Not Your Keys, Not Your Coins? Rechtliche Lücken bei der Sicherstellung von Kryptowerten und Analyse der vorgesehenen Änderungen im Strafprozessrechtsänderungsgesetz 2024*

Evelyne Putz/Nicholas Stifter/Edgar Weippl

Abstract
Im Dezember 2023 hob der VfGH zentrale Bestimmungen zur Sicherstellung im strafrechtlichen Ermittlungsverfahren als verfassungswidrig auf. Dabei betonte das Höchstgericht ua die erweiterten Eingriffsmöglichkeiten, die den Strafverfolgungsbehörden mittlerweile durch den technischen Fortschritt beim Zugriff auf Datenträger bzw Daten zur Verfügung stehen. Der Gesetzgeber hat noch bis zum Ablauf des 31. Dezember 2024 Zeit, eine neue verfassungskonforme Regelung zu schaffen. Ein Entwurf für die Reform wurde am 13. Juni 2024 eingebracht, die Beschlussfassung im Nationalrat war bereits für Anfang Juli vorgesehen. Massive Kritik, ua aus Wissenschaft und Justiz, führte aber zur Verlängerung des Begutachtungsverfahrens und der Verschiebung der Beschlussfassung auf September. Von der medialen Berichterstattung und den kritischen Stellungnahmen weitgehend unbeachtet blieb bislang der Umstand, dass der Gesetzesvorschlag erstmals ausdrücklich einen höchst praxisrelevanten Problembereich berücksichtigt: Die Sicherstellung von Kryptowerten. Dieser Beitrag analysiert die aktuelle Rechtslage sowie die vorgeschlagenen Änderungen durch den Reformentwurf. Dabei wird aufgezeigt, dass die Neuerungen zwar geeignet sind, bestehende gesetzliche Lücken zu schließen, jedoch gleichzeitig neue Probleme aufwerfen.

Schlagworte
Behördenwallet, Beschlagnahme, Blockchain, Daten, Datenträger, Drittverbot, Eigentumsfreiheit, Kryptowährung, Kryptowert, Krypto-Asset, Legalitätsprinzip, Rechtszuständigkeit, Sicherstellung, Strafprozessrechtsänderungsgesetz 2024, Vermögensrechte, virtuelle Währung, Wallet

Rechtsquellen
Art 5 StGG; §§ 109, 110, 111, 114 StPO; Art 1. 1. ZPEMRK

Inhaltsübersicht

DOI 10.52018/SPWR-24H00-B008
* Danksagung:
Diese Forschung wurde teilweise unterstützt durch:
1. FFG Bridge 1 Projekt Nr. 898917 – SecKey
2. das Christian Doppler Labor für Verbesserung von Sicherheit und Qualität in Produktionssystemen (CDL-SQI)
3. SBA Research: das COMET-Zentrum SBA Research (SBA-K1) wird im Rahmen von COMET – Competence Centers for Excellent Technologies durch BMK, BMAW und das Land Wien gefördert. COMET wird durch die FFG abgewickelt.

I. Einleitung

A. Ausgangslage: G 352/2021

Die Befugnis der österreichischen Strafverfolgungsbehörden zur Sicherstellung von Datenträgern und zur Auswertung von Informationen muss neu geregelt werden. Das ist – nach wie vor – der Stand der Dinge, nachdem der VfGH mit Erkenntnis vom 14. Dezember 2023, G 352/2021, grundlegende Normen zur Sicherstellung im Strafverfahren als verfassungswidrig aufhob. Betroffen sind § 110 Abs 1 Z 1 und Abs 4 sowie § 111 Abs 2 der StPO, BGBl Nr 631/1975 idF BGBl I Nr 19/2004 – sie verletzen hinsichtlich der Sicherstellung und Auswertung von Datenträgern das Grundrecht auf Datenschutz sowie auf Achtung des Privat- und Familienlebens. Der Antragsteller des Normprüfungsverfahrens hatte im Wesentlichen einen Wertungswiderspruch bemängelt: Dem tiefgreifenden Einblick in Leben und Privatsphäre, welche die Sicherstellung eines Smartphones ermögliche, stünden zu geringe gesetzliche Voraussetzungen für diese Ermittlungsmaßnahme gegenüber. Der VfGH bestätigte letztlich diese Bedenken und stellte fest, dass die *»durch § 110 Abs 1 Z 1 und § 111 Abs 2 StPO eingeräumte Ermittlungsbefugnis der Staatsanwaltschaft (und der Kriminalpolizei), ohne dass diese einer vorhergehenden Bewilligung durch das Gericht bedarf«* gegen § 1 Abs 2 DSG iVm Art 8 Abs 2 EMRK verstoße.[1] Eine Verletzung dieser Normen liege auch darin, dass die StPO keinen angemessenen Rechtsschutz der betroffenen Personen gewährleiste.[2] Bei der Sicherstellung von Datenträgern ergäbe sich eine besondere Eingriffsintensität aus den geringen Zulässigkeitsvoraussetzungen, der Möglichkeit der Setzung solcher Maßnahmen auch gegenüber (nicht verdächtigen) Dritten sowie der besonderen Menge und Art der betroffenen Daten.[3] Der VfGH betonte diesbezüglich auch die Möglichkeiten der Verknüpfung und des Abgleichs mit anderen Daten sowie der Wiederherstellung gelöschter Daten.[4] Diese Umstände unterscheiden nach Wertung des Höchstgerichts eine Sicherstellung von Datenträgern wie etwa PCs, Notebooks und Smartphones grundlegend von einer solchen anderer Gegenstände iSd § 109 Z 1 lit a StPO.

B. Strafprozessrechtsänderungsgesetz 2024: Initiativantrag 4125/A und Ministerialentwurf 349/ME

Die Aufhebung der Bestimmungen tritt bereits mit Ablauf des 31. Dezember 2024 in Kraft, das Ende der sog Reparaturfrist naht also. Ein Entwurf für die Neuregelung durch das **Strafprozessrechtsänderungsgesetz 2024** (in der Folge auch: StPRÄG 2024) wurde bereits am 13. Juni als Initiativantrag (4125/A) im Nationalrat eingebracht und vier Tage später nochmals inhaltsgleich als Ministerialentwurf (349/ME).[5] Nach Beratung im Justizausschuss befürwortete auch dieser den Vorschlag und die Abstimmung im Nationalrat war – nach außergewöhnlich kurzer zweiwöchiger Begutachtungsfrist – schon für die erste Juliwoche vorgesehen. Nach heftiger Kritik, ua aus der Wissenschaft und Justiz bis hin zu OGH und europäischer Staatsanwaltschaft, kündigte das BMJ jedoch kurz vor diesem Datum an, dass das Begutachtungsverfahren um vier weitere Wochen verlängert und der Entwurf nochmals überarbeitet werde. Die Abstimmung im Nationalrat kann damit erst im September stattfinden.

Die öffentliche Diskussion zum StPRÄG 2024 dreht sich primär um durch den Entwurf vorgesehene sensible Zuständigkeitsverschiebungen, hohen erwarteten Mehraufwand und Fragen der Effizienz. Ein besonders interessanter Aspekt des Reformvorschlags hat dabei bisher kaum Beachtung gefunden: Erstmals sollte ein weiteres, erst seit relativ kurzer Zeit aufgrund des technischen Fortschritts auftretendes Problemfeld ausdrücklich gesetzlich thematisiert werden, nämlich der Zugriff der Strafverfolgungsbehörden auf Kryptowerte. Solche Vermögenswerte werden schon bisher in der Praxis gesichert und zu diesem Zweck insb auf behördlich kontrollierte Adressen übertragen, allerdings ist dieses Vorgehen bislang **nicht dezidiert durch das Gesetz vorgesehen.** Die Behörden berufen sich in Ermangelung einer ausdrücklichen Rechtsgrundlage – erlassmäßig von BMJ bzw BMI vorgegeben – auf die »Sicherstellung von Datenträgern« bzw Daten. Eine kritische Auseinandersetzung mit der Anwendung dieser Bestimmungen auf solche Vermögenswerte ist in der Lit weitgehend unterblieben.[6] Wie in diesem Beitrag dargestellt wird, ist bei genauerer Betrachtung allerdings **fraglich,** ob die herangezogenen Normen solche Maßnahmen **nach aktueller Rechtslage tatsächlich abdecken.** Da es sich dabei gerade auch um jene Bestimmungen handelt, die von der Aufhebungsentscheidung des VfGH betroffen sind,

1 VfGH 14.12.2023, G 352/2021, Rz 82.
2 VfGH 14.12.2023, G 352/2021, Rz 83.
3 Vgl VfGH 14.12.2023, G 352/2021, Rz 71 f.
4 Vgl VfGH 14.12.2023, G 352/2021, Rz 66, 70.
5 Soweit in diesem Beitrag auf die Materialien des behandelten Reformentwurfs verwiesen wird, bezieht sich dies der Einfachheit halber stets auf den Ministerialentwurf. Da der Initiativantrag und die darin enthaltene Begründung inhaltsgleich sind, gelten die Ausführungen ebenso für diesen.
6 Die in diesem Beitrag diskutierte Rechtsansicht von BMI und BMJ wiedergebend *Köck,* Die Sicherstellung von Krypto-Assets im Finanzstrafverfahren, ZWF 2023, 84; ebenso in der Kommentarliteratur, vgl *Kroschl* in Schmölzer/Mühlbacher (Hrsg), StPO Kommentar I² (2021) § 109 StPO Rz 5 sowie *Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 111 (Stand 1.3.2021, rdb.at) Rz 6/1, 12/1, 14/6 (letztere jedoch ablehnend in Bezug auf die Nutzung aufgefundener kryptographischer Schlüssel von einem Computer der Behörde aus).

ist die Berücksichtigung dieser Thematik im Rahmen der nun erforderlich gewordenen gesetzlichen Überarbeitung naheliegend und grundsätzlich aus rechtsstaatlicher Sicht erfreulich. Im vorliegenden Beitrag werden auch die **im Entwurf des StPRÄG 2024 vorgesehenen Neuerungen** darauf untersucht, ob sie die in diesem Bereich bestehenden **rechtlichen Lücken beheben,** somit zukünftig eine **klare Rechtsgrundlage für behördliche Maßnahmen bieten** und **verfassungsrechtliche Bedenken ausräumen** können. Der Fokus liegt dabei auf der in dieser Hinsicht bedeutsamen Abänderung der **§§ 109, 110, 111 und 114 StPO** sowie den neuen **§§ 115f und 115g StPO.** Diese Analyse soll als Anstoß zur rechtswissenschaftlichen und legistischen Diskussion dienen.

C. Gliederung des Beitrags

Zunächst wird kurz auf die – auch durch den VfGH thematisierte – Beziehung zwischen technologischer Entwicklung und staatlichen Eingriffsermächtigungen eingegangen. Die kritische Beurteilung der Reichweite der derzeitigen sowie der im StPRÄG 2024 vorgesehenen Eingriffsermächtigungen erfordert außerdem ein Grundverständnis des technischen Hintergrundes von Kryptowerten. Aus diesem Grund folgt eine detaillierte Beschreibung der wesentlichen technischen Abläufe, die im Kontext einer behördlichen Sicherung entscheidend sind und auf die in den rechtlichen Ausführungen wiederholt Bezug genommen werden kann. Aufbauend darauf werden die Möglichkeiten, Kryptowerte tatsächlich zu sichern, aufgezeigt. Anschließend werden die relevanten Normen nach aktueller und im StPRÄG 2024 vorgeschlagener Fassung einander gegenübergestellt und es wird eine kritische Beurteilung der rechtlichen Änderungen, die sich durch die geplante Reform im betrachteten Bereich ergeben, vorgenommen.

II. Das Spannungsverhältnis zwischen technischem Fortschritt und Eingriffsermächtigungen

A. Steigerung der Eingriffsintensität als Faktor in G 352/2021

Die vom VfGH in G 352/2021 betonten Möglichkeiten, durch die Sicherstellung und Auswertung von (bestimmten) Datenträgern tiefe Einblicke in Leben, Privatsphäre und Persönlichkeit einer Person zu erlangen, beruhen nicht zuletzt auf dem beschleunigten technischen Fortschritt der letzten Jahre. Dies betrifft insb die vom Höchstgericht ausdrücklich wertend einbezogenen Faktoren der Menge, Art und Qualität der regelmäßig lokal und extern abgelegten Daten, die Möglichkeit der Datenwiederherstellung, -verknüpfung und des Datenabgleichs sowie die Erstellbarkeit von Persönlichkeits- und Bewegungsprofilen und prädiktiven Analysen. Zentral für die höchstgerichtliche Bewertung war damit gerade auch die faktische Erweiterung der Eingriffsintensität von Ermittlungsmaßnahmen durch die technologische Entwicklung seit Erlassung der betroffenen Rechtsnormen. Prägnant hielt der VfGH diesbezüglich fest, dass *»die Erweiterung der technischen Möglichkeiten der Strafverfolgungsorgane auch dazu führt, dass den Gefahren, die diese Erweiterung für die Freiheit des Menschen birgt, in einer dieser Bedrohung adäquaten Weise entgegengetreten werden muss«,*[7] und verwies auf seine Aufhebungsentscheidungen zur Vorratsdatenspeicherung[8] und zum sog »Bundestrojaner«[9].

B. Notwendigkeit des Zugriffs auf neuartige Vermögensgüter

Aus rechtsstaatlicher Perspektive kann technischer Fortschritt also eine kritische Analyse, Neubewertung und allenfalls Anpassung existierender Eingriffsermächtigungen verlangen. Auch seitens der Praxis wurde bereits geäußert, dass im Bereich des sog Cybercrime *»immer wieder die aktuelle Gesetzeslage, insb die ›veralteten‹ Ermittlungsbefugnisse der StPO«* Schwierigkeiten hervorrufen: *»Angesichts des rasanten technischen Fortschritts ergeben sich […] laufend neue Problembereiche, in denen zweckmäßige […] Ermittlungsmaßnahmen im Cyberspace zwar technisch möglich wären, jedoch Unsicherheit über deren Zulässigkeit besteht«.*[10] Die Erläuterungen zum Entwurf des StPRÄG 2024 greifen diese Problematik auf und verweisen mehrfach hierauf. So wird angeführt, dass die *»fortschreitende technische Entwicklung […] die Strafverfolgungsbehörden in vielen Bereichen vor große Herausforderungen«* stelle[11] und die Reform ua *»Bedürfnissen der Praxis und der technischen Entwicklung«* Rechnung tragen solle[12]. Neben bereits getroffenen (etwa organisatorischen) Maßnahmen seitens BMI und BMJ wird auf an das BMJ herangetragene *»Erfahrungen und Reformvorschläge«* sowie *»legistische Anregungen zu Anpassungen im Bereich der Sicherstellung, Beschlagnahme, Ausfolgung und Verwertung«* hingewiesen, die mit dem Entwurf umgesetzt werden sollen.[13] Teil dieser Anpassungen ist die gesetzliche Berücksichtigung von Kryptowerten[14] (wie

7 VfGH 14.12.2023, G 352/2021, Rz 76.
8 VfSlg. 19.892/2014.
9 VfSlg. 20.356/2019.
10 *Holzmann,* Die Kompetenzstelle CYBERCRIME bei der Staatsanwaltschaft Wien und aktuelle Phänomene der Cyberkriminalität, ÖJZ 2023, 778 (782).
11 ErlME 349/ME XXVII. GP, 37.
12 ErlME 349/ME XXVII. GP, 6.
13 ErlME 349/ME XXVII. GP, 37.
14 Neben der Bezeichnung »Kryptowert« sind für diese Form von Vermögensgütern auch die Begriffe »Krypto-Asset«, »Krypto-

beispielsweise Bitcoin oder Ether): Einerseits durch die Erweiterung potenzieller Sicherstellungsobjekte in § 109 Z 1 lit a StPO um »Vermögenswerte«, andererseits durch die Anordnung der Übertragung von Kryptowerten auf behördlich kontrollierte Adressen in einem neuen § 114 Abs 1a StPO.

Bei Kryptowerten handelt es sich um neuartige virtuelle Güter, die in aller Regel Vermögenswert besitzen. Sie werden typischerweise durch Einsatz von Distributed-Ledger-Technologie und kryptographischen Verfahren erstellt, können grundsätzlich weiter übertragen werden und dienen beispielsweise als Zahlungsmittel oder Spekulations- bzw Investitionsobjekt. Bitcoin, entwickelt 2008 bzw 2009, gilt gemeinhin als erster Kryptowert dieser Art;[15] seither wurden allerdings unzählige weitere Formen geschaffen.[16] Medienberichte über aufsehenerregende Fälle verdeutlichen immer wieder, dass diese Vermögensgüter auch im kriminellen Kontext genutzt werden – etwa als Entgelt für »Crime as a Service«, zur Geldwäscherei, beim Kauf illegaler Waren oder im Zusammenhang mit Ransomware-Attacken. Ihre spezifischen Eigenschaften (insb die Möglichkeit pseudonymer Nutzung, die schnelle und globale Übertragbarkeit und die weitestgehende Unumkehrbarkeit durchgeführter Transaktionen) machen sie hier offenbar zu einem attraktiven Werkzeug. Es besteht demnach ein kriminalpolitischer Bedarf, auf solche Werte gegebenenfalls im Rahmen eines strafprozessualen Verfahrens zugreifen zu können. Die Berichterstattung zeigt, dass solche Zugriffe sowohl in Österreich[17] als auch international[18] stattfinden (und belegt rechtliche und technische Komplikationen bei solchen Sicherungsmaßnahmen)[19]. Der komplexe technische Hintergrund erschwert aber sowohl die rechtliche Einordnung dieser Vermögenswerte als auch ihre legistische Erfassung. Die Schaffung klarer rechtlicher Rahmenbedingungen durch den Gesetzgeber ist somit tatsächlich dringend erforderlich.

III. Technische Ausgestaltung von Kryptowerten

Die Prüfung, ob ein behördlicher Zugriff auf Kryptowerte von Ermächtigungsnormen abgedeckt ist – Kryptowerte also unter die verwendeten Rechtsbegriffe subsumierbar sind – erfordert gewissermaßen eine Vorprüfung: Zunächst muss evaluiert werden, welche Eigenschaften Kryptowerte aufweisen und welche Prozesse ihrer Übertragung zugrunde liegen, um eine rechtliche Klassifikation zu ermöglichen. Eine Auseinandersetzung mit ihrer grundlegenden technischen Funktionsweise ist somit unabdingbar. Diese ist komplex und kann im vorliegenden Beitrag nur in der für die konkrete Thematik notwendigen Tiefe behandelt werden. Für detailliertere Informationen sei auf die angeführten Literaturquellen verwiesen. An dieser Stelle ist auch zu betonen, dass allgemeingültige Aussagen durch die vielfältigen Variationen, Einsatzmöglichkeiten und die fortlaufende

währung« oder »virtuelle Währung« verbreitet. Im Rahmen des StPRÄG 2024 wurde – in Anlehnung an EU-rechtliche Normen, letztlich verweisend auf die Verordnung (EU) 2023/1114 (Verordnung über Märkte für Kryptowerte), vgl ErlME 349/ME XXVII. GP, 38 – offenbar die Entscheidung getroffen, den Begriff »Kryptowert« zu wählen und diesem auch die Definition des Art 3 Abs 1 Z 5 dieser Verordnung zugrunde zu legen. Bedauerlicherweise wird diese Definition (»digitale Darstellung eines Werts oder eines Rechts, der bzw das unter Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden kann«) nur in den Materialien zitiert, wurde aber nicht in den Gesetzestext selbst übernommen. Abseits der hier behandelten geplanten Gesetzesänderung haben mittlerweile auch die Begriffe »Kryptowährung« und »virtuelle Währung« Eingang in österreichische Gesetze gefunden. Eine Darstellung der Begriffsverwendung seitens Behörden und Normsetzung auf EU- und österreichischer Ebene findet sich auch in *Putz,* Der behördliche Zugriff auf Krypto-Assets (Diplomarbeit, 2023), 3–9. Siehe zur Thematik auch *Stifter/Judmayer/Putz/Brameshuber/Weippl,* Blockchain-Babel: Herausforderungen bei der Entwicklung präziser Begrifflichkeiten zwischen Recht und Technik im Kontext von Kryptowährungen und Distributed-Ledger-Technologien, in Kirchmayr/Miernicki/Weilinger/Wimmer/Wild, Handbuch Besteuerung von Kryptowährungen (2023) 33.

15 2008 wurde die der Bitcoin-Blockchain zugrundeliegende Publikation »Bitcoin: A Peer-to-Peer Electronic Cash System« unter dem Pseudonym *Satoshi Nakamoto* online veröffentlicht und ist unter <https://bitcoin.org/bitcoin.pdf> abrufbar (zuletzt abgefragt am 5.7.2024); abgedruckt ist sie auch enthalten in *Antonopoulos,* Bitcoin und Blockchain – Grundlagen und Programmierung² (2018) 313 ff. Am 3.1.2009 folgte die dazugehörige Software, das sog »Bitcoin-Protokoll«; vgl hierzu *Antonopoulos,* Bitcoin 4.

16 Eine Auflistung des Großteils der zurzeit über sog Krypto-Börsen gehandelte Kryptowerte ist auf der Webseite <http://coinmarketcap.com> einzusehen. Der vom BMI herausgegebenen Cybercrime Report 2023 geht von über zwei Millionen verschiedenen Arten weltweit aus; siehe *BMI,* Cybercrime Report 2023 (April 2024) 12 f, abrufbar unter <https://www.bundeskriminalamt.at/306/files/Cybecrime_Report_2023_WebBF.pdf>, zuletzt abgefragt am 5.7.2024.

