

Quelle: <https://voris.wolterskluwer-online.de/document/fe688c7b-8dd0-4c79-a1f8-646aa9473b27>

Bibliografie

Gericht	OLG Braunschweig
Datum	18.09.2024
Aktenzeichen	1 Ws 185/24
Entscheidungsform	Beschluss
Referenz	WKRS 2024, 32930
Entscheidungsname	[keine Angabe]
ECLI	ECLI:DE:OLGBS:2024:0918.1WS185.24.00

Oberlandesgericht Braunschweig

Beschl. v. 18.09.2024, Az.: 1 Ws 185/24

Anfangsverdacht für eine strafbare Handlung eines Beschuldigten als Voraussetzung für die Anordnung des Vermögensarrestes zur Sicherung der Wertersatzentziehung (hier: sog. Kryptodiebstahl)

Amtlicher Leitsatz

1. **Greift ein Beschuldigter unter Nutzung der zutreffenden und nicht in rechtswidriger Weise erlangten - sondern ihm schlicht schon bekannten - Passwörter auf die Wallet eines Dritten zu, liegt hierin kein Überwinden der besonderen Zugangssicherung i. S. d. § 202a Abs. 1 StGB.**
2. **Die Veranlassung einer Transaktion enthält in dezentralen Blockchain-Netzwerken nicht die Miterklärung einer echten Berechtigung hierzu. Es fehlt daher an einem - für § 263a StGB erforderlichen - täuschungsäquivalenten Datengebrauch.**
3. **§ 303a Abs. 1 StGB ist nicht erfüllt, wenn lediglich eine Verletzung von Interessen des vom Inhalt der Daten Betroffenen vorliegt. Denn strafwürdiges Unrecht liegt nur dann vor, wenn ein anderer als der Täter von der Tathandlung betroffen ist, mithin eine fremde Rechtsposition verletzt wird.**
4. **Die Protokollierung einer Transaktion in der Blockchain und die damit verbundene datenmäßige Veränderung der Zuordnung der Kryptowerte beinhaltet zwar eine Veränderung - und zugleich auch ein teilweises Unbrauchbarmachen - von Daten i. S. d. § 303a Abs. 1 StGB; diese Datenveränderung wird aber durch die Netzwerk-Betreiber und damit durch die diesbezüglich Verfügungsberechtigten selbst vorgenommen.**

In dem Ermittlungsverfahren

**gegen
W**

Verteidigerin:

Rechtsanwältin N

wegen Ausspähens von Daten u.a.

hier: weitere Beschwerde der Staatsanwaltschaft gegen die Aufhebung des Vermögensarrestes
hat der 1. Strafsenat des Oberlandesgerichts Braunschweig
am **18. September 2024** beschlossen:

© 2026 Wolters Kluwer Deutschland GmbH

Tenor:

Die weitere Beschwerde der Staatsanwaltschaft Göttingen gegen den Beschluss des Landgerichts Göttingen vom 31. Mai 2024 wird als unbegründet verworfen.

Die Kosten des Beschwerdeverfahrens fallen der Staatskasse zur Last, die auch die dem Beschuldigten entstandenen notwendigen Auslagen zu tragen hat.

Gründe

Das Rechtsmittel der Staatsanwaltschaft hat keinen Erfolg. Das Landgericht hat den Vermögensarrest mit Recht aufgehoben, denn es liegt kein Anfangsverdacht für eine strafbare Handlung des Beschwerdegegners vor.

I.

Die Staatsanwaltschaft Göttingen führt gegen den Beschwerdegegner (im Folgenden auch: den Beschuldigten) ein Ermittlungsverfahren wegen des Tatvorwurfs des Ausspähens von Daten.

1.

Auf der Grundlage einer Strafanzeige - nebst Strafantrags - des Zeugen A. vom 15. Dezember 2023 sowie den Bekundungen des Anzeigerstatters und der Zeugen B. und C. legt die Staatsanwaltschaft dem Beschuldigten nach derzeitigem Ermittlungsstand zur Last, dieser habe am 11. November 2023 zwischen 23:34 und 23:45 Uhr von einer Krypto-Wallet, die er im Auftrag des Zeugen A. für diesen eingerichtet hatte, 24.973.001 "A-Coins" mit einem zu diesem Zeitpunkt bestehenden Marktwert in Höhe von je 0,10 € - mithin insgesamt 2.497.300,10 € - auf zwei nicht unter der Kontrolle des Zeugen A. stehende Wallets transferiert. Dabei habe er den zutreffenden öffentlichen und auch den zutreffenden privaten Schlüssel des Zeugen A. - auf welchen der Beschuldigte durch Eingabe von 24 Sicherheitspasswörtern, die er bei der Erstellung des Wallets vergeben und absprachewidrig behalten habe, zugegriffen habe - verwendet. Gegenüber dem Zeugen A. habe der Beschuldigte zuvor wahrheitswidrig behauptet gehabt, er verfüge nicht mehr über die Passwörter. Zu den Transfers sei er vom Zeugen A. nicht ermächtigt gewesen. Durch die Transfers seien die Kryptowerte ("A-Coins") der Kontrolle und Verfügungsmöglichkeit des Zeugen A. entzogen worden.

Dem vorstehenden - mutmaßlichen - Geschehen ist Folgendes vorausgegangen:

(...)

Mit der Firma D. AG (...) vereinbarte der Anzeigerstatter am 3. Januar 2022, einen (...) digitalen Zahlungs-Token ("A-Coin") zu entwickeln und öffentlich zu vermarkten. Die insgesamt geschaffenen 440.000.000 A-Coins wurden größtenteils verkauft. Der Anzeigerstatter besaß bis zum 11. November 2023 24.973.001 A-Coins, welche über seine Wallet auf 11 Konten verwahrt wurden.

