Das Metaverse – kein strafrechtsfreier Raum: Anwendbarkeit des schweizerischen Strafgesetzbuches bei Betrugsfällen im Metaverse *

Nadine Jost

A. Einleitung

Technologie ist zu einem integralen Bestandteil des alltäglichen Lebens geworden. Bei technologischen Weiterentwicklungen hat die Gesellschaft stets Anpassungsfähigkeit bewiesen. Disruptive Technologien wie das Metaverse haben daher das Potenzial, zahlreiche Lebensbereiche grundlegend zu verändern.[1] Neue Technologien bieten neben Chancen auch neue Angriffsflächen für Kriminelle. Europol[2] und Interpol[3] warnen bereits vor Kriminalität im Metaverse und empfehlen den Strafverfolgungsbehörden, ihre virtuelle Präsenz auszubauen. Einige Personen nutzen die durch die Avatare vermeintlich vermittelte Anonymität im Metaverse bereits aus, wie von verschiedenen Strafverfolgungsbehörden bestätigt wurde.[4] Auch in den Medien ist vermehrt von ‹Verbrechen› im Metaverse zu lesen. Im Januar 2024 leitete die Polizei im Vereinigten Königreich erstmals ein Verfahren

* Die vorliegende Arbeit wurde als Masterarbeit am 15.04.2024 zur Erlangung des akademischen Grades "Master of Laws " an der Universität Zürich eingereicht. Für die Betreuung und die Ermöglichung dieser Veröffentlichung bedanke ich mich herzlich bei Dr. iur. Lukas Staffler, LL.M. Für diese Veröffentlichung wurde der Text zum Stichtag 31.12.2024 aktualisiert. Soweit und sofern in dieser Arbeit geschlechtsspezifische Terminologie verwendet wird, sind immer auch alle anderen Geschlechter gemeint. Der Beitrag bemüht sich um geschlechtsneutrale Formulierungen. Auf eine Doppelnennung wird zugunsten einer besseren Lesbarkeit verzichtet. Soweit auf nationale Rechtsquellen Bezug genommen wurde, beziehen sich diese auf die Schweiz.

1 Zum Ganzen Whitepaper Interpol, S. 3.

2 Bericht Europol, S. 13 ff.

3 Whitepaper Interpol, S. 12 ff.

4 Whitepaper Interpol, S. 11; Camber.

wegen einer virtuellen Vergewaltigung des Avatars eines 16-jährigen Mädchens im Metaverse ein.[5]

Laut der Prognose einer amerikanischen Großbank könnte das Metaverse bis zum Jahr 2030 einen Wert von bis zu 13 Billionen US-Dollar haben.[6] Ende 2024 betrug das Handelsvolumen der Top-Metaverse-Coins ungefähr drei Milliarden Euro, die Marktkapitalisierung belief sich auf 22 Milliarden Euro[7] und auf der Metaverse-Plattform Decentraland stand ein Stück virtuelles Land für umgerechnet USD 920'381.12 zum Verkauf.[8] Die Konzentration solcher Vermögenswerte zieht zwangsläufig kriminelle Verhaltensweisen an.[9] Diese Anziehungskraft wird dadurch verstärkt, dass Metaverse-Ökosysteme voraussichtlich von verschiedenen Kryptowährungen dominiert sein werden,[10] die aufgrund ihrer Pseudoanonymität bei Kriminellen besonders beliebt sind.[11] Es kann daher die Annahme getroffen werden, dass Wirtschaftsdelikte einen Großteil der Straftaten im Metaverse ausmachen werden.

Avatare, gesteuert von Menschen aus verschiedenen Teilen der Welt, können sich im grenzenlosen Metaverse vernetzen und in Echtzeit miteinander interagieren.[12] Es ist daher zu erwarten, dass Straftaten im Metaverse nicht zwingend, aber häufig Landesgrenzen überschreiten und somit eine internationale Dimension aufweisen werden,[13] was die Bestimmung der maßgeblichen räumlichen Anknüpfungspunkte herausfordert. Wie lassen sich die Regelungen des schweizerischen Strafanwendungsrechts aus dem vordigitalen Jahr 1937 auf Delikte im Metaverse anwenden? Im vorliegenden Beitrag soll untersucht werden, ob die aktuelle rechtliche Konzeption für die räumliche Erfassung von Betrugsfällen im Metaverse genügt.

5 Sales; Kappeler; Müllender, das Verfahren ist aktuell noch nicht abgeschlossen; das Urteil wird voraussichtlich einen Präzedenzfall für den Schutz von Minderjährigen im Metaverse schaffen.
6 Pentsy.
7 https://coinmarketcap.com/de/view/metaverse/, besucht am 28.12.2024.
8 https://decentraland.org/marketplace/contracts/0x959e104e1a4db6317fa58f8295f586e1a978c297/tokens/5717, besucht am 31.12.2024.
9 Vgl. Annison, S. 15.
10 Bericht Europol, S. 12.
11 M.w.H. Simmler/Selman/Burgermeister, S. 964 f.
12 Vgl. Schöbel/Leimeister, S. 6.
13 Vgl. Whitepaper Interpol, S. 21; Oberlin/von Hoyningen-Huene, S. 117.

Anhand des folgenden fiktiven, aber realitätsnahen Sachverhalts soll die Lösung illustriert werden.[14]

NFT-Betrug im Metaverse: A gelingt es, von Russland aus den Decentraland[15] Account des berühmten amerikanischen Künstlers zu hacken. In der Folge erstellt A NFTs[16] nach dem ERC-721-Standard, die auf digitale Werke des Künstlers verweisen. Die Schweizerin B besucht während ihres Urlaubs von Spanien aus mit ihrem Avatar die virtuelle Kunstgalerie, wo sie von dem von A gehackten Avatar über die Echtheit des zum Verkauf stehenden NFTs getäuscht wird. Die Avatare vereinbaren, das angeblich vom amerikanischen Künstler geprägte und damit wertvolle NFT gegen 1000 Einheiten der nativen Währung von Decentraland, MANA[17], zu tauschen[18]. Das Geschäft soll über einen Smart Contract[19] abgewickelt werden.[20] B sendet von ihrer Wallet-Adresse[21] 1000 MANA an die Adresse des Smart Contracts, der anschließend das von ihm gehaltene NFT an Bs und die 1000 MANA an As Wallet-Adresse überträgt. Zurück in ihrer Wohnung in der Schweiz liest B folgende Schlagzeile: «Der Avatar des amerikanischen Künstlers wurde gehackt». B wird klar, sie wurde Opfer eines sog. Impersonation Scams.[22] B fragt sich, ob die Schweizer Strafbehörden überhaupt ermächtigt bzw. verpflichtet sind, Delikte im grenzenlosen Metaverse zu verfolgen.

14 Ein vergleichbarer Vorfall hat sich bereits ereignet, bei dem sich der Täter als Künstler Derek Laufman ausgab und NFTs unter dessen Namen zu hohen Preisen verkaufte, Bijan; siehe auch Oberlin/von Hoyningen-Huene, die einen typischen zukünftigen Tathergang im Metaverse beschreiben, bei dem der Täter an seinem PC in den USA sitzt, während sich die Geschädigte an ihrem PC in der Schweiz befindet.

15 Virtuelles, blockchainbasiertes Metaverse mit einem P2P-Netzwerk für Benutzerinteraktionen, Ordano/Jardi/Meilich/Araoz, S. 4.

16 Einzigartiger auf der Blockchain gespeicherter Token, der einen Vermögenswert repräsentiert, Aref/Fábián/Weber, S. 387.

17 Native Währung von Decentraland basierend auf dem ERC-20 Standard, Ordano/Jardi/Meilich/Araoz, S. 12.

18 «Kauf» eines NFTs im Metaverse ist als Tauschvertrag zu qualifizieren, m.w.H. Wicki-Birchler, N. 29 ff.

19 Programmierter Software-Code, der bei Eintritt der vordefinierten Bedingungen bestimmte Aktionen ausführt, m.w.H. Maute, N. 10 f.

20 Smart Contracts werden im Metaverse voraussichtlich von grosser Bedeutung sein, m.w.H. Takyar.

21 Wird auch als Public Adress bezeichnet und ist eine Art Kontonummer, Brameshuber/Edelmann, S. 7 f.

22 Whitepaper Interpol, S. 13; Madiega/Car/Niestadt/Van de Pol, S. 8.

B. Terminologie

I. Metaverse

Der Hype um das begehbare Internet wurde im Oktober 2021 durch die Umbenennung von Facebook in Meta ausgelöst.[23] Seither ist das öffentliche Interesse und das Bewusstsein für das Metaverse weiter gewachsen. Zuletzt berichteten einige Medien im Zusammenhang mit der im Jahr 2024 neu auf dem Markt erschienenen Apple Vision Pro Brille vom zweiten Frühling oder gar vom Durchbruch ‹des› Metaverses.[24] Für andere ist ‹das› Metaverse hingegen nur ein vorübergehender Hype. Die Techunternehmen selbst scheinen uneinig zu sein, ob und in welchem Ausmaß sich ‹das› Metaverse in Zukunft durchsetzen wird.[25] Doch was genau verbirgt sich hinter diesem abstrakten Begriff?

Der Begriff Metaverse ist eine Kombination aus dem griechischen Wort ‹meta› (jenseits) und dem englischen Wort ‹universe›.[26] Bis heute existiert ‹das› eine umfassende Metaverse (noch) nicht. Vielmehr handelt es sich um einen Oberbegriff für eine Vielzahl virtueller Welten,[27] die sich in ihrer Form und Ausgestaltung unterscheiden.[28] In der Literatur konnte sich daher noch keine einheitliche Definition durchsetzen.[29] Der wissenschaftliche Dienst des Europäischen Parlaments beschreibt das Metaverse als eine dreidimensionale virtuelle Welt, in denen Menschen über Avatare interagieren, arbeiten, handeln und Transaktionen mit Krypto-Assets durchführen.[30]

II. Metacrimes

Bislang existiert keine allgemeingültige Definition des Begriffes ‹Metacrime›. Da Metacrimes regelmäßig Computer- und Internetsachverhalte be-

23 Da Silva/Alto.
24 Apple selbst vermied das Wort Metaverse, Hainzl; Li; Menn.
25 Oberlin/von Hoyningen-Huene, S. 116.
26 Wicki-Birchler, N. 8.
27 Wagner/Holm-Hadulla/Ruttloff, Vorwort.
28 Beispielhafte Auflistung und Kategorisierung von verschiedenen Metaverse-Plattformen bei Broschart/Scheitanov/Gieselmann, N. 46 ff.
29 Ritterbusch/Teichmann ermittelten 28 verschiedene Definitionen, S. 12375.
30 Madiega/Car/Niestadt/Van de Pol, S. 2.

rühren, ist es sinnvoll, sich einer Begriffsbestimmung durch eine Analyse bestehender Definitionen in diesem Bereich anzunähern. Innerhalb der Internetkriminalität hat sich der Begriff Cybercrime etabliert, der i.e.S. alle Straftaten erfasst, die sich gegen die Informations- und Kommunikationstechnik richten, sowie i.w.S. alle Straftaten, die mittels dieser Informationstechnik begangen werden.[31]