17 *BMI,* 20.3.2023, Cybercrime: Mehr als fünf Millionen Euro in Kryptowährungen beschlagnahmt, <https://www.bmi.gv.at>, zuletzt abgefragt am 5.7.2024.

18 ZB Sicherung von 2016 im Rahmen eines Hacking-Angriffs entzogenen Bitcoins im Wert von 3,6 Mrd USD – nach Medienberichten »die größte Beschlagnahmung von Finanzprodukten in der US-Geschichte«; *DerStandard,* 9.2.2022, US-Behörden beschlagnahmen Bitcoins im Milliardenwert, <https://www.derstandard.at>, zuletzt abgefragt am 5.7.2024; siehe etwa auch in Deutschland *ZDF,* 30.1.2024, Rekordsumme an Kryptowährung: BKA stellt Bitcoins mit Milliardenwert sicher, <https://www.zdf.de>, zuletzt abgefragt am 5.7.2024.

19 ZB *FAZ,* 4.2.2021, Wert von 50 Millionen Euro: Computer-Betrüger rückt Bitcoin-Passwort nicht heraus, <https://www.faz.net>, zuletzt abgefragt am 5.7.2024; *t-online,* 1.5.2021, 36 Millionen Euro: Unbekannte stehlen Polizei beschlagnahmtes Bitcoinvermögen, <https://www.tonline.de>, zuletzt abgefragt am 5.7.2024; *Stern,* 30.8.2021, »Das ist alles sehr unglücklich«: Polizei muss Dealer über eine Million Euro in Bitcoin zurückgeben, <https://www.stern.de>, zuletzt abgefragt am 5.7.2024.

Weiterentwicklung der behandelten Technologie erschwert werden und nicht alle Erscheinungsformen erfassen können.[20] Im Einzelfall ist also stets zu prüfen, ob auch der konkret fragliche Wert und die ihm zugrundeliegenden Bestandteile die hier typisiert angeführten Eigenschaften aufweisen. Insb ist die Abgrenzung zwischen öffentlichen Systemen, deren Betrieb auf Dezentralität ausgerichtet ist (umgangssprachlich werden diese Systeme auch als *»permissionless«* bezeichnet) und solchen Systemen, die klar identifizierbare Betreiber aufweisen *(»permissioned«)* wesentlich. Die Ausführungen dieses Beitrags beziehen sich – wie augenscheinlich auch die erlassmäßigen Vorgaben von BMI und BMJ sowie die Materialien zum Entwurf des StPRÄG 2024 – auf erstere Variante.[21]

A. Blockchain

Typische Basis eines Kryptowertes ist eine Blockchain – eine mögliche Variante der Distributed-Ledger-Technologie, die verteilte Datenspeicherung ermöglicht. Bei einer Blockchain handelt es sich um eine Datenstruktur, bei der die Daten in Blöcke gestaffelt und diese Blöcke wiederum mithilfe kryptographischer Verfahren miteinander »verkettet« werden.[22] Eine Aufnahme neuer Daten in diese Datenstruktur geschieht grundsätzlich nicht durch eine Veränderung der bereits enthaltenen Daten – vielmehr gilt die »Unveränderlichkeit« der abgelegten Daten und ihrer chronologischen Reihenfolge im Regelfall geradezu als charakteristisch.[23] Stattdessen wird ein neuer Block erstellt und die Blockchain mit ihm ergänzt, sodass er nun das Ende der Datenstruktur bildet.[24] Das auf diese Art erstellte Datenverzeichnis wird üblicherweise nicht als ein einziges Original zentral (etwa auf einem Bankserver) abgespeichert, sondern idente Kopien davon werden über ein Netzwerk an teilnehmende Rechner übertragen und durch diese gespeichert *(»distributed ledger«);* die Kopien werden laufend aktualisiert, damit alle beteiligten Rechner stets über die neueste Version der Blockchain einschließlich der zuletzt erstellten Blöcke verfügen.[25] Die Teilnahme am Netzwerk ist bei jenen Blockchains, die Kryptowerten zugrunde liegen, idR jedem möglich, der über einen entsprechend leistungsfähigen Rechner verfügt.[26] Diese Art der Datenergänzung und -verwaltung ermöglicht eine weitgehende Absicherung vor nachträglichen Eingriffen und Manipulationen.

Anzumerken ist, dass Blockchains zwar insb im Kontext mit Kryptowerten bekannt geworden sind, sie aber auch in anderen Zusammenhängen als vielversprechende Technologie angesehen bzw auf ihre Eignung geprüft werden. Bereits seit Längerem wird ihr Einsatz beispielsweise bei der Nachverfolgung von Produktions- und Lieferketten argumentiert[27] – ein Thema, das durch Normierungsbemühungen der EU[28] auch aktuell in Diskussion steht. Außerdem hat die Kooperation *Europäische Blockchain-Partnerschaft* auf EU-Ebene ua den Aufbau einer *Europäischen Blockchain Services Infrastruktur* (»EBSI«) zum Ziel, um letztlich EU-weite Verwaltungsdienstleistungen zur Verfügung zu stellen.[29] Allerdings ist zu erwarten, dass für solche Anwendungen konzipierte Blockchain-Modelle wesentlich andere Eigenschaften aufweisen werden als jene, welche idR die Basis von Kryptowerten bilden.

B. Kryptowerte als über die Blockchain verwaltete Werteinheiten

Sollen mithilfe einer Blockchain Kryptowerte verwaltet werden, so handelt es sich bei den dokumentierten Informationen insb um Transaktionsdaten.[30] Die Blockchain dient in diesem Fall als eine **verteilt gespeicherte Datenbank,** die ein **Verzeichnis der durchgeführten Übertragungsvorgänge** darstellt. Um einen Transfer von Kryptowerten (von A an B) durchzuführen, wird die

20 Zu erwähnen ist insb, dass die Ausführungen zu technischen Prozessen in diesem Beitrag va für die sog »Coins« bzw »Native Tokens« Gültigkeit besitzen, während etwa Transaktionen von ERC20-Tokens und anderen nicht nativen Kryptowerten davon abweichen können.

21 Die Bedeutung dieser Differenzierung zeigt sich etwa im Rahmen der Verordnung (EU) 2023/1114 (Verordnung über Märkte für Kryptowerte), wo Unterschiede dieser Art ausschlaggebend für den Anwendungsbereich sind (vgl ErwGr 22).

22 Siehe genauer *Antonopoulos,* Bitcoin 197 ff.

23 *Wittenberg,* Blockchain für Unternehmen (2020) 9.

24 *Wittenberg,* Blockchain 9.

25 *Wittenberg,* Blockchain 24.

26 Vgl für Bitcoin *Narayanan/Bonneau/Felten/Miller/Goldfeder,* Bitcoin and Cryptocurrency Technologies (2016) 66 f.

27 Siehe nur etwa: *Boucher,* Wissenschaftlicher Dienst des Europäischen Parlaments, Wie die Blockchain-Technologie unser Leben verändern könnte (Februar 2017) <https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_DE.pdf>, zuletzt abgefragt am 5.7.2024, 18 ff; *Wittenberg,* Blockchain 199 ff, 212 ff; *Regierer,* Transparenz von Lieferketten durch die Blockchain, in Breidenbach/Glatz (Hrsg), Rechtshandbuch Legal Tech² (2021) 128 (128 ff); *Bundesministerium für Arbeit und Wirtschaft,* Die Rolle moderner Technologien, insbesondere Blockchain, in der Lieferkettenverantwortung, <https://www.bmaw.gv.at/Services/Publikationen/Moderne-Technologien-in-der-Lieferkettenverantwortung.html> (zuletzt abgefragt am 5.7.2024).

28 Hier zu nennen sind insb der Vorschlag für eine RL über die Sorgfaltspflichten von Unternehmen im Hinblick auf Nachhaltigkeit (sog »EU-Lieferkettengesetz«) und der Vorschlag für eine Verordnung zur Schaffung eines Rahmens für die Festlegung von Ökodesign-Anforderungen für nachhaltige Produkte (sog »Ökodesign-Verordnung«).

29 Nähere Informationen sind ebenso der Homepage der Europäischen Kommission zu entnehmen, siehe <https://ec.europa.eu>, zuletzt abgefragt am 5.7.2024.

30 Auf eine Differenzierung zwischen UTXO-Modellen und kontenbasierten Modellen wird der Einfachheit halber an dieser Stelle verzichtet.

gewünschte Transaktion vom übertragenden Teilnehmer digital signiert und ans Netzwerk geschickt. Wird sie erfolgreich in einen neuen Block aufgenommen und dieser wie im Vorkapitel beschrieben ans Ende der Blockchain angereiht, wird dadurch diese Transaktion dokumentiert (siehe dazu genauer im folgenden Kapitel). Die Blockchain bildet folglich die gesamte Transaktionshistorie ab und dokumentiert dadurch sowohl die historische als auch implizit die aktuelle Zuweisung von Werteinheiten.

Kryptowerte werden hierbei nicht etwa identifizierten Personen, sondern Zahlen- und Ziffernfolgen, sog »**Adressen**«, zugeordnet. Um eine solche Adresse zu erstellen, wird im ersten Schritt durch einen Algorithmus eines asymmetrischen Signaturverfahrens ein **kryptographisches Schlüsselpaar,** bestehend aus dem »Public Key« und dem »Private Key«, erstellt.[31] Der Public Key dient in der Folge dazu, die Adresse davon abzuleiten, der anschließend Kryptowerte im Rahmen einer Transaktion zugeordnet werden können.[32] Zur Teilnahme am Netzwerk und zum Handel mit diesen Werten ist idR keine Offenlegung der realen Identität eines Teilnehmers erforderlich. Die verwendeten Adressen können somit als Pseudonym der dahinterstehenden Personen angesehen werden.[33] Wenn ein Nutzer Kryptowerte unmittelbar von einem anderen Nutzer erwirbt, die Zugriffsdaten (insb den Private Key) selbst verwaltet und die Werte gegebenenfalls auch unmittelbar über das Netzwerk weiterveräußert, kann er somit grundsätzlich all diese Schritte pseudonym setzen. Allerdings ist die Inanspruchnahme von Dienstleistungen Dritter (zB sog »Krypto-Börsen«, idR Online-Handelsplattformen) für Erwerb, Verwaltung und Weiterveräußerung weit verbreitet. Aufgrund rechtlicher Vorgaben müssen solche Diensteanbieter regelmäßig die Identität ihrer Kunden erheben. Nehmen Teilnehmer solche Angebote in Anspruch, ist eine Offenlegung der persönlichen Daten also sehr wohl erforderlich. Je nach Ausgestaltung der Geschäftsbeziehung zwischen Diensteanbieter und Nutzer ist es außerdem durchaus üblich, dass der Nutzer selbst nicht über die betreffenden Kryptowerte und Zugriffsdaten (insb den Private Key) verfügt, sondern nur einen diesbezüglichen schuldrechtlichen Anspruch gegenüber dem Anbieter hat. Dieser Unterschied ist, wie unten ausgeführt wird, relevant für die den Behörden offenstehenden Möglichkeiten einer Sicherstellung.

Der Einsatz der Blockchain-Technologie ermöglicht also letztlich die **dezentrale Verwaltung der Kryptowerte** und trägt somit zu jenen Eigenschaften bei, die diese virtuellen Vermögensgüter rechtlich schwer fassbar machen.

C. Die Übertragung von Kryptowerten

Um eigene Kryptowerte an jemanden anderen zu übertragen, schickt der Teilnehmer, wie bereits angeführt, eine Transaktionsanordnung an das Netzwerk aus, die ua den Transaktionsbetrag sowie Herkunfts- und Zieladresse enthält. Zum Nachweis der Verfügungsmacht über die betreffenden Einheiten dient eine digitale Signatur dieser Nachricht, für deren Erstellung der Überträger jenen Private Key verwendet, der zur übertragenden Adresse gehört.[34] Damit die Transaktion vom Netzwerk verarbeitet wird, ist generell auch die Entrichtung einer **Transaktionsgebühr** notwendig, die gewöhnlich derjenige Netzwerkteilnehmer erhält, der die Transaktion in einen neuen Block mit aufnimmt. Diese Belohnung soll die Teilnehmer dazu motivieren, die Transaktion zu verarbeiten, kann jedoch je nach Auslastung des Systems in ihrer Höhe teilweise stark variieren.

Die am Netzwerk teilnehmenden Rechner können anhand ihrer selbst abgespeicherten Kopie der aktuellen Blockchain kontrollieren, ob der angeführten Herkunftsadresse ausreichend Kryptowerte zugeschrieben sind. Mithilfe eines kryptographischen Verfahrens sind sie außerdem in der Lage nachzuprüfen, ob die Transaktionsnachricht mit dem richtigen Private Key signiert wurde.[35] Sind alle Voraussetzungen erfüllt, wird die gewünschte Übertragung schließlich **in einen neuen Datenblock aufgenommen und dieser der Blockchain angefügt.** Die Blockchain dokumentiert ab diesem Zeitpunkt die neue Zuordnung der Kryptowerte.[36] Nunmehr kann nur jemand, der den Private Key zur neuen Zuordnungsadresse kennt, die übertragenen Einheiten erneut an eine andere Adresse übertragen. Die Signatur der Transaktionsnachricht mithilfe des richtigen Private Key ermöglicht es also, über die einer Adresse zugeordneten Kryptowerte zu verfügen. Ohne den Private Key zu kennen, ist eine solche Verfügung **nicht möglich** – andererseits kann aber **jeder,** der Kenntnis von diesem kryptographischen Schlüssel erlangt, eine Transaktion durchführen. Mit der Phrase *»Not Your Keys, Not Your Coins«* wird in diesem Zusammenhang oft die Tatsache betont, dass nur der alleinige Zugriff auf die kryptographischen Schlüssel garantieren kann, dass man tatsächlich die Verfügungsgewalt über die betreffenden Kryptowerte hat und auch behält.

31 Vgl für Bitcoin *Antonopoulos,* Bitcoin 59 ff.
32 Vgl für Bitcoin *Antonopoulos,* Bitcoin 58 f, 68.
33 *Narayanan/Bonneau/Felten/Miller/Goldfeder,* Bitcoin 139.
34 Vgl für Bitcoin *Antonopoulos,* Bitcoin 60; vgl auch *Völkel,* Grundlagen der Blockchain-Technologie und virtueller Währungen, in Piska/Völkel (Hrsg), Blockchain rules (2019) Rz 1.41 ff.
35 Vgl *Antonopoulos,* Bitcoin 58 ff und 140 ff.
36 Vgl etwa *Antonopoulos,* Bitcoin 240 ff.

Durch den Einsatz kryptographischer Verfahren und digitaler Signaturen können somit Transaktionen verlässlich und idR manipulationssicher durchgeführt werden. Die Nutzer können die Werte unmittelbar selbst verwalten und über das Netzwerk einander übertragen, ohne dafür auf eine zentrale Abwicklungsstelle wie etwa Kreditinstitute oder eine staatliche Behörde angewiesen zu sein. Vertrauen in solche Intermediäre oder den Transaktionspartner ist nicht erforderlich.[37] Aufgrund des dezentralen Betriebs des Systems und der verteilten Speicherung auf vielen Rechnern beeinträchtigt ein Ausfall einzelner das System selbst nicht und es können etwa weiterhin Transaktionen durchgeführt werden. Das bedeutet freilich auch, dass behördliche Anordnungen, gerichtet zB an einzelne bekannte Teilnehmer des Netzwerkes, spätere Transaktionen nicht verhindern können, da diese dennoch von anderen Teilnehmern verarbeitet werden würden. Eine zentrale Entität, an die eine solche Anordnung gerichtet werden und die die Einhaltung durch alle anderen Teilnehmer erzwingen könnte, ist in diesen Systemen typischerweise gerade nicht vorgesehen.

Wie aus diesen Ausführungen ersichtlich ist, sind **nicht etwa die Werteinheiten selbst** in der Blockchain »gespeichert«, sondern lediglich die Transaktionshistorie; diese wird ergänzt und dadurch die in der Transaktionsnachricht angegebene Menge einer Adresse ab- und einer anderen zugeschrieben. Insofern wird – anders als der Ausdruck suggerieren könnte – bei einer Transaktion gerade nicht eine Einheit als abgrenzbarer Datensatz »versendet« bzw »übertragen«. Es wird lediglich im verteilt gespeicherten Verzeichnis der Transaktionen notiert, dass bestimmte Kryptowerte nun einer anderen Adresse zugeordnet sein sollen.

D. Wallets

Jene Informationen, die zur Verfügung über Kryptowerte erforderlich sind – vor allem Public und Private Keys – können auf unterschiedliche Weise aufbewahrt und genutzt werden. Die Mittel zu ihrer Verwaltung werden dabei üblicherweise als »Wallets« bezeichnet[38] – beim simplen Notieren oder Ausdrucken auf Papier (zB in Form eines QR-Codes) wird etwa von einer »Paper Wallet« gesprochen.[39] Praktikabler ist oft die Nutzung einer Software auf Smartphone bzw Computer oder in einer Cloud-Anwendung, einer »digitalen Wallet« also.[40] Verfügbar sind außerdem »Hardware Wallets« – spezielle Geräte, die mit einem Computer oder Smartphone verbunden werden können.[41] Je nach technischer Ausgestaltung kann eine Wallet mehrere Schlüssel verwalten und können die Kryptowerte auf viele verschiedenen Adressen verteilt sein. Die Nutzung von Wallet-Arten, bei denen keine aufrechte Verbindung zum Internet besteht und die daher vor Hacking-Angriffen geschützt sind (insb Paper Wallets und nicht angeschlossene Hardware Wallets), wird außerdem häufig als »Cold Storage« (im Gegensatz zur »Hot Storage«) bezeichnet.[42]

Zu beachten ist in diesem Zusammenhang wiederum, dass in all diesen Fällen **nicht** etwa **Einheiten selbst abgespeichert werden**, da sie in diesem Sinn gar nicht als gesonderte Datensätze existieren. In einer solchen Wallet abgelegt, über sie verwaltet und genutzt werden **nur die Zugriffsdaten.** Gelegentlich in der Literatur anzutreffende Aussagen, dass Einheiten selbst auf die Wallet übertragen werden, sind somit zwar bildhaft, aber an sich technisch nicht korrekt. Problematisch ist insofern, dass solche missverständlichen Formulierungen auch in Veröffentlichungen der Verwaltung[43] sowie in Erlässen[44] vorkommen und – wie unten dargestellt wird – vor diesem Hintergrund nach der (noch) geltenden Rechtslage auch die Anwendbarkeit der Sicherstellungsbestimmungen auf Kryptowerte begründet wird. Auch die Materialien des hier behandelten Gesetzesvorschlags enthalten bedauerlicherweise entsprechende Formulierungen.[45]

37 Vgl *Nakamoto,* Bitcoin: A Peer-to-Peer Electronic Cash System, 1: *»an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party«.*

38 *Narayanan/Bonneau/Felten/Miller/Goldfeder,* Bitcoin 76 ff.

39 *Narayanan/Bonneau/Felten/Miller/Goldfeder,* Bitcoin 83.

40 Vgl *Blocher,* The next big thing: Blockchain – Bitcoin – Smart Contracts, dAnwBl 2016, 612 (616), der daher in diesem Zusammenhang von einem »digitalen Schlüsselbund« spricht.

41 *Wittenberg,* Blockchain 33.

42 *Antonopoulos,* Bitcoin XXIV.

43 So etwa in *Tofan,* Verfolgung digitaler Geldflüsse, Öffentliche Sicherheit – Das Magazin des Innenministeriums 7–8/2020, 79 (80), wo ausgeführt wird, dass *»Bitcoins oder andere Kryptowährungen«* in einer Wallet *»gespeichert sind«* und es durch mittlerweile erstellte Behördenwallets möglich ist, *»Bitcoins […] an die Wallets der Polizei beziehungsweise Justiz zu übermitteln«.* Ähnlich wird in *BMI,* Cybercrime Report 2023, 77 erklärt, eine Wallet sei eine *»virtuelle Geldtasche, in der Benutzerinnen und Benutzer Bitcoins oder andere Kryptowährungen aufbewahren«* und eine Wallet könne *»mehrere unterschiedliche Kryptowährungen beinhalten«.*

44 So etwa bei der ersten Auflage des von BMJ herausgegebenen Leitfadens zu vermögensrechtlichen Anordnungen aus dem Jahr 2014 (Erlass des BMJ vom 17. 2. 2014, Leitfaden »Vermögensrechtliche Anordnungen«, BMJ-S90.021/0004-IV 3/2014, 78): Zwar wird in diesem noch nicht detailliert auf Kryptowerte eingegangen, jedoch im Rahmen der Ausführungen zu Sicherstellungen erwähnt, dass Bitcoins *»nur durch Sicherstellung jenes Datenträgers gesichert werden [können], auf denen sie abgespeichert sind (in der Regel in einem sogenannten ›wallet‹)«.* In der Folge wird auf die Gefahr der Existenz von *»Kopien von Bitcoins auf anderen Datenträgern«* hingewiesen, wobei diese *»Kopien« »gleich dem Original verwertbar«* seien.

45 Vgl ErlME 349/ME XXVII. GP, 37, 39 f.

IV. Maßnahmen zur Sicherung von Kryptowerten gegen nachteilige Verfügungen

A. Mögliche Herangehensweisen

Faktisch stehen zur Absicherung von Kryptowerten gegen spätere nachteilige Verfügungen mehrere Optionen mit jeweils unterschiedlichen Auswirkungen zur Wahl:

1. **Sind im konkreten Fall Dienstleistungsanbieter involviert,** die fragliche Kryptowerte ihrer Kunden verwalten (insb Betreiber von Krypto-Börsen oder Wallet-Provider), könnte diesen Anbietern durch eine **Anordnung** insb die Herausgabe, Veräußerung oder Verpfändung dieser Werte verboten und dadurch ein vorläufiger Schutz erreicht werden.