2.

Auf Antrag der Staatsanwaltschaft ordnete das Amtsgericht Göttingen mit Beschluss vom 15. Februar 2024 (Bl. 95-96 d.A.) zur Sicherung der Einziehung des Wertes der Taterträge den Vermögensarrest in Höhe von 2.497.300,10 € in das Vermögen des Beschuldigten an.

Am 16. Februar 2024 erfolgte aufgrund richterlicher Anordnung eine Durchsuchung beim Beschuldigten, in deren Rahmen auch verschiedene Hardware Wallets sowie Recovery Seeds (Wiederherstellungsphrasen) aufgefunden wurde. Die weiteren polizeilichen Ermittlungen ergaben, dass die beim Beschuldigten aufgefundenen Hardware Wallets mit individuell eingerichteten Ethereum Wallets bestückt waren. Diese sind zugehörig zu den aufgefundenen Recovery Seeds, stehen oder standen indes nicht in direkter Verbindung zu den "entwendeten" A.-Coins (Bl. 160 d. A.).

Zur Abwendung der Vollziehung des Arrestes hinterlegte der Beschuldigte auf einer vom Landeskriminalamt Niedersachsen bereitgestellten Behördenwallet insgesamt 25.000.000 A-Coins (...).

Mit Schriftsatz seiner Verteidigerin vom 3. Mai 2024 (Bl. 164 ff. d. A.) erhob der Beschuldigte Beschwerde gegen die mit Beschluss vom 15. Februar 2024 erfolgte Arrestanordnung des Amtsgerichts Göttingen und beantragte zugleich, die derzeit in der Verwahrung des Landeskriminalamtes Niedersachsen befindlichen 25.000.000 A-Coins an ihn zu transferieren. Zur Begründung führte die Verteidigerin aus, der dem Beschuldigten zur Last gelegte Sachverhalt erfülle bereits nicht den Tatbestand des § 202a StGB. Darüber hinaus bestreite der Beschuldigte den Tatvorwurf; durch die Ergebnisse der polizeilichen Ermittlungen sei die Behauptung des Anzeigerstatters widerlegt, der Beschuldigte sei Inhaber der zwei Empfänger-Wallets.

Das Amtsgericht half der Beschwerde nicht ab (Bl. 175 d.A.).

Mit Beschluss vom 31. Mai 2024 (Bl. 178-182 d.A.), auf dessen Gründe verwiesen wird, hat das Landgericht Göttingen den Arrestbeschluss des Amtsgerichts Göttingen vom 15. Februar 2024 aufgehoben. Zur Begründung hat die Kammer ausgeführt, es liege kein die Anordnung des Vermögensarrestes begründender Anfangsverdacht einer strafbaren Handlung gegen den Beschuldigten vor.

Hiergegen wendet sich die Staatsanwaltschaft Göttingen mit ihrer durch Verfügung vom 5. Juni 2024 angebrachten (weiteren) Beschwerde, welche sie unter dem 11. Juni 2024 (Bl. 191 f. d.A.) begründet hat. Die Staatsanwaltschaft ist der Auffassung, es bestehe ein Anfangsverdacht für eine Straftat nach § 202a StGB; daneben komme auch eine Strafbarkeit gemäß § 303a StGB in Betracht, weil die Kryptowerte abgrenzbare Teile der Etherbasierten Blockchain darstellen "dürften". In der nicht nur vorübergehenden Entziehung des Zugriffs des Berechtigten liege ein Unterdrücken von Daten.

Das Landgericht hat am 13. Juni 2024 beschlossen, der weiteren Beschwerde nicht abzuweichen und die Sache dem Oberlandesgericht zur Entscheidung vorgelegt (Bl. 193 d.A.).

Die Generalstaatsanwaltschaft unterstützt das Rechtsmittel der Staatsanwaltschaft Göttingen. Sie hat beantragt, den Beschluss des Landgerichts Göttingen vom 31. Mai 2024 auf die weitere Beschwerde der Staatsanwaltschaft Göttingen vom 5. Juni 2024 mit der Maßgabe aufzuheben, dass der Vermögensarrest in Höhe von 2.347.462,09 € in das bewegliche und unbewegliche Vermögen des Beschuldigten angeordnet wird.

Der Beschuldigte verteidigt die angefochtene Entscheidung. Mit Schriftsatz seiner Verteidigerin vom 19. Juli 2024 (Bl. 213 ff. d.A.), auf den wegen der Einzelheiten Bezug genommen wird, hat er beantragt, die weitere Beschwerde der Staatsanwaltschaft Göttingen als unbegründet zu verwerfen. Er bestreitet weiterhin den Tatvorwurf bereits in tatsächlicher Hinsicht und hält das ihm zur Last gelegte Verhalten im Übrigen auch nach wie vor für nicht strafbar.

Die Generalstaatsanwaltschaft hat unter dem 25. Juli 2024 ihr Beschwerdevorbringen ergänzt.

Der Beschuldigte hat mit Schriftsatz seiner Verteidigerin vom 31. Juli 2024 (Bl. 243 f. d.A.) weiter vorgetragen.

Nach Erteilung eines Hinweises durch den Senat haben die Generalstaatsanwaltschaft unter dem 5. September 2024 und die Verteidigerin unter dem 9. September 2024 jeweils nochmals ergänzend Stellung genommen.

II.

