Strafanwendungsrecht und MiCAR – normentheoretische Überlegungen zur Marktmanipulation auf Krypto-Börsen

Konstantina Papathanasiou

Abstract

Mit der fortschreitenden Digitalisierung entstehen ständig Herausforderungen, welche die traditionellen rechtlichen Rahmen überfordern. Im Bereich der Cyberkriminalität dominieren abstrakte und potentielle Gefährdungsdelikte, die nur über den Handlungsort die Strafbefugnis begründen. Das Strafanwendungsrecht erweist sich als ein verlässlicher Anker, indem es festlegt, wann nationale Strafvorschriften gelten. Die Anwendbarkeit des nationalen Strafrechts ist als unrechtskonstituierendes Merkmal zu betrachten. Die Marktmanipulation auf Krypto-Börsen zeigt die Problematik deutlich auf: Die Verordnung über Märkte für Kryptowährungen (MiCAR), die teilweise ab dem 30.06.2024 gilt, erstreckt sich faktisch weltweit und könnte zu einer unzulässigen Universalgeltung der Strafgesetze führen.

I. Einleitung

Mit der fortschreitenden Digitalisierung entstehen ständig neue Herausforderungen, wie etwa der Schutz personenbezogener Daten. Für den Bereich des Strafrechts ist Cyberkriminalität eine der größten Herausforderungen, da die digitalen Entwicklungen komplexe Fragen aufwerfen, welche die traditionellen rechtlichen Rahmen oft überfordern. Genau hier kommt die Bedeutung des Strafanwendungsrechts ins Spiel: Durch die Klärung der Frage, wann und inwiefern nationale Strafvorschriften für Sachverhalte im digitalen Raum anwendbar sind, kann das Strafrecht gezielt zur Bekämpfung von neuen digitalen Bedrohungen beitragen, sofern dies nötig ist.

Mit anderen Worten: Das Strafanwendungsrecht kann sich als ein verlässlicher Anker inmitten der raschen Entwicklungen des digitalen Zeitalters erweisen. Denn unabhängig davon, welche technisch neuartigen Verhaltensweisen (noch) erscheinen, verfügt das Strafrecht über eigene

Prinzipien, anhand derer beurteilt werden kann, wann nationale Strafvorschriften Anwendung finden. Hinsichtlich der Reichweite einzelner Prinzipien besteht allerdings keine einheitliche Meinung, was zur Folge hat, dass das Anwendungsspektrum je nach Perspektive enger oder weiter ausfallen kann. Die Bedeutung der einschlägigen Diskussion wird im Bereich der grenzüberschreitenden Cyberkriminalität evident, wo die Kategorien von abstrakten und potentiellen Gefährdungsdelikten einen großen Teil der Materie ausmachen und wo es begriffsnotwendig keinen Erfolgsort gibt (sogleich unter II.).

Außerdem soll in diesem Beitrag die grundlegende, bis vor einigen Jahren als geklärt geltende, dogmatische Frage, an welcher Stelle das Strafanwendungsrecht im Deliktsaufbau zu prüfen ist, neu beantwortet werden. Wie ich bereits vertreten habe, erscheint in Anlehnung an *Ulfrid Neumann*[1] die Auffassung vorzugswürdig, die Anwendbarkeit des nationalen Strafrechts (in Deutschland: §§ 3 ff. StGB) als Tatbestandsmerkmal zu betrachten.[2] Denn nur bei Betrachtung der Regelungen der Reichweite der Strafbefugnis als unrechtskonstituierendes Merkmal kann eine unzulässige Universalgeltung der Strafgesetze vermieden werden, zumal *das Unrecht stets rechtsordnungsbezogen*, also relativ zu einer bestimmten Rechtsordnung ist.[3] Der Geltungsbereich von Verhaltensnormen und der Geltungsbereich von Sanktionsnormen sind somit identisch; insofern weisen die §§ 3 ff. StGB eine festlegende Funktion auf und sind konstitutiver Bestandteil der primären Strafrechtsnormen.[4] Die Universalgeltung von Strafgesetzen, wenn diese nicht Verletzungen von völkerrechtlich anerkannten Rechtsgütern sanktionieren, ist unzulässig, weil sie mit dem als Völkergewohnheitsrecht allgemein anerkannten und spätestens in Art. 2 Abs. 7 S. 1 UN-Charta verankerten Einmischungsverbot nicht zu vereinbaren ist.

1 *Neumann*, Normentheoretische Aspekte der Irrtumsproblematik im internationalen Bereich des „Internationalen Strafrechts", in: Britz (Hrsg.), Grundfragen staatlichen Strafens: Festschrift für Heinz Müller-Dietz zum 70. Geburtstag, 2001, S. 589 (601).

2 *Papathanasiou*, Das Bindingsche Model der „Kompetenz-Kompetenz" – Die Normentheorie an der Kreuzung vom sog. internationalen Strafrecht und Völkerrecht, in: Schneider/Wagner (Hrsg.), Normentheorie und Strafrecht, 2018, S. 245 ff. m.w.N.

3 *Neumann* (Fn. 1), S. 603 ff. Diese These hat eine überaus positive Resonanz gefunden. Zustimmend u.a. *Jeßberger*, Der transnationale Geltungsbereich des deutschen Strafrechts, 2011, S. 151.

4 So auch bereits *Böse*, Die Stellung des sog. Internationalen Strafrechts im Deliktsaufbau und ihre Konsequenzen für den Tatbestandsirrtum, in: Bloy et al. (Hrsg.), Gerechte Strafe und legitimes Strafrecht: Festschrift für Manfred Maiwald zum 75. Geburtstag, 2010, S. 61 (63 f.); *ders.* in: NomosKommentar StGB, 6. Aufl. 2023, Vor §§ 3–7 Rn. 54.

Zur Universalgeltung führt aber die bis vor einigen Jahren vorherrschende Betrachtung[5] der Regelungen der Reichweite der Strafbefugnis als unrechtsneutrale objektive Bedingung der Strafbarkeit. Anschaulich lässt sich besagte Grundsatzfrage am hochaktuellen Beispiel des Marktmissbrauchs im Zusammenhang mit Kryptowerten darstellen (unter III.).