Fehlt ein solcher Ansprechpartner, ist eine effektive Sicherung schwieriger:

2. So können **Gegenstände und Daten** übernommen werden, **die solche Verfügungen ermöglichen** – insb körperliche Datenträger, auf denen zugehörige kryptographische Schlüssel abgespeichert sind. Dies kann aber freilich die Durchführung von Transaktionen nur dann verhindern, wenn nicht weitere Kopien dieser Daten vorliegen und genutzt werden.

3. Ein effektiverer Schutz kann erreicht werden, indem – bei Ermittlung der entsprechenden kryptographischen Schlüssel – ein **Transfer der betroffenen Kryptowerte an eine Adresse, deren zugehörige kryptographische Schlüssel ausschließlich behördlich kontrolliert werden,** bewirkt wird.

Anzumerken ist, dass nur im letzten Fall auf den Vermögenswert selbst zugegriffen wird, indem seine Zuordnung (konkret zu einer bestimmten Adresse) verändert wird. Nur in diesem Fall wird somit behördlicherseits eine tatsächliche – Einwirkungen von anderer Seite ausschließende – Verfügungsmacht über den Kryptowert selbst begründet. Beim Entzug einer Wallet (2) hingegen betrifft der Eingriff nur diese und die in ihr gespeicherten Informationen, also gewissermaßen ein Werkzeug zur Verfügung über den Vermögenswert; durch eine Anordnung an einen Dienstleister (1) wird dessen Kooperation mit Verfügungen durch einen Dritten (einen Kunden) verhindert. Die Zuordnung der Kryptowerte selbst wird in diesen beiden Fällen nicht geändert, nur die Einwirkungsmöglichkeit durch den – präsumtiv – Berechtigten faktisch behindert.

B. Vorgehen in der Praxis

Hinsichtlich der praktischen Durchführung von Sicherungsmaßnahmen wurde 2018 im Bundeskriminalamt eine »Kompetenzstelle virtuelle Währungen und Kryptowährungen« eingerichtet[46] und zwischenzeitlich auch im Rahmen interner Schulungen des BMI mit Polizisten die Handhabung von Kryptowerten geübt.[47] Nach offiziellen Angaben ist dementsprechend das Cybercrime Competence Center (C4) *»seit 2018 rechtlich und technisch in der Lage, Sicherstellungen von Kryptowährungen durchzuführen«.*[48] Veröffentlichungen und Erlässe zeigen, dass hierfür alle drei oben genannten Optionen in Anspruch genommen werden: Einerseits werden **Verbote an Dienstleister** ausgesprochen und andererseits werden **Datenträger zum Auslesen der Verfügungsdaten sichergestellt** und diese Daten in der Folge genutzt, um Kryptowerte **auf behördlich kontrollierte Adressen zu übertragen.** In Publikationen wird dabei in erster Linie letztere Methode betont und ausgeführt, dass dafür *»unter höchsten Sicherheitsvorkehrungen sogenannte Behördenwallets erstellt und zur Aufbewahrung von virtuellen Währungseinheiten verwendet«* werden.[49] Nach Angaben des BMI verfügt das Bundeskriminalamt über etwa 1.000 solcher Wallets,[50] die sodann zum Schutz vor unbefugten Zugriffen vom Internet getrennt werden.[51] Erlässe des BMJ stellen außer dieser Möglichkeit auch den Ausspruch der erwähnten Drittverbote bzw Veräußerungs- und Verpfändungsverbote in den Raum, soweit ein entsprechender Adressat vorhanden ist.[52] Aus den Materialien zum StPRÄG 2024 ist erkennbar, dass dieses keine Einschränkung der genannten Optionen beabsichtigt, sondern vielmehr auch in Zukunft an sich alle drei Methoden zum Einsatz kommen sollen.

46 Vgl 793/AB XXVII. GP, 6.

47 *Tofan,* Öffentliche Sicherheit – Das Magazin des Innenministeriums 7–8/2020, 79 (80) bzw *M. R.-E.,* Blockchain-Ermittlungen, Öffentliche Sicherheit – Das Magazin des Innenministeriums 3–4/2020, 44 (44).

48 *BMI,* Cybercrime Report 2023, 70. Vgl auch *M. R.-E.,* Öffentliche Sicherheit – Das Magazin des Innenministeriums 3–4/2020, 44 (44).

49 *BMI,* Cybercrime Report 2023, 70. Vgl auch *Tofan,* Öffentliche Sicherheit – Das Magazin des Innenministeriums 7–8/2020, 79 (80) sowie *M. R.-E.,* Öffentliche Sicherheit – Das Magazin des Innenministeriums 3–4/2020, 44 (44).

50 *BMI,* Cybercrime Report 2023, 70; *M. R.-E.,* Öffentliche Sicherheit – Das Magazin des Innenministeriums 3–4/2020, 44 (44).

51 *Tofan,* Öffentliche Sicherheit – Das Magazin des Innenministeriums 7–8/2020, 79 (80).

52 Erlass des BMJ vom 28. 5. 2020 zur Aktualisierung des Leitfadens Vermögensrechtliche Anordnungen (3. Auflage), GZ 2020-0.303.132 – Leitfaden Vermögensrechtliche Anordnungen (2020), 109; Erlass des BMJ vom 1. 4. 2020 zum Vorgehen bei Sicherstellung, Beschlagnahme und Verwertung von virtuellen Währungen im Bereich der Justiz, GZ 2020-0.163.092, 4 f.

V. Zur Sicherung von Kryptowerten herangezogene Bestimmungen – aktuelle Rechtslage und im Strafprozessrechtsänderungsgesetz 2024 vorgesehene Änderungen

Im Jahr 2017 erklärten die österreichischen Staatsanwälte einem europäischen Evaluierungsbericht zufolge noch, *»dass sie sich bislang zwar noch nicht mit der Bitcoin-Frage auseinandergesetzt haben, sie jedoch der Meinung sind, dass die Suche nach Bitcoin-Vermögenswerten und deren Sicherstellung nach ihren Rechtsvorschriften möglich ist«.*[53] Seither wurde diese Rechtsansicht in Erlässen von BMJ und BMI bestätigt und näher ausgeführt. Als Rechtsgrundlage werden dabei die Sicherstellungsbestimmungen – und dabei insb gerade auch jene, welche der VfGH teils mit Ablauf des 31. Dezember 2024 aufgehoben hat – genannt.

In diesem Kapitel werden die herangezogenen Bestimmungen in ihrer aktuellen Fassung jener **gegenübergestellt**, die im StPRÄG 2024 vorgesehen ist, und es wird auf die **Unterschiede** eingegangen. Um einen besseren Überblick zu schaffen sind Wortfolgen, die nach dem StPRÄG 2024 entfallen sollen, durchgestrichen dargestellt, neu hinzugefügte unterstrichen. Zur Sicherung von Beweismaterial und Vermögenswerten ist nach aktueller Rechtslage in der StPO zunächst die **Sicherstellung** vorgesehen. Diese ist als vorläufige Maßnahme in manchen – aber nicht allen – Fällen später mittels gerichtlicher Verhängung der Beschlagnahme zu bestätigen.[54] Im StPRÄG 2024 ist zusätzlich die Einführung der **»Beschlagnahme von Datenträgern und Daten«** als neue Maßnahme vorgesehen.

A. Begriff der Sicherstellung und der Beschlagnahme von Datenträgern und Daten

1. Legaldefinitionen – Gegenüberstellung

Die Legaldefinition der zur Verfügung stehenden Maßnahmen findet sich im (von der verfassungsgerichtlichen Aufhebung durch G 352/2021 nicht betroffenen) § 109 StPO:

§ 109 StPO, BGBl Nr 631/1975 idF BGBl I Nr 26/2016:

Im Sinne dieses Gesetzes ist
1. »Sicherstellung«
   a. die vorläufige Begründung der Verfügungsmacht über Gegenstände und
   b. das vorläufige Verbot der Herausgabe von Gegenständen oder anderen Vermögenswerten an Dritte (Drittverbot) und das vorläufige Verbot der Veräußerung oder Verpfändung solcher Gegenstände und Werte,

[…]

§ 109 StPO, Fassung StPRÄG 2024 (4125/A, 349/ME):

Im Sinne dieses Gesetzes ist
1. »Sicherstellung«
   a. die vorläufige Begründung der Verfügungsmacht über Gegenstände, außer über Datenträger und Daten zum Zweck der Auswertung von Daten (Z 2a), sowie über Vermögenswerte, und
   b. das vorläufige Verbot der Herausgabe von Gegenständen oder anderen Vermögenswerten an Dritte (Drittverbot) und das vorläufige Verbot der Veräußerung oder Verpfändung solcher Gegenstände und ~~Werte~~ Vermögenswerte,

1a. »Vermögenswerte« Vermögenswerte jeder Art, ob körperlich oder unkörperlich, beweglich oder unbeweglich, einschließlich Vermögensrechte und Kryptowerte sowie Urkunden in jeder Form, die ein Recht an solchen Vermögenswerten belegen,

[…]

2a. »Beschlagnahme von Datenträgern und Daten« eine gerichtliche Entscheidung auf Begründung einer Sicherstellung über
   a. Datenträger und darauf gespeicherte Daten,
   b. Daten, die an anderen Speicherorten als einem Datenträger gespeichert sind, soweit auf sie von diesem aus zugegriffen werden kann, oder
   c. Daten, die auf Datenträgern gespeichert sind, die zuvor für andere Zwecke sichergestellt wurden,

   zum Zweck der Auswertung von Daten,

[…]

2. Änderungen im Bereich der Sicherstellung

Das Gesetz unterscheidet nach (noch) aktueller Rechtslage zwischen zwei Arten der Sicherstellung: Diese Maßnahme kann

1. nach lit a durch »Begründung der Verfügungsmacht über Gegenstände« oder
2. nach lit b durch »Verbot der Herausgabe von Gegenständen oder anderen Vermögenswerten an Dritte« bzw »Verbot der Veräußerung oder Verpfändung solcher Gegenstände und Werte«

durchgeführt werden.

Die beiden Kategorien unterscheiden sich deutlich sowohl in der Art der Sicherung als auch in Bezug auf die Sicherstellungsobjekte: Während eine **Begründung von Verfügungsmacht** ausschließlich bei **Gegenständen** vor-

53 *Rat der EU,* Evaluierungsbericht über die siebte Runde der gegenseitigen Begutachtungen »Praktische Umsetzung und Durchführung europäischer Strategien zur Verhütung und Bekämpfung von Cyberkriminalität« – Bericht über Österreich vom 18.5.2017, 152054/EU XXV. GP, 57, abrufbar unter <https://www.parlament.gv.at/gegenstand/XXV/EU/140779>, zuletzt abgefragt am 5.7.2024.

54 Vgl *Tipold/Zerbes; Flora* in Fuchs/Ratz, WK StPO § 109 (Stand 13.11.2017, rdb.at) Rz 1, 4 ff; *Tipold/Zerbes* in Fuchs/Ratz, WK StPO Vor §§ 110–115 (Stand 1.3.2021, rdb.at) Rz 3. Nach dem gesetzlichen Konzept der gerichtlichen Beschlagnahme könnte eine solche in Bezug auf körperliche Gegenstände (wie etwa einen Datenträger) auch unabhängig von einer vorangegangenen Sicherstellung stattfinden, dies ist jedoch nach den Ausführungen in der Begründung zum StPRÄG 2024 kaum der Fall; ErlME 349/ME XXVII. GP, 9.

gesehen ist, kann sich die **Erlassung eines Drittverbots bzw Veräußerungs- oder Verpfändungsverbots** sowohl auf **Gegenstände** als auch auf **andere Vermögenswerte** beziehen. Schon den Gesetzesmaterialien[55] ist zu entnehmen, dass der Begriff des Gegenstands in dieser Bestimmung ausschließlich körperliche Sachen umfasst. Dies wird folglich von der hL[56] und der Rsp[57] so anerkannt und auch der VfGH führt in G 352/2021 aus: *»Bei den Gegenständen, die gemäß § 110 Abs 1 Z 1 iVm § 109 Z 1 lit a StPO zu Beweiszwecken sichergestellt werden dürfen, handelt es sich um jegliche bewegliche körperliche Sache, sodass darunter auch ein Laptop, PC, Mobiltelefon (»Smartphone«) oder ein sonstiges IT-Endgerät fallen.«*[58] Demgegenüber ist der Begriff des Vermögenswerts weiter und umfasst auch unkörperliche Sachen, sodass etwa auch Forderungen (wie Bankguthaben) durch ein Drittverbot sichergestellt werden können.[59]

Die im StPRÄG 2024 vorgeschlagene Legaldefinition der Sicherstellung nach § 109 Z 1 lit a StPO führt einerseits zu einer Einschränkung, andererseits zu einer Ausdehnung:

- Fälle, in denen Verfügungsmacht über Gegenstände begründet werden soll, fallen demnach **dann nicht** unter den Begriff der Sicherstellung nach § 109 Z 1 lit a StPO, wenn es sich erstens beim Sicherungsobjekt um **Datenträger bzw Daten** handelt **und** zweitens **Zweck der Maßnahme die Auswertung von Daten** ist. Diese Konstellationen werden gleichsam aus dem Sicherstellungsbegriff herausgelöst und fallen stattdessen in die neue, an strengere Voraussetzungen geknüpfte, Ermittlungsmaßnahme der »Beschlagnahme von Datenträgern und Daten« nach § 109 Z 2a StPO. In Hinblick auf die Abgrenzung dieser Maßnahmen voneinander ist zu betonen, dass nach dem Gesetzesvorschlag somit **nicht alle Zugriffe auf Datenträger bzw Daten** aus dem Sicherstellungsbegriff ausgeschlossen werden, sondern die Differenzierung gerade auch aus der **Zielrichtung** der Maßnahme erfolgt. Deutlich drücken dies die Erläuterungen zum StPRÄG 2024 aus, wenn zu den (strengeren) Voraussetzungen für eine Maßnahme nach § 109 Z 2a StPO ausgeführt wird: *»Zum Tragen kommen die Regelungen nur dann und verdrängen damit die allgemeinen Bestimmungen der Sicherstellung und Beschlagnahme (§§ 110 ff StPO), wenn die Beschlagnahme aus Beweisgründen und zum Zweck der Auswertung der Daten erfolgt«.*[60] Soll ein Datenträger aus anderen Gründen gesichert werden – die Materialien nennen an anderer Stelle etwa die Sicherung von Blutspuren oder Fingerabdrücken –, so kann er durchaus hierfür iSd § 109 Z 1 lit a StPO sichergestellt werden. Sollen im Nachhinein aber auch darauf gespeicherte Daten ausgewertet werden, handelt es sich sodann um eine »Beschlagnahme von Datenträgern und Daten« nach § 109 Z 2a lit c StPO.[61]
- Zu einer deutlichen Erweiterung des Sicherstellungsbegriffs soll es demgegenüber durch die Aufnahme von (im neuen § 109 Z 1a StPO definierten) »**Vermögenswerten**« in die Legaldefinition nach § 109 Z 1 lit a kommen. Wie den Materialien zu entnehmen ist, soll *»das System breitflächig um (auch immaterielle) Vermögenswerte ergänzt werden«,* und zwar in einem Vorgriff auf europarechtliche Vorgaben, nämlich die Richtlinie 2024/1260 über die Abschöpfung und Einziehung von Vermögenswerten.[62] Dafür soll *»der Begriff der Vermögenswerte klar, umfassend und technologieneutral in die StPO eingeführt werden«.*[63] Weiters erklären die Materialien ausdrücklich, dass diese Ergänzung bezweckt, *»unter anderem die Sicherstellung (und allfällige Beschlagnahme samt nachfolgender Verwertung) von digitalen Kryptowerten zu ermöglichen«*[64]. **Bisher** seien Vermögenswerte **nicht von § 109 Z 1 lit a StPO, sondern lediglich von lit b leg cit erfasst,** was gerade bei Krypto-

55 ErlRV 25 BlgNR XXII. GP, 153: *»Nach der Definition der Z 1 soll der Begriff ›Sicherstellung‹ sowohl die Begründung der (tatsächlichen) Verfügungsmacht über Gegenstände (bewegliche körperliche Sachen – lit a) als auch das (vorläufige) Verbot der Herausgabe, Veräußerung oder Verpfändung solcher Gegenstände und das Verbot der Herausgabe von anderen Vermögenswerten (Geld, Wertpapiere, Forderungen, Inhaber- und Überbringersparbücher) an Dritte (›Drittverbot‹ – lit b) umfassen.«*

56 *Tipold/Zerbes; Flora* in Fuchs/Ratz, WK StPO § 109 Rz 2; *Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 110 (Stand 1.3.2021, rdb.at) Rz 3; *Kroschl* in Schmölzer/Mühlbacher, § 109 StPO Rz 2. *Keplinger/Prunner/Pühringer/Rebisant* in Birklbauer/Haumer/Nimmervoll/Wess (Hrsg), StPO – Linzer Kommentar zur Strafprozessordnung (2020) zu § 109 StPO Rz 3 vertreten demgegenüber, Gegenstände könnten *»alle Sachen iSd Zivilrechts sein […]. Die Verfügungsmacht im Sinne der lit a kann jedoch nur über bewegliche körperliche Sachen begründet werden«.* Das Ergebnis ist dasselbe.

57 Vgl zB OGH 12.10.2021, 14 Os 107/21y, EvBl-LS 2022/72.

58 VfGH 14.12.2023, G 352/2021, Rz 35.

59 *Tipold/Zerbes; Flora* in Fuchs/Ratz, WK StPO § 109 Rz 2; *Keplinger/Prunner/Pühringer* in Birklbauer/Haumer/Nimmervoll/Wess, § 109 StPO Rz 10. Auch in *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) werden dafür Kontoguthaben angeführt, bei denen es sich *»um Forderungen gegenüber einem Kredit- oder Finanzinstitut und somit nicht um einen ›Gegenstand‹, sondern um einen Vermögenswert im Sinne des § 109 Z 1 lit b StPO«* handle – die Sicherstellung sei somit mittels Ausspruchs eines Drittverbots zu vollziehen; *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 61.

60 ErlME 349/ME XXVII. GP, 15.

61 ErlME 349/ME XXVII. GP, 11.

62 ErlME 349/ME XXVII. GP, 6, 37. Die Legaldefinition für »Vermögensgegenstände« in Art 3 Z 2 der genannten Richtlinie bezieht ausdrücklich Kryptowerte mit ein und stimmt auch sonst fast wortgleich mit jener für § 109 Z 1a StPO vorgeschlagenen Begriffsbestimmung überein.

63 ErlME 349/ME XXVII. GP, 6, 37.

64 ErlME 349/ME XXVII. GP, 37.

werten zu Problemen führe, nämlich, *»dass die Sicherstellung von immateriellen Vermögenswerten nur verlässlich durchgeführt wurden [sic!] kann, wenn auch tatsächlich ein valider Dritter vorhanden ist, dem gegenüber das entsprechende Dritt- oder Veräußerungs- und Verpfändungsverbot wirksam ausgesprochen werden kann«.*[65]

Im Gegensatz zu dieser maßgeblichen Umgestaltung des Konzepts der Sicherstellung nach § 109 Z 1 lit a StPO soll die Abänderung von »Werte« auf ebenfalls »Vermögenswerte« in § 109 Z 1 lit b StPO keine inhaltliche Änderung bringen, sondern nur der sprachlichen Angleichung dienen.[66]

In diesem Zusammenhang ist anzumerken, dass der Begriff des Vermögenswertes nach den Erläuterungen zum StPRÄG *»im Übrigen auch Gegenstände einschließt«.*[67] Hierdurch erscheint dann freilich die Anführung von Gegenständen in der Definition der Sicherstellung nach § 109 Z 1 lit a StPO (»vorläufige Begründung der Verfügungsmacht über Gegenstände […] sowie über Vermögenswerte«) redundant.