Der Begriff Metacrime – wie er in dieser Arbeit verstanden wird – soll deutlich enger gefasst werden. Es sollen lediglich strafrechtlich relevante Handlungen erfasst werden, die durch Menschen mittels ihrer Avatare[32] zumindest teilweise innerhalb einer Metaverse-Plattform durch gewöhnliche Nutzungsmethoden verwirklicht werden. Diese Fälle weisen Besonderheiten auf, die eine analytische Begutachtung aus strafanwendungsrechtlicher Sicht rechtfertigen. Handlungen im Zusammenhang mit der Programmierung, der Gestaltung, dem Aufbau und dem Betrieb des Metaverses sowie Handlungen außerhalb der Plattform mit Bezugspunkten zum Metaverse sollen dagegen nicht erfasst sein.[33]

C. Die Blockchain-Technologie

Blockchains bilden das Rückgrat des Metaverses und sind für dessen Entwicklung von großer Bedeutung. Sie bilden insbesondere die technische Grundlage für die nativen Bezahlmittel, Smart Contracts und damit auch NFTs.[34] Weiter könnte die Blockchain-Technologie die Interoperabilität ermöglichen, sodass sich Nutzende mit ihren Avataren und virtuellen Gü-

31 Graf, N. 7.

32 Zum (umstrittenen) Begriff Funna/Sey, S. 1; Sevtap/Tevfik/Ezgi, S. 38 ff.; Tümmler, S. 7 ff.

33 Anlehnend an Bosch, S. 63 ff.; im Gegensatz zur hier vorgeschlagenen Definition umfassen die von Interpol aufgelisteten Straftaten sämtliche Delikte, die mit dem Metaverse in Verbindung stehen, Whitepaper, S. 12 ff.; in diesem Sinne auch Krebs/Rüdiger, S. 68, die aber zwischen In- und Out-World-Delikten differenzieren; für eine weitergehende Differenzierung siehe Oberlin/von Hoyningen-Huene S. 118 ff., die vier Deliktskategorien unterscheiden: Delikte, die im Metaverse nicht vorkommen können (1. Kategorie), bereits bekannte Delikte wie Cybercrimes (2. Kategorie), Delikte, die im Metaverse in neuer Form auftreten (3. Kategorie), und schließlich neue Delikte, die nur im Metaverse existieren können (4. Kategorie).

34 Eingehend dazu Huynh-The et al., S. 405 ff.

tern zwischen verschiedenen Metaverse-Plattformen hin- und herbewegen können.[35]

Bei der Blockchain handelt es sich um eine Art digitales Kontobuch, das die gesamte Transaktionshistorie enthält.[36] Sie ist dezentral auf den (privaten) Rechnern aller Netzwerkteilnehmenden (Nodes) gespeichert.[37] Das sog. Public-/Private-Key-Konzept, das allen Teilnehmenden zwei Schlüssel zuteilt, einen privaten (Private Key) und einen öffentlichen (Public Key),[38] ermöglicht es, den Teilnehmenden Tokens[39] auf der Blockchain zuzuordnen.[40] Das Schlüsselpaar wird in einer Wallet gespeichert.[41]

Die meisten Teilnehmenden verfügen zwar über Tokens, betreiben jedoch selbst keinen Node. Um den Zugang zum Netzwerk dennoch sicherzustellen und insbesondere Transaktionen tätigen zu können, nehmen die Teilnehmenden i.d.R. die Dienstleistungen eines Wallet-Anbieters in Anspruch.[42] Es gibt zwei Arten von Wallet-Anbietern: verwahrende und nichtverwahrende (engl. Custodian und Non-Custodian). Erstere verwahren den Private Key für die Teilnehmenden, während zweitere es ermöglichen, den Private Key selbst abzuspeichern.[43]

Um einen Token On-Chain zu transferieren, muss eine Transaktionsnachricht an das Netzwerk übermittelt werden, wo sie von verschiedenen Nodes empfangen und weitergeleitet wird.[44] Die Full-Nodes, die eine vollständige, aktuelle Version der Blockchain lokal abgespeichert haben, überprüfen pendente Transaktionen und fassen die bestätigten Transaktionen regelmäßig zu Blöcken zusammen. Letztere werden vom Netzwerk validiert und anschließend an die lokale Kopie sämtlicher Full-Nodes angehängt.[45] Die Tokens werden nicht tatsächlich übermittelt, sondern es ändern sich lediglich die Zuordnungsverhältnisse auf der Blockchain.[46] Die Transaktion ist i.d.R. als endgültig zu betrachten, wenn sie sich sechs Blöcke tief in der

35 Bericht Europol, S. 12.
36 Müller/Ong, S. 199; Willems, S. 326.
37 Geiger/Keller, S. 259 f.
38 Fromberger/Zimmermann, N. 15.
39 Werteinheit, die in einem DLT-basierten Register gespeichert ist, m.w.H. Gyr, Anhang N. 30 ff.
40 Fdhila, S. 47.
41 Zu den verschiedenen Arten von Wallets siehe Brameshuber/Edelmann, S. 5 ff.
42 Zum Ganzen Gyr, N. 100 und 550.
43 Zum Ganzen Fromberger/Zimmermann, N. 26.
44 Fromberger/Zimmermann, N. 18.
45 Meyer, § 1 N. 39 f.
46 Fromberger/Zimmermann, N. 19.

Blockchain befindet.[47] Die gesamte Transaktionshistorie ist bei öffentlichen Blockchains von allen jederzeit einsehbar.[48]

D. Schweizer Strafanwendungsrecht

Da es sich beim virtuellen Raum um keinen (straf-)rechtsfreien Raum handelt,[49] stellt sich insbesondere die Frage nach der konkreten Anwendbarkeit des Schweizer Strafrechts bei Betrugsfällen im Metaverse.

I. Einführung

Gemäß ihrer Marginalie regeln die Art. 3–8 i.V.m. Art. 333 Abs. 1 schwStGB den räumlichen Geltungsbereich des Schweizer (Neben-)Strafrechts (sog. Strafanwendungsrecht[50]). Sie legen autonom fest, wann das schwStGB anwendbar ist und bestimmen somit über die Zuständigkeit der Schweizer Strafverfolgungsbehörden.[51] Die Autonomie wird durch das Völkerrecht begrenzt, wobei Inhalt und Tragweite dieser Grenzen umstritten sein können.[52] Aufgrund des Fehlens eines internationalen Normenkomplexes besteht die Möglichkeit, dass neben der Schweiz auch andere Jurisdiktionen für denselben Sachverhalt ihre eigene Strafzuständigkeit beanspruchen.[53]

II. Allgemeiner Überblick

Das Schweizer Strafanwendungsrecht folgt bestimmten Prinzipien, die international weit verbreitet und völkerrechtlich grundsätzlich anerkannt sind.[54] Das Territorialitätsprinzip konstituiert die uneingeschränkte Anwendbarkeit des schwStGB auf inländische Straftaten (Art. 3). Bei Auslandstaten kommt das schwStGB nur in Ausnahmefällen zur Anwendung.

47 Rückert, Strafanwendungsrecht, § 21 N. 23.
48 Ronc/Schuppli, S. 533.
49 M.w.H. Bosch, S. 87 ff.
50 Eingehend zum Begriff Payer, S. 5 ff.
51 Zum Ganzen BGE 117 IV 369 E. 4e; Trechsel/Vest, vor Art. 3 N. 1.
52 BGE 126 II 212 E. 6b; Payer, S. 12.
53 BGE 117 IV 369 E. 4e; Donatsch/Godenzi/Tag, S. 52.
54 BGE 126 II 212 E. 6b.

Letztere umfassen Verbrechen oder Vergehen gegen den Staat oder die Landesverteidigung (Art. 4 schwStGB; Staatsschutzprinzip), Straftaten gegen Minderjährige (Art. 5 schwStGB; unbeschränktes Weltrechtsprinzip), Fälle, in denen die Schweiz zur Strafverfolgung staatsvertraglich verpflichtet ist (Art. 6 schwStGB; stellvertretende Strafrechtspflege), sowie Situationen, in denen Schweizer Interessen i.S.v. Art. 7 Abs. 1 schwStGB betroffen sind, sei es, weil sich die Tat entweder gegen eine Person mit Schweizer Staatsangehörigkeit richtet (passives Personalitätsprinzip) oder von einer solchen begangen wird (aktives Personalitätsprinzip).[55] Der Fokus der vorliegenden Analyse liegt im Folgenden auf dem Territorialitäts- und Personalitätsprinzip.

III. Territorialitätsprinzip

Ausgangspunkt des Strafanwendungsrechts bildet das Territorialitätsprinzip.[56] Sobald eine Tat (teilweise) in der Schweiz begangen wird, ist darauf ohne Weiteres das schwStGB anwendbar (Art. 3 Abs. 1 schwStGB).[57] In Art. 8 schwStGB wird für die Schweiz definiert, dass die Tat dort als begangen gilt, wo die Person sie ausführt oder pflichtwidrig untätig bleibt und am Ort des Erfolgseintrittes. Nach der vorherrschenden Auffassung genügt es, wenn entweder der Handlungs- oder der Erfolgsort in der Schweiz liegt (Ubiquitätsprinzip).[58] Das Primat des Handlungsortes in Art. 31 schwStPO und die weiteren Gerichtsstandsregeln in den folgenden Artikeln kommen erst zum Tragen, wenn das schwStGB auf eine Tat überhaupt anwendbar ist.[59]

Das etablierte Territorialitätsprinzip scheint herausgefordert zu sein, da sich Nutzende aus verschiedenen Staaten im grenzenlosen Metaverse bewegen. Im Folgenden wird anhand des Fallbeispiels untersucht, ob sich die für die Anwendbarkeit des Schweizer Strafrechts relevanten Handlungs- und Erfolgsorte bei Betrugsfällen im Metaverse bestimmen lassen.

55 Zum Ganzen Trechsel/Vest, vor Art. 3 N. 5.
56 BGE 144 IV 265 E. 2.3.1; Payer, S. 67.
57 M.w.H. BGer 6B_178/2011 vom 20.6.2011 E. 3.1.2.
58 BGE 105 IV 326 E. 3c; Donatsch, Art. 8 N. 1; Wohlers, Art. 8 N. 1; a.A. Popp/Keshelava, Art. 8 N. 9.
59 BGE 120 IV 146 E. 2a; Popp/Keshelava, Art. 8 N. 2.

I. Anknüpfung an den inländischen Handlungsort

Als Handlungsort gilt der Ort, wo der Täter die Tat ausführt bzw. versucht auszuführen, und der Ort des pflichtwidrigen Untätigbleibens (Art. 3 Abs. 1 i.V.m. Art. 8 Abs. 1 oder 2 schwStGB). Bei Begehungsdelikten wird auf den physischen Aufenthaltsort des Täters zum Zeitpunkt der (versuchten) Vornahme einer tatbestandlichen Handlung abgestellt,[60] während bei Unterlassungsdelikten der Ort maßgeblich ist, wo der Täter hätte handeln sollen.[61] Bei Metacrimes lassen sich für die Bestimmung des Handlungsortes meines Erachtens mehrere Ansätze vertreten.

a) Aufenthaltsort des Avatars

Zunächst wäre es meines Erachtens vertretbar, für die Ermittlung des Ausführungsortes an den (virtuellen) Aufenthaltsort des täuschenden Avatars anzuknüpfen. Da sich die einzelnen virtuellen Räume keinem bestimmten Hoheitsgebiet zuordnen lassen,[62] müssen hier Fragen bezüglich der Verortung des virtuellen Raumes aufgeworfen werden, die je nach Aufbau der Metaverse-Plattform unterschiedlich zu beantworten sind.