II. Die Problematik in Bezug auf Cyberkriminalität

Die Cyberkriminalität, auch Internetkriminalität oder Computerkriminalität genannt, bezieht sich auf (a) die Nutzung von Informations- und Kommunikationsnetzen ohne geographische Begrenzung und (b) die Übertragung von nicht erfassbaren und kurzlebigen Daten.[6] Das Spektrum der Cyberkriminalität erfasst sämtliche Verhaltensweisen, welche informationstechnische Systeme entweder als Tatobjekt angreifen oder als Tatmittel einsetzen.[7]

Auf der Suche nach dem Tatort eines Cybercrimes führt die Analyse des Territorialitätsprinzips insbesondere über die sog. potentiellen Gefährdungsdelikte, auch Eignungs- oder abstrakt-konkrete Gefährdungsdelikte genannt. Bei ihnen ist nicht die Rede von dem Eintritt einer konkreten Gefahr, sondern nur von einer generellen Gefährlichkeit von Handlung oder Tatmittel.[8] Es wäre eine eindeutige Interpretation *contra legem*, diese generelle Gefährlichkeit (oder, je nach Begriff, Geeignetheit) mit dem Tatbestandsmerkmal des Eintrittes einer konkreten Gefahr gleichzusetzen. Zwischen den Begrifflichkeiten „generell" und „konkret" gibt es erhebliche

5 Vertreten von *Ambos* in: Münchener Kommentar, StGB , Band 1, 4. Aufl. 2020, Vor § 3 Rn. 3; *Baumann* et al., Strafrecht Allgemeiner Teil, 12. Aufl. 2016, § 5 Rn. 24; *Eser/Weißer* in: Schönke/Schröder, StGB, 30. Aufl. 2019, Vor § 3 Rn. 6; *Heger* in: Lackner/Kühl/Heger, StGB, 30. Aufl. 2023, Vor § 3 Rn. 10 jeweils m.w.N.; *Jescheck/Weigend*, Strafrecht Allgemeiner Teil, 5. Aufl. 1996, S. 180; *Henrich*, Das passive Personalitätsprinzip im deutschen Strafrecht, 1994, S. 156 ff.; *Schneider*, Die Verhaltensnorm im Internationalen Strafrecht, 2011, S. 274; *Walter*, JuS 2006, 870 (871).

6 BuA 4/2009, I.1. [Bericht und Antrag der Regierung an den Landtag des Fürstentums Liechtenstein betreffend die Abänderung des Strafgesetzbuches (Cyber Crime) vom 10.3.2009].

7 Vgl. *Brodowski/Freiling*, Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft, 2011, S. 30; *Grözinger,* Cybercrime und Datenkriminalität, in: Müller/Schlothauer/Knauer (Hrsg.), Münchener Anwaltshandbuch Strafverteidigung, 3. Aufl. 2022, § 50 Rn. 8.

8 *Hilgendorf*, NJW 1997, 1873 (1875); *Wessels/Beulke/Satzger*, Strafrecht Allgemeiner Teil, 52. Aufl. 2022, Rn. 45.

Unterschiede, die eine insofern sachlich begründete unterschiedliche Behandlung rechtfertigen. Eine Gefahr, die keine konkrete ist und mithin kein genuines Tatbestandsmerkmal sein kann, sollte keinen Gerichtsstand begründen.

Paradigmatisch zum Ausdruck gebracht wird dies in dem bekannten Fall der Verbreitung der sog. Auschwitzlüge im Internet.[9] Der Erste Strafsenat des BGH hat mit seinem Urteil vom 12.12.2000 zum einen die hier in Rede stehende Deliktskategorie angesprochen: „Mit der Eignungsformel wird die Volksverhetzung nach § 130 Abs. 1 und Abs. 3 StGB zu einem abstrakt-konkreten Gefährdungsdelikt (…); teilweise wird diese Deliktsform auch als 'potentielles Gefährdungsdelikt' bezeichnet (…). Dabei ist die Deliktsbezeichnung von untergeordneter Bedeutung; solche Gefährdungsdelikte sind jedenfalls eine Untergruppe der abstrakten Gefährdungsdelikte".[10] Zum anderen hat er in international-strafrechtlicher Hinsicht u.a. Folgendes angenommen: „Stellt ein Ausländer von ihm verfasste Äußerungen, die den Tatbestand der Volksverhetzung i.S.d. § 130 Abs. 1 oder des § 130 Abs. 3 StGB erfüllen (‚Auschwitzlüge'), auf einem ausländischen Server in das Internet, der Internetnutzern in Deutschland zugänglich ist, so tritt ein zum Tatbestand gehörender Erfolg (§ 9 Abs. 1 3. Alt. StGB) im Inland ein, wenn diese Äußerungen konkret zur Friedensstörung im Inland geeignet sind".[11]

Das Merkmal der *Eignung* einer Äußerung zur Störung des öffentlichen Friedens basiert auf dem Rechtsguts- bzw. Schutzprinzip. Dieses Prinzip ist vor allem für § 5 StGB relevant, der Regelungen für ausschließlich im *Ausland* begangene Taten betrifft. Das Rechtsgutsprinzip spielt eine wichtige Rolle bei der Frage der Nichteinmischung in die Souveränität eines *anderen* Staates. Im Gegensatz dazu bezieht sich § 9 StGB auf die Territorialität im Sinne des § 3 StGB und betrifft daher *Inland*staten. Diese Inlandstaten fallen logischerweise nicht in den Anwendungsbereich der §§ 5–7 StGB, welche Straftaten im Ausland bzw. Straftaten mit Auslandsbezug erfassen. Das bedeutet, dass § 9 StGB zur Schaffung einer rechtlichen Grundlage für die Verfolgung von Straftaten dient, die innerhalb des Staatsgebiets begangen werden, und nicht auf die Anwendung des Rechtsgutsprinzips angewiesen ist, das bei Auslandstaten relevant ist.[12]

9 BGHSt 46, 212; krit. Bspr. u.a. *Koch*, JuS 2002, 123; *Lagodny*, JZ 2001, 1198; *Hilgendorf*, NJW 1997, 1873.
10 BGHSt 46, 212 (218).
11 BGHSt 46, 212 (220); zust. *Walter*, JuS 2006, 870 (873).
12 Vgl. *Lagodny*, JZ 2001, 1198 (1200).