3. Einführung der »Beschlagnahme von Datenträgern und Daten« als neue Ermittlungsmaßnahme

Die nach dem Gesetzesentwurf zum StPRÄG 2024 in § 109 Z 2a StPO definierte und an vergleichsweise strenge Voraussetzungen geknüpfte »Beschlagnahme von Datenträgern und Daten« löst bestimmte Fälle der Begründung von Verfügungsmacht aus § 109 Z 1 lit a StPO heraus. Für diese Fälle ist eine gerichtliche Entscheidung »auf Begründung einer Sicherstellung« von Datenträgern bzw Daten vorgesehen, die »zum Zweck der Auswertung von Daten« erfolgen soll. Dabei kann es sich um »Datenträger und darauf gespeicherte Daten« (lit a) handeln, aber auch um »Daten, die an anderen Speicherorten als einem Datenträger gespeichert sind, soweit auf sie von diesem aus zugegriffen werden kann« (lit b), oder zuletzt um »Daten, die auf Datenträgern gespeichert sind, die zuvor für andere Zwecke sichergestellt wurden« (lit c). Während lit a die jeweils lokal auf einem Datenträger abgelegten Daten betrifft, soll lit b ganz offensichtlich die umstrittene Thematik des Zugriffs auf externe Speicherplätze (siehe dazu weiter unten) lösen und lit c die spätere Auswertung von bereits sichergestellten Datenträgern abdecken. Nach den Ausführungen in den Erläuterungen zum StPRÄG 2024 *»handelt es sich […] um eine neue Ermittlungsmaßnahme, die sich von der Sicherstellung von Gegenständen grundlegend unterscheidet und zudem eine Reihe von Begleitbestimmungen erforderlich macht«* und welche als Sonderform der Beschlagnahme eingeordnet wird.[68]

Wie der VfGH in seiner Aufhebungsentscheidung gefordert hatte,[69] erfolgt damit eine Differenzierung zwischen der Sicherung von Datenträgern und deren Auswertung einerseits und der Sicherstellung sonstiger Gegenstände andererseits. Wie in Kapitel V.A.2. bereits angeführt, erfasst der vorgeschlagene § 109 Z 2a StPO freilich nicht alle Fälle der Begründung von Verfügungsmacht über einen Datenträger sowie die darauf (lokal oder extern) gespeicherten Daten, sondern nur solche Fälle, in denen damit eine Auswertung von Daten bezweckt wird.[70] Ein Zugriff der Strafverfolgungsbehörden auf Datenträger (bzw Daten) zu anderen Zwecken (etwa der Sicherung privatrechtlicher Ansprüche oder vermögensrechtlicher Anordnungen) soll im begrifflichen Bereich der Sicherstellung nach § 109 Z 1 lit a StPO verbleiben, wie auch in den Materialien ausgeführt wird: *»Das Abstellen auf den Zweck der Auswertung soll zudem den Praxisbedürfnissen Rechnung tragend die vom Erkenntnis des VfGH unberührt gebliebene Möglichkeit der Sicherstellung von Datenträgern zu anderen gesetzlichen Zwecken (§ 110 Abs 1 Z 2 und 3 StPO) weiterhin erlauben, solange nicht in weiterer Folge eine Auswertung erfolgen soll.«*[71] Differenziert werden soll letztlich nicht nach Art des Datenträgers, sondern hinsichtlich des Zwecks, zu dem die Sicherung erfolgt. Dies soll *»eine klare Abgrenzung zu anderen Ermittlungsmaßnahmen […], insbesondere zur Sicherstellung«* schaffen.[72] Für solche Konstellationen, die dem vorgeschlagenen § 109 Z 2a StPO unterfallen, sollen strengere Voraussetzungen – insb das Erfordernis einer gerichtlichen Bewilligung und eine Erhöhung der Begründungspflicht – gelten. Zusätzlich sollen nach dem Gesetzesvorschlag diese Fälle *»mehrstufigen und technisch aufwendigen und mit jeweils unterschiedlichen rechtsstaatlichen Garantien ausgestatteten Phasen des Auswertungsvorgangs«*[73] unterworfen werden: Vorgesehen ist die Herstellung einer Originalsicherung, darauffolgend einer Arbeitskopie und anhand Letzterer die Aufbereitung der

65 ErlME 349/ME XXVII. GP, 37 f. Angesprochen wird in den Materialien hier insb die Wirkungslosigkeit solcher Verbote bei ausländischen Dritten.
66 ErlME 349/ME XXVII. GP, 39.
67 ErlME 349/ME XXVII. GP, 38.
68 ErlME 349/ME XXVII. GP, 9.
69 Vgl VfGH 14.12.2023, G 352/2021, Rz 65–70.
70 Angesichts dessen, wie allgegenwärtig Datenträger als Bestandteile diverser Gegenstände sind, würde ein reines Abstellen auf diese Eigenschaft eine noch viel weiter gehende Beschneidung von § 109 Z 1 lit a StPO bedeuten. Man denke dabei etwa an die Ausstattung moderner Fahrzeuge mit Datenträgern, die auch in den Materialien als Beispiel (für zunächst zu anderen Zwecken sichergestellte und somit allenfalls später unter § 109 Z 2a StPO fallende Objekte) genannt werden; vgl ErlME 349/ME XXVII. GP, 11.
71 ErlME 349/ME XXVII. GP, 1.
72 ErlME 349/ME XXVII. GP, 10.
73 ErlME 349/ME XXVII. GP, 10.

Daten durch eine gesonderte Organisationseinheit der Kriminalpolizei; lediglich das Ergebnis dieser Datenaufbereitung soll dann (samt Aufbereitungsbericht) an die für die Führung des Ermittlungsverfahrens zuständige Organisationseinheit übermittelt werden.

Auffällig ist (gerade auch im Vergleich zu den in § 109 Z 1a StPO umschriebenen Vermögenswerten), dass der Begriff »Datenträger« keiner Legaldefinition zugeführt wurde und keine Differenzierung zwischen verschiedenen Arten von Datenträgern getroffen wurde. Für alle unter diesen Begriff fallenden Objekte sollen (im Fall ihrer Sicherung zum Zweck der Auswertung) die strengeren Voraussetzungen dieser Maßnahme, insb das Erfordernis einer vorherigen richterlichen Kontrolle, und das beschriebene anschließende Prozedere gleichermaßen gelten – unabhängig von ihrem tatsächlichen Potential, sensible Einblicke zu gewähren.

B. Voraussetzungen für die Sicherstellung und Beschlagnahme von Datenträgern bzw Daten

1. Formelle und materielle Voraussetzungen – Gegenüberstellung

§ 110 StPO legt die formellen und materiellen Voraussetzungen für die Durchführung einer Sicherstellung nach § 109 Z 1 StPO fest, jene für die neue Ermittlungsmaßnahme der Beschlagnahme von Datenträgern und Daten sollen nach dem StPRÄG 2024 in **§ 115f** StPO normiert werden:

§ 110 StPO, BGBl Nr 631/1975 idF BGBl I Nr 71/2014:

Sicherstellung

(1) Sicherstellung ist zulässig, wenn sie

1. aus Beweisgründen,
2. zur Sicherung privatrechtlicher Ansprüche oder
3. zur Sicherung der Konfiskation (§ 19a StGB), des Verfalls (§ 20 StGB), des erweiterten Verfalls (§ 20b StGB), der Einziehung (§ 26 StGB) oder einer anderen gesetzlich vorgesehenen vermögensrechtlichen Anordnung

erforderlich scheint.

(2) Sicherstellung ist von der Staatsanwaltschaft anzuordnen und von der Kriminalpolizei durchzuführen.

(3) Die Kriminalpolizei ist berechtigt, Gegenstände (§ 109 Z 1 lit. a) von sich aus sicherzustellen,

[…]

(4) Die Sicherstellung von Gegenständen aus Beweisgründen (Abs. 1 Z 1) ist nicht zulässig und jedenfalls auf Verlangen der betroffenen Person aufzuheben, soweit und sobald der Beweiszweck durch Bild-, Ton- oder sonstige Aufnahmen oder durch Kopien schriftlicher Aufzeichnungen oder automationsunterstützt verarbeiteter Daten erfüllt werden kann und nicht anzunehmen ist, dass die sichergestellten Gegenstände selbst oder die Originale der sichergestellten Informationen in der Hauptverhandlung in Augenschein zu nehmen sein werden.

§ 110 StPO, Fassung StPRÄG 2024 (4125/A, 349/ME): Sicherstellung

(1) Sicherstellung ist zulässig, wenn sie

1. aus Beweisgründen,
2. zur Sicherung privatrechtlicher Ansprüche oder
3. zur Sicherung der Konfiskation (§ 19a StGB), des Verfalls (§ 20 StGB), des erweiterten Verfalls (§ 20b StGB), der Einziehung (§ 26 StGB) oder einer anderen gesetzlich vorgesehenen vermögensrechtlichen Anordnung

erforderlich scheint.

(2) Sicherstellung ist von der Staatsanwaltschaft anzuordnen und von der Kriminalpolizei durchzuführen.

(3) Die Kriminalpolizei ist berechtigt, Gegenstände und Vermögenswerte (§ 109 Z 1 lit. a) von sich aus sicherzustellen,

[…]

(4) Die Sicherstellung von Gegenständen oder Vermögenswerten aus Beweisgründen (Abs. 1 Z 1) ist nicht zulässig und jedenfalls auf Verlangen der betroffenen Person aufzuheben, soweit und sobald der Beweiszweck durch Bild-, Ton- oder sonstige Aufnahmen oder durch Kopien schriftlicher Aufzeichnungen oder automationsunterstützt verarbeiteter Daten erfüllt werden kann und nicht anzunehmen ist, dass die sichergestellten Gegenstände oder Vermögenswerte selbst oder die Originale der sichergestellten Informationen in der Hauptverhandlung in Augenschein zu nehmen sein werden.

[…]

§ 115f StPO, Fassung StPRÄG 2024 (4125/A, 349/ME): Beschlagnahme von Datenträgern und Daten

(1) Die Beschlagnahme von Datenträgern und Daten ist zulässig, wenn sie aus Beweisgründen erforderlich scheint und aufgrund bestimmter Tatsachen anzunehmen ist, dass dadurch Informationen ermittelt werden können, die für die Aufklärung einer Straftat wesentlich sind.

(2) Die Beschlagnahme von Datenträgern und Daten ist durch die Staatsanwaltschaft auf Grund einer gerichtlichen Bewilligung anzuordnen und von der Kriminalpolizei durchzuführen.

(3) […]

(4) Die Kriminalpolizei ist berechtigt, bei Gefahr im Verzug, wenn andernfalls der Verlust des Datenträgers und der darauf oder an anderen Speicherorten (§ 109 Z 2a lit. a und b) gespeicherten Daten zu befürchten wäre, sowie in den Fällen der § 110 Abs. 3 und § 170 Abs. 1 Z 1 Datenträger, die einer Beschlagnahme nach Abs. 1 unterliegen, von sich aus sicherzustellen. Zu einem Zugriff auf die Daten ist die Kriminalpolizei von sich aus nicht berechtigt.

(5) […]

(6) § 110 Abs. 4 und § 115 Abs. 6 gelten sinngemäß.

[…]

2. Änderungen im Bereich der Sicherstellung

§ 110 Abs 1 StPO erklärt die Sicherstellung für zulässig, wenn sie aus bestimmten Gründen »erforderlich scheint«: nach Z 1 aus Beweisgründen, nach Z 2 zur Sicherung privatrechtlicher Ansprüche und nach Z 3 zur Sicherung vermögensrechtlicher Anordnungen. Im Anlassfall zu G 352/2021 wurde eine Sicherstellung aus Beweisgründen durchgeführt (und dementsprechend im

Normprüfungsverfahren die Aufhebung von Z 1 beantragt). Gemäß § 110 Abs 2 StPO ist grundsätzlich eine Anordnung der Staatsanwaltschaft erforderlich; in bestimmten Fällen darf die Kriminalpolizei jedoch nach Abs 3 leg cit auch von sich aus Sicherstellungen nach § 109 Z 1 lit a StPO durchführen. § 110 Abs 4 StPO erklärt die Sicherstellung von Gegenständen aus Beweisgründen grundsätzlich für subsidiär.

Von der Aufhebung durch den VfGH betroffen waren in Bezug auf § 110 StPO dessen Abs 1 Z 1 und Abs 4. Die Materialien zum StPRÄG 2024 führen aus, dass diese Bestimmungen jedoch nach wie vor erforderlich seien und sie daher neu erlassen werden sollen, *»§ 110 Abs 4 StPO mit geringfügigen sprachlichen, nicht jedoch inhaltlichen Änderungen«;* sie hätten *»für die Sicherstellung von (sonstigen) Gegenständen, die nicht ausgelesen und ausgewertet werden sollen, sowie für Vermögenswerte nach wie vor Bedeutung«.*[74] Soweit § 110 StPO die Objekte der Sicherstellung benennt, wurde der Gesetzestext zudem auch hier – naheliegenderweise – um Vermögenswerte ergänzt.

3. Voraussetzungen für die Beschlagnahme von Datenträgern und Daten iSd § 109 Z 2a StPO

Die Regelung der inhaltlichen und formalen Voraussetzungen für die Durchführung der neuen Maßnahme der Beschlagnahme von Datenträgern und Daten iSd § 109 Z 2a StPO soll nach dem Entwurf zum StPRÄG 2024 in einem neu einzufügenden **§ 115f** StPO erfolgen. Nach Abs 1 dieser Bestimmung soll dafür auf materieller Ebene erstens vorausgesetzt werden, dass die Maßnahme »aus Beweisgründen erforderlich scheint« (diese Formulierung stimmt mit § 110 Abs 1 Z 1 StPO überein); hierfür ist nach den Materialien notwendig, *»dass der Datenträger und die Daten geeignet sind, das Beweisthema zu führen«*[75]. Überdies muss aber »aufgrund bestimmter Tatsachen anzunehmen [sein], dass dadurch Informationen ermittelt werden können, die für die Aufklärung einer Straftat wesentlich sind«. In formeller Hinsicht soll die Ermittlungsmaßnahme nach **§ 115f** Abs 2 StPO eine staatsanwaltliche Anordnung aufgrund einer gerichtlichen Bewilligung erfordern, wobei beide Akte einer erhöhten Begründungspflicht nach Abs 3 leg cit unterliegen.

74 ErlME 349/ME XXVII. GP, 12.
75 ErlME 349/ME XXVII. GP, 14.

C. Kooperationspflicht betroffener Personen

1. Mitwirkungspflicht – Gegenüberstellung

§ 111 StPO, BGBl Nr 631/1975 idF BGBl I Nr 52/2009:

(1) Jede Person, die Gegenstände oder Vermögenswerte, die sichergestellt werden sollen, in ihrer Verfügungsmacht hat, ist verpflichtet (§ 93 Abs. 2), diese auf Verlangen der Kriminalpolizei herauszugeben oder die Sicherstellung auf andere Weise zu ermöglichen. Diese Pflicht kann erforderlichenfalls auch mittels Durchsuchung von Personen oder Wohnungen erzwungen werden; dabei sind die §§ 119 bis 122 sinngemäß anzuwenden.

(2) Sollen auf Datenträgern gespeicherte Informationen sichergestellt werden, so hat jedermann Zugang zu diesen Informationen zu gewähren und auf Verlangen einen elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat auszufolgen oder herstellen zu lassen. Überdies hat er die Herstellung einer Sicherungskopie der auf den Datenträgern gespeicherten Informationen zu dulden.

[...]

(4) In jedem Fall ist der von der Sicherstellung betroffenen Person sogleich oder längstens binnen 24 Stunden eine Bestätigung über die Sicherstellung auszufolgen oder zuzustellen und sie über das Recht, Einspruch zu erheben (§ 106) und eine gerichtliche Entscheidung über die Aufhebung oder Fortsetzung der Sicherstellung zu beantragen (§ 115), zu informieren. Von einer Sicherstellung zur Sicherung einer Entscheidung über privatrechtliche Ansprüche (§ 110 Abs. 1 Z 2) ist, soweit möglich, auch das Opfer zu verständigen.

§ 111 StPO, Fassung StPRÄG 2024 (4125/A, 349/ME):

(1) Jede Person, die Gegenstände oder Vermögenswerte, die sichergestellt werden sollen, in ihrer Verfügungsmacht hat, ist verpflichtet (§ 93 Abs. 2), diese auf Verlangen der Kriminalpolizei herauszugeben oder die Sicherstellung auf andere Weise zu ermöglichen. Diese Pflicht kann erforderlichenfalls auch mittels Durchsuchung von Personen oder Wohnungen erzwungen werden; dabei sind die §§ 119 bis 122 sinngemäß anzuwenden. Die Pflicht gilt nicht für Gegenstände, die zum Zweck der Auswertung von Daten sichergestellt werden sollen (§ 115g).

(2) ~~Sollen auf Datenträgern gespeicherte Informationen sichergestellt werden, so hat jedermann Zugang zu diesen Informationen zu gewähren und auf Verlangen einen elektronischen Datenträger in einem allgemein gebräuchlichen Dateiformat auszufolgen oder herstellen zu lassen. Überdies hat er die Herstellung einer Sicherungskopie der auf den Datenträgern gespeicherten Informationen zu dulden.~~ Sollen Daten, die mittels Bild- und Tonaufzeichnungsgeräten an öffentlichen oder öffentlich zugänglichen Orten aufgenommen wurden, sichergestellt werden, so ist jede Person verpflichtet (§ 93 Abs. 2), Zugang zu diesen zu gewähren und sie auf Verlangen in einem allgemein gebräuchlichen Dateiformat auszufolgen oder eine Kopie herzustellen zu lassen.

[...]

(4) In jedem Fall ist der von der Sicherstellung betroffenen Person sogleich oder längstens binnen 24 Stunden eine Bestätigung über die Sicherstellung auszufolgen oder zuzustellen und sie über das Recht, Einspruch zu erheben (§ 106) und eine gerichtliche Entscheidung über die Aufhebung oder Fortsetzung der Sicherstellung zu beantragen (§ 115), zu informieren. Von einer Sicherstellung zur Sicherung einer Entscheidung über privatrechtliche Ansprüche (§ 110 Abs. 1 Z 2) ist, soweit möglich, auch das Opfer zu verständigen.

[...]

§ 115g StPO, Fassung StPRÄG 2024 (4125/A, 349/ME):

(1) Sollen Datenträger und Daten beschlagnahmt werden (§ 109 Z 2a), so ist jede Person verpflichtet (§ 93 Abs. 2), Zugang zu diesen zu gewähren und auf Verlangen Daten in einem allgemein gebräuchlichen Dateiformat auszufolgen oder eine Kopie herstellen zu lassen. Überdies hat sie die Herstellung einer Originalsicherung (§ 109 Z 2c) der auf den Datenträgern oder an anderen Speicherorten gespeicherten Daten zu dulden; § 111 Abs. 3 gilt sinngemäß.

(2) § 112 und§ 112a sind sinngemäß anzuwenden.

(3) Über jede Sicherstellung eines Datenträgers nach § 115f Abs. 4 hat die Kriminalpolizei unverzüglich, längstens jedoch binnen 14 Tagen der Staatsanwaltschaft zu berichten (§ 100 Abs. 2 Z 2), welche im Nachhinein sogleich beim Gericht die Beschlagnahme von Datenträgern und Daten (§ 115f Abs. 1 bis 3) zu beantragen oder, wenn deren Voraussetzungen nicht vorliegen oder weggefallen sind, die Aufhebung der Sicherstellung anzuordnen hat. Wird die Bewilligung nicht erteilt, so haben Staatsanwaltschaft und Kriminalpolizei mit den ihnen zu Gebote stehenden rechtlichen Mitteln den der gerichtlichen Entscheidung entsprechenden Rechtszustand herzustellen.

2. Aktuelle Deutung als Grundlage für den Zugriff auf (lokal und extern gespeicherte) Daten

§ 111 Abs 1 StPO legt eine allgemeine Pflicht zur Herausgabe sicherzustellender Gegenstände oder Vermögenswerte bzw zur Ermöglichung einer Sicherstellung »auf andere Weise« fest. Der von G 352/2021 betroffene Abs 2 leg cit spezifiziert in seiner aktuellen Fassung die Verpflichtung, bei der Sicherstellung von »auf Datenträgern gespeicherte[n] Informationen« Zugang zu diesen zu gewähren, auf Verlangen einen diese Informationen enthaltenden Datenträger auszufolgen oder herstellen zu lassen sowie die Herstellung einer Sicherungskopie zu dulden. Dies betrifft den Fall, dass die Sicherstellung eines Gegenstandes – hier des Datenträgers – zumindest auch dem Zugriff auf bestimmte Informationen dient.[76] Aus der Bezugnahme auf sichergestellte Informationen in § 110 Abs 4 und § 111 Abs 2 StPO wird bislang geschlossen, dass § 110 StPO nicht nur die Sicherstellung von körperlichen Datenträgern erlaubt, sondern im Weiteren **auch den Zugriff auf Daten, die auf solchen Datenträgern gespeichert sind** – diese dürfen (mit oder ohne Ingewahrsamnahme des Datenträgers) etwa angesehen, kopiert, gespeichert und ausgewertet werden.[77] Ganz allgemein ist aber festzustellen, dass ein **Zugriff auf Daten ohne Sicherstellung von Geräten,** über die ein solcher Zugriff getätigt wird, **nicht durch die §§ 109 ff StPO gedeckt** ist: *»Jedenfalls ist ein solcher Fernzugriff nur vom Rechner des Betroffenen aus zulässig.«*[78] Wie sowohl die Gesetzesmaterialien zur Bestimmung[79] als auch die Rsp[80] und die Lit[81] unzweifelhaft darlegen, ist nämlich jeweils **der körperliche Datenträger das Objekt der Sicherstellung iSd § 109 Z 1 lit a StPO.** Hieran ändert auch die Möglichkeit des späteren Auslesens nichts. Ein Auslesen bzw Kopieren der Daten vom oder über das Gerät vor Ort kann allerdings als vorübergehende Sicherstellung dieses Gerätes angesehen werden.[82] Auch der VwGH hat diese **Gegenstandsbindung** unmissverständlich zusammengefasst: *»›Informationen‹ (›immaterielle Objekte‹) sind keine Gegenstände. Sie können daher nicht unabhängig von ihrer Bindung an einen Gegenstand sichergestellt werden, sondern nur durch die Sicherstellung des Datenträgers, auf dem sie unmittelbar gespeichert sind oder auf dem sie zwar nicht gespeichert sind, aber über den mittels Internet-Verbindung virtuell auf den Datenträger zugegriffen wird, auf dem sie gespeichert sind. Ohne die Sicherstellung derartiger Hardware, die den Zugang zu Informationen ermöglicht, erlauben § 109 Z 1 und §§ 110 ff StPO keinen Zugang zu digital gespeicherten Informationen.«*[83] Die Formulierung des § 111 Abs 2 StPO, die aber »Informationen« selbst als sichergestellt bezeichnet, wurde in der Lit dementsprechend teils als »misslungen«[84], »nicht gelungen«[85], »nicht präzise«[86] bzw »bedenklich«[87] kritisiert.