Die weitere Beschwerde der Staatsanwaltschaft ist gemäß § 310 Abs. 1 Nr. 3 StPO statthaft und auch ansonsten zulässig; in der Sache hat sie indes keinen Erfolg.

Das Landgericht hat den Arrestbeschluss mit Recht aufgehoben. Die Voraussetzungen für die Anordnung des Vermögensarrestes zur Sicherung der Wertersatzentziehung gemäß § 111e Abs. 1, Abs. 4, 111j Abs. 1 StPO i. V. m. §§ 73 Abs. 1, 73c, 73d StGB liegen nicht vor, denn es besteht kein Anfangsverdacht für eine strafbare Handlung des Beschuldigten.

1.

Das dem Beschuldigten vorgeworfene Verhalten erfüllt nicht den Tatbestand des § 202a StGB (Ausspähen von Daten).

Richtig ist zwar, dass die Daten des Anzeigerstatters A. auf seiner Wallet durch eine besondere Zugangssicherung i. S. d. § 202a Abs. 1 StGB geschützt waren. Diese wurde durch den Beschuldigten - seine Tatbegehung vorausgesetzt - indes nicht überwunden.

a.

Die Sicherung des Zugangs zu der Wallet des Zeugen A. durch (hier: 24) Passwörter ist eine besondere Zugangssicherung i. S. d. § 202a Abs. 1 StGB. Dass diese gegenüber dem Beschuldigten aufgrund dessen - etwaiger - Kenntnis von den von ihm eingerichteten Passwörtern keine Wirksamkeit entfaltete, ist insoweit unschädlich. Denn für das Vorliegen einer Zugangssicherung ist es nicht erforderlich, dass die Sicherung gerade gegenüber dem Täter wirkt. Vielmehr ist auf die allgemeine Sicherung der Daten gegenüber dem Zugriff Unbefugter abzustellen, nicht darauf, ob Eingeweihte oder Experten leicht auf die Daten zugreifen können (

BGH, Beschluss vom 13. Mai 2020 - 5 StR 614/19, Rn. 21, juris).

b.

Durch die - mutmaßliche - Nutzung der zutreffenden Passwörter für den Zugriff auf die Wallet des Zeugen A. - und damit auf dessen privaten kryptographischen Schlüssel - hat der Beschuldigte die besondere Zugangssicherung aber nicht i. S. d. § 202a Abs. 1 StGB überwunden.

aa)

Unter Überwinden der Zugangssicherung i.S.v. § 202a StGB ist diejenige Handlung zu verstehen, die geeignet ist, die jeweilige Sicherung auszuschalten oder zu umgehen. Auch wenn eine Zugangssicherung aufgrund besonderer Kenntnisse, Fähigkeiten oder Möglichkeiten schnell und ohne besonderen Aufwand überwunden wird, ist der Tatbestand erfüllt. Für das geschützte Rechtsgut - das formelle Geheimhaltungsinteresse des Verfügungsberechtigten - ist es unerheblich, ob die Sicherung von Daten vor unberechtigtem Zugang schnell oder langsam, mit viel oder wenig Aufwand überwunden wird. Der Gesetzgeber wollte aus dem Tatbestand neben Bagatelldaten lediglich solche Fälle ausschließen, in denen die Durchbrechung des Schutzes für jedermann ohne weiteres möglich ist, nicht aber solche, in denen die Zugangssicherung aufgrund spezieller Kenntnisse oder Möglichkeiten im Einzelfall leicht überwunden wird (

BGH, Beschluss vom 13. Mai 2020 - 5 StR 614/19, Rn. 24, juris).

In dem Überwinden der besonderen Sicherung gegen unberechtigten Zugang liegt nach dem Willen des Gesetzgebers gerade die strafwürdige kriminelle Energie, die sanktioniert werden soll (BT-Drs. 16/3656, S. 10; Hilgendorf in: Leipziger Kommentar zum StGB, 73. Aufl., § 202a, Rn. 29). Ausgegrenzt werden sollen Handlungen, bei denen die besonders gesicherten Daten auf andere Weise als durch Überwinden erlangt werden (BT-Drs. 16/3656, S. 10).

bb)

Gemessen an diesem Maßstab erfüllt das dem Beschuldigten zur Last gelegte Verhalten nicht das Tatbestandsmerkmal der *Überwindung* der besonderen Zugangssicherung. Denn der Beschuldigte soll den Passwortschutz gerade nicht umgangen oder ausgeschaltet, sondern vielmehr die ihm bereits bekannten Passwörter in der vorgesehenen Art und Weise verwendet haben.

Damit liegt der Fall - entgegen der Auffassung der Staatsanwaltschaft - auch entscheidend anders als in der

Entscheidung des Bundesgerichtshofs vom 13. Mai 2020 (5 StR 614/19, juris): In dem dort zu beurteilenden Fall hatte der Administrator den Passwortschutz der persönlichen E-Mail-Accounts nämlich - wenn auch nur mit wenigen "Maus-Clicks" - dadurch *umgangen*, dass er sich als Administrator in verbotener Weise und unter Manipulation des Ordners "Zugriffsberechtigung" den Zugriff auf die E-Mail-Daten der Behördenmitarbeitenden verschaffte (BGH, a.a.O., Rn. 8, 25; Hervorhebung durch den Senat). Durch diese widerrechtliche Verhaltensweise war es dem besagten Administrator möglich, auf die passwortgeschützten E-Mail-Accounts der Mitarbeitenden zuzugreifen, ohne deren Passwörter eingeben zu müssen, mithin, den Passwortschutz zu umgehen. Diese Zugangsart wollte der Verfügungsberechtigte in jenem Fall erkennbar durch die klare Beschränkung der Administratorenrechte und die Vorgabe eines bestimmten Prozederes beim Zugriff auf einen E-Mail-Account verhindern (BGH, Beschluss vom 13. Mai 2020 - 5 StR 614/19, Rn. 25, juris; Hervorhebung durch den Senat). Hiervon unterscheidet sich der vorliegende Fall maßgeblich. Denn der Beschuldigte hat - seine Täterschaft vorausgesetzt - vorliegend den Passwortschutz der Wallet des Anzeigeerstatters gerade nicht auf einem anderen (Zugangs-)Weg umgangen bzw. diesen ausgeschaltet; vielmehr soll er gerade (nur) "*seine nach wie vor bestehende Zugriffsmöglichkeit (...) ausgenutzt*" haben.