Zu begrüßen ist deshalb, dass andere Strafsenate des BGH in jüngerer Rechtsprechung starke Bedenken geäußert und die gegenteilige Auffassung vertreten haben. So hat der Dritte Strafsenat – bezogen auf denselben Tatbestand – in seinem Beschluss vom 3.5.2016 ausgeführt, dass das Merkmal der Eignung zur Störung des öffentlichen Friedens im Sinne des § 130 Abs. 3 StGB, das zur Einstufung der Vorschrift als potentielles Gefährdungsdelikt führe, keinen zum Tatbestand gehörenden Erfolg umschreibe, so dass eine Inlandstat nicht begründet werden könne.[13] Diese Rechtsprechungsänderung veranlasste sogar den Gesetzgeber zu handeln: In § 5 StGB, der sich ausschließlich auf im *Ausland* begangene Taten bezieht, wurde mit Wirkung vom 1.1.2021 durch Gesetz vom 30.11.2020 eine neue Nr. 5a lit. c) eingefügt.[14]

Ähnlich hat der Dritte Strafsenat am 19.8.2014 in Bezug auf das abstrakte Gefährdungsdelikt des § 86a StGB entschieden, dass dieses Delikt keinen zum Tatbestand gehörenden Erfolg umschreibe. Selbst wenn die Frage nach dem Erfolgsort normspezifisch am Schutzzweck der jeweiligen Strafvorschrift ausgerichtet werden müsste, wäre an dem Ort, an dem die hervorgerufene abstrakte Gefahr in eine konkrete umgeschlagen sei oder gar nur umschlagen könne, kein zum Tatbestand gehörender Erfolg eingetreten.[15] In diese Richtung geht auch eine jüngere, in Bezug auf Internetdelikte ergangene Entscheidung des österreichischen Obersten Gerichtshofs. Dort wird ausgeführt: „Mit dem Empfang und dem Lesen der E-Mails in Österreich verbundene Wirkungen sind für das (…) bereits in Spanien vollendete Delikt nicht von Bedeutung. Ein inländischer Tatort liegt somit nicht vor."[16]

Diese Rechtsprechung verdeutlicht die Notwendigkeit einer präzisen und differenzierten Betrachtung bei der Bestimmung des Tatortes, insbesondere im Kontext von Delikten im digitalen Raum. Spätestens nach der oben genannten gesetzgeberischen Aktivität soll als klargestellt gelten, dass selbst potentielle Gefahren die inländische Gerichtsbarkeit nicht begründen können. Die gegenteilige Auffassung würde dazu führen, über das Vehikel der abstrakten Gefährdungsdelikte eine universelle Geltung der einschlägigen Strafgesetze anzunehmen, was angesichts der eingangs[17]

13 BGH NStZ 2017, 146 (147). Vgl. jüngst *Klaas* in: Klaas/Momsen/Wybitul DatenschutzsanktionenR-HdB, 1. Aufl. 2023, § 25 Rn. 97.
14 Vgl. *Böse* in: NomosKommentar StGB, 6. Aufl. 2023, § 5 Rn. 27.
15 BGH NStZ 2015, 81 (82). Vgl. *Kudlich/Berberich*, NStZ 2019, 633.
16 OGH JSt 2019, 154 (157).
17 Siehe oben zu Fn. 1–3.

erwähnten Relativität des Unrechts und auch bereits völkerrechtlich unzulässig wäre.

Potentielle (und umso weniger: abstrakte) Gefährdungsdelikte können deshalb keinen Erfolgsort begründen. Es ist vielmehr erforderlich, dass stets konkrete Realisierungen der einschlägigen Gefahren verlangt werden,[18] um überhaupt von einem Erfolgsort im Sinne des § 9 Abs. 1 StGB sprechen zu können. Somit muss die Ausdehnung der Strafbefugnis mit einem anderen Prinzip hinsichtlich der Tathandlung begründet werden, wie etwa der Staatsangehörigkeit oder dem Wohnsitz des Täters.[19] Die Herausforderung der Internetkriminalität rechtfertigt nicht *eo ipso* unzulässige Gesetzesanwendungen; die Lösung ist vielmehr in der internationalen Zusammenarbeit zu suchen.[20] Der innerstaatliche Bereich der Verletzungs- und Gefährdungsdelikte hat sein völkerrechtliches Pendant im sog. (Aus-)Wirkungsprinzip. Dieses gilt nach vorherrschender Meinung allerdings ebenfalls nicht uneingeschränkt, vielmehr bedarf es eines gesteigerten Inlandsbezuges.[21]

III. EU-Regulierung von Krypto-Börsen und nationale Strafbestimmungen

Nun soll auf die einleitend aufgeworfene, grundlegende dogmatische Frage zurückgekommen werden: An welcher Stelle ist das Strafanwendungsrecht im Deliktsaufbau zu prüfen? Die vorzugswürdige Antwort, die eine universelle Geltung der Strafgesetze dogmatisch stringent verhindert, lautet: Die Anwendbarkeit des nationalen Strafrechts ist als Tatbestandsmerkmal anzusehen. Die Bedeutung dieser dogmatischen Frage lässt sich am Beispiel manipulativer Verhaltensweisen auf Krypto-Börsen unter dem Gesichtspunkt des Marktmissbrauchs verdeutlichen. Dieses Beispiel wird zeigen, wie weit sich der Geltungsanspruch von Normen im Kontext der Krypto-Entwicklungen faktisch erstreckt und was das für das nationale Strafrecht bedeutet. Die nachfolgenden Ausführungen bieten zugleich einen prägnanten Überblick über die MiCAR.

---

18 Vgl. hierzu *Morozinis*, GA 2011, 475 (481).

19 Vgl. *Werle/Jeßberger* in: Leipziger Kommentar, StGB, 12. Aufl. 2007, § 9 Rn. 102; *Eisele*, Computer- und Medienstrafrecht, 2013, § 3 Rn. 16. Weniger verlangt insofern *Hilgendorf*, NJW 1997, 1873 (1876).

20 So bereits *Koch*, JuS 2002, 123 (127).

21 Siehe hierzu *von Arnauld*, Völkerrecht, 3. Aufl. 2016, § 4 Rn. 347, allerdings ohne weitere Quellenangaben.

Verhaltensweisen auf Krypto-Börsen waren bis vor Kurzem vollständig unreguliert. Seit anderthalb Jahren existiert die Verordnung über Märkte für Kryptowährungen in der regulatorischen Landschaft,[22] die eine risikogerechte Regulierung gewährleistet und darauf abzielt, den Schutz der Anleger:innen zu stärken und die Funktionsfähigkeit der Märkte zu verbessern.[23]

Krypto-Börsen sind Online-Plattformen in der Gestalt von Märkten für Kryptowerte, mithin Börsen der digitalen Welt. Krypto-Börsen fungieren vor allem als Vermittlungsplattformen, die Käufer:innen und Verkäufer:innen von Kryptowerten zusammenführen, wodurch Nutzer:innen die Möglichkeit erhalten, verschiedene Kryptowährungen wie Bitcoin, Ethereum und Ripple sowohl untereinander als auch gegen traditionelle Fiat-Währungen wie den US-Dollar oder den Euro zu handeln. Krypto-Börsen bieten darüber hinaus eine breite Palette an Funktionen im Zusammenhang mit Blockchain und Kryptowährungen an; zu diesen Funktionen gehören vor allem Anwendungen aus dem dezentralen Finanzsektor (sog. DeFi-Anwendungen)[24] oder der Handel mit digitalisierter Kunst (sog. nicht fungible Tokens; NFTs).[25]