Um die Location des Avatars zu bestimmen, könnte bei blockchainbasierten Metaverse-Plattformen, die den Avatar als NFT auf der Blockchain registrieren,[63] an die physische Lage der einzelnen Full-Nodes angeknüpft werden. Aufgrund ihrer weltweiten Verteilung[64] läge der Aufenthaltsort des Avatars überall und doch nirgendwo. Gegen eine solche Anknüpfung spricht aber primär, dass nur der Username auf der Blockchain hinterlegt ist: 3D-Modelle, Texte etc. werden dagegen aus Kosten- und Praktikabilitätsgründen außerhalb der Blockchain gespeichert.[65] Für die Verortung des virtuellen Aufenthaltsortes des Avatars käme daher der Standort des zentralen Servers in Frage, auf dem die fraglichen Inhalte gespeichert

60 BGE 141 IV 336 E. 1.1; BGE 104 IV 175 E. 3a; BGer 6B_127/2013 vom 3.9.2013 E. 4.2.1.
61 BGE 125 IV 14 E. 2c/aa; BGE 82 IV 65 E. 2; BGer 6B_123/2014 vom 2.12.2014 E. 2.3.
62 Klaas/Klose, N. 7.
63 Decentraland speichert der Avatar-Username auf der Ethereum Blockchain nach dem ERC-721 Standard, https://nftplazas.com/decentraland/decentraland-avatars/, besucht am 30.3.2024.
64 Verteilung der Ethereum-Nodes: https://etherscan.io/nodetracker, besucht am 1.3.2024.
65 Aref/Fábián/Weber, S. 388; für Decentraland https://decentraland.github.io/catalyst-api-specs/#tag/Global/operation/getStatsParcels, besucht am 27.3.2024.

werden. Aufgrund der hohen Rechenleistung genügt ein einzelner Server bei Metaverse-Plattformen nicht. Vielmehr besteht der Server aus einer Vielzahl von Rechnern (sog. Cluster).[66] Ein einzelner Rechner ist z.B. für bestimmte Abschnitte der virtuellen Welt zuständig, während ein anderer für die Verwaltung der virtuellen Güter verantwortlich ist.[67] Die Details der Serverstrukturen und insbesondere die jeweiligen Standorte sind den Nutzenden i.d.R. nicht bekannt, weshalb die Anknüpfung daran meines Erachtens willkürlich erscheint.[68] Beruht die Metaverse-Plattform dagegen auf einer P2P-Architektur, werden die Inhalte lokal von den verschiedenen Nutzenden (sog. Peers) gespeichert,[69] was wiederum eine eindeutige Lokalisierung erschwert bzw. verunmöglicht. Insgesamt führt meines Erachtens jeder Versuch, den virtuellen Raum anhand von physischen Komponenten zu lokalisieren (z.B. Nodes, Server oder Peers), zu realitätsfernen bzw. willkürlichen Ergebnissen.

Gegen die Anknüpfung an den Aufenthaltsort des täuschenden Avatars spricht aber hauptsächlich, dass er lediglich die Marionette oder, um im Strafrechtsjargon zu bleiben, das willenlose Werkzeug des dahinterstehenden Menschen ist, das, technische Fehler vorbehalten, ausführt, was ihm befohlen wird.[70] Der Avatar selbst ist ein Konstrukt aus Daten und Protokollen, aus denen grafische Darstellungen erzeugt werden (sog. Rendering).[71] Ihm kommt keine Rechtspersönlichkeit zu.[72] Die im Metaverse dargestellten (Nicht-)Aktionen eines Avatars bilden damit lediglich den menschlichen Steuerungsbefehl ab und weisen selbst nicht die Qualität einer Handlung im strafrechtlichen Sinne auf,[73] worunter jedes willensgetragene menschliche Verhalten verstanden wird.[74] Damit scheidet der Aufenthaltsort des Avatars als Anknüpfungskriterium für den Handlungsort aus. Vielmehr ist der Steuerungsbefehl des hinter dem Avatar stehenden Menschen Ausgangs- bzw. Anknüpfungspunkt.[75]

66 Bartle, S. 129 ff.
67 Bosch, S. 32.
68 Vgl. Bosch, S. 101.
69 Simmler/Selman/Burgermeister, S. 365; Tanner, Disruptive Opportunities.
70 Vgl. Nida-Rümelin/Weidenfeld, N. 8.
71 Grasnick, S. 354; Klose/Kreutzer, S. 51.
72 Oberlin/von Hoyningen-Huene, S. 118.
73 Bosch, S. 59; vgl. auch Oberlin/von Hoyningen-Huene, die davon ausgehen, dass dem Avatar im bekannten Rechtsgefüge keine Rechtspersönlichkeit zukommt, S. 118.
74 Wohlers, Vorbemerkungen zu den Art. 10 ff N. 13.
75 Vgl. Klaas/Klose, N. 31 ff.

b) Aufenthaltsort der steuernden Person

Die Handlungen des Avatars im Metaverse sind zwar strafrechtlich nicht relevant, der Steuerungsbefehl des Menschen hingegen schon.[76] Im Zusammenhang mit den Cybercrimes wurde in der Lehre und Rechtsprechung festgehalten, dass der Ausführungsort dort liegt, wo sich der Täter bei der Eingabe des entsprechenden Übermittlungs- bzw. Abspeicherungsbefehls physisch aufhält.[77] Für die Metacrimes kann meines Erachtens nichts anderes gelten. Die Vorgänge unterscheiden sich einzig im Punkt des ausführenden ‹Kommunikationswerkzeugs›. Beim Cyberbetrug bedient sich der Täter z.B. einer täuschenden Webseite, im Metaverse eines täuschenden Avatars. Somit muss der Ausführungsort meiner Meinung nach auch bei Metacrimes dort liegen, wo sich die Person, die den fraglichen Avatar durch Gestik, Mimik, verbale Sprache oder Berühren eines Touchdisplays steuert, im Moment der Erteilung der entsprechenden Befehle physisch aufhält.[78]

A steuert den gehackten Avatar, der die Täuschungshandlungen im Metaverse verwirklicht, von Russland aus. Somit liegt der Handlungsort des fiktiven Meta-Betruges in Russland. Bei den strafbaren Vorbereitungshandlungen, dem Hacken des User-Accounts (Cybercrime i.e.S.) und der Abspeicherung des digitalen Werkes des amerikanischen Künstlers, das dem NFT zugrunde liegt (Urheberrechtsverletzung), handelt es sich hingegen nicht um Metacrimes, wie sie in dieser Arbeit definiert wurden. Bei diesen ‹klassischen› Delikten läge der Ausführungsort nach den allgemeinen Grundsätzen ebenfalls in Russland.

c) Ort der Auswirkung

In der deutschen Literatur wird konstatiert, dass auch der Ort, wo sich die konkrete Wirkung im Metaverse entfalte, für die Bestimmung des Handlungsortes in Betracht komme.[79] Nach diesem Ansatz würden im Fallbeispiel zusätzlich die Aufenthaltsorte aller Nutzenden, die die Täuschungs-

76 Bosch, S. 60.
77 BGer 8G.43/1999 vom 11.8.1999, referiert von Weissenberger, S. 705; BStGer BG.2016.23 vom 25.11.2016 E. 3.4; Donatsch/Godenzi/Tag, S. 54; Graf, N. 19; Schwarzenegger, E-Commerce, S. 339.
78 Mit ähnlicher Begründung für das deutsche StGB Klaas/Klose, N. 12.
79 Im Ergebnis aber ablehnend Klaas/Klose, N. 12.

handlungen des gehackten Avatars aufgrund ihrer virtuellen Anwesenheit wahrgenommen haben, einen Handlungsort begründen.[80] Dies ist meiner Ansicht nach aus mehreren Gründen abzulehnen. Es ist in Erinnerung zu rufen, dass das Strafrecht an die unmittelbare tatbestandliche Handlung anknüpft. Der Radius der Wahrnehmbarkeit einer Handlung ist nicht Teil ihrer selbst.[81] In diesem Sinne hat das Bundesgericht in einem älteren Entscheid bereits entschieden, dass bei einer im Fernsehen übertragenen strafbaren Äußerung nicht das gesamte Sendegebiet als Ausführungsort gelte, sondern nur derjenige Ort, wo die Person vor die Kamera getreten sei.[82] Zuletzt spricht die Gefahr, dass dadurch die Grenzen zum Erfolgsort verwischt werden, gegen diesen Ansatz.[83]

d) Standorte der Server bzw. der Peers

Es wäre meines Erachtens auch vertretbar, auf den Ort abzustellen, wo die entsprechenden Befehle verarbeitet bzw. ausgeführt werden. Hierfür werden im Folgenden die Prozesse hinter den Avatar-Interaktionen stark vereinfacht erläutert.

Bei einer Metaverse-Plattform mit einer Client-Server-Struktur wird der Befehl von der Client-Software an den zentralen Server gesendet, der ihn wiederum an den spezifischen Rechner schickt, wo er registriert, interpretiert, und anschließend an die entsprechenden Nutzenden zurückgesendet wird.[84] Verwendet die Plattform dagegen ein P2P-Netzwerk für die Interaktionen, werden die Daten direkt zwischen den Peers ausgetauscht. Die Speicherung und die Verarbeitung erfolgen dezentral auf den individuellen Geräten der Peers.[85] Folglich könnten die Standorte der involvierten Server bzw. Peers einen Handlungsort begründen.

Im Zusammenhang mit den Cybercrimes hat die Lehre und Rechtsprechung den Standort des penetrierten Servers als Ausführungsort abgelehnt, mit der Begründung, dass dem Täter beim Transport und der Speicherung

80 Vgl. Fallbeispiel bei Klaas/Klose, N. 12.
81 Vgl. für das österreichische Strafrecht Schmoller, S. 86.
82 BGE 119 IV 250 E. 2.
83 Klaas/Klose, N. 12.
84 Eingehend dazu Schmidt/Dreyer/Lampert, S. 27 f.
85 Eingehend dazu Schmidt/Dreyer/Lampert, S. 29 f.

der Daten keine Kontrolle zukomme.[86] Gleiches muss meiner Meinung nach für Metacrimes gelten. Durch die oben beschriebenen Strukturen werden die Befehle automatisch und innert Sekundenbruchteilen gespeichert und verarbeitet. Der Täter kann im Metaverse nicht in den Prozess der Befehlsübermittlung und -speicherung eingreifen. Der Transit[87] durch die allfälligen Länder, wo sich die Server oder die Peers befinden, gehört nach der hier vertretenen Auffassung nicht zur Ausführungshandlung i.S.v. Art. 8 schwStGB.

2. Anknüpfung an den inländischen Erfolgsort

Neben dem Handlungsort gilt auch der Ort, wo der Erfolg eingetreten ist bzw. hätte eintreten sollen, als Begehungsort (Art. 3 Abs. 1 i.V.m. Art. 8 Abs. 1 bzw. Abs. 2 schwStGB). Da es sich beim Betrug um ein Erfolgsdelikt handelt, hat die langjährige Kontroverse[88] um den Erfolgsbegriff in Art. 8 schwStGB keine Auswirkung auf die hier untersuchte territoriale Anknüpfung.