cc)

Die Systematik der §§ 202a bis 202c StGB zwingt nicht zu einer weiteren Auslegung des Tatbestandsmerkmals des *Überwindens* der Zugangssicherung dahingehend, dass auch jede Nutzung des zutreffenden Passwortes ein solches darstellt, soweit diese nur ohne entsprechende Befugnis erfolgt.

Richtig ist allerdings, dass § 202c Abs. 1 Nr. 1 StGB auch das Sicherverschaffen von Passwörtern als Vorbereitung des Ausspähens und Abfangens von Daten unter Strafe stellt. Deshalb ist es nach Überzeugung des Senates in der Tat schon aus systematischen Gründen nahezu zwingend, dass die Verwendung von zutreffenden Passwörtern das Tatbestandsmerkmal des *Überwindens* der besonderen Zugangssicherung erfüllt, wenn diese zuvor mit dem Vorsatz, eine Straftat nach § 202a StGB oder § 202b StGB zu begehen bzw. einem Dritten die Tatbegehung zu ermöglichen, durch eine der von § 202c Abs. 1 StGB bezeichneten Tathandlungen erlangt wurden. Weil die in derartigen Fällen entfalteten rechtswidrigen Aktivitäten zur Beschaffung des - zutreffenden - Passwortes grundsätzlich einen nicht unerheblichen zeitlichen und/oder technischen Aufwand erfordern, ist es zudem - über die systematischen Erwägungen hinaus - auch zutreffend, in derartigen Fällen eine *Überwindung* der Zugangssicherung anzunehmen.

Für die Auffassung, dass darüber hinaus auch die Verwendung des zutreffenden Passwortes, zu dessen Erlangung der Täter keinerlei rechtswidrige Aktivitäten entfaltet hat - weil es ihm schlicht schon bekannt ist - als Überwinden i. S. d. § 202a StGB zu bewerten sein soll, lässt sich die Systematik zwischen § 202c StGB und § 202a StGB dagegen nicht heranziehen. In derartigen Fällen kommt eine Strafbarkeit nach § 202c StGB schon mangels diesbezüglicher Tathandlung nicht in Betracht, so dass aus dieser auch keine Rückschlüsse auf die Auslegung des Tatbestandsmerkmals des *Überwindens* i. S. d. § 202a Abs. 1 StGB gezogen werden können. Dass die vom Senat für richtig erachtete Auslegung des Tatbestandsmerkmals des *Überwindens* der Zugangssicherung dazu führen würde, dass § 202c Abs. 1 Nr. 1 StGB "*praktisch vollständig ins Leere*" liefe, ist aus den vorstehend dargelegten Gründen unzutreffend.

dd)

Schließlich hält der Senat das von der Generalstaatsanwaltschaft zugrunde gelegte Verständnis des Tatbestandsmerkmals des *Überwindens* der Zugangssicherung auch für mit dem Wortlaut der Vorschrift, an den die Strafgerichte strikt gebunden sind (

BVerfG, Beschlüsse vom 17. Januar 1978 - 1 BvL 13/76, Rn. 39, juris, und vom 5. Juli 1983 - 2 BvR 200/81, Rn. 20, juris), nicht mehr vereinbar. Es muss daher dabei bleiben, dass ein *Überwinden* der Zugangssicherung ausscheidet, wenn der Täter lediglich eine für ihn bestehende - nicht rechtswidrig erlangte - Zugriffsmöglichkeit nutzt und damit, wie hier, den Zugang auf dem hierfür vorgesehenen Weg erzielt.

2.

Das dem Beschuldigten zur Last gelegte Verhalten erfüllt auch nicht den Tatbestand des Computerbetruges gemäß § 263a Abs. 1 StGB, weil es jedenfalls auch an einem täuschungsäquivalenten Datengebrauch fehlt. Denn eine Miterklärung einer echten Berechtigung zur Transaktion kann in dezentralen Blockchain-Netzwerken nicht angenommen werden. Eine Strafbarkeit wegen Fälschung beweiserheblicher Daten gemäß §§ 269, 270 StGB scheitert schon an der fehlenden Erkennbarkeit des Ausstellers. Ergänzend nimmt der Senat insoweit auf die auch vom Landgericht für zutreffend erachteten diesbezüglichen Ausführungen der Staatsanwaltschaft Göttingen in dem dortigen Vermerk vom 13. Februar 2024 (Bl. 70 f. d.A.) Bezug.

Darüber hinaus merkt der Senat an, dass auch keine Strafbarkeit wegen Untreue nach § 266 StGB in Betracht kommt. Dass der Beschuldigte für den Zeugen A. eine Wallet eingerichtet und diese mit Passwörtern geschützt hat, führt nicht zur Annahme einer Vermögensbetreuungspflicht und vermag auch eine Treuepflicht nicht zu begründen.