---

22 Verordnung 2023/1114/EU des Europäischen Parlaments und des Rates v. 31.5.2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937, ABl. EU L 150/40. Nach Art. 149 Abs. 2 MiCAR gilt die Krypto-Regulierung seit dem 30.12.2024. Obwohl die neuen Vorschriften ursprünglich innerhalb von 20 Tagen nach ihrer Veröffentlichung im Amtsblatt in Kraft treten sollten (Art. 149 Abs. 1 MiCAR), erfolgte ihre tatsächliche Umsetzung erst am 30.12.2024. Einige Teile der Verordnung sind jedoch nach Art. 149 Abs. 3 MiCAR bereits seit dem 30.6.2024 wirksam. Zum Zeitpunkt der Erstellung dieses Manuskriptes (Vortrag im September 2022) lag nur noch der Entwurf der Verordnung vor. Daher musste der Text für die Publikation (Druckfahnen im Januar 2025) mehrfach aktualisiert werden.

23 Vgl. BaFin-Mitteilung vom 17.5.2023, https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2023/fa_bj_2305_Mica.html (zuletzt abgerufen am 21.1.2025).

24 Zum Begriff vgl. nur Mitteilungen auf der Internetseite der BaFin: „Die vielfältigen Anwendungsfälle von DeFi-Anwendungen, wie dezentrale Handelsplattformen („DEXes"), dezentrale Formen der Kreditvergabe, dezentral erzeugte Stablecoins, dezentral emittierte und gehandelte Derivate sowie erste Formen dezentraler Versicherungen und Vermögensverwaltung, ähneln denen des konventionellen Finanzsystems", https://www.bafin.de/DE/Aufsicht/FinTech/Geschaeftsmodelle/DLT_Blockchain_Krypto/DAOS/DAOS_artikel.html%20 (zuletzt abgerufen am 21.1.2025).

25 Hierzu siehe das Online-Glossar der BaFin: „Ein Non-Fungible Token (NFT) ist ein Kryptotoken, der nicht fungibel ist. Nicht fungibel bedeutet, dass diese Kryptotoken nicht untereinander ersetzt werden können. So kann etwa ein Bitcoin durch einen

Als *Kryptowerte* (auch Krypto-Assets oder Krypto-Token genannt) werden Vermögenswerte bezeichnet, die vor allem durch Blockchains abgebildet werden. Eine Blockchain ist das Beispiel par excellence einer dezentralen Ledger-Technology (DLT): Bei einer DLT handelt es sich im Allgemeinen um eine digitale, dezentrale Datenbank, die von allen Teilnehmer:innen abgespeichert und regelmäßig auf dem neuesten Stand gehalten wird; letztendlich handelt es sich um ein verteiltes Kassenbuch, in das jede:r Beteiligte neue Daten eintragen kann, während einmal eingetragene Datensätze nicht rückwirkend geändert werden können.[26]

Die Krypto-Verordnung enthält in Art. 3 Abs. 1 insgesamt 51 Begriffsbestimmungen; dies ist ein *Symptom für die Komplexität* der behandelten Materie. Der Begriff „Kryptowert" wird in Art. 3 Abs. 1 Nr. 5 MiCAR wie folgt definiert: Es handelt sich um eine digitale Darstellung eines Wertes oder eines Rechtes, der bzw. das unter Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden kann. Mit „Distributed Ledger" ist in Nr. 2 ein Informationsspeicher gemeint, der Aufzeichnungen über Transaktionen enthält und der unter Verwendung eines Konsensmechanismus auf eine Reihe von DLT-Netzwerkknoten verteilt und zwischen ihnen synchronisiert wird. Der „Konsensmechanismus" nach Nr. 3 umfasst die Regeln und Verfahren, die eine Übereinstimmung zwischen den DLT-Netzwerkknoten herbeiführen, um die Validierung einer Transaktion zu gewährleisten. Bei den „DLT-Netzwerkknoten" geht es wiederum nach Nr. 4 um ein Gerät oder Verfahren, das Teil eines Netzwerks ist und das eine vollständige oder partielle Kopie von Aufzeichnungen aller Transaktionen in einem Distributed Ledger enthält.

Der Adressat:innenkreis der Krypto-Regulierung der EU ist weit gefasst: Adressat:innen sind nach Art. 2 Abs. 1 MiCAR natürliche und juristische Personen sowie bestimmte andere Unternehmen, die in der EU

anderen ersetzt werden, ist also fungibel. Ein original Picasso-Werk kann aber nicht durch ein anderes original Picasso-Werk ersetzt werden, ist also nicht fungibel", https://www.bafin.de/DE/Aufsicht/FinTech/InnovativeFinanztechnologien/DLT_Blockchain/Glossar/glossar_node.html (zuletzt abgerufen am 21.1.2025).

26 Vgl. *Hosp*, Blockchain 2.0, 2018, S. 36; siehe auch unter https://wirtschaftslexikon.gabler.de/definition/distributed-ledger-technologie-dlt-54410 (zuletzt abgerufen am 1.9.2014). Zu Blockchain und Strafrecht siehe näher *Papathanasiou*, ZWF 2022, 178.

- mit der *Ausgabe*, dem *öffentlichen Angebot* und der *Zulassung zum Handel* von Kryptowerten befasst sind oder
- die *Dienstleistungen* im Zusammenhang mit Kryptowerten erbringen.

Als „Anbieter:innen" gilt eine natürliche oder juristische Person oder ein anderes Unternehmen, die bzw. das Kryptowerte öffentlich anbietet, oder der:die Emittent:in, der:die Kryptowerte öffentlich anbietet (Art. 3 Abs. 1 Nr. 13 MiCAR). Als „Anbieter:in von Kryptowerte-Dienstleistungen" wird nach Art. 3 Abs. 1 Nr. 15 MiCAR jede juristische Person oder jedes andere Unternehmen angesehen, deren bzw. dessen berufliche oder gewerbliche Tätigkeit darin besteht, eine oder mehrere Kryptowerte-Dienstleistungen gewerblich für Kund:innen zu erbringen. Nach Art. 3 Abs. 1 Nr. 16 MiCAR fallen unter den Begriff „Krypto-Dienstleistung" folgende Dienstleistungen und Tätigkeiten im Zusammenhang mit Kryptowerten: a) Verwahrung und Verwaltung von Kryptowerten für Kunden; b) Betrieb einer Handelsplattform für Kryptowerte; c) Tausch von Kryptowerten gegen einen Geldbetrag; d) Tausch von Kryptowerten gegen andere Kryptowerte; e) Ausführung von Aufträgen über Kryptowerte für Kund:innen; f) Platzierung von Kryptowerten; g) Annahme und Übermittlung von Aufträgen über Kryptowerte für Kund:innen; h) Beratung zu Kryptowerten; i) Portfolioverwaltung von Kryptowerten; j) Erbringung von Transferdienstleistungen für Kryptowerte für Kund:innen.