Als Erfolgsorte kommen beim Betrug gemäß bundesgerichtlicher Rechtsprechung der Ort der Entreicherung sowie der Ort der (beabsichtigten) Bereicherung in Frage (sog. kupiertes Erfolgsdelikt).[89] Fallen Irrtum, Vermögensdisposition und -schaden räumlich auseinander, vertritt ein Teil der Lehre die Ansicht, dass diesfalls an allen drei Orten angeknüpft werden könne.[90] Das Bundesgericht hat sich bis anhin nicht vertieft damit auseinandergesetzt, im Allgemeinen pflegt es aber eine großzügige Praxis und bejaht die Schweizer Zuständigkeit zur Vermeidung negativer Kompetenzkonflikte auch in Fällen ohne engen Bezug zur Schweiz.[91] Die genauen Erfolgsorte sind bei Betrugsfällen mit Tokens nicht immer eindeutig,[92] wie folgende Ausführungen zeigen.

---

86 BGer 8G.43/1999 vom 11.8.1999, referiert von Weissenberger, S. 705; Heimgartner, S. 123; Schwarzenegger, E-Commerce, S. 339.
87 Zu den sog. Transitdelikten Schwarzenegger, Geltungsbereich, S. 118.
88 Zur Entwicklung der Rechtsprechung und zum Meinungsstand siehe Payer, S. 75 f.
89 BGE 124 IV 241 E. 4c; BGE 125 IV 177 E. 2a; BGE 109 IV 1 E. 3c; kritisch dazu Schwarzenegger, Betrug, S. 151 f.
90 Schwarzenegger, Betrug, S. 154 f.; ferner Bartetzko, N. 2a; m.w.H. BGer 6B.127/2013 vom 3.9.2013
E. 4.2.2.
91 BGE 141 IV 205 E. 5.2; BGE 141 IV 336 E. 1.1; BGE 133 IV 177 E. 6.3.
92 Vgl. Reischl/Stilz, N. 279.

a) Ort des Irrtums (1. Erfolgsort)

Der Ort des Irrtums liegt dort, wo sich die getäuschte Person im Moment der Irrtumserregung physisch aufhält.[93] In Bezug auf das Metaverse ergeben sich in diesem Punkt keine Besonderheiten. A ruft mittels des gehackten Avatars bei B, nicht ihrem Avatar, einen Irrtum hervor. Im Fallbeispiel liegt der Ort der Irrtumserregung folglich in Spanien.

b) Ort der Vermögensdisposition (2. Erfolgsort)

Maßgebend ist der physische Aufenthaltsort der verfügenden Person zum Zeitpunkt der Vermögensdisposition.[94] Nicht der Avatar, sondern die dahinterstehende Person disponiert über ihr Vermögen. Als Vermögensdisposition gilt jede Handlung oder Unterlassung, die unmittelbar dazu geeignet ist, das Vermögen zu vermindern.[95]

Beim Eingehungsbetrug[96] ist der Vertrag wegen der absichtlichen Täuschung gemäß bundesgerichtlicher Rechtsprechung ex tunc ungültig, weshalb das Vermögen im Moment des Vertragsschlusses im Metaverse (noch) nicht als unmittelbar vermindert gilt.[97] Doch wann ist dies bei einer Token-Transaktion der Fall?

Die Tatsache, dass die transferierten Tokens nicht im Moment der Übermittlung der Transaktionsnachricht an das Netzwerk unmittelbar ‹abgezogen› bzw. einer anderen Adresse zugeordnet werden, sondern effektiv erst nach der Validierung durch die Full-Nodes,[98] kann meines Erachtens nicht zum Entfallen der Unmittelbarkeit führen. Eine Nichtvalidierung oder ein rechtzeitiger Abbruch der Transaktion sowie ein allfälliger Rücktransfer der Tokens durch den Smart Contract bei Nichteintritt der Bedingungen hätte lediglich die Folge, dass der Vermögensschaden ausbliebe.

Bei einer nicht-verwahrenden Wallet signiert und übermittelt die irrende Person die Transaktionsnachricht an das Netzwerk eigenständig. Bei einer

93 BStGer BG.2021.17 vom 16.6.2021 E. 3.3.1 f.; Schwarzenegger, Betrug, S. 156.
94 BGer 6B.127/2013 vom 3.9.2013 E. 4.2.2 mit Verweis auf Schwarzenegger, Betrug, S. 156.
95 BGE 126 IV 113 E. 3a; BGE 128 IV 255 E. 2e/aa; BGer 6B_480/2018 vom 13.9.2019 E. 1.1.2; kritisch zur Formulierung Maeder/Niggli, N. 133 ff.
96 Eingehend dazu Maeder/Niggli, N. 175 ff.
97 BGE 114 II 131 E. 3b; m.w.H. Maeder/Niggli, N. 177; kritisch Vest, N. 192 ff.
98 Siehe Kapitel C.

verwahrenden Wallet übernimmt dies der Anbieter im Auftrag der irrenden Person.[99] Bei letzterer Konstellation könnte, wie im Zusammenhang mit Buchgeld, umstritten sein,[100] ob bereits die Erfassung des Transaktionsauftrags oder erst dessen Vollzug durch die Mittelsperson (verwahrender Wallet-Anbieter) als Verfügung gilt. Da die Eignung zur Vermögensverminderung genügt, gilt meines Erachtens bereits die Transaktionsanweisung der irrenden Person als Verfügungshandlung.[101]

Maßgebend ist damit der Aufenthaltsort der irrenden Person im Moment der Übermittlung der Transaktionsnachricht bzw. der Erfassung des Transaktionsauftrages.

c) Ort der Entreicherung (3. Erfolgsort)

Bislang bestehen territoriale Anknüpfungspunkte in Russland (Ausführungsort) und in Spanien (1. und 2. Erfolgsort). Zu prüfen bleibt, ob der Ort der Entreicherung die Schweizer Strafverfolgungsbehörden zur Verfolgung des Meta-Betruges ermächtigt bzw. verpflichtet.

aa) Vermögensbegriff

Zuerst soll kurz eruiert werden, ob Tokens überhaupt vom strafrechtlichen Vermögensbegriff erfasst sind. Gemäß h.L.[102] und Praxis[103] ist von einem wirtschaftlich-juristischen Vermögensbegriff auszugehen, wonach alle rechtlich geschützten wirtschaftlichen Güter, die gegen Geld getauscht werden können, erfasst sind.[104]

---

99 Zum Ganzen Bericht Bundesrat DLT, S. 145 f.

100 Donatsch, Strafrecht III, S. 243 erachtet bereits die Erfassung des Zahlungsauftrags zugunsten der Bank als Vermögensverfügung, während bei Stratenwerth/Bommer, § 15 N. 33 erst der Vollzug des Zahlungsauftrags durch die Mittelsperson (Bank) als Verfügung gilt.

101 Vgl. Donatsch, Strafrecht III, S. 243; in diesem Sinne auch BStGer BG.2021.17 vom 16.6.2021 E. 3.3.2, wo bereits die zahlungsauslösende Anweisung als Verfügung gilt.

102 Donatsch, Strafrecht III, S. 96; Stratenwerth/Bommer, § 15 N. 47; Trechsel/Crameri, N. 21.

103 BGE 117 IV 139 E. 3d/aa; BGE 122 IV 179 3d; BGer 6B_236/2009 vom 18.1.2010 E. 2.3.

104 Gless, Festschrift, S. 49.

Metaverse-Tokens[105] werden i.d.R. an verschiedenen Krypto-Börsen oder über Broker gehandelt und können entweder direkt oder indirekt über eine andere Kryptowährung in
Fiat-Geld[106] umgetauscht werden.[107] Solche Metaverse-Tokens haben damit sowohl innerhalb als auch außerhalb des Metaverses einen Wert, womit sie meines Erachtens klar vom strafrechtlichen Vermögensbegriff erfasst sind.[108] Dasselbe muss für Metaverse-NFTs gelten, die auf externen und internen Marktplätzen gehandelt werden.[109]

bb) Eintritt des Vermögensschadens

Bei On-Chain Token-Transaktionen liegt der Vermögensschaden in der endgültigen Veränderung Zuordnungsverhältnisse auf der Blockchain:[110] Nach erfolgreicher Abwicklung über den Smart Contract wird der NFT Bs Wallet-Adresse zugeordnet. Im Gegenzug reduziert sich das ihrer Wallet-Adresse zugeordnete MANA-Guthaben um 1000. Der Schaden ergibt sich aus der Wertdifferenz der erbrachten Leistung (1000 MANA) und der erhaltenen Gegenleistung (wertloser NFT) und kann mithilfe des MANA-Kurses[111] ohne Weiteres beziffert werden.

cc) Ort des Vermögensschadens

Für das Strafanwendungsrecht ist es von Bedeutung, wo der Vermögensschaden eingetreten ist, wobei auch bei strittiger dinglicher Lokalisierbarkeit soweit möglich auf die konkrete Lage der geschädigten Person bzw. ihrer Vermögenswerte und nicht generell auf ihren Wohn- oder Steuersitz

105 Bezahlmittel innerhalb der Metaverse-Plattformen (auch Metaverse Coins und Metaverse Crypto): z.B. IBAT, LBOCK, MANA, ONT, SAND, m.w.H. Übersicht Metaverse Coins.
106 Zum Begriff siehe Willems, S. 325.
107 Shirin/Wenz.
108 Vgl. Gless/Kugler/Stagno, S. 10 f.; Meyer, § 9 N. 521; Rückert, Phänomenologie, § 20 N. 1 f.
109 Vgl. Peterson.
110 Siehe Kapitel C.
111 Am 21.4.2024 entsprach der Schaden ca. Fr. 452 (1 MANA = Fr. 0.45), https://www.coinbase.com/de/converter/mana/chf#:~:text=Der%20aktuelle%20Kurs%20von%20Decentraland,.386%2C57%20CHF%20gefallen.

abzustellen ist.[112] Demnach stellt sich die Frage, wo die konkreten Vermögenswerte zu verorten sind bzw. was als Anknüpfungspunkt hierfür dienen kann. Es sind meines Erachtens mehrere Ansätze vertretbar.

(1) Belegenheitsort der transferierten Tokens

Der Speicher- oder Aufbewahrungsstandort der Wallet kommt als Anknüpfungspunkt für den Belegenheitsort der Tokens nicht in Betracht, da die transferierten Tokens nicht in die Wallet übertragen werden, sondern stets auf der Blockchain verbleiben.[113] Folglich kommt die Blockchain als Belegenheitsort der transferierten Tokens in Frage.[114] Hier ergibt sich aber folgendes Problem: Die gesamte Blockchain ist nicht auf einem zentralen Server, sondern dezentral auf einer Vielzahl von Full-Nodes gespeichert.[115] Diese Dezentralität hätte zur Folge, dass in jedem Land, in dem ein solcher Full-Node betrieben wird, mitunter auch in der Schweiz, ein (dezentraler) Erfolgsort läge.[116]

Dieser Betrachtungsweise ist entgegenzuhalten, dass die Tokens auf der Blockchain auch dann weiter existieren, wenn ein einzelner Full-Node die Blockchain löscht. Allein aus diesem Grund kann der Ort des Betriebes eines einzelnen Full-Nodes aus tatsächlicher Sicht keinen physischen Belegenheitsort der Tokens begründen.[117] Aus normativer und praktischer Sicht spricht Folgendes dagegen: Die Anerkennung des Erfolgsortes als Begehungsort beruht auf dem Gedanken, dass das schwStGB Anwendung findet, wenn es zu Schädigungen oder Gefährdungen geschützter Rechtsgüter im Inland kommt.[118] Der alleinige Betrieb von Nodes genügt hierfür offen-

112 Schwarzenegger, Betrug, S. 155 f.; ferner BGE 125 III 103 E. 2bb im Zusammenhang mit der Bestimmung des Erfolgsortes bei der unerlaubten Handlung im internationalen Privatrecht.