3.

Es besteht schließlich auch kein Anfangsverdacht gegen den Beschuldigten wegen Datenveränderung (§ 303a StGB).

Soweit es die Blockchain und die A-Coins selbst betrifft, fehlt es (jedenfalls) an einer Verletzung des Datenverfügungsrechts eines anderen. Dagegen liegt hinsichtlich der Wallet und dem in dieser gespeicherten Private Key keine tatbestandsmäßige Handlung vor.

Im Einzelnen:

a.

Gemäß § 303a Abs. 1 StGB macht sich strafbar, wer rechtswidrig Daten (§ 202a Abs. 2 StGB) löscht, unterdrückt, unbrauchbar macht oder verändert.

aa)

Die Tathandlungen des § 303a Abs. 1 StGB überschneiden sich, um jede denkbare Beeinträchtigung des Bestandes der geschützten Daten erfassen zu können (vgl. Fischer, 71. Aufl., § 303a, Rn. 8). Erfasst sind - über die Anlehnung an den Tatbestand der Sachbeschädigung hinaus - auch Beeinträchtigungen der Verfügbarkeit (Unterdrücken) sowie der inhaltlichen Zweckbestimmung (Verändern).

Ein Verändern liegt vor bei einem Herbeiführen von Funktionsbeeinträchtigungen der Daten, die eine Änderung ihres Informationsgehalts oder des Aussagewerts zur Folge haben, mithin insbesondere bei jeder Form der inhaltlichen Umgestaltung von Daten (

BGH, Beschluss vom 27. Juli 2017 - 1 StR 412/16, Rn. 33, juris). Eine Änderung des Informationsgehaltes kann aber auch dadurch bewirkt werden, dass der selbst unveränderte Datensatz - etwa durch Hinzufügen weiterer Daten - in einen anderen Zusammenhang gestellt oder - z.B. durch Teillöschung - aus dem ursprünglichen Zusammenhang gelöst wird (Goeckenjan in: Leipziger Kommentar zum StGB, 13. Aufl., § 303a, Rn. 33, m.w.N.). Führt die Veränderung zu einer Beeinträchtigung der bestimmungsgemäßen Verwendbarkeit, liegt (zugleich) ein Unbrauchbarmachen von Daten vor (Fischer, a.a.O., Rn. 11; Goeckenjan in: Leipziger Kommentar zum StGB, a.a.O., Rn. 32). Das Löschen von verknüpfenden Datensätzen ist zudem bereits für sich tatbestandsmäßig (Goeckenjan in: Leipziger Kommentar zum StGB, a.a.O.).

Ein Unterdrücken von Daten liegt vor, wenn diese dem Zugriff des Berechtigten für - zumindest - einen nicht unerheblichen Zeitraum entzogen werden und deshalb nicht mehr verwendet werden können, ohne dass ihre physische Integrität beeinträchtigt wird (Hecker in: Schönke/Schröder, 30. Aufl. 2019, § 303a Rn. 6; Fischer, a.a.O., Rn. 10; Goeckenjan in: Leipziger Kommentar zum StGB, a.a.O., Rn. 32; Heger in: Lackner/Kühl/Heger, 30. Aufl. 2023, § 303a Rn. 3).

bb)

§ 303a StGB ist ein der Sachbeschädigung (§ 303 StGB) nachgebildetes Delikt und deshalb auch systematisch in den 27. Abschnitt des Strafgesetzbuches ("Sachbeschädigung") eingeordnet. Im Gegensatz zu § 303 StGB setzt der Tatbestand des § 303a Abs. 1 StGB aber seinem Wortlaut nach nicht voraus, dass es sich bei den betroffenen Daten um "fremde" handeln muss.

Dementsprechend wird in der Gesetzesbegründung ausgeführt, eine Verletzung von *Interessen* des vom Inhalt der Daten Betroffenen sei zur Begründung der Rechtswidrigkeit ausreichend (vgl. Drs. 10/5058, S. 34). Dem kann jedoch nicht gefolgt werden. Um in einer Art. 103 Abs. 2 GG genügenden Weise ein hinreichend bestimmtes Verhalten zu beschreiben, bedarf der Tatbestand des § 303a StGB vielmehr nach allgemeiner Auffassung einer Einschränkung. Denn strafwürdiges Unrecht liegt nur dann vor, wenn ein anderer als der Täter von der Tathandlung betroffen ist, mithin eine fremde Rechtsposition verletzt wird (

OLG Nürnberg, Beschluss vom 23. Januar 2013 - 1 Ws 445/12, Rn. 11, m. w. N., juris; Goeckenjan in: Leipziger Kommentar zum StGB, 13. Aufl., § 303a, Rn. 11; Wieck-Noodt in: Münchener Kommentar zum StGB, 4. Aufl., § 303a Rn. 3; Hecker in: Schönke/Schröder, 30. Aufl., § 303a, Rn. 3; Bär in: Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 3. Aufl., StGB § 303a Rn. 11).