Obwohl die Emission, das Angebot und die Zulassung von Kryptowerten sowie die Erbringung von Kryptowerte-Dienstleistungen in der EU stattfinden sollen, führt ihre tatsächliche Durchführung faktisch dazu, dass alle Kryptowerte weltweit vom Anwendungsbereich der MiCAR erfasst werden können. Der Geltungsbereich der MiCAR erstreckt sich praktisch weltweit: Da die Kryptowelt nicht auf nationale Märkte beschränkt ist, werden Services und herausgegebene Token in der Regel international beworben, oft in englischer Sprache. Internationale Verkäufe erfolgen üblicherweise mittels Currency Tokens oder Kreditkarten. Aufgrund dieser Umstände erfolgen Kryptowertemissionen und -services häufig auch innerhalb der EU, wodurch ein Bezug zur EU hergestellt wird und sie der Regulierung durch MiCAR unterliegen.[27]

Die Regelungen zur Verhinderung und Untersagung von Marktmissbrauch im Kontext von Kryptowerten sind in Titel VI (Art. 86–92) der MiCAR verankert. Dabei behandelt Art. 89 MiCAR das Verbot von Insider-

27 Vgl. *Maume*, RDi 2022, 461 (463).

geschäften, während Art. 90 sich mit der unrechtmäßigen Offenlegung von Insiderinformationen befasst und Art. 91 MiCAR das Verbot der Marktmanipulation normiert. Diese Verhaltensweisen sind geeignet, die Integrität des Marktes zu gefährden und das Vertrauen der Nutzer:innen in die Märkte zu untergraben.[28] Den *Geltungsbereich der Marktmissbrauchsregelungen* legt Art. 86 MiCAR fest, der in strafanwendungsrechtlicher Hinsicht von erheblicher Bedeutung ist: „(1) Dieser Titel gilt für von jedweden Personen vorgenommene Handlungen im Zusammenhang mit Kryptowerten, die zum Handel zugelassen sind oder deren Zulassung zum Handel beantragt wurde. (2) Dieser Titel gilt auch für alle Geschäfte, Aufträge und Handlungen, die in Absatz 1 genannte Kryptowerte betreffen, unabhängig davon, ob ein solches Geschäft, ein solcher Auftrag oder eine solche Handlung auf einer Handelsplattform getätigt wurde. (3) Dieser Titel gilt für Handlungen und Unterlassungen in der Union und in Drittländern im Zusammenhang mit den in Absatz 1 genannten Kryptowerten."

Das Zusammenlesen des Art. 86 MiCAR mit den drei *kryptowertebezogenen Verbotsnormen* (d.h. Verbot von Insidergeschäften, Verbot der unrechtmäßigen Offenlegung von Insiderinformationen und Verbot der Marktmanipulation) ergibt deren *extraterritoriale Geltung*. Was bedeutet dies konkret für das Straf(anwendungs)recht? Die Materie ist komplex und bedarf bedachtsamer Annäherung. Um die extraterritoriale Geltung der drei kryptobezogenen Verbotsnormen und ihre Bedeutung für das Strafrecht anschaulich zu erklären, soll als Beispiel für eine Krypto-Marktmanipulation das *Wash-Trading* dienen, eine klassische Form von Manipulation in den geregelten Märkten.

Diese Praxis ist in Deutschland nach § 119 WpHG strafbar. Bei diesem Straftatbestand handelt es sich um ein Blankettstrafgesetz; die tatbestandlichen Voraussetzungen ergeben sich erst durch das Zusammenlesen von § 119 Abs. 1 WpHG und Art. 15, 12 MAR[29].[30] Wash-Trading wird unter den Indikatoren für manipulatives Handeln im Sinne des Art. 12 Abs. 3 mit Anhang I Abschnitt A. MAR genannt. Nach der Erläuterung in Nr. 3 geht es beim Wash-Trading um „Vorkehrungen für den Kauf oder Verkauf eines

28 Vgl. Erwägungsgrund 95 der MiCAR.

29 MAR steht für „Market Abuse Regulation" und dabei handelt es sich um die Verordnung 596/2014/EU des Europäischen Parlaments und des Rates v. 16.4.2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission, ABl. EU L 2014/173.

30 Hierzu vgl. *Merwald*, JURA 2022, 188.

Finanzinstruments, eines verbundenen Waren-Spot-Kontrakts oder eines auf Emissionszertifikaten beruhenden Auktionsobjekts, bei dem es nicht zu einer Änderung des wirtschaftlichen Eigentums oder des Marktrisikos kommt oder bei dem eine Übertragung des wirtschaftlichen Eigentums oder des Marktrisikos zwischen den gemeinschaftlich oder in Absprache handelnden Parteien stattfindet. Diese Praxis lässt sich auch anhand der folgenden zusätzlichen Indikatoren für Marktmanipulation veranschaulichen: i) ungewöhnliche Wiederholung einer Transaktion zwischen einer kleinen Anzahl von Parteien über einen gewissen Zeitraum; ii) Transaktionen oder Handelsaufträge, durch die sich die Bewertung einer Position verändert bzw. wahrscheinlich verändert, obwohl der Umfang der Position weder kleiner noch größer wird. (…)".

Wash-Trading ist zwar eine klassische Form von Manipulation in den *geregelten Märkten*, findet aber gleichermaßen in *Märkten der digitalen Welt* statt, mithin bezogen auf Kryptowerte. Bei diesem Krypto-Wash-Trading kaufen und verkaufen Börsen gleichzeitig Krypto-Token, um das eigene Handelsvolumen in die Höhe zu treiben und so neue Kund:innen anzuziehen. Ein im Dezember 2022 publizierter Bericht des US-amerikanischen National Bureau of Economic Research zeigt, dass der überwiegende Teil (über 70%) des gemeldeten Volumens auf unregulierten Krypto-Börsen auf gefälschtes Wash-Trading zurückzuführen ist.[31] Auch das Forbes-Magazin weist in einem Artikel von Juli 2022 darauf hin, dass sich Krypto als nichts anderes als ein groß angelegtes *Pump-and-Dump-Schema* entpuppt,[32] eine betrügerische Praxis, die häufig in den Finanzmärkten vorkommt, insbesondere bei wenig regulierten Märkten wie Kryptowährungen.[33]

---

31 Vgl. unter https://www.thetradenews.com/illegal-wash-trading-accounts-for-up-to-70-of-crypto-volumes-finds-study/ (zuletzt abgerufen am 21.1.2025).