113 Ebenso Grzywotz, S. 122 f.; ähnliche Argumentation (Private Keys ändern sich durch Transaktion nicht) bei Rückert, Strafanwendungsrecht, § 21 N. 15 und Schmoller, S. 87.

114 Grzywotz, S. 122; Rückert, Strafanwendungsrecht, § 21 N. 15.

115 Kapitel C.

116 Bejahend Grzywotz, S. 123.

117 Zum Ganzen Rückert, Strafanwendungsrecht, § 21 N. 17.

118 BGer 6B.127/2013 vom 3.9.2013 E. 4.2.1; für eine restriktive Auslegung des Ubiquitätsprinzips Cassani,
S. 248 ff.

sichtlich nicht.[119] Zuletzt würde es die Schweizer Strafverfolgungsbehörden überfordern, da das schwStGB bei sämtlichen On-Chain Token-Transaktionen Anwendung finden würde.

Abschließend kann festgehalten werden, dass der physische Belegenheitsort der transferierten Tokens nach der hier vertretenen Auffassung nicht ermittelt werden kann.[120] Der Vermögensschaden tritt stets nur virtuell in der Blockchain ein. In diesem Sinne hat auch das Bundesstrafgericht in einem Urteil erwogen, dass es sich bei Kryptowährungen um dematerialisierte Vermögenswerte ohne eindeutige örtliche Zuordnung handle.[121]

(2) Belegenheitsort des betroffenen Wallet-Kontos

Bei Buchgeldtransaktionen hat das Bundesgericht bereits auf den Ort abgestellt, an dem sich das Bankkonto befindet, auf welchem sich das Vermögen vermindert.[122] Wird diese Rechtsprechung auf Token-Transaktionen angewendet, wäre das schwStGB immer dann anwendbar, wenn das Wallet-Konto, auf welchem sich der Token-Bestand vermindert, einem Wallet-Anbieter mit Sitz in der Schweiz zugeordnet werden könnte.

Eine Übertragung dieser Rechtsprechung ist nach der hier vertretenen Auffassung jedenfalls für nicht-verwahrende Wallet-Anbieter abzulehnen. Letztere stellen lediglich die Software zur Verfügung und sind selbst nicht an der Übertragung der Tokens beteiligt. Im Übrigen sind sie regelmäßig als dezentral organisierte Open Source-Projekte konzipiert, die keinen eindeutigen Sitz haben, woran angeknüpft werden könnte.[123]

Ähnlich wie eine Bank haben die verwahrenden Wallet-Anbieter die Verfügungsmacht über die Tokens inne und lösen im Auftrag und im Namen ihrer Kundschaft Transaktionen aus.[124] Es ist allerdings erneut darauf hinzuweisen, dass auch die verwahrenden Wallet-Anbieter die Tokens nicht direkt bei sich aufbewahren, sondern nur die Private Keys. Sie signieren und übermitteln lediglich die Transaktionsnachricht an die Full-Nodes, die anschließend die Transaktion vollziehen.[125] Aus diesen Gründen scheitert

119 Rückert, Strafanwendungsrecht, § 21 N. 18.
120 Rückert, Strafanwendungsrecht, § 21 N. 17; a.A. Grzywotz, S. 123.
121 BStGer BG.2021.28 vom 24.9.2021 E. 6.2.
122 BGE 124 IV 241 E. 4d; Schwarzenegger, Betrug, S. 157.
123 Zum Ganzen Bericht Bundesrat DLT, S. 28 und 146.
124 Bericht Bundesrat DLT, S. 145 f.
125 Siehe Kapitel C.

meines Erachtens auch bei nicht-verwahrenden Wallet-Anbietern die Übertragung der obigen Rechtsprechung.

Weiter führt die Tatsache, dass ein Wallet-Konto heute von überall aus eröffnet und verwaltet werden kann, dazu, dass die Anknüpfung an dessen Belegenheitsort meines Erachtens ohnehin eher zufällig als präzisierend erscheint. Im Übrigen ist die Inanspruchnahme eines Wallet-Anbieters nicht zwingend.[126] Zusammenfassend ist der Belegenheitsort des Wallet-Kontos für die Lokalisierung der Vermögensverminderung nach der hier vertretenen Auffassung abzulehnen.

(3) Das Vermögen

Die obigen Ausführungen haben gezeigt, dass sich die Vermögensverminderung im Zusammenhang mit On-Chain Token-Transaktionen nicht (zweckmäßig) lokalisieren lässt. Daher erachte ich es für sachgerecht, das Vermögen als Ganzes als geschädigt zu betrachten und entsprechend auf den Lebensschwerpunkt (natürliche Person) bzw. Sitz (juristische Person) der geschädigten Person abzustellen.[127]

d) Ort der Bereicherung

Nach erfolgreicher Übermittlung durch den Smart Contract, werden As Wallet-Adresse 1000 MANA mehr zugeordnet. Bezüglich der Lokalisierung der Vermögensvermehrung kann auf die zuvor dargelegten Ausführungen zum Ort des Vermögensschadens verwiesen werden. Es ergeben sich dieselben Problematiken. Da es nach der hier vertretenen Auffassung nicht möglich ist, die Vermögensvermehrung zu lokalisieren bzw. diese rein virtuell eintritt, gilt das Vermögen als Ganzes als bereichert, weshalb auf den Lebensschwerpunkt bzw. Sitz der bereicherten Person abzustellen ist.

126 Fromberger/Zimmermann, N. 26.

127 Gleiches Ergebnis für das österreichische Strafrecht bei Schmoller, S. 89 f; im Schweizer Zwangsvollstreckungsrecht plädiert die Lehre ebenfalls dafür, dass der physische Belegenheitsort von Crypto-Tokens nicht ermittelbar sei, weshalb auf den Wohnsitz des Schuldners abzustellen sei, Sievi, N. 24; Zogg, S. 10.

3. Ergebnis

Beim Handlungsort ist meines Erachtens die ausschließliche Anknüpfung an den Ort, wo sich die den Avatar steuernde Person physisch aufhält, am überzeugendsten. Hier wird unmittelbar an das menschliche Verhalten angeknüpft, wie dies der Gesetzeswortlaut verlangt.

Bei den Erfolgsorten der Irrtumserregung und der Vermögensdisposition treten de lege lata keine wesentlichen Schwierigkeiten im Zusammenhang mit Token-Transaktionen auf. Mangels Lokalisierbarkeit der Vermögensverminderung bzw. -vermehrung ist nach der hier vertretenen Auffassung das Vermögen bei einer On-Chain Token-Transaktion insgesamt als geschädigt bzw. bereichert anzusehen, weshalb subsidiär auf den Lebensschwerpunkt oder Sitz der geschädigten bzw. bereicherten Person abzustellen ist.

Anhand des Fallbeispiels konnte illustriert werden, dass grundsätzlich auch die Handlungs- und Erfolgsorte bei Betrugsfällen im Metaverse bestimmt werden können und dies zu vertretbaren Ergebnissen führt. Obwohl in casu lediglich der Ort des Vermögensschadens in der Schweiz liegt, muss dies meiner Ansicht nach genügen, um die Schweizer Strafzuständigkeit zu begründen, da das Bundesgericht in internationalen Verhältnissen tendenziell eine großzügige Praxis pflegt. Damit sind die Schweizer Strafverfolgungsbehörden ermächtigt bzw. verpflichtet den vorliegenden Betrugsfall im grenzenlosen, aber nicht strafrechtsfreien Metaverse zu verfolgen.

IV. Personalitätsprinzip

In Art. 7 schwStGB wird eine gegenüber Art. 4–6 schwStGB subsidiäre und abschließende schweizerische Zuständigkeit für extraterritoriale Handlungen begründet. Im Zentrum steht der Schutz von Personen mit Schweizer Staatszugehörigkeit im Ausland (passives Personalitätsprinzip) bzw. die Anwendung des schwStGB auf Personen mit Schweizer Staatszugehörigkeit für ihre Taten im Ausland (aktives Personalitätsprinzip). Dies ergibt sich implizit aus Art. 7 Abs. 2 schwStGB.[128] Dieses Prinzip lässt sich grundsätzlich auch auf das Metaverse übertragen, sofern der Avatar einer bestimmten

128 Zum Ganzen BGer 6B_452/2022 vom 16.11.2023 E. 2.1.2; Popp/Keshelava, Art. 7 N. 2 und 21; ferner Botschaft Revision StGB, S. 1998.

(natürlichen oder juristischen) Person zugeordnet werden kann.[129] Maßgeblich ist die Staatsangehörigkeit der Person, die den Avatar steuert.

In der Praxis wird sich der Begehungsort eines Metacrimes oft nur schwer bestimmen lassen. Dies liegt einerseits daran, dass der Täter regelmäßig vom Ausland aus agieren wird und andererseits häufig Tokens involviert sein werden, was zusätzlich zur Verschleierung des Begehungsortes beiträgt.[130] Bei Fehlen eines (ermittelbaren) Schweizer Handlungs- und Erfolgsortes könnte daher das Personalitätsprinzip als ‹Auffangprinzip› dienen. Im Zentrum soll nachfolgend das passive Personalitätsprinzip stehen.

1. Passives Personalitätsprinzip

Gemäß dem passiven Personalitätsprinzip findet das schwStGB Anwendung, wenn ein Täter im Ausland ein Delikt gegen eine (natürliche oder juristische) Person mit Schweizer Staatszugehörigkeit begeht,[131] die Tat auch am ausländischen Begehungsort strafbar ist oder sie dort keiner Strafgewalt unterliegt und sich der Täter in der Schweiz aufhält oder ihr wegen dieser Tat ausgeliefert wird.[132] Weiter darf er nicht ins Ausland ausgeliefert werden, obwohl eine Auslieferung nach Schweizer Recht zulässig wäre.[133] Unter diesen Voraussetzungen findet das schwStGB auch auf alle hinter den Avataren stehenden Personen Anwendung, selbst wenn kein Begehungsort in der Schweiz liegt oder ein solcher nicht ermittelbar ist.

Wäre der von A begangene Meta-Betrug gegen die Schweizerin B auch nach russischem Recht strafbar und würde er der Schweiz gestützt auf Art. 35 Abs. 1 lit. a schwIRSG i.V.m. Art. 146 schwStGB ausgeliefert werden, sind die Schweizer Strafbehörden unabhängig davon, ob der Handlungs- oder Erfolgsort in der Schweiz liegt, zur Verfolgung des Metacrimes ermächtigt bzw. verpflichtet.