Nach herrschender Auffassung werden von § 303a StGB daher - als ungeschriebenes Tatbestandsmerkmal - nur *fremde* Daten geschützt, mithin solche, *an denen ein unmittelbares Recht einer anderen Person* - im Sinne einer eigentümerähnlichen Datenverfügungsbefugnis - auf Verarbeitung, Löschung oder Nutzung *besteht* (Fischer StGB, 71. Aufl. § 303a, Rn. 4a; Wieck-Noodt in: Münchener Kommentar zum StGB, 4. Aufl., § 303a Rn. 3 u. Rn. 9; Hecker in: Schönke/Schröder StGB, 30. Aufl., § 303a Rn. 3). Nach anderer Ansicht soll die gebotene Begrenzung des Tatbestandes des § 303a StGB darüber erreicht werden, dass das Merkmal "*rechtswidrig*" als Tatbestandsmerkmal aufgefasst und dahingehend verstanden werden soll, dass *die Daten rechtlich einem anderen* als dem sie verändernden Täter *zustehen* müssen (Goeckenjan in: Leipziger Kommentar zum StGB, 13. Aufl., § 303a StGB, Rn. 11). Die unterschiedlichen Ansätze sind in erster Linie dogmatischer Natur; zu abweichenden Beurteilungen führen sie in der Rechtsanwendung nicht (vgl. hierzu auch: Fischer, a.a.O., Rn. 8). Entscheidend ist im Ergebnis daher, dass das Verfügungsrecht über die betroffenen Daten - als Tatobjekt - neben dem Täter einer weiteren Person oder überhaupt einer anderen Person als dem Täter zusteht (Wieck-Noodt in: Münchener Kommentar zum StGB, a.a.O., Rn. 9; Bär in: Graf/Jäger/Wittig Wirtschafts- und Steuerstrafrecht, a.a.O., Rn. 11).

Die Bestimmung, wem das Verfügungsrecht über die Daten zusteht, bereitet in der Praxis allerdings mitunter Schwierigkeiten. Denn anders als beim sachenrechtlichen Begriff der Fremdheit fehlt es an einer eindeutigen Regelung der Verfügungsbefugnis über Daten, auf welche sich die Zivilrechtsakzessorietät stützen könnte (Fischer, a.a.O., Rn. 5; Hecker in: Schönke/Schröder, 30. Aufl., § 303a Rn. 1 u. Rn. 3).

Überwiegend wird daher anhand von Fallgruppen versucht, Anknüpfungspunkte der Datenzuordnung zu gewinnen. Unter Berufung auf den Charakter der Datenverfügungsbefugnis als eigentumsähnliches Recht soll dabei im Ausgangspunkt die originäre Datenverfügungsbefugnis in Abhängigkeit von der sachenrechtlichen Zuordnung des Datenträgers bestimmt werden. Diese steht mithin dem Eigentümer oder rechtmäßigen Besitzer des Datenträgers zu (Fischer, a.a.O., Rn. 5). Fallen Eigentum und/oder Besitz am Datenträger und Nutzungsrecht auseinander, so soll sich die Verfügungsbefugnis nach dem schuldrechtlichen Rechtsverhältnis der Beteiligten bestimmen (Fischer a.a.O., Rn. 6; Wieck-Noodt in: Münchener Kommentar zum StGB, a.a.O., Rn. 3), d.h. der schuldrechtlich Nutzungsberechtigte soll hinsichtlich der überlassenen Daten neben oder sogar an die Stelle des dinglichen Nutzungsberechtigten treten (Hecker in: Schönke/Schröder, 30. Aufl., § 303a, Rn. 3).

Nach anderer Ansicht soll die Datenverfügungsbefugnis grundsätzlich demjenigen zustehen, der die Speicherung der Daten unmittelbar selbst bewirkt und sie mithin in einem Skripturakt erzeugt hat (

OLG Nürnberg, Beschluss vom 23. Januar 2013 - 1 Ws 445/12, Rn. 14, juris; BayObLG, Urteil vom 24. Juni 1993 - 5 St RR 5/93, CR 1993, 779 ff., 780; Mansdörfer in: BeckOK IT-Recht, 15. Ed. Stand: 1. Juli 2024, StGB § 303a, Rn. 7 StGB; Bär in: Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, a.a.O., Rn. 12).

Der letztgenannte Ansatz hat den Vorteil, dass er grundsätzlich auf jede Fallkonstellation Anwendung finden kann. Die Anknüpfung an die "Urheberschaft" bzgl. der Daten wird zudem dem Umstand gerecht, dass bei Daten deren geistiger Gehalt im Vordergrund steht (Goeckenjan in: Leipziger Kommentar zum StGB, a.a.O., Rn. 12). Dagegen stößt der dinglich/obligatorische Ansatz an seine Grenzen sowohl in Fällen von in fremdem Auftrag erstellter Daten als auch dann, wenn - wie hier - die Datenspeicherung im Internet über ein Netzwerk erfolgt (vgl. hierzu: Fischer, a.a.O., Rn. 6 und Rn. 7). Für derartige Fälle wollen daher auch dessen Vertreter ergänzend auf den Skripturakt abstellen (vgl. Fischer, a.a.O., Rn. 6). Der Senat kann deshalb im Ergebnis dahinstehen lassen, welchem Ansatz zu folgen ist.

cc)

Die vorstehend dargelegten Maßstäbe führen für den hier zur Entscheidung stehenden Fall zu folgenden Ergebnissen:

Bezüglich der Wallet und des privaten Schlüssels fehlt es an einer tatbestandsmäßigen Datenveränderung (vgl. nachfolgend unter (2)). Soweit es die Blockchain und die dort erfolgende Speicherung der Veränderung der Zuweisung der A-Coins betrifft, liegt zwar eine Veränderung von Daten vor; diese Datenveränderung wurde jedoch nicht durch den Beschuldigten, sondern das hierzu berechtigte Netzwerk vorgenommen (vgl. nachfolgend unter (3)).