32 *Adkisson*, Crypto Turns Out To Be Nothing But A Massive Pump And Dump Scheme Fueled By Widespread Manipulation, Forbes v. 31.7.2022, https://www.forbes.com/sites/jayadkisson/2022/07/31/crypto-turns-out-to-be-nothing-but-a-massive-pump-and-dump-scheme-fueled-by-widespread-manipulation/?sh=6a11e39f4aad (zuletzt abgerufen am 21.1.2025).

33 Ausf. hierzu *Kamps/Kleinberg*, Crime Sci 7, 18 (2018). Siehe auch *Trozze et al.*, Crime Sci 11, 1 (2022). Das *Pump-and-Dump*-Schema besteht aus zwei Hauptphasen: 1. Pump (Aufpumpen)**:** Die Täter:innen kaufen eine beträchtliche Menge einer bestimmten Aktie oder Kryptowährung, um den Preis künstlich in die Höhe zu treiben (Manipulation des Preises). Sie verbreiten irreführende oder falsche Informationen über das betreffende Wertpapier, um andere Anleger:innen dazu zu bringen, ebenfalls zu kaufen. Dies kann über soziale Medien, Foren, Newsletters oder andere Kommunikationskanäle geschehen (Verbreitung von Fehlinformationen). Durch diese Takti-

Solche manipulativen Spielchen in Krypto-Börsen bleiben allerdings straflos, weil Krypto-Börsen z.B. in der EU bis vor Kurzem nicht geregelt waren. Es wäre eine Überlegung, auf der Suche nach einer Strafbarkeit an den Wertpapierhandel zu denken: Eine Strafbarkeit nach § 119 WpHG hätte jedoch ebenso wenig in Betracht kommen können, weil die beeinflussenden Informationen des jeweiligen Kryptowährungskurses nicht vom Regelungsgehalt umfasst sind. Bitcoin selbst ist etwa kein Finanzinstrument, das zum Handel auf einem geregelten Markt zugelassen worden ist.[34] Eine Krypto-Börse ähnelt außerdem, wie der faktische Geltungsbereich der MiCAR nachweist, einem globalen Markt weitaus mehr als einem klassischen Wertpapierhandel.

Das Krypto-Wash-Trading ist sozialethisch unbestreitbar zu beanstanden. Aus normentheoretischer Sicht stellt sich die Situation aber folgendermaßen dar: In Bezug auf das „traditionelle" Wash-Trading existiert eine durchaus internalisierte, sanktionsbewehrte Verhaltensnorm, die sich im Kontext herkömmlicher Finanzmärkte in einer Sanktionsnorm widerspiegelt. Dies gilt jedoch nicht für Krypto-Börsen.

Am Beispiel des Krypto-Marktmissbrauchs wird somit deutlich, dass sich die Verhaltensnorm eben nicht aus dem Erfolg, und damit auch nicht im Umkehrschluss aus der Strafbestimmung, herleiten lässt. Vielmehr sind für die Verhaltensnorm die finanzmarktrechtlichen Regelungen entscheidend. Nunmehr könnte in der Tat eine Strafbarkeit nach § 119 Abs. 1 WpHG i.V.m. jener Regelung in Betracht kommen, die Art. 91 MiCAR konkret umschreibt.[35] Mit anderen Worten: Die Verhaltensweise „Marktmissbrauch" bzw. „Verbreiten unrichtiger Informationen zum Einwirken auf den Kurs" erstarkt in Bezug auf Krypto-Börsen erst zu einer Verhaltensnorm, sobald dieser Bereich reguliert ist. Dies geschah durch die MiCAR, die am

ken erzeugen sie ein künstliches Interesse und eine erhöhte Nachfrage, was den Preis weiter steigen lässt (Steigerung des Interesses). 2. Dump (Abstoßen): Sobald der Preis ausreichend gestiegen ist und eine große Anzahl von Anleger:innen investiert hat, verkaufen die Täter:innen ihre Anteile zu diesen künstlich hohen Preisen (Verkauf zu hohen Preisen). Nachdem die Täter:innen ihre Positionen verkauft haben, fällt der Preis stark, da die Nachfrage nicht mehr durch den künstlichen Hype unterstützt wird (Kursverfall). Diejenigen, die spät eingestiegen sind und die manipulierten Wertpapiere zu hohen Preisen gekauft haben, erleiden erhebliche Verluste, wenn der Preis fällt (Verluste für andere Anleger:innen).

34 Vgl. *Börner*, NZWiSt 2018, 48 (50).

35 Ähnlich wie bisher nach § 119 Abs. 1 WpHG i.V.m. Art. 15, 12 MAR (hierzu oben Fn. 29).

29.6.2023 in Kraft getreten ist und teilweise bereits seit dem 30.6.2024, im Übrigen seit dem 30.12.2024, gilt.

Der Umfang des Manipulationsverbots in Art. 91 MiCAR entspricht weitgehend der MAR für die herkömmlichen Märkte. Dort hieß es insbesondere im Erwägungsgrund 7 MAR: „Marktmissbrauch ist ein Oberbegriff für unrechtmäßige Handlungen an den Finanzmärkten und sollte für die Zwecke dieser Verordnung Insidergeschäfte oder die unrechtmäßige Offenlegung von Insiderinformationen und Marktmanipulation umfassen. Solche Handlungen verhindern vollständige und ordnungsgemäße Markttransparenz, die eine Voraussetzung dafür ist, dass alle Wirtschaftsakteure an integrierten Finanzmärkten teilnehmen können". Die Mitgliedstaaten haben – wie üblicherweise – im Einklang mit dem nationalen Recht angemessene verwaltungsrechtliche Sanktionen im Hinblick auf Verstöße gegen das Kryptowerte-Marktmanipulationsverbot vorzusehen. Davon erfasst wird sowohl die handels-, handlungs- als auch die informationsgestützte Marktmanipulation. Für (schwerwiegende) Manipulationen auf Märkten für Kryptowerte sind zwar keine strafrechtlichen Sanktionen vorgeschrieben; ausgeschlossen sind solche Sanktionen jedoch nicht und ihre Festlegung ist Sache der Mitgliedstaaten.[36] Art. 99 MiCAR sieht jedenfalls eine Übermittlungspflicht vor, die auch gesetzgeberische Aktivitäten im Bereich des Strafrechts miteinschließt: „Die Mitgliedstaaten übermitteln der Kommission, der EBA und der ESMA bis zum 30. Juni 2025 die Rechts- und Verwaltungsvorschriften, einschließlich der einschlägigen strafrechtlichen Vorschriften, zur Umsetzung dieses Titels. Die Mitgliedstaaten teilen der Kommission, der EBA und der ESMA spätere Änderungen dieser Vorschriften unverzüglich mit".

