgend, wäre die Sicherstellung mittels Drittverbots nach § 109 Abs. 1 lit. b StPO auch in Bezug auf virtuelle Währungen grundsätzlich zulässig. Die Voraussetzungen für die Durchführung sind deckungsgleich mit jenen nach § 109 Abs. 1 lit. a StPO mit dem Unterschied, dass die Ausnahmeregelung § 110 Abs. 1 StPO nicht greift, nach welcher die Kriminalpolizei unter bestimmten Voraussetzungen keine Anordnung der Staatsanwaltschaft für die Durchführung einer Sicherstellung braucht.

Der Kreis der Drittverbotsverpflichteten ist grundsätzlich nicht eingeschränkt.[25] Somit kann ein Drittverbot sowohl gegenüber Hot Wallet Providern, als auch gegenüber Handelsplattformen ausgesprochen werden. Die StPO normiert aber weder für Hot Wallet Provider noch für Handelsplattformen eigenständige Auskunftspflichten. Auch eine Subsumtion unter § 116 StPO (Auskunft aus dem Kontenregister und Auskunft über Bankkonten und Bankgeschäfte) wird wohl ausscheiden, denn dieser bezieht sich auf «Kredit- oder Finanzinstitute» und somit auf § 1 Abs. 1 und 2 BWG,[26] denn er sieht in Abs. 4 Z. 2 vor, dass die gerichtliche Bewilligung das verpflichtete «Kredit- oder Finanzinstitut» zu bezeichnen hat.

Cold Wallets werden grundsätzlich direkt vom Nutzer geführt, welcher innerhalb eines Strafverfahrens nicht als «Dritter» i.S.d. § 109 Abs. 1 lit. b StPO zu sehen ist. Daher kann ihm gegenüber kein Drittverbot ausgesprochen werden. Wie oben bereits erwähnt, wäre es denkbar, dass Dritte eine Kopie einer Cold Wallet innehaben. Hier wäre ein Drittverbot nach § 109 Abs. 1 lit. b StPO denkbar. In der Praxis wird es jedoch ohnehin die Ausnahme sein, dass es einen solchen Dritten gibt, und noch weniger wahrscheinlich wird sein, dass dieser den Sicherheitsbehörden bekannt ist.

Beim Drittverbot stellt sich das Problem, dass virtuelle Währungseinheiten beliebig kopiert werden können und der Sicherstellungsgegner somit eine Kopie der sicherungsgegenständlichen virtuellen Währungseinheiten haben könnte, insbesondere in Form einer Cold Wallet. In diesen Fällen hat der Hot Wallet Provider keine exklusive Verfügungsmacht über bei ihm vorliegende Währungseinheiten, und ob dies der Fall ist, kann der Hot Wallet Provider nicht beurteilen, sodass stets davon ausgegangen werden muss, dass der Hot Wallet Provider potenziell nicht die exklusive Verfügungsmacht über bei ihm vorliegende Währungseinheiten hat.

Es stellt sich daher auch im Falle der Zulässigkeit des Drittverbots die Frage, ob die Sicherheitsbehörden befugt sind, die Währungseinheiten zur Sicherstellung auf eine behördeneigene Wallet zu transferieren, da dies die einzige Möglichkeit ist, um sie der Verfügungsmacht des Sicherstellungsgegners vollständig zu entziehen. Dabei ist zu berücksichtigen, dass ein Transfer der Währungseinheiten in die faktische Verfügungsmacht des Hot Wallet Providers eingreifen würde. Es ist zwar denkbar, dass dies unter den Wortlaut «die Sicherstellung auf andere Weise ermöglichen» des § 111 Abs. 1 StPO subsumiert werden kann. Da es allerdings dafür keinerlei Durchführungsbestimmungen gibt, ist dies angesichts der Schwere eines solchen Eingriffs im Lichte von § 5 StPO und des Legalitätsprinzips gemäß Art. 18 B-VG als unzulässig zu qualifizieren. Ein Transfer sicherstellungsgegenständlicher Währungseinheiten, die sich bei einem Hot Wallet Provider befinden, auf eine behördliche Wallet, wäre daher jedenfalls nur dann zulässig, wenn dafür spezifische und eindeutige gesetzliche Bestimmungen bestünden.

---

23 Strafprozeßordnung 1975 BGBl 1975/631.

24 ErlRV 25 BlgNR 22. GP, 153; Tipold/Flora/Zerbes, in: Fuchs/Ratz, Wiener Kommentar zur StPO, 2017, § 109 Rz. 2.

25 Nach § 111 Abs. 1 StPO ist jede Person verpflichtet, eine Sicherstellung zu ermöglichen.

26 Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG) BGBl 1993/532.