(1)

Blockchain ("Blockkette") ist eine spezielle Technologie zur Datenhaltung in dezentral verteilten Netzwerken, d.h. in Netzwerken, die nicht von einer zentralen Instanz verwaltet werden. Die Daten werden in einzelnen Blöcken aneinandergereiht - wobei neue

Datenblöcke am Ende angehängt werden - und so auf den Rechnern im Netzwerk gespeichert. Durch den Einsatz kryptographischer Methoden bleibt diese chronologische Reihenfolge stets erhalten und jede nachträgliche Manipulation an den Daten kann sofort entdeckt werden. Ein sogenannter Konsensmechanismus sorgt dafür, dass sich alle Rechner im Netzwerk über den jeweils aktuellen Stand der Blockkette einig sind. Blockchain macht Daten praktisch unveränderbar (Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen- und -Verbraucher/Informationen- und -Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung_node.html).

Die Teilnahme an der Blockchain (als Unterkategorie von Distributed-Ledger-Technologie) erfolgt über die Wallet (Leupold/Wiebe/Glossner, Begriffserklärungen, beck-online). In einer Wallet werden Kryptowährungen verwaltet, sie enthält selbst jedoch keine Kryptowerte (Eckhold/F.Schäfer in: Assmann/Schütze/Buck-Heeb, Handbuch des Kapitalanlagerechts, 6. Aufl., § 17, Fn. 8 zu Rn. 1; Ummenhofer/Zeitler in: Beck'sches Handbuch der Rechnungslegung, Stand: 72. EL Juni 2024, B 731, Rn. 4). Die Wallet interagiert mit der Blockchain, um die Kryptowährungen zu verwalten, indem sie Public und Private Keys speichert, die für das Senden und Empfangen von digitalen Währungen unerlässlich sind. Durch diese Schlüssel kann die Wallet Transaktionen verifizieren und Nutzern ermöglichen, auf "ihre" Kryptowerte zuzugreifen (Eckhold/F.Schäfer in: Assmann/Schütze/Buck-Heeb, Handbuch des Kapitalanlagerechts, a.a.O.).

Nutzer der Blockchain verfügen entweder selbst über eine Wallet oder haben eine andere Person mit der Verwahrung dieser beauftragt ("Kryptowährungen, Token und das Kapitalstrafrecht" - Schelzke,

wistra 2022, 182-188 (183)).

Die elektronische Werteinheit wird durch einen Token bzw. Coin abgebildet, also einen digitalen Code (Datensatz), der einzigartig und als solcher nicht vervielfältigbar ist (Eckhold/F.Schäfer in: Assmann/Schütze/Buck-Heeb, Handbuch des Kapitalanlagerechts, a.a.O., Rn. 2). Vereinfacht kann man Coin und Token als einen digitalen Gutschein für das, was bei der Ausgabe versprochen wird, begreifen (Schelzke, a.a.O.).

Die Token/Coins werden durch die Blockchain einem bestimmten Public und Private Key eines Teilnehmers zugeordnet. Die Inhaberschaft eines Teilnehmers bzgl. der Token/Coins basiert darauf, dass faktisch nur er über den privaten Schlüssel (Private Key) und damit auch über die Token/Coins verfügen kann (Rückert in: Maume/Maute, Rechtshandbuch Kryptowerte, 1. Aufl., § 22 Rn. 22 u. Rn. 23).

Auf einer Blockchain einmal vorgenommene Einträge können technisch nicht widerrufen oder geändert werden, sondern sind fest in der Blockchain integriert; die Blockchain lässt nur Hinzufügungen zu (Eckhold/F.Schäfer in: Assmann/Schütze/Buck-Heeb, Handbuch des Kapitalanlagerechts, a.a.O., Rn. 5).

Die Übertragung der Kryptowerte erfolgt, indem der Veräußerer veranlasst, dass (s)einem Token / Coin nicht mehr sein, sondern der öffentliche Schlüssel eines anderen Teilnehmers als Erwerber zugeordnet und dies in einem neuen Datenblock protokolliert wird (vgl. Rückert in: Maume/Maute, Rechtshandbuch Kryptowerte, 1. Aufl., § 22 Rn. 24; Eckhold/F.Schäfer in: Assmann/Schütze/Buck-Heeb, Handbuch des Kapitalanlagerechts, a.a.O.). Zur Durchführung der Transaktion ist deren Signierung mit dem zutreffenden - zu dem öffentlichen Schlüssel des Veräußerers gehörenden - Private Key erforderlich. Eine Aussage über die Identität der hinter der Transaktion stehenden Person und einer "echten" Berechtigung zur Transaktion wird hiermit nicht getroffen. Weil schuldrechtliche Beziehungen - wie etwa im Giralgeldverkehr - in dezentralen Blockchain-Netzwerken nicht bestehen, hat kein Netzwerk-Computer (sog. Node) bzw. keiner der Miner (d.h. die die Transaktion bestätigenden Netzwerk-Teilnehmer, vgl. Altwegger in: Leupold/Wiebe/Glossner, IT-Recht, Teil 16.2, Rn. 34; Ummenhofer/Zeitler in: Beck'sches Handbuch der Rechnungslegung, Stand: 72. EL Juni 2024, B 731, Rn. 5) selbst ein Interesse daran, dass nur der (materiell-rechtlich) Berechtigte Token überträgt (Rückert in: Maume/Maute, Rechtshandbuch Kryptowerte, 1. Aufl., § 22, Rn. 22).

Sofern eine Transaktion durch das Netzwerk verifiziert wurde, wird die neue Zuordnung der Kryptowerte durch die Netzwerk-Betreiber in der Blockchain protokolliert, indem ein diesbezüglicher neuer Datenblock gespeichert wird.