Wie auch im obigen Zitat des VwGH anklingt, steht den Strafverfolgungsbehörden nach der Rsp[88] und dem

76 Vgl *Kroschl* in Schmölzer/Mühlbacher, § 109 StPO Rz 4; OGH 11.9.2018, 14 Os 51/18h, RS0132239.

77 So auch VfGH 14.12.2023, G 352/2021, Rz 36 unter Verweis auf *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht (2018) Rz 5.3; sowie VfGH 14.12.2023, G 352/2021, Rz 61.

78 *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht Rz 5.15; vgl auch *Zerbes/Ghazanfari,* AnwBl 2022, 640 (641 f).

79 ErlRV 25 BlgNR XXII. GP, 156: Daten sind *»immaterielle Objekte«,* die *»für ihre Existenz materieller Verkörperung«* bedürfen; *»Eine Suche nach Daten ist somit untrennbar an die vorhergehende Suche nach entsprechenden Datenträgern verknüpft.«*

80 OGH 11.9.2018, 14 Os 51/18h, RS0132239.

81 *Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 111 Rz 12; *Keplinger/Prunner/Pühringer* in Birklbauer/Haumer/Nimmervoll/Wess (Hrsg), StPO – Linzer Kommentar zur Strafprozessordnung (2020) zu § 111 StPO Rz 6; *Kroschl* in Schmölzer/Mühlbacher, § 109 StPO Rz 4; *Zerbes/Ghazanfari,* AnwBl 2022, 640 (641).

82 Vgl *Zerbes/Ghazanfari,* AnwBl 2022, 640 (641); *Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 111 Rz 12.

83 VwGH 20.4.2022, Ra 2021/01/0418. Vgl auch *Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 111 Rz 12.

84 *Zerbes,* Beweisquelle Handy, ÖJZ 2021, 176 (178).

85 *Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 111 Rz 12.

86 *Keplinger/Prunner/Pühringer* in Birklbauer/Haumer/Nimmervoll/Wess, § 111 StPO Rz 6.

87 *Keplinger/Prunner/Pühringer/Rebisant* in Birklbauer/Haumer/Nimmervoll/Wess, § 109 Rz 6.

88 OGH 11.9.2018, 14 Os 51/18h. Der Gerichtshof führt darin aus, dass *»eine Sicherstellung der relevanten Informationen überhaupt unmöglich wäre, wenn derjenige, der in der Lage ist, der Kriminalpolizei im Sinn des § 111 Abs 2 StPO den Zugang zu gespeicherten Daten zu verschaffen, gar nicht über den Datenträger verfügt, auf dem diese gespeichert sind (etwa bei Nutzung externer Speicherplätze, vor allem bei […] ausgelagerter Datenbetreuung durch Cloud-Computing- oder Cloud-Storage-Dienste).«* Dies widerspräche der Intention des Gesetzgebers. Auch VfGH 14.12.2023, G 352/2021geht von dieser Sachlage aus, vgl Rz 38 und 95.

Vorgehen in der Praxis[89] – jedoch in der Lit durchaus umstritten[90] – nicht nur der Zugriff auf die **am sichergestellten Datenträger selbst lokal gespeicherten** Informationen offen, sondern auch auf solche, die **extern gespeichert, aber vom Datenträger aus zugänglich** sind. Dies betrifft etwa vom Laptop des Betroffenen aus abrufbare Daten, die auf Servern von Cloud- oder anderen IT-Diensten abgespeichert sind. Auch diesen Umstand bezog der VfGH in G 352/2021 wertend mit ein.[91]

§ 111 Abs 4 StPO legt schließlich eine Verpflichtung fest, dem Betroffenen gegenüber die Sicherstellung zu bestätigen und ihn über bestimmte Rechte zu informieren. Dies hat sogleich, jedenfalls aber innerhalb von 24 Stunden zu erfolgen. UU ist auch ein Opfer zu verständigen. Auch über die Sicherung von Daten ist nach der Lit zu informieren.[92]

3. Vorgeschlagene Änderungen im Rahmen des Strafprozessrechtsänderungsgesetzes 2024

Im StPRÄG 2024 ist eine Umgestaltung bzw Verlagerung dieser Bestimmung vorgesehen. Statt den bislang für die Sicherung von Datenträgern und Daten geltenden Voraussetzungen in §§ 110 ff StPO soll § 111 Abs 2 StPO *»künftig aufgrund der Aufhebung durch den VfGH nur mehr einen sehr eingeschränkten Anwendungsbereich haben«.*[93] Die neu zu schaffenden spezielleren Normen der §§ 115f bis 115l StPO, *»die technologieneutral auf den Sammelbegriff Datenträger abstellen«* sollen diesen Bestimmungen vorgehen und diesbezüglich den Zugriff auf (und die Herausgabepflicht für) lokal oder extern gespeicherte Daten regeln.[94] § 111 Abs 1 StPO soll in der vorgeschlagenen Fassung dementsprechend ein Satz angefügt werden, der »Gegenstände, die zum Zweck der Auswertung von Daten sichergestellt werden sollen« von der allgemeinen Kooperationspflicht der Norm ausschließt und hierfür auf den neu zu schaffenden § 115g StPO verweist. Dies betrifft jene Fälle, in denen *»bereits zum Zeitpunkt der Aufforderung oder Sicherstellung der Zweck verfolgt wird, die auf dem Gegenstand befindlichen (oder von dort aus zugänglichen) Daten auszuwerten«.*[95] Die Differenzierung zwischen Konstellationen der Sicherstellung nach § 109 Z 1 lit a StPO und solchen der Beschlagnahme von Datenträgern und Daten nach § 109 Z 2a StPO soll also auf dieser Ebene fortgesetzt werden und eine Kooperationspflicht hinsichtlich Letzterer sich nur mehr nach § 115g StPO richten.[96] Eine allgemeine Verpflichtung zur Herausgabe von »auf Datenträgern gespeicherten Informationen«, wie sie bislang in § 111 Abs 2 StPO vorgesehen ist, soll demgegenüber nicht mehr bestehen. Der neu zu schaffende § 115g Abs 1 StPO *»soll zum einen als lex specialis zu § 111 Abs 1 StPO die Herausgabe eines Datenträgers sowie zum anderen als Nachfolgebestimmung des aufzuhebenden § 111 Abs 2 StPO die Pflicht zur Herausgabe von auf Datenträgern gespeicherten Daten regeln und damit der Ermöglichung der Beschlagnahme von Datenträgern und Daten dienen.«*[97] Die Anordnung des § 111 Abs 2 StPO würde somit im Wesentlichen in diese neue Bestimmung verschoben, auf die Maßnahme der Beschlagnahme von Datenträgern und Daten bezogen und zusätzlich erstmals explizit festgehalten, dass die Herstellung einer Kopie nicht nur der lokal, sondern auch der extern gespeicherten Daten zu dulden ist.

§ 115g Abs 3 StPO soll nach dem Vorschlag des StPRÄG 2024 eine gesonderte Berichtspflicht für den Fall einer Sicherung eines Datenträgers durch die Kriminalpolizei aus Eigenem bei Gefahr im Verzug und nachträglicher Beantragung der Beschlagnahme enthalten.

D. Erstmalige gesetzliche Verankerung der behördlichen Übertragung von Kryptowerten im Rahmen des Strafprozessrechtsänderungsgesetzes 2024

Wie bereits angeführt, erfolgt der Zugriff bzw die Sicherung von Kryptowerten durch die Strafverfolgungsbehörden bereits bisher auf verschiedene Arten, insb durch Übertragung der Werte auf eine behördlich kontrollierte Adresse. Eine ausdrückliche gesetzliche Grundlage für diese Vorgehensweise fehlt jedoch bisher, stattdessen wird sie als herkömmliche Sicherstellung von Datenträgern, welche auch den Zugriff auf (lokal oder extern gespeicherte) Daten zulasse, begründet – hierauf wird in nachfolgenden Kapiteln kritisch eingegangen.

Das StPRÄG 2024 sieht in diesem Zusammenhang eine Neuerung vor: § 114 StPO, welcher die Verwahrung sichergestellter Gegenstände (und in der vorgeschlagenen Fassung auch Vermögenswerte) regelt, soll um einen Abs 1a ergänzt werden, der genau diese Übertragung von Kryptowerten anordnet:

89 *Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 111 Rz 14/2.
90 Krit *Zerbes/Ghazanfari,* AnwBl 2022, 640 ff, unter Hinweis auf die Entstehung der Gesetzesbestimmungen vor der Entwicklung von »Big Data« bzw moderner Informationstechnologie und auf die daraus resultierenden, rechtsstaatlich problematisch niedrigen Voraussetzungen für solch umfangreiche Eingriffe in die Privatsphäre. Ablehnend aufgrund eines engeren Verständnisses auch *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht Rz 5.11 und *Schrank/Stücklberger/Kleinbrod,* Sicherstellung im digitalen Zeitalter, ZWF 2020, 289 (289 f) sowie *Zerbes,* ÖJZ 2021, 176 (177 ff).
91 Vgl VfGH 14.12.2023, G 352/2021, Rz 38, 95.
92 *Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 111 Rz 22.
93 Vgl ErlME 349/ME XXVII. GP, 12.
94 ErlME 349/ME XXVII. GP, 12.
95 ErlME 349/ME XXVII. GP, 12.
96 Vgl ErlME 349/ME XXVII. GP, 12.
97 ErlME 349/ME XXVII. GP, 17.

§ 114 StPO, Fassung StPRÄG 2024 (4125/A, 349/ME):

(1) Für die Verwahrung sichergestellter Gegenstände und Vermögenswerte hat bis zur Berichterstattung über die Sicherstellung (§ 113 Abs. 2) die Kriminalpolizei, danach die Staatsanwaltschaft zu sorgen.

(1a) Sichergestellte Kryptowerte sind auf behördeneigene Infrastruktur der Kriminalpolizei zu transferieren und dort zu verwahren. Soweit dies aus rechtlichen oder tatsächlichen Gründen erforderlich ist, kann die Staatsanwaltschaft anordnen, dass die Verwahrung von Kryptowerten auch nach der Berichterstattung durch die Kriminalpolizei erfolgt.

(2) Wenn der Grund für die weitere Verwahrung sichergestellter Gegenstände und Vermögenswerte wegfällt, sind diese sogleich jener Person auszufolgen, in deren Verfügungsmacht sie sichergestellt wurden, es sei denn, dass diese Person offensichtlich nicht berechtigt ist. In diesem Fall sind sie der berechtigten Person auszufolgen oder, wenn eine solche nicht ersichtlich ist und nicht ohne unverhältnismäßigen Aufwand festgestellt werden kann, nach § 1425 ABGB gerichtlich zu hinterlegen. Die hievon betroffenen Personen sind zu verständigen.

Begründend wird in den Materialien angeführt, dass die Verfügungsmacht über Vermögenswerte im Rahmen einer Sicherstellung nach § 109 Z 1 lit a StPO *»auf unterschiedliche Weise, je nach Art des Vermögenswertes«* hergestellt werden könne – maßgeblich sei, *»dass durch die gewählte Form der Vermögenswert vor unrechtmäßigem Zugriff von dritter Seite geschützt und der Vermögenswert für privatrechtliche Ansprüche oder vermögensrechtliche Anordnungen erhalten«* werde.[98] Hinsichtlich Kryptowerten wird erklärt, dass *»in der Regel eine Sicherstellung durch Transfer auf ein sog ›Behördenwallet‹ durchzuführen«* sei, um Zugriffe von dritter Seite zu verhindern; durch *»den Transfer auf eine ›Behördenwallet‹«* werde *»letztlich eine Verfügungsmacht über die Kryptowährung begründet«,* dabei handle es sich um einen *»Sonderfall der Begründung von Verfügungsmacht (§ 109 Z 1 lit a StPO)«.*[99] Der vorgeschlagene § 114 Abs 1a StPO soll *»eine ausdrückliche Rechtsgrundlage für die bisher nicht explizit gesetzlich verankerte Möglichkeit der effektiven Sicherung von Kryptowerten durch deren Übertragung auf behördeninterne Infrastruktur der Kriminalpolizei (ein sog behördeninternes Wallet; § 114 Abs 1a StPO)«* schaffen.[100]

Anzumerken ist, dass vor dem Hintergrund dieser Erläuterungen sowohl die vorgeschlagene Einbindung dieser Bestimmung in § 114 StPO als auch der Wortlaut nicht völlig stimmig sind: So soll nach der angeführten Begründung damit eine neue Rechtsgrundlage für eine spezifische Art der Sicherstellung nach § 109 Z 1 lit a StPO – also die **Begründung** von Verfügungsmacht – geschaffen werden. § 114 StPO regelt jedoch erst die (der Sicherstellung nachfolgende) **Verwahrung.** Hinzu kommt, dass die vorgeschlagene Formulierung explizit »**sichergestellte**« Kryptowerte referenziert, also auch dem Wortlaut nach den Umgang mit Kryptowerten regelt, über welche **bereits Verfügungsmacht iSd § 109 Z 1 lit a StPO begründet** wurde. Insgesamt stellt die Bestimmung des § 114 Abs 1a StPO in der vorgeschlagenen Fassung somit genau genommen nicht eine neue Rechtsgrundlage für eine Vorgehensweise **bei** der Sicherstellung von Kryptowerten, sondern für die **nach** einer solchen zu bewirkende Verwahrungsart dar. Dies ist – nach den Ausführungen in den Materialien zu schließen – nicht beabsichtigt.

98 ErlME 349/ME XXVII. GP, 38.
99 ErlME 349/ME XXVII. GP, 39 f.
100 ErlME 349/ME XXVII. GP, 37.

VI. Kritische Betrachtung der aktuellen Rechtslage und der Änderungen durch das Strafprozessrechtsänderungsgesetz 2024

Der Rechtsstandpunkt von BMI und BMJ hinsichtlich der Zulässigkeit und Art der Sicherung von Kryptowerten in Strafverfahren nach aktueller Rechtslage wird insb im (vom BMJ 2020 in aktualisierter Fassung erlassenen) »Leitfaden Vermögensrechtliche Anordnungen«[101] und weiteren gesonderten Erlässen[102] erläutert. Die Möglichkeit des Ausspruchs eines Drittverbots bzw Veräußerungs- und Verpfändungsverbots wird dabei auf § 109 Z 1 lit b StPO gestützt. Als primäre Sicherungsmethode wird aber die Übertragung auf eine behördlich kontrollierte Adresse und darauffolgend die Verwaltung über eine sog »Behördenwallet« dargestellt und dieses Vorgehen unter § 109 Z 1 lit a StPO subsumiert. Im Folgenden werden beide Vorgehensweisen und die im Rahmen des StPRÄG 2024 vorgeschlagenen Neuerungen in diesem Zusammenhang analysiert.

A. Vorüberlegung: Sicherung von Kryptowerten als Eigentumseingriff und Erforderlichkeit einer gesetzlichen Eingriffsermächtigung

Dass ermittlungsbehördliche Zugriffe auf Vermögensgüter regelmäßig einen Eingriff in die verfassungsge-

101 Erlass des BMJ vom 28.5.2020 zur Aktualisierung des Leitfadens Vermögensrechtliche Anordnungen (3. Auflage), GZ 2020-0.303.132 – Leitfaden Vermögensrechtliche Anordnungen (2020). Der Leitfaden wurde in erster Auflage 2014 veröffentlicht (Erlass des BMJ vom 17.2.2014, BMJ-S90.021/0004-IV 3/2014) und 2020 zum zweiten Mal aktualisiert.
102 Erlass des BMI vom 14.3.2019, BMI-KP1000/0730-II/BK/5.2/2018, Richtlinie – Sicherstellung von Kryptowährungen; Erlass des BMJ vom 1.4.2020 zum Vorgehen bei Sicherstellung, Beschlagnahme und Verwertung von virtuellen Währungen im Bereich der Justiz, GZ 2020-0.163.092.

setzlich gewährleistete Eigentumsfreiheit darstellen, ist naheliegend.[103] Dieses Grundrecht, garantiert insb in Art 5 StGG sowie in Art 1 1. ZPEMRK, umfasst nach hL und stRsp nicht nur das Eigentum ieS als sachenrechtliches Vollrecht an körperlichen Sachen, sondern alle »vermögenswerten Privatrechte« – etwa auch Forderungs- oder Jagdrechte.[104] Die Frage, ob auch Kryptowerte bzw die Rechtszuständigkeit an ihnen ein durch die Rechtsordnung anerkanntes »vermögenswertes Privatrecht« darstellen und daher vom Schutzbereich der Eigentumsfreiheit umfasst sind, wird in der Lit bisher zwar nur selten ausdrücklich thematisiert, dann aber übereinstimmend bejaht.[105] Angesichts der technischen Besonderheiten und der Neuartigkeit von Kryptowerten erfordert diese Frage jedoch eine genauere Betrachtung.

Die Frage der rechtlichen Klassifikation dieser Vermögenswerte, ihrer Zuordnung zu einer Person und der zugrundeliegenden Technologie wurde bereits früh in parlamentarischen Anfragen aufgegriffen.[106] In der rechtswissenschaftlichen Lit wurde vor dem Hintergrund des wirtschaftlichen Werts und der technischen Übertragbarkeit von Kryptowerten insb auch ihre zivilrechtliche Einordnung thematisiert. In der überwiegenden Lit werden Kryptowerte diesbezüglich einhellig als unkörperliche Sachen iSd ABGB beurteilt:[107] Die Charakterisierung als Sache wird überzeugend mit dem weiten Sachbegriff des ABGB, der Gebrauchsmöglichkeit als Tausch- und Zahlungsmittel bzw Gegenstand des Rechtsverkehrs, und mit ihrer ausgeprägten Beherrschbarkeit (nur) mithilfe des zugehörigen Private Key begründet. Auch über die Eigenschaft der Unkörperlichkeit herrscht grundsätzlich Einigkeit,[108] auch wenn von manchen Autoren eine analoge Anwendung einiger sachenrechtlicher Bestimmungen befürwortet wird.[109] Da Eigentum ieS nach heute ganz hA[110] nur an körperlichen Sachen bestehen kann, scheidet ein geschütztes Recht dieser Art an Kryptowerten also grundsätzlich aus. Auch eine Einordnung diesbezüglicher Rechtspositionen als Forderungsrecht wird, soweit diskutiert, in der Lit gut nachvollziehbar abgelehnt,[111] da (anders als etwa bei einer Forderung gegenüber einem Kreditinstitut) dem über die Zugriffsdaten Verfügenden kein Schuldner gegenübersteht.[112]

Anzumerken ist allerdings, dass in den letzten Jahren einige Gesetzesänderungen explizit oder implizit verdeutlicht haben, dass Kryptowerte auch rechtlich als Teil des einer Person zugeordneten Vermögens anzusehen sind. So wurde bereits 2017 in § 43 Abs 2 Z 3

103 Vgl *Tipold/Zerbes* in Fuchs/Ratz, WK StPO Vor §§ 110–115 Rz 4 mwN.

104 Vgl zB *Klaushofer* in Kahl/Khakzadeh/Schmid, Kommentar zum Bundesverfassungsrecht B-VG und Grundrechte Art. 5 StGG (Stand 1.1.2021, rdb.at) Rz 7.

105 Vgl *Piska,* Kryptowährungen und ihr Rechtscharakter – eine Suche im Bermuda-Dreieck, ecolex 2017, 632 (634); *Schmidt,* Kryptowährungen und Blockchains (2019) 108; *Piska/Völkel,* Kryptorecht, in Kolonovits/Muzak/Piska/Perthold/Strejcek (Hrsg), Besonderes Verwaltungsrecht[2] (2017) 357 (359); *Piska/Völkel,* Blockchain und Kryptorecht. Regulierungs-Chancen de lege lata und de lege ferenda, ZTR 2017, 97 (98); *Diwok/Gritsch,* Bitcoin, Geldbegriffe und Zahlungsmittel, ZFR 2020, 64 (65).

106 Vgl nur zB zur rechtlichen Einordnung die Anfragen 1577/J XXV. GP (2014), 382 bzw 383/J XXVI. GP (2018), 222, 223 und 224/J XXVI. GP (2018), 2373/J XXVI. GP, sowie 2374 und 2375/J XXVI. GP (2018); zu Risiken etwa 2294/J XXVI. GP (2018), 3207/J XXVII. GP (2020), 4338/J XXVII. GP (2020) und 6806/J XXVII. GP (2021).