Vor diesem Hintergrund könnten einzelne Verstöße gegen die besagten drei kryptobezogenen Verbote unter Kriminalstrafe gestellt werden. Es stellt sich die Frage, wie die einschlägigen Tatbestände umschrieben und die Verstöße dagegen sanktioniert werden könnten. Die Strafnormen würden, sofern sie entsprechend gestaltet sind, im Einklang mit § 119 WpHG dem Schutz der Marktintegrität sowie dem Schutz der Verbraucher:innen und Anleger:innen dienen. Ziel der MiCAR war es außerdem, Innovation und die Einführung neuer Finanztechnologien zu fördern und dabei einen angemessenen Verbraucher:innen- und Anleger:innenschutz zu gewährleis-

36 Vgl. *Rascher*, BKR 2022, 217 (223).

ten.[37] Es würde sich deshalb um ein überindividuelles Rechtsgut handeln, welches hierdurch geschützt wird. Derartige Tatbestände haben *keinen vermögens- oder individualschützenden Charakter* und entfalten lediglich mittelbare Schutzwirkung für einzelne Anleger:innen bzw. Marktteilnehmer:innen.[38]

Angesichts des übergeordneten Schutzzweckes der Funktionsfähigkeit der organisierten Kapitalmärkte bzw. des Emissionshandels werden Marktmanipulationen (vgl. Art. 91 MiCAR) als abstrakte Gefährdungsdelikte klassifiziert. Dennoch handelt es sich dabei um Erfolgsdelikte, sofern sie eine tatsächliche Beeinflussung des Börsen- oder Marktpreises des betreffenden Vermögenswertes oder die Berechnung des Referenzwertes erfordern.[39] Eine differenzierte Betrachtung ist bezogen auf Insidergeschäfte erforderlich: Das Verbot des Tätigens von Insidergeschäften (vgl. Art. 89 Abs. 2 MiCAR) ist rein tätigkeitsbezogen ausgestaltet, ohne dass der:die Insider:in tatsächlich einen wirtschaftlichen Vorteil aus seinem Informationsvorsprung ziehen muss. Dadurch erhält der Tatbestand eine überindividuelle Schutzorientierung, die es zu einem abstrakten Gefährdungsdelikt macht. Ähnliches lässt sich in Bezug auf das insiderrechtliche Empfehlungsverbot (vgl. Art. 89 Abs. 3 MiCAR) sowie das Verbot unrechtmäßiger Offenlegung von Insiderinformationen (vgl. Art. 90 MiCAR) feststellen: Hierbei handelt es sich um Vorfeldtatbestände des eigentlichen Insiderhandelsverbots, die sicherstellen sollen, dass die Anzahl der Personen mit Zugang zu Insiderinformationen, und somit auch die Gefahr von Insidergeschäften aufgrund von Informationsvorsprüngen, möglichst geringgehalten werden.[40]

Die MiCAR bedarf zwar als EU-Verordnung keiner Umsetzung im technischen Sinne des EU-Rechts wie eine EU-Richtlinie,[41] aber doch einer *Durchführung*, zumal an einigen Stellen generisch auf die zuständigen nationalen Behörden oder nationale Regelungen verwiesen wird. Zu die-

37 https://www.consilium.europa.eu/de/press/press-releases/2021/11/24/digital-finance-package-council-reaches-agreement-on-mica-and-dora/ (zuletzt abgerufen am 1.9.2024).

38 *Kämpfer/Travers* in: BeckOK WpHR, WpHG, 11. Aufl. 2023, § 119 Rn. 10.

39 *Kämpfer/Travers* in: BeckOK Wertpapierhandelsrecht, 12. Edition, Stand 1.7.2024, § 119 WpHG Rn. 11; *Pananis* in: Münchener Kommentar, StGB, Band 6, 4. Aufl. 2023, § 119 Rn. 10.

40 *Pananis* in: Münchener Kommentar, StGB, Band 6, 4. Aufl. 2023, § 119 WpHG Rn. 11.

41 Vgl. Erläuterung des Begriffs „Umsetzung" unter https://eur-lex.europa.eu/DE/legal-content/glossary/transposition.html (zuletzt abgerufen am 21.1.2025).

sem Zweck wurde sogar das neue Finanzmarktdigitalisierungsgesetz vom 27.12.2024 (FinmadiG) konzipiert:[42] Mit Art. 1 FinmadiG wird das Gesetz zur Aufsicht über Märkte für Kryptowerte (Kryptomärkteaufsichtsgesetz – KMAG) eingeführt, dessen § 1 Abs. 1 als klares Ziel die Durchführung der MiCAR benennt.

Ausweislich der Gesetzesbegründung soll das FinmadiG den derzeitigen nationalen Aufsichtsrahmen für das Betreiben bzw. das Erbringen von Bank- und Finanzdienstleistungen im Hinblick auf Kryptowerte einschließlich der erteilten Erlaubnisse in den neuen Regelungsrahmen der MiCAR überführen und die erforderlichen Regelungen zu ihrer Anwendung in Deutschland treffen.[43] Wie treffend hierzu angemerkt, ist das FinmadiG „als Omnibus-Gesetz konzipiert, das Änderungen an zahlreichen Rechtsvorschriften vorsieht und damit nahezu das gesamte Spektrum des aufsichtsrechtlichen Kanons deutscher Gesetze umfasst (so unter anderem: KWG, WpIG, WpHG, KAGB, ZAG, VAG, GwG, HGB, GewO, BörsG, SAG, VermAnlG)".[44]