(2)

Vorstehendes zugrunde gelegt, führt die Durchführung einer Transaktion weder zu einer Veränderung der Wallet noch des Private Keys.

In der Wallet sind - wie oben dargelegt - nicht die Token / Coins selbst, sondern (nur) die Schlüssel (Private und Public Key) des Nutzers gespeichert. Diese werden bei einer Transaktion aber nicht verändert, sondern lediglich verwendet (Rückert in: Maume/Maute, Rechtshandbuch Kryptowerte, 1. Aufl., § 22, Rn. 24). Auch die bestimmungsgemäße Brauchbarkeit des Private Keys wird durch die Transaktion nicht beeinträchtigt. Dieser kann weiterhin zur Transaktion von dem zugehörigen Public Key (aktuell oder später) zugeordneten Kryptowerten verwendet werden. Dies soll vorliegend im Übrigen auch gerade geschehen sein, denn die betroffenen "A-Coins" sollen in mehr als einer Transaktion übertragen worden sein.

(3)

Die Protokollierung einer Transaktion in der Blockchain und die damit verbundene datenmäßige Veränderung der Zuordnung der Kryptowerte (hier: A-Coins) beinhaltet zwar eine Veränderung - und zugleich auch ein teilweises Unbrauchbarmachen - von Daten; denn mit der Zuweisung der Coins zu einem anderen Public Key ist eine Änderung des Informationsgehalts bzw. Aussagewertes des zuvor die Zuweisung dokumentierenden Datensatzes verbunden.

Diese Datenveränderung ist aber nicht durch den Beschuldigten, sondern durch die Netzwerk-Betreiber und damit durch die diesbezüglich Verfügungsberechtigten selbst vorgenommen worden: Wie ausgeführt, wird die Blockchain durch ein dezentrales Netzwerk von Servern (sog. Knoten = "Nodes") verwaltet und gesteuert. Die in der Blockchain gespeicherten Daten werden in identischer Form auf allen teilnehmenden Rechnern gespeichert. Skribent der Blockchain-Daten sind mithin die Netzwerk-Betreiber in ihrer Gesamtheit, denn (nur) diese bewirken die Speicherung der Daten unmittelbar selbst.

Die "Inhaber" der Kryptowerte speichern die Blockchain-Daten hingegen weder unmittelbar selbst noch sind sie zu diesbezüglichen Veränderungen schuldrechtlich berechtigt.

Dementsprechend waren (nur) die Netzwerk-Betreiber zu der - unmittelbar durch sie selbst - vorgenommenen Datenveränderung in Form einer Ergänzung der Blockchain berechtigt.

Dass die Protokollierung einer Transaktion die Folge einer Verfügung des Nutzers unter Verwendung des zutreffenden öffentlichen und privaten Schlüssels ist und er diese damit - kausal - veranlasst hat, rechtfertigt keine andere Beurteilung. Denn hieraus folgt lediglich eine - gerade dem vorgesehenen Betrieb des Systems entsprechende - *mittelbare* Bewirkung der die Veränderung auslösenden Datenspeicherung. Dies genügt für den das Verfügungsrecht begründenden Skripturakt nicht. Wollte man auf die mittelbare Verursachung der Protokollierung der Transaktion abstellen, wäre im Übrigen zunächst auch (nur) der Nutzer des verwendeten Private und Public Keys als Datenverfügungsberechtigter in den Blick zu nehmen. Denn es kann nicht außer Betracht bleiben, dass Transaktionen innerhalb der Blockchain bewusst und gewollt anonym durchgeführt werden und die Zuordnung der Kryptowerte deshalb auch nicht zu Personen, sondern nur zu "Schlüsseln" erfolgt. Zur Ausführung einer Transaktion betreffend die einem öffentlichen Schlüssel zugeordneten Kryptowerte befugt ist im Verhältnis zur Blockchain nach deren Regeln damit zunächst jede Person, die über den zutreffenden Private Key verfügt. Ob dies anders zu beurteilen wäre, wenn diese Person den zutreffenden Private Key durch rechtswidriges Handeln erlangt hätte, braucht hier nicht entschieden zu werden. Denn dem Beschuldigten wird (lediglich) zur Last gelegt, er habe den Zugriff auf den Private Key des Anzeigeerstatters durch Verwendung der ihm bereits bekannten Passwörter erlangt und mithin eine schuldrechtliche Nebenpflicht - die von ihm erstellten Passwörter nicht (mehr) zu verwenden - verletzt. Eine Kriminalisierung von (bloßen) Vertragsverletzungen wird von § 303a StGB jedoch nicht erfasst (Fischer, a.a.O., Rn. 6).

4.

Weil das dem Beschuldigten zur Last gelegte Verhalten bereits aus rechtlichen Gründen den Anfangsverdacht einer strafbaren Handlung nicht begründet, konnte der Senat dahinstehen lassen, ob zureichende tatsächliche Anhaltspunkte dafür bestehen, dass der Beschuldigten die verfahrensgegenständlichen Transaktionen veranlasst hat.

III.

Die Kostenentscheidung beruht auf einer entsprechenden Anwendung von § 467 StPO.

Hinweis:

Hinweis: Das Dokument wurde redaktionell aufgearbeitet und unterliegt in dieser Form einem besonderen urheberrechtlichen Schutz. Eine Nutzung über die Vertragsbedingungen der Nutzungsvereinbarung hinaus - insbesondere eine gewerbliche Weiterverarbeitung außerhalb der Grenzen der Vertragsbedingungen - ist nicht gestattet.