In der Praxis könnte insbesondere die Voraussetzung der doppelten Strafbarkeit[134] Probleme bereiten. Um dies zu illustrieren, werden im Folgenden einige nicht abschließende Überlegungen im Zusammenhang mit dem Betrugstatbestand angestellt. Die Problematik liegt meines Erachtens

129 Vgl. Kettemann/Böck, N. 11.
130 Bartetzko, N. 2a.
131 BGE 131 IV 145 E. 2bb; kritisch Gless, Internationales Strafrecht, N. 201.
132 Eicker, S. 300; Wohlers, Art. 7, N. 3 und 4; Trechsel/Vest, Art. 7 N. 2.
133 Zum Ganzen Eicker, S. 306; Stratenwerth/Bommer, A§ 5 N. 22; Trechsel/Vest, Art. 7 N. 2.
134 M.w.H. BGE 147 II 432 E. 2.2; Popp/Keshelava, vor Art. 3 N. 2; Staffler, S. 152.

zunächst beim Tatbestandsmerkmal des Vermögensschadens. Hier stellt sich insbesondere die Frage, ob virtuelle Gegenstände, NFTs und Metaverse-Währungen vom strafrechtlichen Vermögensbegriff der jeweiligen Rechtsordnung erfasst sind. Im Zusammenhang mit der schweizerischen Besonderheit der Arglist stellt sich sodann die Frage, ob dieselben Maßstäbe wie in der realen Welt gelten. Bedient sich der Täter besonderer Machenschaften allein dadurch, dass er die Täuschungshandlungen mittels eines Avatars im Metaverse ausführt? Dies muss meiner Einschätzung nach verneint werden. Die Registrierung bei einer Metaverse-Plattform und die Erstellung eines Avatars sind mit wenigen Klicks und für ein überschaubares Entgelt möglich und stellen für sich allein keine besonderen Vorkehrungen dar. Für die Begründung der Arglist müssen zusätzliche Umstände hinzutreten (z.B. das Hacking eines User-Accounts). Auch kann im Zusammenhang mit der Opfermitverantwortung erwartet werden, dass einem fremden Avatar respektive der dahinterstehenden Person nicht gleich (schnell) vertraut werden kann wie einer physisch vor sich stehenden Person.

Die Frage nach der Strafbarkeit im Zusammenhang mit Metacrimes ist neu und bislang in den meisten Jurisdiktionen noch ungeklärt. Daher scheint die Funktion des passiven Personalitätsprinzips als Auffangprinzip derzeit noch eingeschränkt zu sein.[135] Meines Erachtens wäre es zu begrüßen, nach dem Vorbild des Übereinkommens über Cyberkriminalität (CCC) Regelungen zur Angleichung materiell-strafrechtlicher Strafbarkeitsvoraussetzungen auf internationaler Ebene zu erlassen, um die internationale Zusammenarbeit diesbezüglich zu erleichtern. Dies ist notwendig, weil bei Metacrimes nicht zwangsläufig, aber regelmäßig mehrere Staaten involviert sein werden.

2. Aktives Personalitätsprinzip

Die ratio legis des aktiven Personalitätsprinzips ist nicht die Begründung einer Personalhoheit, sondern der Umstand, dass Schweizer Staatsangehörige ohne ihre Einwilligung nicht ausgeliefert werden können.[136] Im Übrigen gelten die gleichen Voraussetzungen wie beim passiven Personalitätsprinzip (Doppelte Strafbarkeit, Anwesenheit im Inland, Auslieferungsdelikt

135 Bosch, S. 103.
136 Trechsel/Vest, Art. 7 N. 12 ff.

und fehlende Auslieferung).[137] Bezüglich der Problematik im Zusammenhang mit der doppelten Strafbarkeit gilt das oben Gesagte im gleichen Masse.

E. Schlussfolgerungen und Ausblick

I. Schlussfolgerungen

Da es sich beim Metaverse nicht um einen strafrechtsfreien Raum handelt, müssen die schweizerischen Strafverfolgungsbehörden im Einzelfall prüfen, ob sie zur Verfolgung des konkreten Metacrimes ermächtigt bzw. verpflichtet sind.

Der Handlungsort im Metaverse lässt sich insbesondere anhand der in der Rechtsprechung und Literatur aufgestellten Grundsätze zu den Cybercrimes bestimmen. Die Berücksichtigung des Aufenthaltsortes des Avatars, des Auswirkungsortes im Metaverse sowie der Standorte der Server bzw. der Peers ist abzulehnen, da hier nicht an die unmittelbare menschliche Handlung angeknüpft wird. Nach der hier vertretenen Auffassung ist auch bei Metacrimes ausschließlich der physische Aufenthaltsort des Täters maßgebend.

Im Zusammenhang mit Token-Transaktion treten bei der Ermittlung des Ortes der Irrtumserregung und der Vermögensdisposition keine größeren Probleme auf. Nicht der Avatar, sondern die dahinterstehende Person irrt sich bzw. verfügt über ihr Vermögen. Allerdings treten bei der Verortung der Vermögensverminderung bzw. -vermehrung aufgrund der Dezentralität der Blockchain-Technologie einige Schwierigkeiten auf. Wird der in dieser Arbeit vertretenen Auffassung gefolgt und ein (dezentraler) Erfolgsort an allen Standorten der Full-Nodes verneint und stattdessen an den Lebensmittelpunkt bzw. Sitz der entreicherten bzw. bereicherten Person angeknüpft, erfordert es de lege lata keine Modifikation des Erfolgsortes im Sinne einer Einschränkung desselben bei Vorliegen solch dezentraler Strukturen.[138]

Beim passiven und aktiven Personalitätsprinzip bestehen keine Besonderheiten im Zusammenhang mit Metacrimes. Maßgeblich ist die Staatsan-

137 Popp/Keshelava, Art. 7 StGB N. 2.

138 Vgl. Schmoller, S. 88; a.A. Grzywotz, S. 131 ff., die Lösungswege über das Strafanwendungsrecht und bi- oder multilaterale Abkommen vorschlägt, um den (dezentralen) Erfolgsort einzuschränken.

gehörigkeit des hinter dem Avatar stehenden Menschen. Jedoch bestehen (inter-)national auf materiellrechtlicher Ebene in Bezug auf Metacrimes noch viele ungeklärte Fragen, was die Funktion als Auffangprinzip derzeit noch einschränken dürfte.

Zusammenfassend wurde im vorliegenden Beitrag anhand des fiktiven Fallbeispiels aufgezeigt, dass die im vordigitalen Zeitalter verankerten Bestimmungen des schweizerischen Strafanwendungsrechts in Art. 3 ff. schwStGB grundsätzlich auch Betrugsfälle im Metaverse räumlich zu erfassen vermögen. Die (theoretische) Bestimmung des Handlungs- und Erfolgsortes erweist sich damit im Metaverse unproblematisch bzw. nicht problematischer als bisher. Sie verstärkt allerdings ein bereits bestehendes Problem, nämlich die Überlastung der Strafverfolgungsbehörden.[139]

II. Ausblick

Diese Arbeit beschränkte sich auf Fragen im Zusammenhang mit dem Schweizer Strafanwendungsrecht. Spannend bleibt die effektive Verfolgung von Metacrimes und damit die Durchsetzung des Schweizer Strafrechts. In diesem Zusammenhang ist fraglich, ob die Schweizer Strafverfolgungsbehörden mit den gegenwärtigen Rechtsgrundlagen, technischen Ressourcen und Fachkenntnissen für die Ermittlung und die Verfolgung im Metaverse gerüstet sind. Auch hinsichtlich des materiellen Strafrechts stellen sich viele interessante Fragen. Offensichtlich können Handlungen eines Avatars nicht ohne Weiteres mit den entsprechenden Handlungen in der analogen Welt gleichgesetzt werden. So führt ein Faustschlag eines Avatars gegen einen anderen Avatar zu keiner körperlichen Beeinträchtigung des dahinterstehenden Menschen.[140] Das Metaverse wird sodann neue ‹Delikte› zum Vorschein bringen (z.B. die Tötung eines Avatars oder der virtuelle Hausfriedensbruch).[141] In diesem Zusammenhang muss (inter-)national über die Notwendigkeit der Anerkennung neuer Rechtsgüter und Strafnormen nachgedacht werden. Dabei ist zu beachten, dass Nutzende mit ihrer Registrierung bei der konkreten Metaverse-Plattform in bestimmte Handlungen ‹einwilligen›. In einer virtuellen Welt, in der es gerade das Ziel ist, gegenseitig Avatare zu ‹töten›, muss die Frage nach der Strafbarkeit unter-

139 Gerny.
140 Zum Ganzen Klaas/Klose, N. 3 f.
141 Vgl. Oberlin/von Hoyningen-Huene, S. 119.

schiedlich beantwortet werden als in einer sozialen Welt wie z.B. Decentraland.[142]

Auch im Zusammenhang mit dem Konzept des Avatars gibt es auf (inter-)nationaler Ebene noch viele Fragen zu klären. In der Literatur finden sich bereits mehrere Ansätze für die rechtliche Einordnung des Avatars. Diese reichen von der Qualifikation als bloßes Werkzeug oder Stellvertreter der steuernden Person bis hin zur Anerkennung einer eigenständigen Rechtspersönlichkeit.[143] Insbesondere im Zusammenhang mit der Möglichkeit KI im Metaverse einzusetzen, müssen grundlegende Entscheidungen getroffen werden. Können KI-Avatare, die aus Erfahrungen lernen und autonom entscheiden, im strafrechtlichen Sinne handeln?[144]

Das Metaverse ist keinesfalls bloß ein Hype oder eine Fantasie aus einem Science-Fiction Roman. Eine frühzeitige Auseinandersetzung mit den tatsächlichen und rechtlichen Herausforderungen einer solch mächtigen Technologie ist notwendig, um dem ihr inhärenten Bedrohungspotenzial adäquat zu begegnen. Es muss untersucht werden, an welchen Stellen Anpassungen des nationalen Straf- und Strafprozessrechts vorgenommen werden müssen. Angesichts der Tatsache, dass Metacrimes nicht zwingend, aber regelmäßig über die Landesgrenzen hinweg begangen werden, muss über die Notwendigkeit internationaler Übereinkommen zur Harmonisierung der Gesetzeslage nachgedacht werden, um eine effektive Strafverfolgung im Metaverse zu ermöglichen.[145] Gleichzeitig müssen die (straf-)rechtlichen Rahmenbedingungen so ausgestaltet werden, dass die wirtschaftlichen und gesellschaftlichen Chancen, die das Metaverse zweifellos bietet, nicht untergraben werden.

Literatur – und Materialenverzeichnis

Annison Tara, The Future of Financial Crime in the Metaverse, Fighting Crypto-crime in Web3.0, Elliptic Metaverse Report 2022, https://www.elliptic.co/hubfs/Crime%20in%20the%20Metaverse%202022%20final.pdf, besucht am 31.12.2024.

Aref Magda/Fábián Luca/Weber Simon, Digitale Originale dank NFTs?, GesKR 2021, S. 385–399.

Bartetzko Urs, Kommentierung zu Art. 32 StPO, in: Niggli Alexander Marcel/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung, Jugendstrafprozessordnung, 3. Aufl., Basel 2023.

142 M.w.H. Bosch, S. 231 ff.
143 Kozuka, S. 7 ff.; Whitepaper Interpol, S. 22.
144 M.w.H. Seher, S. 46 ff.
145 Vgl. Interpol Whitepaper, S. 23.

Bartle Richard A., Designing Virtual Worlds, San Francisco 2003.