4.2. Einfrieren von Transaktionen

§ 17 ff FM-GwG (in Umsetzung von Art. 32 Abs. 7 RL 2015/849) verpflichtet Kredit- und Finanzinstitute zum Einfrieren einzelner Transaktionen. Die Möglichkeit der Sperrung eines gesamten Kontos ist daraus jedoch nicht abzuleiten. Dies wird auch in der Judikatur[27] zum nicht mehr bestehenden, aber gleichlautenden § 41 Abs. 3 BWG so gesehen.[28] Hier moniert der UVS Wien, dass völlig oder weitgehend unbestimmte Transaktionen den Begriff «bevorstehen» nicht zu erfüllen vermögen. Zwar findet sich keine höchstgerichtliche Entscheidung zu dieser Problematik, die dargelegte Argumentation ist jedoch überzeugend. Mit der kommenden Ausweitung des Schutzbereiches durch die 5. Geldwäscherichtlinie wären diese Regeln auch auf Handelsplattformen und Hot Wallet Provider anwendbar. Wenn allerdings ein gesamtes Bankkonto nicht eingefroren werden kann, wird dies auch für gesamte Wallets gelten. Einzufrieren wären demnach nur einzelne Transaktionen und Währungseinheiten, nicht jedoch die Wallet als Ganzes. Daher ist anzunehmen, dass dem Nutzer auch nach der Umsetzung von RL 2018/843 der Zugang zu seinem Benutzerkonto nicht genommen werden kann. Damit steht es dem Nutzer frei eine Cold Wallet zu generieren, mit welcher er unabhängig von allfälligen Beschränkungen durch den Hot Wallet Provider weiterhin Transaktionen durchführen kann.

5. Conclusio

Die Definition «virtueller Währungen» der RL 2018/843 ist ein wichtiger Ansatz, um das Phänomen der Kryptowährungen zu regulieren. Dennoch birgt sie, wie gezeigt wurde, noch Schwächen und auch in der RL 2018/843 scheint das grundsätzliche Problem der Anti-Geldwäsche-Regulierung durch, dass Verpflichtete umsetzungsaufwendigen Regelwerken unterstellt werden, welche zu weitreichenden Eingriffen in Persönlichkeitsrechte führen, und trotzdem verhältnismäßig leicht umgangen werden können. Im Speziellen unterwandert die Anonymität von Kryptowährungen wie Zcash und Monero das System. Auch die Effektivität weiterführender Regelungsansätze, etwa mittels einer Erfassung von Krypto-zu-Krypto-Tauschbörsen oder Black-/Whitelisting, ist in Zweifel zu ziehen.

Bei Transaktionssperren ist eine Anknüpfung an Transaktionen im Zusammenhang mit Kryptowährung nicht zielführend, da Mining Pools und nicht Hot Wallet Provider die Herren der Transaktionen sind. Selbst wenn man eine Sperre des Nutzerkontos vorsehen würde, wäre es einem Nutzer, welcher präventiv eine Cold Wallet erstellt hat, trotz Sperre möglich, Transaktionen zu tätigen. Einzig der Transfer der sich in der Hot Wallet befindlichen Währungseinheiten auf eine behördliche Wallet würde zu einer effektiven Sperre führen, weshalb es sinnvoll wäre, eine diesbezügliche Ermächtigung in der StPO zu schaffen.

Insgesamt weist die Regulierung der Geldwäschebekämpfung bei Fiatwährungen und bei Kryptowährungen weitreichende Synergien auf. Dennoch sollte zukünftig auch in inhaltlichen Belangen auf die Spezialitäten beider Systeme durch maßgeschneiderte Regelungen Bedacht genommen werden. Insbesondere sollte bei der Umsetzung auf die besondere Beschaffenheit von Krypto-Dienstleistern Bedacht genommen werden, bei welchen im Grundfall kein Ausfallsrisiko besteht und sie u.A. deshalb nicht aufgrund der Umsetzungspflicht vollumfänglich dem BWG unterstellt werden sollten. Daher sollte die Umsetzung on RL 2018/843 nicht mittels einer Erweiterung des Anwendungsbereiches des BWG sondern vielmehr mithilfe eines maßgeschneiderten Tatbestandes in § 1 FM-GwG erfolgen.

---

27 UVS Wien GZ: 02/13/127/97 vom 6. August 1998. Die UVS (Unabhängige Verwaltungssenate) waren eine verwaltungsrechtliche Rechtsmittelinstanz. Mit 1. Januar 2014 wurden sie durch die Verwaltungsgerichte ersetzt.

28 Siehe § 41 Abs. 3 BWG in der Fassung zum Entscheidungszeitpunkt am 6. August 1998; im Vergleich dazu §17 Abs. 4 FM-GwG gleicher Wortlaut: «anzuordnen, dass eine laufende oder bevorstehende Transaktion […] unterbleibt oder vorläufig aufgeschoben wird und dass Aufträge des Kunden über Geldausgänge nur mit Zustimmung der Behörde durchgeführt werden dürfen».