107 Vgl etwa *Dafinger,* Bitcoins im Pfandleihgewerbe, ecolex 2020, 241 (242); *Völkel,* Privatrechtliche Einordnung virtueller Währungen, ÖBA 2017, 385 (387); *Völkel,* Privatrechtliche Einordnung der Erzeugung virtueller Währungen, ecolex 2017, 639 (640); *Fleißner,* Eigentum an unkörperlichen Sachen am Beispiel von Bitcoins, ÖJZ 2018, 437 (437 f); *Schmidt,* Kryptowährungen 118; *Vonkilch/Knoll,* Bitcoins und das Sachenrecht des ABGB, JBl 2019, 139 (141 f); *Aigner,* Das Pfandrecht und die Blockchain, ÖBA 2019, 816 (819 ff); Völkel, Vertrauen in die Blockchain und das Sachenrecht, ZFR 2020, 492 (494 f); *Anderl/Aigner/Schelling,* Krypto-Assets und Tokenisierung, in Anderl (Hrsg), Blockchain in der Rechtspraxis (2020) 57 (59); *Holzner* in Rummel/Lukas (Hrsg), ABGB[4] § 292 (Stand 1.7.2016, rdb.at) Rz 2; *Helmich* in Kletečka/Schauer (Hrsg), ABGB-ON[1.05] § 292 (Stand 1.8.2022, rdb.at) Rz 8/1; *Holzner* in Kletečka/Schauer (Hrsg), ABGB-ON[1.06] § 353 (Stand 1.1.2023, rdb.at) Rz 1; *Völkel,* Grundlagen der privatrechtlichen Einordnung, in Piska/Völkel (Hrsg), Blockchain rules (2019) Rz 3.13; *Rassi,* Exekution auf Internetrechte nach der GREx, ecolex 2021, 1070 (1071); *Weidinger,* Zur Eigentumsrechtsfähigkeit nach § 354 ABGB: Ein Plädoyer zur Abkehr von der strikten Dichotomie zwischen körperlichen und unkörperlichen Sachen anhand von Bitcoin, ZIIR 2023, 370 (371, 374 f).

108 In manchen Beiträgen findet sich zwar die Überlegung, dass die – an sich unkörperlichen – Kryptowerte bei Verwendung einer physischen Wallet als gleichsam ebenfalls körperlich eingestuft werden könnten (vgl *Stadler/Chochola,* Kryptowährungen: Aufklärungspflichten im Verhältnis Unternehmer – Verbraucher, ecolex 2017, 641 [642]; *Völkel,* ÖBA 2017, 385 [388]); bei den so »verkörperten« Daten handelt es sich allerdings stets nur um die Verfügungsdaten (insb Private Keys), nicht um die Vermögenswerte selbst. Diese bleiben durch Eintragung in der Blockchain einer bestimmten Adresse zugeordnet, unabhängig davon, ob und in welcher Form die Verfügungsdaten abgelegt werden. Eine Änderung der Beurteilung von unkörperlich zu körperlich lediglich aufgrund der Art der Ablage der Verfügungsdaten ist daher abzulehnen – so auch *Dafinger,* ecolex 2020, 241 (242 f) und *Vonkilch/Knoll,* JBl 2019, 139 (142); *Anderl/Aigner/Schelling* in Anderl (Hrsg), Blockchain in der Rechtspraxis, 57 (60).

109 *Aigner,* ÖBA 2019, 816 (820 ff); *Fleißner,* ÖJZ 2018, 437 (440 ff); *Vonkilch/Knoll,* JBl 2019, 139 (145 ff); *Völkel,* ÖBA 2017, 385 (388 f); *Diwok/Gritsch,* ZFR 2020, 64 (68 f); *Schmidt,* Kryptowährungen 118 ff.

110 Vgl zB *Winner* in Rummel/Lukas (Hrsg) ABGB[4] § 354 (Stand 1.7.2016, rdb.at) Rz 1, 3; *Holzner* in Kletečka/Schauer, ABGB-ON[1.06] § 353 Rz 1 und *Holzner* in Kletečka/Schauer (Hrsg), ABGB-ON[1.06] § 354 (Stand 1.1.2023, rdb.at) Rz 1; vgl auch *Staudegger,* Datenhandel – ein Auftakt zur Diskussion, ÖJZ 2014, 107 (114) und *Dürager,* Sind Daten ein schutzfähiges Gut? ÖBl 2018, 260 (262). Zur Entwicklung dieser Interpretation entgegen der ursprünglichen Intention des historischen Gesetzgebers vgl *Klammer,* Dateneigentum (2019) Rz 204 ff.

111 Vgl etwa *Völkel,* ZFR 2020, 492 (496), *Völkel,* ÖBA 2017, 385 (387) und *Fleißner,* ÖJZ 2018, 437 (438).

112 Dies ist von jener in Kapitel III.B. erwähnten Konstellation zu unterscheiden, in der ein Vertragsverhältnis mit einem Dienstleister besteht, durch welches schuldrechtliche Ansprüche begründet werden können.

BiBuG 2014 eine Legaldefinition des Begriffs »Vermögensbestandteile« aufgenommen, die auch »Einheiten virtueller Währungen und die auf diese entfallenden Wertzuwächse« umfasst.[113] Diese Definition wurde 2021 auch in § 165 Abs 6 StGB leicht abgeändert übernommen[114] – dort werden seither »Einheiten virtueller Währungen und die auf diese entfallenden Wertzuwächse oder durch diese belegte Rechte« in den Begriff des »Vermögensbestandteils« miteinbezogen. Ebenfalls 2021 wurde zudem – zurückgehend auf EU-Vorgaben – die Legaldefinition für ein »unbares Zahlungsmittel« in § 74 Abs 1 Z 10 StGB erweitert.[115] Sie umfasst nunmehr (dem Willen des europäischen Normsetzers entsprechend)[116] auch digitale Wallets, womit etwa die Benützung einer »falschen, verfälschten oder entfremdeten« digitalen Wallet zur Erfüllung der Qualifikation des § 147 Abs 1 Z 1 StGB führt und auch die Delikte der §§ 241a ff StGB in Frage kommen, sofern die Tathandlungen nach diesen Bestimmungen digitale Wallets betreffen. Beachtenswert ist schließlich insb die Einbeziehung von Kryptowerten in die Exekutionsordnung im Rahmen der Gesamtreform des Exekutionsrechts (GREx) 2021.[117] § 326 Abs 1 EO definiert nun die »Vermögensrechte des Verpflichteten im Sinn dieser Abteilung« und bezieht in diese explizit auch »Rechte aus virtuellen Währungen« mit ein. Nach den Mat[118] soll dadurch klargestellt werden, *»dass auch auf so genannte ›Krypto-Assets‹ des Verpflichteten gegriffen werden kann«.* An ihnen besteht ein Vermögensrecht des Verpflichteten und sie können – nun durch den Gesetzgeber klargestellt – Gegenstand einer Geldexekution auf Vermögensrechte sein.[119] Damit drückt diese Gesetzesänderung im Rahmen des Exekutionsrechts letztlich die **Akzeptanz von Kryptowerten als valide Teile des jemandem zugeordneten Vermögens** auch durch den Gesetzgeber aus. Sie stellen also einen Vermögenswert dar, an dem ein auch durch die Rechtsordnung anerkanntes Vermögensrecht im Sinne einer Rechtszuständigkeit einer Person bestehen kann.[120] Somit stellt auch die Sicherstellung von privat gehaltenen Kryptowerten durch Vollzugsorgane jedenfalls einen **Grundrechtseingriff** dar. Die **Erforderlichkeit einer gesetzlichen Grundlage** für einen solchen Eingriff wird auf verfassungsrechtlicher Ebene schon vom allgemeinen Legalitätsprinzip in Art 18 B-VG[121] sowie durch den formellen Gesetzesvorbehalt des Art 5 StGG[122] statuiert. Einfachgesetzlich hält § 5 Abs 1 StPO dies für den Strafprozess nochmals explizit fest: Rechtseingriffe durch Kriminalpolizei, Staatsanwaltschaft und Gericht sind nur zulässig, soweit sie »gesetzlich ausdrücklich vorgesehen« (sowie zur Aufgabenerfüllung erforderlich und verhältnismäßig) sind.

Nach der in den angeführten Erlässen erläuterten Rechtsauffassung von BMJ und BMI bilden die §§ 110 ff StPO schon bisher eine ausreichende Rechtsgrundlage für die Sicherung von Kryptowerten – sowohl in Form eines Herausgabe-, Veräußerungs- oder Verpfändungsverbots nach § 109 Z 1 lit b StPO als auch durch Übertragung auf behördeneigene Adressen. Letzteres wird dabei erkennbar als eine Art Sicherstellung von Datenträgern unter § 109 Z 1 lit a StPO subsumiert. Vorgeschlagene Änderungen im Rahmen des StPRÄG 2024 sollen ersichtlich auch in diesem Bereich für einen eindeutigeren rechtlichen Rahmen und mehr Rechtssicherheit sorgen.[123]

B. Übertragung auf behördlich kontrollierte Adressen als Sicherstellung nach § 109 Z 1 lit a StPO

Im Gesetzesentwurf zum StPRÄG 2024 wird ausgeführt, dass es sich in der Praxis bewährt habe, *»Kryptowährungen auf ein sog ›Behördenwallet‹ der Kriminalpolizei zu transferieren«.*[124] Wie bereits erläutert, soll diese Vorgehensweise nach dem Reformvorschlag zukünftig explizit in § 114 Abs 1a StPO angeführt werden. Nach der Rechtsauffassung von BMJ und BMI ist diese Art der Sicherung allerdings an sich schon bislang zulässig und von den bereits vorhandenen gesetzlichen Grundlagen gedeckt, die Begründung dafür weist allerdings einige Widersprüche und Unklarheiten auf, wie im Folgenden dargestellt wird.

113 Eingefügt mit BGBl I Nr 135/2017. In den ErlRV dazu wird erklärt: *»Virtuelle Währungen werden berücksichtigt, um der FATF (FATF, Guidance for a Risk-Based Approach Virtual Currencies, June 2015) Genüge zu tun«* (ErlRV 1668 BlgNR XXV. GP, 4).

114 Eingefügt durch BGBl I Nr 159/2021.

115 Erfolgt durch BGBl I Nr 201/2021.

116 Vgl Richtlinie (EU) 2019/713, ErwGr 8 und 10.

117 Erfolgt durch BGBl I Nr 86/2021.

118 ErlRV 770 BlgNR XXVII. GP, 51.

119 Vgl *Rassi,* ecolex 2021, 1070 (1070).

120 So führt auch *Rassi,* ecolex 2021, 1070 (1070) aus: *»Insoweit vertreten wird, dass mit solchen Währungen keine ›Rechte‹ verbunden seien, […] ist dem (nur) insoweit zuzustimmen, dass die Verfügungsmacht über Krypto-Assets iaR nicht (wie etwa bei einem Guthaben auf einem Konto) mit Forderungen bzw Ansprüchen gegen einen Dritten verbunden sind. Dessen ungeachtet können derartige Währungen (bzw die entsprechenden Registereinträge) einer bestimmten Person rechtmäßig zugeordnet werden, der dann (iS des weiten Eigentumsbegriffs des § 353 ABGB) ein Eigentumsrecht im weiteren Sinne (Rechtszuständigkeit) an diesen digitalen Werten zukommt.«*

121 Vgl etwa *Winkler/Pöschl,* Rechtswissenschaftliche Grundlagen, in Winkler (Hrsg), Öffentliches Wirtschaftsrecht (2008) 43 (59 f).

122 Vgl etwa *Berka/Binder/Kneihs,* Die Grundrechte: Grund- und Menschenrechte in Österreich² (2019) 461.

123 So etwa ErlME 349/ME XXVII. GP, 40 in Bezug auf den Transfer auf behördlich kontrollierte Adressen.

124 Vgl ErlME 349/ME XXVII. GP, 40.

1. Einordnung als unkörperliche Vermögenswerte sowie Gleichsetzung von Kryptowerten mit der Blockchain

Wie bereits in Kapitel V.A. erläutert, deckt die Legaldefinition der Sicherstellung in § 109 Z 1 lit a StPO die Begründung von Verfügungsmacht über Gegenstände, also körperliche Sachen, ab. Aus § 110 Abs 4 und § 111 Abs 2 StPO, die ua von »sichergestellten Informationen« sprechen, wird die Zulässigkeit auch des Zugriffs auf Daten, die auf Datenträgern gespeichert sind, abgeleitet, und zwar auch in Bezug auf externe Speicherplätze. Auch das BMJ führt bislang zunächst in seinem Leitfaden Vermögensrechtliche Anordnungen (2020) sowie im Erlass zum Vorgehen bei Sicherstellung, Beschlagnahme und Verwertung von virtuellen Währungen im Bereich der Justiz aus, dass die Sicherstellung nach § 109 Z 1 lit a StPO auf körperliche bewegliche Sachen beschränkt[125] und bei einer »Sicherstellung« von Daten der Datenträger als körperlicher Gegenstand Objekt dieser Maßnahme ist.[126] In Bezug auf § 111 Abs 2 StPO wird zudem angemerkt, dass diese Bestimmung technologieneutral gehalten sei, *»letztlich auch um angesichts des laufenden technischen Fortschritts wiederkehrende Gesetzesänderungen hintanzustellen«,* und der Begriff »Informationen« daher etwa *»auch Datenblöcke in einer Blockchain«* abdecke; bei einer Blockchain könnten *»die Datenträger, auf denen die Einträge gespeichert sind, auf der ganzen Welt verteilt«* sein.[127] Dem ist grundsätzlich zuzustimmen, da die Blockchain – bei Kryptowerten also das Transaktionsverzeichnis – in Kopien verteilt auf den Rechnern der Netzwerkteilnehmer abgespeichert ist. In den weiteren Rechtsausführungen wird allerdings sodann bemerkenswerterweise diese Charakterisierung auch auf die Kryptowerte als Vermögenswerte selbst ausgedehnt: *»Virtuelle Vermögenswerte wie Kryptowährungen unterliegen dieser Bestimmung, weil es sich dabei um auf Datenträgern (= in einer dezentralen Datenbank, die auf diversen auf der ganzen Welt verteilten Rechnern gespeichert sein kann) gespeicherte Informationen (= Anzahl, Transaktionen ua) handelt.«*[128] Für die im Klammerausdruck angeführten Daten, nämlich Anzahl und Transaktionen, ist diese Feststellung richtig; letztlich wird nach dieser Rechtsansicht aber der virtuelle Vermögenswert selbst mit jener Datenbank, über die er verwaltet wird (mag diese auch verteilt abgespeichert sein), gleichgesetzt, was technisch völlig verkürzt ist und auch einem Vergleich mit anderen, etablierten digitalen Verwaltungsdatenbanken nicht standhält. Äquivalent wäre es zu erklären, die Forderungen von Kunden gegen ein Kreditinstitut seien lediglich jene Daten über Bestehen und Höhe dieser Forderungen, die in einer (diesfalls zentral verwalteten) Datenbank des Kreditinstituts abgelegt sind. In diesem Zusammenhang wird jedoch problemlos zwischen den schuldrechtlichen Ansprüchen und dem Register, in dem diese Ansprüche dokumentiert sind, unterschieden. Eine solche Differenzierung ist auch im Zusammenhang mit Kryptowerten sachlich geboten: die **Zugriffsdaten** (insb Private Keys, auf welche im Rahmen der Auswertung eines sichergestellten körperlichen Datenträgers zugegriffen werden kann) sind zu unterscheiden von der **Datenstruktur** (über welche Kryptowerte zugeordnet werden) sowie den **Kryptowerten** selbst (über die durch aktive Nutzung der Zugriffsdaten verfügt und eine Neuzuordnung in der Datenstruktur bewirkt wird). Die Einheiten sind als virtuelle Vermögenspositionen weder mit der Blockchain noch mit den Zugriffsdaten ident, mag ihre Existenz und Verwaltung auch eng mit diesen Daten verknüpft sein. Aus der Verwendung von Daten zur Verwaltung von Vermögenswerten zu schließen, dass diese Vermögensgüter selbst mit diesen Daten ident sind, ist irreführend. Es bietet sich insofern auch ein Vergleich mit dem Grundbuch an – schließlich wird dieses mittlerweile digital geführt, es erfolgt also auch die rechtliche Zuordnung von Liegenschaften durch Datenbankeinträge.[129] Dennoch wird keineswegs vertreten, dass eine »Sicherstellung« von Liegenschaften in der Form zulässig wäre, dass die Kriminalpolizei auf Grundlage von § 109 Z 1 lit a StPO auf die Zugangsdaten zugreift und sodann die Zuordnung der Liegenschaften in der Grundstücksdatenbank abändert. Denn: »Gegenstände« in § 109 Z 1 lit a StPO sind »bewegliche körperliche Sachen«,[130] Liegenschaften davon also nicht erfasst,[131] und die Zuordnung einer Liegenschaft durch Einträge in einer Datenbank macht diese Liegenschaft ganz offenkundig nicht zu Daten iSd § 111 Abs 2 StPO. Ein solches Vorgehen der Kriminalpolizei wäre mit der gesetzlichen Beschränkung auf bewegliche Sachen nicht vereinbar und würde diese umgehen – die Sicherstellung von Kryptowerten

125 *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 61; Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092, 2.

126 *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 70.

127 *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 71.

128 *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 109; Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092, 4.

129 Vgl § 2 Abs 1 GUG: *»Das Hauptbuch ist nur durch Speicherung der Eintragungen in einer Datenbank zu führen und mit dem Grundstücksverzeichnis des Grundsteuer- oder Grenzkatasters zu verknüpfen (Grundstücksdatenbank).«*

130 ErlRV 25 BlgNR XXII. GP, 153.

131 Liegenschaften können nach dem vorgesehenen Modell in der StPO zwar gemäß § 109 Z 2 lit b durch gerichtlichen Beschluss beschlagnahmt, jedoch nicht sichergestellt werden; *Tipold/Zerbes; Flora* in Fuchs/Ratz, WK StPO § 109 Rz 2; *Keplinger/Prunner/Pühringer/Rebisant* in Birklbauer/Haumer/Nimmervoll/Wess, § 109 StPO Rz 10; *Kroschl* in Schmölzer/Mühlbacher (Hrsg) StPO Kommentar I² (2021) § 110 StPO Rz 9.

auf vergleichbarem Weg wiederum umgeht die gesetzliche Einschränkung auf körperliche Sachen. Die Unterscheidung zwischen Zugriffsdaten, Blockchain und den Kryptowerten selbst ist **technisch, und nicht zuletzt aufgrund der verschiedenen grundrechtlichen Folgen auch rechtlich geboten:** Während die Entziehung von Kryptowerten in die verfassungsgesetzlich garantierte Eigentumsfreiheit eingreift, ist dies etwa bei der Herausgabe einer Kopie von Adressen, kryptographischen Schlüsseln und Transaktionsdaten im Rahmen von § 111 Abs 2 StPO nicht notwendigerweise der Fall.

Die weiteren Ausführungen im zitierten Leitfaden scheinen auch zunächst wieder einzulenken und erklären: *»Kryptowährungen fallen nicht unter den Begriff des ›Gegenstandes‹ im Sinne des § 109 Z 1 lit a StPO. Sie können am ehesten als unkörperliche Vermögenswerte eingeordnet werden.* **Der einzelne Wert der Kryptowährung kann nicht nach § 109 Z 1 lit a StPO sichergestellt werden,** *weil darüber keine Verfügungsmacht begründet werden kann […]«*[132] [Hervorhebung hinzugefügt]. Diese Erkenntnis wird jedoch sogleich revidiert, indem fortgesetzt wird: *»sehr wohl aber kann das körperliche Speichermedium des Wallet (zB der Computer, das Smartphone, der USB-Stick oder das Blatt Papier, auf dem der Key abgedruckt ist), in dem die Schlüssel für Transaktionen verwaltet werden, nach dieser Bestimmung sichergestellt werden. Da Kopien der Schlüssel vorhanden sein können und somit Zugriffsmöglichkeiten von dritter Seite drohen, ist eine Sicherstellung durch Transfer auf ein sog »Behördenwallet« durchzuführen. […]* **Mit der Transaktion auf ein Behördenwallet ist der Vermögenswert gesichert«**[133] [Hervorhebung hinzugefügt]. Die Bedenken hinsichtlich vorhandener Kopien spiegeln die Problematik wider, die in der bereits erwähnten Redewendung *»Not Your Keys, Not Your Coins«* angesprochen wird. Die zuerst als nicht nach § 109 Z 1 lit a StPO durchführbare Sicherstellung des einzelnen Vermögenswertes wird somit letztlich doch vorgesehen und offenbar genau auf diese Norm gestützt. Während zuerst zwischen dem unkörperlichen Vermögenswert und einem körperlichen Speichermedium mit Zugriffsdaten deutlich unterschieden wird, wird diese Differenzierung unmittelbar darauf ohne Begründung verworfen und die Sicherung des Wertes selbst anvisiert. Dadurch **begründen die Strafverfolgungsbehörden effektiv Verfügungsmacht über diesen unkörperlichen Vermögenswert,** und schaffen hiermit einen Zustand, den man mit *»Their Keys, Their Coins«* umschreiben könnte. Dass dies nach Auffassung von BMI und BMJ tatsächlich eine »Sicherstellung« des Kryptowertes im Sinne der durch die StPO vorgesehenen Maßnahme darstellt, macht die Zusammenschau mit den anderen Erlässen deutlich, die dieses Vorgehen dezidiert so bezeichnen.[134] Dies wird bestätigt durch den Hinweis, es sei *»sicherzustellen, dass der betroffenen Person sogleich oder längstens binnen 24 Stunden eine Bestätigung über die Sicherstellung ausgefolgt oder zugestellt wird und sie über das Recht, Einspruch zu erheben (§ 106 StPO) und eine gerichtliche Entscheidung über die Aufhebung oder Fortsetzung der Sicherstellung zu beantragen, informiert wird«;*[135] dies entspricht exakt den derzeitigen Vorgaben für Sicherstellungen nach § 111 Abs 4 StPO.