Bijan Stephen, NFT mania is here, and so are the scammers, Artists are seeing their work showing up in NFTs they did not mint themselves, The Verge vom 20.3.2021, https://www.theverge.com/2021/3/20/22334527/nft-scams-artists-opensea-rarible-marble-cards-fraud-art, besucht am 31.12.2024.

Bericht des Bundesrates zu den rechtlichen Grundlagen für Distributed Ledger Technologie und Blockchain in der Schweiz vom 14.12.2018, abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/55150.pdf, besucht am 12.28.2024 (zit. Bericht Bundesrat DLT).

Bosch Sebastian, Straftaten in virtuellen Welten, Eine materiellrechtliche Untersuchung,
in: Heckmann Dirk (Hrsg.), Internetrecht und Digitale Gesellschaft, Band 14, Berlin 2018.

Botschaft zur Änderung des Schweizerischen Strafgesetzbuches (Allgemeine Bestimmungen, Einführung und Anwendung des Gesetzes) und des Militärstrafgesetzes sowie zu einem Bundesgesetz über das Jugendstrafrecht vom 21.9.1998, BBl. 1999 S. 1979 ff., abrufbar unter https://www.bj.admin.ch/bj/de/home/sicherheit/gesetzgebung/archiv/stgb-at.html, besucht am 12.28.2024 (zit. Botschaft Revision StGB).

Brameshuber Georg/Edelmann Barbara, Einführung, Krypto 1x1 für Strafrechtler,
in: Leitner Roman/Brandl Rainer (Hrsg.), Finanzstrafrecht 2022, Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht, Wien 2023, S. 1–12.

Broschart Jonas/Scheitanov Marc/Gieselmann Max, § 1 Definition und Bedeutung des «Metaverse», in: Steege Hans/Chibanguza Kuuya J. (Hrsg.), Metaverse, Rechtshandbuch, Baden-Baden 2023, S. 41–63.

Cassani Ursula, Die Anwendbarkeit des schweizerischen Strafrechts auf internationale Wirtschaftsdelikte (Art. 3–7 StGB), ZStrR 114 (1996), S. 237–262.

Camber Rebecca, Police investigating dozens of crimes as serious as rape and threats to kill in the metaverse, new figures show – amid warnings that virtual reality offences 'could become a major issue' for officers, mailonline vom 01.09.2024, https://www.dailymail.co.uk/news/article-13803125/Police-crimes-rape-kill-metaverse-new-figures-virtual-reality-crimes.html, besucht am 31.12.2024.

Da Silva Gioia/Alto Palo, Neuer Name, neue Strategie: Facebook heisst künftig Meta, NZZ online vom 28.10.2021, https://www.nzz.ch/technologie/neuer-name-der-facebook-konzern-heisst-kuenftig-meta-ld.1652470, besucht am 31.12.2024.

Donatsch Andreas, Kommentierung zu Art. 8 StGB, in: Donatsch Andreas (Hrsg.), StGB/JStG Kommentar, 21. Aufl., Zürich 2022 (zit. Donatsch, Art. 8).

Donatsch Andreas, Strafrecht III, Delikte gegen den Einzelnen, in: Jositsch Daniel (Hrsg.), Zürcher Grundrisse des Strafrechts, 11. Aufl., Zürich 2018 (zit. Donatsch, Strafrecht III).

Donatsch Andreas/Godenzi Gunhild/Tag Brigitte, Strafrecht I, Verbrecherlehre, in: Jositsch Daniel (Hrsg.), Zürcher Grundrisse des Strafrechts, 10. Aufl., Zürich 2022.

Eicker Andreas, Das Schweizerische Internationale Strafrecht vor und nach der Revision des Allgemeinen Teils des Strafgesetzbuchs – zur Interpretation des «engen Bezug» als verstecktes Opportunitätsprinzip, ZStrR 124 (2006), S. 295–320.

Europol, Policing in the Metaverse: what law enforcement needs to know, an observatory report from the Europol Innovation Lab, Luxemburg 2022, abrufbar unter: https://doi.org/10.2813/81062, besucht am 31.12.2024 (zit. Bericht Europol).

Fdhila Walid, Blockchain Security Risks, in: Kirchmayr-Schliesselberger Sabine/Klas Wolfgang/Miernicki Martin/Rinderle-Ma Stefanie/Weilinger Arhtur, (Hrsg.), Kryptowährungen, Krypto-Assets, ICOs und Blockchain, Recht – Technik – Wirtschaft, Wien 2019, S. 45–66.

Finixio (promoted), Die besten Metaverse Coins in der Übersicht, NZZ online vom 25.7.2022, https://www.nzz.ch/promoted-content/die-besten-metaverse-coins-in-der-uebersicht-ld.1694902, besucht am 31.12.2024 (zit. Übersicht Metaverse Coins).

Fromberger Mathias/Zimmermann Patrick, § 1 Technische und rechtstatsächliche Grundlagen, in: Maume Philipp/Maute Lena/Fromberger Mathias (Hrsg.), Rechtshandbuch Kryptowerte, München 2020, S. 1–31.

Funna Radia/Sey Araba, Considering online and offline implications in efforts to build confidence and security in the metaverse, Working Group 6: Security, Data & Personally identifiable information (PII) Protection, ITU Focus Group on metaverse, Technical Report 03 (2024), https://www.itu.int/en/ITU-T/focusgroups/mv/Documents/List%20of%20FG-MV%20deliverables/FGMV-23.pdf, besucht am 31.12.2024.

Geiger Alexandra/Keller Stefan, Kryptowährungen in der Nachlassplanung und -abwicklung, successio 2021, S. 259–271.

Gerny Daniel, Das sagt der Strafverteidiger Fingerhuth zur Überlastung der Justiz: «Wenn wir nicht bald etwas tun, wird die Lage unhaltbar», NZZ vom 12.10.2023.

Gless Sabine, Strafrechtsschutz für virtuelles Geld?, in: Jositsch Daniel/Schwarzenegger Christian/Wohlers Wolfgang (Hrsg.), Festschrift für Andreas Donatsch, Zürich 2017, S. 41–56 (Gless, Festschrift).

Gless Sabine, Internationales Strafrecht, 2. Aufl., Basel 2015 (zit. Gless, Internationales Strafrecht)

Gless Sabine/Kugler Peter/Stagno Dario, Was ist Geld? Und warum schützt man es?, recht 2015, S. 82–97.

Graf Damian K., § 26 Cyber Economic Crimes, in: Ackermann Jürg-Beat/Heine Günter (Hrsg.), Wirtschaftsstrafrecht der Schweiz, Hand- und Studienbuch, 2. Aufl., Bern 2021,
S. 1015–1033.

Grasnick Armin, Digitale Avatare = humanoide Phantome?, Wirtschaftsinformatik & Management 6 (2022), S. 352–360.

Grzywotz Johanna, Virtuelle Kryptowährungen und Geldwäsche, in: Heckmann Dirk (Hrsg.), Internetrecht und Digitale Gesellschaft, Band 15, Berlin 2018.

Gyr Eleonor, Blockchain und Smart Contracts, Die vertragsrechtlichen Implikationen einer neuen Technologie, Basel 2019.

Hainzl Florian, Metaverse: Kommt mit der Apple Vision Pro der Durchbruch?, extraETF vom 22.2.2024, https://extraetf.com/de/news/etfs-im-fokus/metaverse-kommt-mit-der-apple-vision-pro-der-durchbruch, besucht am 31.12.2024..

Heimgartner Stefan, Die internationale Dimension von Internetstraffällen, Strafhoheit und internationale Rechtshilfe in Strafsachen, in: Schwarzenegger Christian/Arter Oliver/Jörg Florian S. (Hrsg.), Internet und Strafrecht, 4. Band, Bern 2005, S. 117–150.

Huynh-The Thien et al., Blockchain for the metaverse: A Review, Future Generation Computer Systems, Elsevier 143 (2023), S. 401–419, https://doi.org/10.1016/j.future.2023.02.008

Interpol, Metaverse, A Law Enforcement Perspective, Use Cases, Crime, Forensics, Investigation, and Governance, White Paper, Januar 2024, abrufbar unter: https://www.interpol.int/News-and-Events/News/2024/Grooming-radicalization-and-cyber-attacks-INTERPOL-warns-of-Metacrime, besucht am 31.12.2024 (zit. Whitepaper Interpol).

Kappeler Anna, Avatar von britischem Mädchen wird vergewaltigt – auch in der Schweiz möglich, watson vom 22.1.2024, https://www.watson.ch/digital/schweiz/952001826-avatar-von-maedchen-wird-vergewaltigt-auch-in-der-schweiz-moeglich, besucht am 31.12.2024.

Kettemann Matthias C./Böck Caroline, § 6 Regulierung des Metaverse, in: Steege Hans/Chibanguza Kuuya J. (Hrsg.), Metaverse, Rechtshandbuch, Baden-Baden 2023,
S. 113–134.

Klaas Arne/Klose Kathrin, § 32 Strafrechtliche Verantwortlichkeit, in: Steege Hans/Chibanguza Kuuya J. (Hrsg.), Metaverse, Rechtshandbuch, Baden-Baden 2023,
S. 531–559..

Klose Sonja/Kreutzer Ralf T., Metaverse – Technologien, Infrastruktur und Use Case, in: Schuster Gabriele/Wecke Bernhard (Hrsg.), Marketingtechnologien, Innovative Unternehmenspraxis: Insights, Strategien und Impulse, Wiesbaden 2023, S. 45–59.

Kozuka Souichirou, The avatar law and (cyber) transnational contracts, Uniform Law Review 2024, S. 1–12, https://doi.org/10.1093/ulr/unae008

Krebs Cindy/Rüdiger Thomas-Gabriel, Gamecrime und Metacrime, Strafrechtlich relevante Handlungen im Zusammenhang mit virtuellen Welten, Frankfurt a.M. 2010.

Li Cathy, Headset competition heats up, industrial metaverse 'exceeding expectations', and other metaverse stories you need to read, World Economic Forum, Global Future Council on the Future of Metaverse vom 3.7.2023, https://www.weforum.org/agenda/2023/07/headset-competition-industrial-metaverse-exceeding-expectations-and-other-metaverse-stories-you-need-to-read/, besucht am 31.12.2024.

Ludwiczak Maria, Une compétence pénale fondée sur le critère du domicile : analyse de lege lata et réflexions de lege ferenda, ZSR 136 (2017) I, S. 5–30.

Madiega Tambiama/Car Polona/Niestadt Maria/Van de Pol Louise, Metaverse, Opportunities, risks and policy implications, EPRS, Juni 2022, https://www.europarl.europa.eu/cmsdata/268589/eprs-briefing-metaverse_EN.pdf, besucht am 31.12.2024.

Maeder Stefan/Niggli Marcel Alexander, Kommentierung zu Art. 146 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht, Strafgesetzbuch/Jugendstrafgesetz, 4. Aufl., Basel 2019.

Maute Lena, § 6 Verträge über Kryptotoken, in: Maume Philipp/Maute Lena/Fromberger Mathias (Hrsg.), Rechtshandbuch Kryptowerte, München 2020, S. 138–196.

Menn Andreas, Im Metaverse scheint langsam wieder Licht, WirtschaftsWoche vom 2.2.2024, https://www.wiwo.de/technologie/digitale-welt/virtual-reality-im-metaverse-scheint-langsam-wieder-licht/29635038.html, besucht am 31.12.2024.