Die Sanktionierung u.a. der drei oben genannten kryptobezogenen Verbote kann somit erst aufgrund des FinmadiG erfolgen, das auf die einzelnen MiCAR-Regelungen verweist. Die Umschreibung der einschlägigen Blankettstraftatbestände findet sich in den §§ 46 und 47 KMAG, wobei der erstgenannte Paragraph Strafvorschriften und der zweitgenannte Paragraph Bußgeldvorschriften normiert. Beide traten nach Art. 23 Abs. 1 FinmadiG am 1.7.2024 in Kraft. Im Einzelnen:

a) Der vorsätzliche *Verstoß gegen das Verbot von Insidergeschäften* im Sinne des Art. 89 MiCAR ist eine strafbare Handlung (Vergehen) nach § 46 Abs. 1 Nr. 4, 5 KMAG. Die fahrlässige Begehung wird nach § 47 Abs. 1 KMAG als Ordnungswidrigkeit sanktioniert.
b) Der vorsätzliche *Verstoß gegen die unrechtmäßige Offenlegung von Insiderinformationen* im Sinne des Art. 90 MiCAR ist eine strafbare Handlung (Vergehen) nach § 46 Abs. 1 Nr. 6 KMAG. Die fahrlässige Begehung wird nach § 47 Abs. 1 KMAG als Ordnungswidrigkeit sanktioniert.
c) Der vorsätzliche oder fahrlässige *Verstoß gegen das Verbot der Marktmanipulation* im Sinne des Art. 91 MiCAR ist eine Ordnungswidrigkeit nach § 47 Abs. 3 Nr. 113 KMAG. Es liegt eine strafbare Handlung (Vergehen in der Gestalt eines Erfolgsdeliktes) nach § 46 Abs. 2 KMAG

42 BGBl. 2024 I, 438; Inkrafttreten überwiegend am 30.12.2024. Vgl. BR-Drs. 670/23.
43 BT-Drs. 20/11178, 2.
44 *Bauerfeind/Hille*, ZRP 2024, 9.

vor, wenn der:die Täter:in die besagte Handlung vorsätzlich begeht und dadurch den Kurs eines oder mehrerer Kryptowerte beeinflusst (Nr. 1) oder eine unmittelbare oder mittelbare Festsetzung des Kauf- oder Verkaufskurses bewirkt (Nr. 2).

An dieser Stelle ist auf Art. 86 MiCAR zurückzukommen, der den Geltungsbereich der Marktmissbrauchsregelungen weit normiert und mithin in strafanwendungsrechtlicher Hinsicht von erheblicher Bedeutung ist. Die Reichweite der Strafbefugnis in Bezug auf Krypto-Börsen-Manipulationen, wie Krypto-Wash-Trading, hängt aufgrund des § 9 Abs. 1 StGB davon ab, ob der jeweils vertypte Tatbestand einen Erfolg hat oder ob es sich um ein abstraktes Gefährdungsdelikt handelt.

Dies führt zu Folgendem: Wenn die einzelnen kryptobezogenen Verbote (Art. 89-91 MiCAR) auf Handlungen und Unterlassungen sowohl in der EU als auch in Drittstaaten angewandt werden und mithin extraterritorial gelten sollten, was aufgrund der Natur einer Blockchain sogleich die ganze Welt betreffen kann, eröffnet sich faktisch ein Weg, diesen MiCAR-Regelungen universelle Geltung zu verschaffen. Für die den §§ 46 und 47 KMAG zugrundeliegenden Verhaltensnormen darf dies nicht der Fall sein. Es besteht jedoch die Gefahr, dass (hier: deutsche) Strafgesetze durch die Hintertür eine universelle Geltung erfahren, sofern der jeweilige typisierte (Blankett-)Straftatbestand ein abstraktes Gefährdungsdelikt darstellt. Um dies zu verhindern, ist in solchen Fällen ein *genuine link*, mithin ein Anknüpfungspunkt nach den §§ 3 ff. StGB, erforderlich. Der Geltungsbereich der Verhaltensnorm: „Du darfst keine manipulativen Spielchen mit Krypto-Börsen machen!" sowie jener der entsprechenden Sanktionsnorm werden nach der hier vertretenen Auffassung ausschließlich durch das Strafanwendungsrecht festgelegt.

IV. Zusammenfassung & Ausblick

Die Digitalisierung und insbesondere die Token-Economy stellen in erster Linie das Bank- und Finanzmarktrecht, aber zwangsläufig auch das Strafrecht vor neue Herausforderungen – zumal nahezu jedes einschlägige Gesetz abschließend ein Kapitel mit „Strafbestimmungen" enthält. Internetkriminalität umfasst viele abstrakte und potentielle Gefährdungsdelikte; nach hier vertretener Auffassung kann nur der Handlungsort die Strafbefugnis begründen. Die digitalen Herausforderungen rechtfertigen nicht *eo*

ipso unzulässige Gesetzesanwendungen; vielmehr kann die internationale Rechtshilfe gefördert werden.

Der Kryptomarktmissbrauch zeigt das Ausmaß der Problematik sehr anschaulich: Der Geltungsbereich der neuen Verordnung über Märkte für Kryptowährungen, die teilweise bereits seit 30.6.2024 gilt, erstreckt sich faktisch weltweit und sieht insbesondere drei kryptowertebezogenen Verbotsnormen vor: das Verbot von Insidergeschäften, das Verbot der unrechtmäßigen Offenlegung von Insiderinformationen und das Verbot der Marktmanipulation. Die Sanktionierung dieser drei Verbote erfolgt erst aufgrund bzw. im Rahmen des FinmadiG. Die Umschreibung der einschlägigen Blankettstraftatbestände findet sich in den §§ 46 und 47 KMAG. Die MiCAR könnte bezogen auf die vertypten abstrakten Gefährdungsdelikte angesichts der vorgesehenen Ausdehnung des Geltungsbereichs von Verhaltensnormen auf Handlungen in Drittstaaten zu einer unzulässigen Universalgeltung der Strafgesetze durch die Hintertür führen.[45]

Das Strafanwendungsrecht bietet somit eine verlässliche Grundlage, um den rechtlichen Herausforderungen der Digitalisierung effektiv zu begegnen, und sorgt dafür, dass die Rechtsordnung auch in einer zunehmend digitalen Welt weiterhin stabil bleibt und funktioniert. Die Zukunft wird zeigen, ob und inwieweit das Schwert des Strafrechts im Bereich des Bank- und Finanzmarktrechts sinnvoll, angemessen und verhältnismäßig ist oder ob Geldbußen effektiver und abschreckender wirken.

45 Ausführlich zum Strafanwendungsrecht *Papathanasiou*, Ius puniendi und staatliche Souveränität – Genese, völkerrechtlicher Rahmen und straftheoretische Kontextualisierung des sog. Internationalen Strafrechts (Habilitationsschrift; in Vorbereitung bei NOMOS).