Ganz ersichtlich sollen die **mit dem StPRÄG 2024 vorgeschlagenen Änderungen** ua einen **neuen Rechtsrahmen für die Sicherstellung von Kryptowerten** im strafrechtlichen Ermittlungsverfahren schaffen, insbesondere durch die Einbeziehung von »Vermögenswerten«, deren Legaldefinition ausdrücklich auf Kryptowerte Bezug nimmt. Die Materialien lassen diesbezüglich auf einen **bemerkenswerten Argumentationswandel** schließen. So wird ausgeführt: *»Insbesondere soll die Legaldefinition der Sicherstellung in § 109 Z 1 lit a StPO […] um diesen Begriff der Vermögenswerte erweitert werden,* **um** *unter anderem* **die Sicherstellung** *(und allfällige Beschlagnahme samt nachfolgender Verwertung)* **von digitalen Kryptowerten zu ermöglichen«**[136] [Hervorhebung hinzugefügt]. Die Formulierung suggeriert – anders als die bislang von BMI und BMJ vertretene Rechtsansicht – sehr deutlich, dass »digitale Kryptowerte« bis zu der vorgeschlagenen Änderung überhaupt nicht auf Grundlage des § 109 Z 1 lit a StPO sichergestellt werden können. Die Deutung von Kryptowerten als mit der Blockchain letztlich idente Daten und der Rückgriff auf § 109 Z 1 lit a StPO in Verbindung mit § 111 Abs 2 StPO, um so doch ihre Sicherstellung argumentieren zu können, wird offenbar in den Materialien des StPRÄG 2024 fallen gelassen. Stattdessen soll die Einordnung von Kryptowerten als von der Blockchain zu unterscheidende, unkörperliche Vermögenswerte in einen gesetzlichen Rahmen gegossen und somit eine tatsächlich tragfähige Rechtsgrundlage für ihre Sicherstellung nach § 109 Z 1 lit a StPO geschaffen werden. Dies ist zu begrüßen: Der Bedarf für die Möglichkeit einer Sicherung dieser Werte ist zweifelsohne gegeben, allerdings fehlt eine eindeutige gesetzliche Basis für diesen Grundrechtseingriff bisher, was dringend behoben werden sollte.

132 *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 109. Inhaltlich gleich der Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092, 2.

133 *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 109. Inhaltlich gleich der Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092, 3.

134 *BMI,* Richtlinie – Sicherstellung von Kryptowährungen, 8, 10 ff; Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092, 3.

135 *BMI,* Richtlinie – Sicherstellung von Kryptowährungen, 11.

136 ErlME 349/ME XXVII. GP, 37.

2. Auflösung der Gegenstandsbindung der Sicherstellung

Neben der Frage des Sicherstellungsobjekts ist auch zu berücksichtigen, welcher technische Vorgang mit der in dieser Hinsicht unpräzisen[137] Formulierung *»Transfer auf ein sog ›Behördenwallet‹«* (die sich sowohl in den Ausführungen des BMJ zur aktuellen Rechtslage[138] als auch in den Materialien zum StPRÄG 2024[139] findet) tatsächlich gemeint ist. Anders als diese Formulierungen auf den ersten Blick suggerieren könnten (da in Wallets grundsätzlich kryptographisches Schlüsselmaterial abgespeichert wird), handelt es sich nicht um eine Übertragung der Zugriffsdaten von einem Datenträger auf einen anderen – ein solcher würde das Risiko eines Zugriffs von dritter Seite, das durch dieses Vorgehen gerade vermieden werden soll, nicht verringern. Um diesem entgegenzutreten ist eine – in Kapitel III.C. geschilderte – Übertragung des Kryptowertes selbst von einer Adresse an eine andere Adresse erforderlich. Gemeint ist also offenbar, dass die ermittelten Verfügungsdaten (Adresse, Public Key und Private Key) behördlicherseits eingesetzt werden, um über das Netzwerk eine Zuschreibung der Kryptowerte zu einer behördlich kontrollierten Adresse zu erwirken. Die Verfügungsdaten für diese Adresse werden sodann in der genannten »Behördenwallet« abgespeichert.[140]

Die Berücksichtigung dieses technischen Vorgangs macht deutlich, dass bei Subsumtion der Übertragung eines Kryptowertes an eine Behördenadresse die Gegenstandsbindung der Sicherstellung – nach aktueller Rechtslage ein wesentlicher Aspekt dieser Maßnahme – aufgelöst wird. Bereits der Fernzugriff auf extern (etwa in »Clouds«) gespeicherte Daten im Rahmen der Sicherstellung wird bisher in der Lit kritisiert, weil dies *»im Widerspruch zum Charakter der Sicherstellung als gegenstandsbezogene Maßnahme«* stehe.[141] Wie bereits im Zusammenhang mit § 111 StPO in Kapitel V.C.2. angeführt, **erfordert die Zulässigkeit eines Abrufs von Daten** aber jedenfalls zunächst **die Sicherstellung eines Geräts,** über die dieser Abruf erfolgt – mag diese Sicherstellung auch nur sehr vorübergehend erfolgen. Um die diesbezüglich deutliche Entscheidung des VwGH erneut zu zitieren: *»Ohne die Sicherstellung derartiger Hardware, die den Zugang zu Informationen ermöglicht, erlauben § 109 Z 1 und §§ 110 ff StPO keinen Zugang zu digital gespeicherten Informationen.«*[142] **Unzulässig** wäre es demnach, unter Nutzung von zunächst ermittelten Zugangsdaten **von einem anderen Gerät (etwa einem Rechner der Polizei) aus** auf extern abgespeicherte Daten zuzugreifen.[143] Wie festzustellen ist, geht allerdings die Übertragung von Kryptowerten an einer Behördenadresse sogar noch einen wesentlichen Schritt weiter. Aufgeschlüsselt sind in einer solchen Konstellation folgende Daten und Datenträger beteiligt:

1. zunächst wird ein **Datenträger sichergestellt,** der Zugriffsdaten für bestimmte Kryptowerte enthält (insb kryptographische Schlüssel) – diese **Zugriffsdaten** werden iSd § 111 Abs 2 StPO kopiert bzw anderweitig behördlich **gesichert;**
2. in der Folge wird insb der erlangte Private Key genutzt, um eine Transaktion zu signieren und im Netzwerk zu verteilen, die darauf abzielt, die betreffenden Kryptowerte einer neuen Adresse zuzuschreiben. Für die erfolgreiche Verarbeitung der Transaktion ist im Allgemeinen zudem eine Transaktionsgebühr zu entrichten. Wird die Transaktion erfolgreich vom Netzwerk in einen neuen Block inkludiert, so geht aus der so aktualisierten Blockchain die Neuzuschreibung der Kryptowerte an die behördlich vorgegebene Adresse hervor. Durch diese faktische Ergänzung der im Netzwerk **verteilt auf Datenträgern gespeicherten Blockchain** wird weder ein Datenträger sichergestellt noch werden Daten iSd § 111 Abs 2 StPO gesichert. Es erhalten lediglich jene Organe, die über die Zugriffsdaten für **diese behördlich kontrollierte Adresse** verfügen, die (ausschließliche) Kontrolle über die ihr nun zugeschriebenen Kryptowerte;
3. die **Zugriffsdaten für diese behördlich kontrollierten Adressen** werden (oder sind bereits) in einer **»Behördenwallet« (als Datenträger)** abgespeichert, die vom Internet getrennt aufbewahrt wird.

Nur am Beginn des Vorgangs kommt es zu einer Sicherung von (Zugriffs-)Daten, die in Verbindung mit einem sichergestellten Datenträger stehen. Der – später – an-

137 Wie in Kapitel III.D. ausgeführt, werden im Rahmen einer Transaktion bzw Verwaltung von Kryptowerten über Wallets nicht die Werte selbst »auf eine Wallet übertragen« bzw in dieser verwahrt, sondern lediglich das kryptographische Schlüsselmaterial.

138 *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 109. Inhaltlich gleich der Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092, 3.

139 ErlME 349/ME XXVII. GP, 39 f.

140 Sollten die Zugriffsdaten (insb die kryptographischen Schlüssel) nicht in Erfahrung zu bringen sein, ist dieses Vorgehen freilich unmöglich.

141 *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht Rz 5.11.

142 VwGH 20.4.2022, Ra 2021/01/0418. So auch *Tipold/Zerbes* in Fuchs/Ratz, WK StPO § 111 Rz 12; diese vertreten aber in der Folge – basierend auf einer missverständlichen Schilderung der technischen Hintergründe –, die Strafverfolgungsbehörden dürften *»den Speicherplatz von Bitcoins etc von einem Computer des Betroffenen aus«* erreichen und *»die dort vorgefundenen Vermögenswerte abbuchen«* (allerdings nicht von einem Computer der Behörde aus bei Auffinden nur der kryptographischen Schlüssel), siehe Rz 14/6 und 14/7.

143 *Reindl-Krauskopf/Salimi/Stricker,* IT-Strafrecht Rz 5.15.

geordnete Transfer betrifft nicht *»das körperliche Speichermedium des Wallet […], in dem die Schlüssel für Transaktionen verwaltet werden«* oder diese »Schlüssel« selbst, sondern die durch die Schlüssel zugänglichen Vermögensgüter. Bei den Daten, die somit letztlich in »Behördenwallets« abgespeichert sind, handelt es sich nicht um Original oder Kopie von iSd § 111 Abs 2 StPO ausgefolgten Informationen, sondern um behördlicherseits gänzlich neu generierte Daten (nämlich insb den mit der Behördenadresse korrespondierenden Private Key). Diese haben **mit den ursprünglich gesicherten Zugriffsdaten inhaltlich nichts gemein** und **waren auch nie auf einem sichergestellten Datenträger abgespeichert oder durch diesen zugänglich**, sondern wurden neu zu dem Zweck erzeugt, die alleinige Kontrolle über »sichergestellte« unkörperliche Vermögenswerte zu erlangen. Auch der Umstand, dass sich die Sicherstellung eines Datenträgers nicht nur auf den ursprünglichen Datenträger beziehen kann, sondern auch einen allenfalls auszufolgenden oder durch die Strafverfolgungsbehörden hergestellten, auf welchem die zu sichernden Daten abgespeichert wurden,[144] kann also nicht ins Treffen geführt werden. Die Strafverfolgungsbehörden legen letztlich völlig andere Daten auf ihrem Datenträger ab als jene, die sie iSd § 109 Z 1 lit a iVm § 111 Abs 2 StPO sichergestellt haben.

Die angeführten, zur (noch) aktuellen Rechtslage ergangenen Erlässe enthalten keine genauere Erörterung, auf welcher Rechtsgrundlage die Übertragung der Kryptowerte von der Herkunfts- auf die behördlich kontrollierte Adresse gestützt wird. Das BMJ beruft sich für die Zulässigkeit der Transaktion in einem der Erlässe lediglich kurz darauf, dass es sich um einen *»Ausfluss der Verfügungsmacht über Datenträger«* handle.[145] Dabei wird die Geschäftszahl einer OGH-Entscheidung angeführt, in welcher das Höchstgericht den bereits oben behandelten Umstand ausführt, dass zwar das Sicherstellungsobjekt ein auszufolgender oder herzustellender körperlicher Datenträger ist, die Sicherstellung aber auch den Zugriff auf Daten ermöglicht und dies auch in Form der Ausfolgung einer Kopie der Daten zulässig ist.[146] Der OGH prüfte in diesem Fall die Zulässigkeit eines Vorgehens, bei dem Kopien von Kameraaufnahmen ohne gleichzeitige Sicherung des originalen Datenträgers samt umschließendem Gegenstand herausverlangt worden waren. Vergleichbar hierzu wäre in Bezug auf Kryptowerte ein behördliches Begehren auf Herausgabe von Kopien der Private Keys, anstatt eine Hardware-Wallet, auf der diese Daten abgespeichert sind, in Verwahrung zu nehmen. Die Sicherung der Kamerabilder bei der angeführten Entscheidung wurde in Verbindung mit einem körperlichen Datenträger – auf welchem die Kopie abgespeichert wurde – durchgeführt. Die Strafverfolgungsbehörden gehen jedoch eben gerade bedeutende Schritte weiter, wenn sie in der Folge losgelöst vom ursprünglich sichergestellten Datenträger die kopierten Daten nutzen, um über die – davon verschiedenen – unkörperlichen Vermögenswerte zu verfügen. Die vergleichbare Konstellation, im Rahmen der Sicherstellung eines Smartphones nach § 109 Z 1 lit a StPO nach dessen Rückgabe die ausgelesene Benutzerkennungen später einzusetzen, um geräteunabhängig extern gespeicherte Daten einzusehen, wurde in der Lit dementsprechend ebenso als nicht von dieser Bestimmung gedeckt beurteilt.[147] Ebenso wenig kann sie friktionsfrei herangezogen werden, um mithilfe ausgelesener Daten zu einem späteren Zeitpunkt extern gespeicherte Datenstrukturen über ein Netzwerk zu verändern (nicht bloß abzurufen oder zu kopieren) und den Berechtigten auf Dauer vom Zugang zu virtuellen Vermögensgütern auszuschließen. Die angeführte OGH-Entscheidung weist somit nicht die erforderlichen Parallelen zur Übertragung von Kryptowerten auf eine behördlich kontrollierte Adresse auf, um die Zulässigkeit dieser als »Ausfluss der Verfügungsmacht über Datenträger« begründen zu können. Insbesondere ist bei Normen, die staatliche Eingriffe in grundrechtlich geschützte Freiheiten erlauben, Folgendes zu berücksichtigen: *»Ihrer Funktion entsprechend sind sie restriktiv auszulegen.«*[148]

Durch die vorgeschlagenen Änderungen im Rahmen des StPRÄG 2024 würde diese Problematik augenscheinlich auf zwei Ebenen entschärft: Erstens, indem (wie bereits erläutert) die Sicherstellung nach § 109 Z 1 lit a StPO auf Vermögenswerte ausdrücklich ausgedehnt wird und die Begründung der Verfügungsmacht über Kryptowerte somit nicht mehr als »Ausfluss der Verfügungsmacht über Datenträger« gerechtfertigt werden muss; zweitens, indem durch den vorgeschlagenen neuen § 114 Abs 1a StPO die Sicherung von Krypowerten durch ihre Übertragung auf »behördeneigene Infrastruktur« zumindest explizit gesetzlich vorgesehen ist (wenn auch nach Gesetzessystematik und Wortlaut zu urteilen erst nach erfolgter Sicherstellung). Das Erfordernis, dass bei einem Datenzugriff im Zusammenhang mit einer Sicherstellung nach § 109 Z 1 lit a StPO eine

144 Vgl auch *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 70.

145 Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092, 3.

146 OGH 11.9.2018, 14 Os 51/18h. Die Entscheidung betraf die Ausfolgung von Videoaufnahmen, die eine Bankomatkamera von einer verdächtigen Person angefertigt hatte. Es war dem OGH nach nicht erforderlich, die Festplatte des Bankomaten samt Originaldaten sicherzustellen, sondern die Sicherstellung einer Kopie dieser Daten auf einem anderen Datenträger war ausreichend.

147 *Zerbes,* ÖJZ 2021, 176 (180 f).

148 *Funk,* Online-Durchsuchung und Grundrechte, in BMI (Hrsg), Online-Durchsuchung (2008), 55 (57).

Verbindung mit einem körperlichen Datenträger als Gegenstand bestehen muss, würde in Bezug auf Kryptowerte durch die vorgeschlagenen Gesetzesänderungen effektiv entfallen.

3. Begründung von Verfügungsmacht durch Transaktion auf Behördenadressen

Die Übertragung von Kryptowerten auf eine behördlich kontrollierte Adresse und nachfolgende Verwaltung der zugehörigen kryptographischen Schlüssel über eine »Behördenwallet« führt nach aktueller Rechtslage paradoxerweise zu genau jenem Zustand, der zunächst im Leitfaden Vermögensrechtliche Anordnungen (2020) als unmöglich beurteilt wird *(»Der einzelne Wert der Kryptowährung kann nicht nach § 109 Z 1 lit a StPO sichergestellt werden, weil darüber keine Verfügungsmacht begründet werden kann«*[149]*):* Kryptowerte sind zwar unkörperlich und können daher nicht in körperliche Verwahrung genommen werden – allerdings ist argumentierbar, dass durch Übertragung an eine streng behördlich kontrollierte Adresse, zu der niemand sonst (schon gar nicht der ursprünglich Verfügungsbefugte) Zugriff hat, sehr wohl eine »Begründung von Verfügungsmacht« iSd § 109 Z 1 lit a StPO eintritt. Mangels Körperlichkeit scheitert eine Subsumtion unter den Gegenstandsbegriff und damit unter diese Legaldefinition freilich dennoch. Der OGH hat in der Vergangenheit für eine vergleichbare Konstellation – nämlich die Überweisung eines Bankguthabens auf ein Konto der Verwahrungsabteilung des OLG – ausdrücklich festgehalten, dass *»eine Sicherstellung oder Beschlagnahme durch vorläufige Begründung der Verfügungsmacht nur in Bezug auf Gegenstände, das sind bewegliche körperliche Sachen zulässig«* ist.[150] Durch die Überweisung gelangte die Forderung effektiv in die alleinige Verfügungsmacht der Behörde, obwohl die Sicherstellung oder Beschlagnahme eines Bankguthabens nur durch Verbot der Herausgabe dieses Vermögenswerts an Dritte erfolgen darf. In Hinblick auf die Beschlagnahme, jedoch auf die Sicherstellung umlegbar, erklärte das Höchstgericht in einer anderen Entscheidung noch ausführlicher: *»(Nur) Bei Gegenständen, also beweglichen körperlichen Sachen, kann die Beschlagnahme (auch) durch Begründung der behördlichen Verfügungsmacht über diese erfolgen (§ 109 Z 2 lit a iVm Z 1 lit a StPO; vgl [zur Sicherstellung] § 111 Abs 1, § 114 Abs 1 StPO). Steht hingegen die Beschlagnahme eines anderen Vermögenswertes in Rede, kommt nur das Drittverbot oder das Verbot der Veräußerung oder Verpfändung desselben in Betracht (§ 109 Z 2 lit a iVm Z 1 lit b StPO).* **Das Gesetz sieht daher nicht vor, dass sich andere Vermögenswerte (als Gegenstände) in behördlicher Verwahrung befinden«**[151] [Hervorhebung hinzugefügt]. Solche Verfügungen sind bislang also hinsichtlich unkörperlicher Sachen im Gesetz nicht vorgesehen und entbehren damit einer Rechtsgrundlage. Es ist kein Grund ersichtlich, weshalb diese Feststellung nicht auch für unkörperliche Vermögenswerte, die nicht in einer Forderung bestehen, und somit für Kryptowerte gelten sollte: Das Gesetz sieht bisher nicht vor, dass sich diese als *»unkörperliche Vermögenswerte«*[152] in behördlicher Verwahrung befinden – was effektiv nach Transaktion auf eine behördlich kontrollierte Adresse und Abspeicherung der kryptographischen Schlüssel in einer Behördenwallet der Fall ist. Solche Verfügungen über Kryptowerte sind somit selbst in Zusammenschau mit § 111 Abs 2 StPO aktuell nicht von § 109 Z 1 lit a StPO erfasst und daher gesetzlich nicht vorgesehen.

Das Strafprozessänderungsgesetz 2024 würde diesen Mangel beheben, indem auch Vermögenswerte und somit Kryptowerte ausdrücklich zu potenziellen Objekten des § 109 Z 1 lit a StPO werden, die durch »Begründung der Verfügungsmacht« sichergestellt werden können. Wie in den Materialien festgehalten wird, soll dies je nach Art des Vermögenswerts auf unterschiedliche Weise geschehen können, wobei bei Kryptowerten eben auf den *»Transfer auf eine sog ›Behördenwallet‹«* verwiesen wird.[153]

4. Abzug der Transaktionskosten vom »sichergestellten« Vermögenswert

In diesem Zusammenhang soll auch Bewusstsein für eine andere Problematik geschaffen werden, welche die mangelnde Passgenauigkeit der Sicherstellungsbestimmungen auf die Übertragung von Kryptowerten verdeutlicht und bedauerlicherweise auch im Rahmen der vorgeschlagenen Änderungen durch das StPRÄG

149 *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 109. Inhaltlich gleich der Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092, 2.

150 OGH 12.10.2021, 14 Os 107/21y, EvBl-LS 2022/72; in diesem Fall kam es zur – unzulässigen – »Beschlagnahme« eines Bankguthabens durch eine solche Überweisung.

151 OGH 28.3.2023, 14 Os 137/22m. Bemerkenswert ist, dass durch die im StPRÄG 2024 vorgeschlagenen Ergänzung der Sicherstellung um die Begründung von Verfügungsmacht über »Vermögenswerte« auch hinsichtlich Forderungen eine wesentliche Änderung eintreten würde. Wie die Materialien zum Gesetzesvorschlag auch explizit festhalten, würden den Strafverfolgungsbehörden dadurch mehr Möglichkeiten offenstehen: *»Die Begründung der Verfügungsmacht über Vermögenswerte, gemäß § 109 Z 1 lit a StPO, kann auf unterschiedliche Weise, je nach Art des Vermögenswertes erfolgen […] Bei unkörperlichen Vermögenswerten wie Forderungsrechten stehen mehrere Wege zur Übertragung der Rechte und damit der Verfügungsmacht auf die Strafverfolgungsbehörden offen.«* (ErlME 349/ME XXVII. GP, 38). Eine Kontoüberweisung – wie im geschilderten Fall – wäre danach nicht mehr per se unzulässig.

152 *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 109; Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092) 2.