Meyer Stephan Dominik, Rechte an und aus Blockchain-basierten Crypto Tokens, Zürcher Studien zum Privatrecht, Zürich et al. 2022.

Müllender Moritz, Übergriffe im Metaverse, «Zieh doch einfach die Brille ab», In mehreren Berichten erzählen Betroffene von sexualisierter Gewalt im Metaverse. Doch die aktuelle Rechtslage schützt Betroffene kaum, taz vom 2.2.2024, https://taz.de/Uebergriffe-im-Metaverse/!5987684/, besucht am 18.12.2024.

Müller Lukas/Ong Malik, Aktuelles zum Recht der Kryptowährungen, AJP 2020, S. 198–212.

Nida-Rümelin Julian/Weidenfeld Nathalie, § 3 Metaverse – sein ontologischer und ethischer Status, in: Steege Hans/Chibanguza Kuuya J. (Hrsg.), Metaverse, Rechtshandbuch, Baden-Baden 2023, S. 79–86.

Oberlin Jutta Sonja/von Hoyningen-Huene Sarah, Strafrecht im Metaverse: Den Verbrechen der Zukunft auf der Spur, forumpoenale 2 (2024), S. 116–123.

Ordano Esteban/Jardi Yemel/Meilich Ariel/Araoz Manuel, Decentraland, White paper, https://decentraland.org/whitepaper.pdf, besucht am 31.12.2024.

Payer Andrés, Territorialität und grenzüberschreitende Tatbeteiligung, in: Bommer Felix/Fiolka Gerhard/Gless Sabine/Meyer Frank/Vest Hans (Hrsg.), International Criminal Law, Völkerstrafrecht und internationales Strafrecht, Band 8, Zürich 2021.

Pentsy Thomas, Citi: Bis zu fünf Milliarden Metaverse-User in zehn Jahren, finews vom 1.4.2022, https://www.finews.ch/news/finanzplatz/50876-citi-metaverse-13-billionen-user-nutzer-goldman-sachs, besucht am 31.12.2024.

Peterson Christoph, Die Top 7 Metaverse NFTs im Vergleich: So funktioniert das Metaverse NFT kaufen, Coincierge vom 2.11.2023, https://coincierge.de/nft/metaverse-nft/, besucht am 31.12.2024.

Popp Peter/Keshelava Tornike, Kommentierung zu Art. 7 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht, Strafgesetzbuch/Jugendstrafgesetz, 4. Aufl., Basel 2019 (zit. Popp/Keshelava, Art. 7).

Popp Peter/Keshelava Tornike, Kommentierung zu Art. 8 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht, Strafgesetzbuch/Jugendstrafgesetz, 4. Aufl., Basel 2019 (zit. Popp/Keshelava, Art. 8).

Popp Peter/Keshelava Tornike, Kommentierung zu vor Art. 3 StGB, in: Niggli Marcel Alexander/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Strafrecht, Strafgesetzbuch/Jugendstrafgesetz, 4. Aufl., Basel 2019 (zit. Popp/Keshelava, vor Art. 3).

Reischl Marcus/Stilz Moritz, § 5 Compliance & Investigations, in: Wagner Eric/Holm-Hadulla Moritz/Ruttloff Marc (Hrsg.), Metaverse und Recht, München 2023, S. 81–103.

Ritterbusch Georg David/Teichmann Malte Rolf, Defining the Metaverse: A Systematic Literature Review, IEEE Access, 11 (2023), S. 12368–12377, https://doi.org/10.1109/ACCESS.2023.3241809, besucht am 9.4.2024.

Ronc Pascal/Schuppli Benedikt, Kryptowährungen im Lichte der schweizerischen Geldwäschereigesetzgebung, forumpoenale 6 (2018), S. 529–535.

Rückert Christian, § 20 Phänomenologie, in: Maume Philipp/Maute Lena/Fromberger Mathias (Hrsg.), Rechtshandbuch Kryptowerte, München 2020, S. 527–546 (zit. Rückert, Phänomenologie).

Rückert Christian, § 21 Strafanwendungsrecht, in: Maume Philipp/Maute Lena/Fromberger Mathias (Hrsg.), Rechtshandbuch Kryptowerte, München 2020, S. 537–546 (zit. Rückert, Strafanwendungsrecht).

Sales Nancy Jo, A girl was allegedly raped in the metaverse, Is this the beginning of a dark new future?, The Guardian vom 5.1.2024, https://www.theguardian.com/commentisfree/2024/jan/05/metaverse-sexual-assault-vr-game-online-safety-meta, besucht am 31.12.2024.

Schmidt Jan/Dreyer Stephan/Lampert Claudia, Spielen im Netz, Zur Systematisierung des Phänomens «Online-Games», Arbeitspapiere des Hans-Bredow-Instituts, Nr. 19, Hamburg 2008, https://doi.org/10.21241/ssoar.71699

Schmoller Kurt, Kryptowährungen/-Assets – wann ist österreichisches Strafrecht anwendbar?, in: Leitner Roman/Brandl Rainer (Hrsg.), Finanzstrafrecht 2022, Virtuelle Währungen und Kryptoassets im Steuer(straf)recht und Strafrecht, S. 73–94.

Schöbel Sofia Marlena/Leimeister Jan Marco, Metaverse platform ecosystems, Electronic Marktes 33:12 (2023), https://doi.org/10.1007/s12525-023-00623-w

Schwarzenegger Christian, E-Commerce – Die strafrechtliche Dimension, in: Arter Oliver/Jörg Florian S. (Hrsg.). Internet-Recht und Electronic Commerce Law, 1. Band,
Schwyz et al. 2001, S. 329–375 (zit. Schwarzenegger, E-Commerce).

Schwarzenegger Christian, Handlungs- und Erfolgsort beim grenzüberschreitenden Betrug, in: Ackermann Jürg-Beat/Donatsch Andreas/Rehberg Jörg (Hrsg.), Wirtschaft und Strafrecht, Festschrift für Niklaus Schmid zum 65. Geburtstag, Zürich 2001, S. 143–159
(zit. Schwarzenegger, Betrug).

Schwarzenegger Christian, Der räumliche Geltungsbereich des Strafrechts im Internet, Die Verfolgung von grenzüberschreitender Internetkriminalität in der Schweiz im Vergleich mit Deutschland und Österreich, ZStrR 118 (2000), S. 109–130 (zit. Schwarzenegger, Geltungsbereich).

Seher Gerhard, Intelligente Agenten als «Personen» im Strafrecht?, in: Gless Sabine/Seelmann Kurt (Hrsg.), Intelligente Agenten und das Recht, Baden-Baden 2016, S. 45–60, https://doi.org/10.5771/9783845280066

Sevtap Ünal/Tevfik Dalgic/Ezgi Akar, Avatars as the Virtual World's Personality, in: Basar Enes Emre/Ercis Aysel/Sevtap Ünal, The Virtual World and Marketing, Newcastle 2018, S. 33–53.

Shirin Jennifer/Wenz Daniel, Metaverse Coins: 10 NFT Projekte mit Potenzial, Bitcoin2Go vom 1.3.2024, https://bitcoin-2go.de/die-besten-metaverse-coins-2023/, besucht am 31.12.2024.

Sievi Nino, Kommentierung zu Art. 89 SchKG, in: Staehelin Daniel/Bauer Thomas/Lorandi Franco (Hrsg.), Basler Kommentar, Bundesgesetz über Schuldbetreibung und Konkurs,
3. Aufl., Basel 2021.

Simmler Monika/Selman Sine/Burgermeister Daniel, Beschlagnahme von Kryptowährungen im Strafverfahren, AJP 2018, S. 963–978.

Staffler Lukas, Reichweite und Grenzen der Sachverhaltswürdigung im Auslieferungsverfahren bei Unterstützung terroristischer Organisationen, forumpoenale 2 (2021), S. 149–155.

Stratenwerth Günter/Bommer Felix, Schweizerisches Strafrecht, Besonderer Teil I: Straftaten gegen Individualinteressen, 8. Aufl., Bern 2022.

Takyar Akash, Metaverse and Smart Contracts, LeewayHertz, https://www.leewayhertz.com/metaverse-and-smart-contracts/, besucht am 31.12.2024.

Tanner Gabrielle, Peer-to-Peer platforms in the metaverse, wiggin vom 24.5.2023, https://www.wiggin.co.uk/insight/peer-to-peer-platforms-in-the-metaverse/#_ftnref2, besucht am 31.12.2024.

Trechsel Stefan/Crameri Dean, Kommentierung zu Art. 146 StGB, in: Trechsel Stefan/Pieth Mark (Hrgs.), Praxiskommentar, Schweizerisches Strafgesetzbuch, 4. Aufl., Zürich 2021.

Trechsel Stefan/Vest Hans, Kommentierung zu Art. 7 StGB, in: Trechsel Stefan/Pieth Mark (Hrgs.), Schweizerisches Strafgesetzbuch, Praxiskommentar, 4. Aufl., Zürich 2021
(zit. Trechsel/Vest, Art. 7).

Trechsel Stefan/Vest Hans, Kommentierung zu vor Art. 3 StGB, in: Trechsel Stefan/Pieth Mark (Hrgs.), Praxiskommentar, Schweizerisches Strafgesetzbuch, 4. Aufl., Zürich 2021 (zit. Trechsel/Vest, vor Art. 3).

Tümmler Jörn, Avatare in Echtzeitsimulationen, Kassel 2007.

Vest Hans, § 13 Allgemeine Vermögensdelikte, in: Ackermann Jürg-Beat/Heine Günter (Hrsg.), Wirtschaftsstrafrecht der Schweiz, Hand- und Studienbuch, 2. Aufl., Bern 2021,
S. 313–421.

Wagner Eric/Holm-Hadulla Moritz/Ruttloff Marc (Hrsg.), Metaverse und Recht, München 2023

Weissenberger Philippe, Zum Begehungsort bei Internet-Delikten, ZBJV 135 (1999), S. 703–706.

Wicki-Birchler David, NFT und Metaverse: Ausgewählte Aspekte im Schweizer Recht, Jusletter IT vom 31.5.2022.

Willems Marion, Funktionsweise und Risiken von virtuellen Währungen, CB 9 (2016), S. 325–328.

Wohlers Wolfgang, Kommentierung zu Art. 7 StGB, in: Wohlers Wolfgang/Godenzi Gunhild/Schlegel Stephan, Schweizerisches Strafgesetzbuch, Handkommentar, 4. Aufl., Bern 2020 (zit. Wohlers, Art. 7).

Wohlers Wolfgang, Kommentierung zu Art. 8 StGB, in: Wohlers Wolfgang/Godenzi Gunhild/Schlegel Stephan, Schweizerisches Strafgesetzbuch, Handkommentar, 4. Aufl., Bern 2020 (zit. Wohlers, Art. 8).

Wohlers Wolfgang, Kommentierung zu Vorbemerkungen zu den Art. 10 ff, in: Wohlers Wolfgang/Godenzi Gunhild/Schlegel Stephan, Schweizerisches Strafgesetzbuch, Handkommentar, 4. Aufl., Bern 2020 (zit. Wohlers, Vorbemerkungen zu den Art. 10 ff.).

Zogg Samuel, Zwangsvollstreckungsrechtliche Behandlung von Kryptowährungen, recht 2020, S. 1–23.