153 ErlME 349/ME XXVII. GP, 39.

2024 keiner Lösung zugeführt wird. Wie bereits in Kapitel III.C. erwähnt, ist bei Initiierung einer Transaktion grundsätzlich die Bezahlung von Transaktionsgebühren erforderlich, um die Verarbeitung durch andere Netzwerkteilnehmer zu incentivieren. Die bisherigen erlassmäßigen Vorgaben des BMI machen deutlich, dass tatsächlich auch mit dem Anfall von Transaktionsgebühren und deren Abzug von den »sicherzustellenden« Kryptowerten gerechnet wird, wobei nach Übertragung an eine Behördenadresse die *»Höhe der angefallenen Transaktionsgebühren«* und der *»Wert der sichergestellten Kryptowährungen in Euro (nach Abzug der Transaktionsgebühren)«* zu dokumentieren sind.[154] Dies ist insofern technisch nachvollziehbar, als bei der Durchführung einer Transaktion allenfalls anfallende Transaktionskosten grundsätzlich vom Saldo der zu übertragenden Kryptowerte abgezogen werden. Die dadurch eintretende **Verringerung der als »sicherzustellende Daten« interpretierten Vermögenswerte** erscheint allerdings rechtlich äußerst fragwürdig und ist gesetzlich nicht vorgesehen. Weiters wird ausgeführt, dass bei einer allfälligen (Wieder-)Ausfolgung von *»sichergestellten Kryptowährungen«* an einen Berechtigten *»auf Grund der Transaktionsgebühren nicht mehr der ursprünglich sichergestellte Vermögenswert ausgefolgt werden kann«.*[155] Die Vermögensgüter werden damit nicht vollständig (zurück-)erstattet, sondern reduziert um die Kosten der Weg- und Rückübertragung. Durch wen allfällige Kosten für Sicherstellung, Transport und Verwahrung zu tragen sind, ist allerdings eigentlich explizit gesetzlich geregelt: Bis zur Berichterstattung über die Sicherstellung sind sie von der Kriminalpolizei zu tragen, danach durch die Staatsanwaltschaft.[156] Kosten für Sicherstellung, Transport und Verwahrung sind außerdem zunächst vom Bund vorzuschießen.[157] Erst später sind sie uU von einer zum Kostenersatz verpflichteten Partei zu ersetzen[158] oder, wenn das Verfahren anders als durch Schuldspruch endet, überhaupt vom Bund zu tragen.[159] Soll die Übertragung von Kryptowerten auf eine behördlich kontrollierte Adresse eine Art der Sicherstellung darstellen, handelt es sich bei den Transaktionskosten um ebensolche Kosten – vergleichbar mit dem in Lit[160] erwähnten Beispiel der Abschleppkosten für ein sichergestelltes Fahrzeug. Es ist nachvollziehbar, warum der gesetzlich deutlich vorgezeichnete Weg der vorläufigen Kostentragung und eines allfälligen Kostenersatzes in diesem Fall technisch nicht umgesetzt wird bzw allenfalls technisch gar nicht umsetzbar ist. Dies zeigt aber auch auf, dass **ein solches Vorgehen nach aktueller Rechtslage gerade nicht vorgesehen** ist und daher auch nicht von der gesetzlichen Regelung berücksichtigt wird. Eine spätere Rückerstattung eines sichergestellten Vermögenswertes an den Berechtigten nur in einem durch ebendiese Kosten reduzierten Ausmaß entspricht ganz augenscheinlich nicht dem in der StPO festgelegten Modell der Kostentragung und erscheint im Hinblick auf die verfassungsgesetzlich geschützte Rechtsposition an Kryptowerten problematisch. Gerade die geplante ausdrückliche Verankerung des Transfers von Kryptowerten auf behördlich kontrollierte Adressen durch das StPRÄG 2024 würde nahelegen, auch eine gesetzliche Lösung für die beschriebene Diskrepanz zwischen den Kostentragungsbestimmungen der StPO und dem Vorgehen in der Praxis zu finden. Diese Problematik wurde aber im bisher bekannten Gesetzesvorschlag augenscheinlich nicht aufgegriffen.

C. Ausspruch eines Verbots gegenüber Dienstleistern als Sicherstellung nach § 109 Z 1 lit b StPO

§ 109 Z 1 lit b StPO umfasst im Gegensatz zu lit a leg cit schon nach aktueller Rechtslage neben Gegenständen auch **andere Vermögenswerte** und deckt somit **auch unkörperliche Sachen** – einschließlich virtueller Vermögenswerte wie Kryptowerte – ab.

Sind **Dienstleister,** wie etwa Betreiber von Krypto-Börsen, **involviert,** so wird auch schon bisher seitens des BMJ die Erlassung eines Herausgabe-, Veräußerungs- oder Verpfändungsverbots iSd § 109 Z 1 lit b StPO als Möglichkeit zur Sicherung von Kryptowerten angeführt.[161] Dabei wird betont, dass allerdings bei diesen aufgrund ihrer Verschiedenartigkeit das Erfordernis eines **wirtschaftlichen Wertes, der in Zahlen ausgedrückt werden kann,** nicht pauschal bejaht werden könne.[162]

Sind diese Voraussetzungen gegeben, so erscheint das Zurückgreifen auf § 109 Z 1 lit b StPO in solchen Konstellationen tatsächlich **rechtlich unproblematisch.**[163] Verwaltet in diesem Fall der Dienstleister die

154 *BMI,* Richtlinie – Sicherstellung von Kryptowährungen, 12.
155 *BMI,* Richtlinie – Sicherstellung von Kryptowährungen, 13.
156 *Kroschl* in Schmölzer/Mühlbacher (Hrsg), StPO Kommentar I² (2021) § 114 StPO Rz 22.
157 Vgl § 381 Abs 2 StPO.
158 Nach § 389 Abs 1 StPO ist das im Fall eines Schuldspruchs etwa der Angeklagte. Konkret fallen diese Kosten unter § 381 Abs 1 Z 5 StPO, vgl *Kroschl* in Schmölzer/Mühlbacher, § 114 StPO Rz 22.
159 Vgl § 390 Abs 1 StPO.
160 *Kroschl* in Schmölzer/Mühlbacher § 114 StPO Rz 22.
161 *BMJ,* Leitfaden Vermögensrechtliche Anordnungen (2020) 109; Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092) 4 f.
162 Erlass des BMJ vom 1.4.2020, GZ 2020-0.163.092) 2 f.
163 Anzumerken ist außerdem, dass – wie bereits in Kapitel III angesprochen – auch Systeme bestehen, die nicht dezentral betrieben werden, sondern bei denen ein oder mehrere identifizierte Betreiber vorhanden ist bzw sind (sog *»permissioned«* Systeme). In einem solchen Fall wäre es je nach technischer Ausgestaltung ebenfalls möglich, dass ein Betreiber selbst – und nicht nur ein dritter Diensteanbieter – Transaktionen von

Kryptowerte und kennt demgegenüber der Kunde die für Verfügungen erforderlichen kryptographischen Schlüssel nicht, so hat der Dienstleister die faktische Verfügungsmacht über die Vermögensgüter.[164] Ein effektiver Schutz vor nachteiligen Vermögensverschiebungen ist somit auf diese Weise möglich. Zu berücksichtigen ist auch in dieser Konstellation die bereits im Vorkapitel angesprochenen Rsp, wonach bislang eine Sicherstellung bzw Beschlagnahme von Forderungen in Form einer Überweisung von Bankguthaben durch die Strafverfolgungsbehörden unzulässig ist.[165] Eine Übertragung solcher (fremd-)verwalteten Kryptowerte auf eine behördlich kontrollierte Adresse wäre demnach auch hier nach aktueller Rechtslage nicht gesetzlich gedeckt.

Auch die Materialien des StPRÄG 2024 beziehen sich auf die Möglichkeit, bei Vorhandenseins eines »validen Dritten« ein **Herausgabe-, Veräußerungs- oder Verpfändungsverbot nach § 109 Z 1 lit b StPO** auszusprechen, thematisieren jedoch auch diesbezügliche Schwierigkeiten bei Kryptowerten, insb bei ausländischen Diensteanbietern.[166] Interessant ist in dieser Hinsicht auch die in den Materialien angestellte Überlegung – die allerdings nicht Eingang in den vorgeschlagenen Gesetzestext gefunden hat –, dass bei Vorhandensein eines »validen Dritten« *»aufgrund des Verhältnismäßigkeitsgebots des § 5 StPO wohl regelmäßig mit Sicherstellung in Form eines Drittverbots vorzugehen sein«* werde.[167]

D. Zugriff auf kryptographische Schlüssel: Ein Anwendungsfall der »Beschlagnahme von Datenträgern und Daten«?

Wie ersichtlich ist, zielen die Vorschläge des StPRÄG 2024 in Bezug auf Kryptowerte darauf ab, einen klaren Rechtsrahmen für ihre effektive Sicherstellung im Ermittlungsverfahren zu schaffen. Als primäre Sicherungsart zur Verhinderung von Drittzugriffen auf sichergestellte Kryptowerte ist die Übertragung auf behördlich kontrollierte Adressen vorgesehen. In diesem Zusammenhang ist allerdings ein **signifikantes Problem** absehbar, das durch andere im Rahmen des StPRÄG 2024 vorgeschlagene Änderungen entsteht. Wie bereits in Kapitel V.A.3. erörtert, ist mit dem Ziel der Umsetzung der verfassungsgerichtlichen Vorgaben aus G 352/2021 die Einführung der »Beschlagnahme von Datenträgern und Daten« als neue Ermittlungsmaßnahme geplant. Eine solche liegt ua dann vor, wenn ein Zugriff auf »Datenträger und darauf gespeicherte Daten« oder auf »Daten, die an anderen Speicherorten als einem Datenträger gespeichert sind, soweit auf sie von diesem aus zugegriffen werden kann«, erfolgen soll, und wenn dabei die Auswertung von Daten bezweckt wird. In diesem Fall müssten nach dem Reformvorschlag die – im Vergleich zur Sicherstellung nach § 109 Z 1 StPO strengeren – Voraussetzungen nach § 115f StPO erfüllt sein. Insb ist eine vorherige richterliche Kontrolle vorgesehen, es soll also *»schon die Begründung der Verfügungsmacht über einen Datenträger sowie die darauf (lokal oder extern) gespeicherten Daten […] einer gerichtlichen Bewilligung unterliegen«.*[168] Eine solche ist nach aktueller Rechtslage nicht erforderlich.

Zu bedenken ist nun jedoch, dass die Strafverfolgungsbehörden, wenn sie Kryptowerte sichern und hierzu iSd vorgeschlagenen § 114 Abs 1a StPO auf »behördeneigene Infrastruktur« übertragen möchten, dafür **zunächst die relevanten kryptographischen Schlüssel in Erfahrung bringen** müssen. Es ist davon auszugehen, dass zu diesem Zweck idR auf Datenträger – beispielsweise Hardware Wallets, Computer oder Smartphones – oder gar auf externe Speicherorte zugegriffen werden muss. In beiden Konstellationen handelt es sich geradezu um Musterfälle der »Beschlagnahme von Datenträgern und Daten« zum Zweck der Auswertung von Daten, wie sie in § 109 Z 2a StPO definiert werden soll. Dadurch entstehen nun **zwei Problemfelder:**

Zwar sind Kryptowerte nach der vorgeschlagenen Ergänzung des § 109 Z 1 lit a StPO um Vermögenswerte von dieser Bestimmung erfasst und könnten gemäß § 110 Abs 2 StPO aufgrund einer staatsanwaltlichen Anordnung sichergestellt werden; auch wäre ein Transfer auf eine behördlich kontrollierte Adresse nach § 114 Abs 1a StPO vorgesehen. Der **Zugriff auf die dafür nötigen Daten** jedoch unterläge den **erhöhten Voraussetzungen der »Beschlagnahme von Datenträgern und Daten«** – nämlich einer vorherigen gerichtlichen Bewilligung – und dem für diese Ermittlungsmaßnahme vorgesehenen komplexen organisatorischen Ablauf. Nicht nur ist diese Divergenz unerfreulich, sondern die dadurch zu befürchtenden Verzögerungen erscheinen gerade hinsichtlich der spezifischen Eigenschaften von Kryptowerten (insb der raschen, pseudonymen und grenzüberschreitenden Transferierbarkeit durch Dritte) bedenklich. Selbst die in § 115f Abs 4 StPO vorgeschlagene Möglichkeit der Kriminalpolizei, bei Gefahr im Verzug und in bestimmten anderen Fällen Datenträger aus Eigenem sicherzustellen, bietet keine Möglichkeit zur Verhinderung von Verzögerungen: Erstens soll es sich

dritter Seite verhindern könnte und somit als geeigneter Ansprechpartner für den Ausspruch eines Herausgabe-, Veräußerungs- oder Verpfändungsverbots dienen könnte.

164 So auch die Generalprokuratur in ihrem Rechtssatz vom 18.7.2022, Gw 163/22m im Zusammenhang mit der Frage des tatbestandmäßigen Erfolgseintritts nach § 146 StGB in dieser Konstellation.

165 OGH 12.10.2021, 14 Os 107/21y, EvBl-LS 2022/72.

166 ErlME 349/ME XXVII. GP, 37 f.

167 ErlME 349/ME XXVII. GP, 39.

168 ErlME 349/ME XXVII. GP, 14.

dabei nach den Materialien um eine *»auf absolute – in der Regel situative – Ausnahmefälle beschränkte Befugnis«* handeln,[169] sodass ihre allgemeine Anwendung bei einer bestimmten Art von Vermögenswert kaum argumentierbar wäre; zweitens soll der Kriminalpolizei selbst in solchen Fällen nach § 115f Abs 4 lS StPO ein Zugriff auf die Daten selbst nicht erlaubt sein – kryptographisches Schlüsselmaterial zu extrahieren kommt demnach ausnahmslos nicht in Frage. Deutlich insofern auch die Materialien: *»Keinesfalls soll in diesem Stadium jedoch der grundrechtsintensivere inhaltliche Zugriff auf die Daten zulässig sein […]; selbst ein Versuch, auf die gespeicherten Daten in irgendeiner Form zuzugreifen (z.B. Versuch der Entsperrung), soll ausgeschlossen sein. Vielmehr soll lediglich die physische ›Inbesitznahme‹ des Datenträgers zur Sicherung einer nachfolgenden Anordnung und Bewilligung iSd § 115f Abs 2 und 3 StPO zulässig sein.«*[170] Extern gespeicherte Datenbestände, auf die lediglich über den Datenträger zugegriffen wird, können so außerdem zwischenzeitlich nicht gesichert werden, sondern bleiben dem Risiko ihrer Veränderung oder Vernichtung (von einem anderen Datenträger aus) ausgesetzt.

Die erläuterte Diskrepanz bei den formellen Voraussetzungen der unterschiedlichen Ermittlungsmaßnahmen ist unpraktikabel. Demgegenüber betrifft das zweite Problemfeld die materiellen Erfordernisse und ist bei genauerer Betrachtung noch bedenklicher: Der vorgeschlagene § 115f Abs 1 StPO gibt vor, dass eine **Beschlagnahme von Datenträgern und Daten nur zulässig** sei, »wenn sie aus Beweisgründen erforderlich scheint und aufgrund bestimmter Tatsachen anzunehmen ist, dass dadurch Informationen ermittelt werden können, die für die Aufklärung einer Straftat wesentlich sind«. Soll kryptographisches Schlüsselmaterial lediglich ausgelesen werden, um in der Folge Kryptowerte sicherzustellen, wird dies aber häufig nicht zutreffen: Weder ist dies **aus Beweisgründen** erforderlich (was nach den Materialien bedeutet, *»dass der Datenträger und die Daten geeignet sind, das Beweisthema zu führen«*[171]), noch sind die dadurch allenfalls ermittelten Informationen **für die Aufklärung** einer Straftat wesentlich. Vielmehr wird in der Regel die (letztlich anvisierte) Sicherstellung von Kryptowerten der Sicherung von privatrechtlichen Ansprüchen oder vermögensrechtlichen Anordnungen dienen. Diese Zwecke können zwar nach § 110 Abs 1 Z 2 bzw Z 3 StPO die Zulässigkeit der späteren Sicherstellung des Vermögenswertes begründen, würden nach § 115f Abs 1 StPO aber keinen Zugriff auf Datenträger bzw Daten rechtfertigen. Ein **Datenzugriff, um die Begründung von Verfügungsmacht über sicherzustellende Vermögenswerte zu ermöglichen,** wäre nach der vorgeschlagenen Reform **schlicht nicht vorgesehen** und damit nicht mehr möglich. Ein Ausweichen auf die Argumentation, dass die Begründung der Verfügungsmacht über die Datenträger bzw Daten letztlich der Sicherung privatrechtlicher Ansprüche oder vermögensrechtlicher Anordnungen diene und daher noch unter § 109 Z 1 lit a StPO zu subsumieren sei, ist zwar denkbar, erscheint jedoch insgesamt fragwürdig. Dies, weil die Maßnahme selbst in einem solchen Fall zunächst ganz klar dem Zweck der Auswertung von Daten (des kryptographischen Schlüsselmaterials) dient, jedoch insofern in den Materialien deutlich *»der gesetzgeberische Wille […], dass eine Sicherstellung niemals ›zum Zweck der Auswertung von Daten‹ […] erfolgen kann«*[172] geäußert wird. Die in den Erläuterungen genannten Beispiele für eine zulässige Sicherstellung von Datenträgern zu anderen Zwecken (Sicherung von Spuren wie Blutspuren oder Fingerabdrücke) unterscheiden sich von einer solchen Konstellation, in der ein klares (ausschließlich) inhaltliches Interesse an den Daten besteht, stark. Ob es für die Zulässigkeit der Maßnahme ausreichen würde zu behaupten, dass den zu erlangenden kryptographischen Schlüsseln bzw ihrem Vorliegen auf dem Datenträger selbst Beweiswert zukommt, muss angesichts der zitierten, sehr klar geäußerten Intention des Gesetzgebers bezweifelt werden.

VII. Conclusio

Im eingangs erläuterten, zur Aufhebung der Sicherstellungsbestimmungen führenden Verfahren übermittelte der VfGH den Parteien und dem Sachverständigen ua zahlreiche, auch ins Detail gehende technische Fragen.[173] Das Höchstgericht erachtete offenbar etwa die Funktionsweise von IT-Endgeräten, die Möglichkeiten des Zugangs zu bestimmten Daten, zu ihrer Wiederherstellung und Veränderung sowie die technische Vorgehensweise bei der Auswertung – also den **tatsächlichen technologischen Hintergrund des behördlichen Handelns und der Auswirkungen auf die Betroffenen** – von Beginn an für relevant. Im Erkenntnis stellte der VfGH sodann fest, dass *»staatliches Handeln durch die rasche Verbreitung der Nutzung ›neuer‹ Kommunikationstechnologien (zB Mobiltelefonie, E-Mail, Informationsaustausch im Rahmen des World Wide Web etc) in vielerlei Hinsicht – nicht zuletzt auch im Rahmen der Bekämpfung der Kriminalität, der die Sicherstellung von Datenträgern dienen soll – vor besondere Herausforderungen gestellt wurde und wird.«*[174] Das-

169 ErlME 349/ME XXVII. GP, 16.
170 ErlME 349/ME XXVII. GP, 16.
171 ErlME 349/ME XXVII. GP, 14.
172 ErlME 349/ME XXVII. GP, 10 f.
173 *Soyer/Marsch,* VfGH und Handysicherstellung – technische und rechtliche Fragen aus dem Verfahren, AnwBl 2024, 164.
174 VfGH 14.12.2023, G 352/2021, Rz 76.

selbe gilt zweifelsohne für die Entwicklung, Verbreitung und – auch kriminelle – Nutzung von Kryptowerten. Unbestreitbar muss es den Strafverfolgungsbehörden möglich sein, diese effektiv zu sichern. Wie in diesem Beitrag dargelegt wurde, sind nach der bisher **geltenden Rechtslage** jedoch unkörperliche virtuelle Vermögenswerte dieser Art **nicht** problemlos **unter die in der Praxis herangezogenen Sicherstellungsbestimmungen der StPO subsumierbar.** Die in den Materialien ausgedrückte Intention, mit dem StPRÄG 2024 auf durch technische Entwicklungen entstandene Herausforderungen in diesem Zusammenhang zu reagieren und einen klaren Rechtsrahmen zu schaffen, ist zu begrüßen. Besonders die im Gesetzesentwurf vorgeschlagene Miteinbeziehung der Begründung von Verfügungsmacht auch über unkörperliche Vermögenswerte in § 109 Z 1 lit a StPO ist in dieser Hinsicht ein wesentlicher Schritt. Für mehr Rechtssicherheit kann auch die gesetzliche Verankerung der (schon bisher praktizierten) Übertragung von Kryptowerten auf behördlich kontrollierte Adressen sorgen, auch wenn der im Gesetzesentwurf konkret gewählte Wortlaut und die Verortung in § 114 StPO nicht stimmig erscheinen. **Signifikante Probleme** wären allerdings bezüglich der Möglichkeit, **auf kryptographisches Schlüsselmaterial sicherzustellender Kryptowerte zuzugreifen** zu erwarten: Die Ausgestaltung der im Rahmen der Reform neu vorgesehenen Ermittlungsmaßnahme der Beschlagnahme von Datenträgern und Daten lässt hier Verzögerungen bzw sogar wesentliche Einschränkungen befürchten. Es ist zu hoffen, dass die angekündigte Überarbeitung des Entwurfs auch zu einer Nachbesserung in diesem Bereich führen wird.

Korrespondenz:
Mag. Evelyne Putz,
Univ.-Prof. Dipl.-Ing. Mag. Dr. techn. Edgar Weippl,
Forschungsgruppe Security und Privacy,
Fakultät für Informatik,
Universität Wien ,
Kolingasse 14–16, 5. OG,
1090 Wien
Mail: evelyne.putz@univie.ac.at

Mag. Nicholas Stifter, Bakk.techn.,
SBA Research,
Floragasse 7, 5. OG,
1040 Wien
Mail: nstifter@sba-research.org