Weisser/Bliesener/Schmidt/Schmid

Geldwäsche – Terrorismusfinanzierung – Kryptowerte

Eine Bewertung des Phänomenbereichs sowie des Einsatzes von Open Source Intelligence (OSINT) als Ermittlungsvehikel in Deutschland

With the support of Erasmus | Programm of the European Union

Jean Monnet Centre of Excellence

CICJ

Crime Investigations and Criminal Justice

Forschungsprojekt G.E.K.O.
Stand: September 2025

Autoren:

Prof. Dr. **Niclas-Frederic Weisser**, LL.M. (Osnabrück), LL.M. (Hull) ist Professor an der Hochschule für Öffentliche Verwaltung Bremen (HfÖV) sowie stellv. Leiter des Jean Monnet Centre of Excellence Crime Investigations and Criminal Justice (CCICJ) und Leiter der dortigen Forschungsgruppe I (Geldwäsche & Wirtschaftskriminalität). Zuvor war er lange Zeit Staatsanwalt insb. in den Bereichen der Organisierten Kriminalität und Wirtschaftskriminalität.

Dipl.-Kfm. **Christian Bliesener**, LL.B., CFE ist Compliance Officer bei der wpd GmbH, Lehrbeauftragter an der HfÖV und Mitglied des CCICJ.

KHK`in Dipl. Verww. (FH) **Susanne Schmidt** ist Polizeibeamtin in Hamburg, derzeit im Leitungsstab im Bereich parlamentarische Angelegenheiten tätig und Mitglied des CCICJ. Nach 13 Jahren kriminalpolizeilicher Ermittlungen mit dem Schwerpunkt Wirtschaftskriminalität war sie in verschiedenen Stabsfunktionen im Landeskriminalamt aktiv, unter anderem in der Steuerungsgruppe „Kripo weiterdenken“.

RiLG **Florian Schmid** ist Richter am Landgericht Hamburg in einer Großen Wirtschaftsstrafkammer und derzeit abgeordnet zum Generalbundesanwalt beim Bundesgerichtshof in der Ermittlungsabteilung Terrorismus (Islamismus) in Karlsruhe. Ferner ist er Mitglied der WiSteV und des CCICJ.

Danksagung:

Besonderer Dank gilt dem Bundeskriminalamt, dem Zollkriminalamt (samt Zollfahndungsdienst) sowie den Landeskriminalämtern Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt, Schleswig-Holstein und Thüringen sowie der LPD Saarland für ihre umfangreiche Mitwirkung und Unterstützung, welche das Forschungsprojekt erst möglich gemacht haben.

Zusammenfassung:

Geldwäsche und Terrorismusfinanzierung gehören zu den größten Herausforderungen der internationalen Finanzkriminalität. Beide Deliktsbereiche zeichnen sich durch verdeckte Finanzströme mit hohem gesellschaftlichem Gefährdungspotenzial aus. Durch den technologischen Wandel werden klassische Bargeldgeschäfte allerdings zunehmend durch digitale Transaktionen abgelöst, allen voran von Kryptowerten wie Bitcoin. Diese bieten besondere Verschleierungsmöglichkeiten, da die Transaktionen grenzüberschreitend, pseudonym, dezentral und unter nur teilweiser Regulierung erfolgen. Die fortschreitende Digitalisierung eröffnet dabei aber auch neue Ermittlungswege. So wird zunehmend die sog. Open Source Intelligence (OSINT), also die systematische und gezielte Beschaffung von frei verfügbaren Informationen in den konventionellen Quellen und weltweiten Datennetzen unter Nutzung des gesamten Spektrums der öffentlich zugänglichen Informationskanäle in allen möglichen Sprachen, zur Ermittlung dieser Deliktsfelder eingesetzt.

Bedingt durch die ansteigende inkriminierte Nutzung von Kryptowerten ist eine umfassende statistische und disziplinübergreifende Auseinandersetzung mit dem Phänomenbereich bedeutsam. Aus diesem Grund erfolgte durch das EU-geförderte Jean Monnet Centre of Excellence Crime Investigations and Criminal Justice (CCICJ) an der Hochschule für Öffentliche Verwaltung Bremen (HfÖV) im Jahr 2025 das Forschungsprojekt G.E.K.O, an welchem sich alle Landeskriminalämter, das Bundeskriminalamt sowie das Zollkriminalamt samt dem Zollfahndungsdienst beteiligt haben. Ziel war es, bestehende Datenlücken zu schließen, das Ermittlungsinstrument der Open Source Intelligence in dem hiesigen Kontext zu bewerten und Verbesserungsmöglichkeiten aufzuzeigen.

Die Ergebnisse des Forschungsprojekts zeigen, dass die bestehende Datenlage lückenhaft ist. Die derzeit bekannten Fälle der Geldwäsche und Terrorismusfinanzierung spiegeln wohl in keiner Weise den geschätzten Gesamtumfang dieser Deliktsfelder wider, so dass von einem erheblichen Dunkelfeld ausgegangen werden muss. Der Einsatz von Kryptowerten wird in keiner amtlichen Statistik systematisch erfasst. Nur wenige Behörden führen eigene Erhebungen durch. Die Mehrheit der befragten Ermittlungsbehörden geht dabei von einem hohen Dunkelfeld bei der Verwendung von Kryptowerten bei Taten der Geldwäsche- und Terrorismusfinanzierung aus.

Das Forschungsprojekt hat ferner ergeben, dass OSINT bereits in vielen Behörden zur Ermittlung eingesetzt wird, insbesondere im Bereich der Terrorismusfinanzierung. Auch bei Geldwäscheverfahren, vor allem in komplexeren Fallkonstellationen, kommt OSINT zunehmend zum Einsatz. Die Bedeutung des Instruments wurde von den Befragten mit einem Durchschnittswert von 4,5 (auf einer Skala von 0 bis 5) als sehr hoch eingeschätzt. Gleichwohl zeigen sich strukturelle Defizite. So sind die eingesetzten Konzepte, Tools und Schulungsangebote unzureichend standardisiert. Ein bundesweites OSINT-Netzwerk mit interoperabler Infrastruktur fehlt bisher. Die Wirksamkeit dieses Ermittlungsvehikels hängt aber stark von der technischen und personellen Ausstattung sowie der internen Organisation ab.

Im Rahmen des Forschungsprojekts konnten zahlreiche Empfehlungen erarbeitet werden. So sind beispielsweise die Einführung eines bundesweit einheitlichen Merkmals „Krypto-Bezug“ in polizeilichen und justiziellen Statistiken, die Bündelung der Lagebildkompetenz, die Einführung von flächendeckenden Schulungsstandards und Fortbildungsangeboten für OSINT-Ermittler, eine Koordinierung auf bundes- oder europarechtlicher Ebene, der Aufbau zentraler Analyse-Hubs oder lizenzfinanzierten Schwerpunktstellen für ressourcenintensive Tools sowie der Einsatz von künstlicher Intelligenz in OSINT-Verfahren und schließlich die Förderung einer proaktiven sowie disruptiven Ermittlungsstrategie denkbar.

Aufgrund der Tatsache, dass ein zukünftiger Anstieg der Geldwäsche und Terrorismusfinanzierung mittels Kryptowerten anzunehmen ist, bedarf es eines Paradigmenwechsels in der Bekämpfung dieses Phänomenbereichs. Die Ermittlungsbehörden stehen dabei vor der Aufgabe, ihre technischen, rechtlichen und organisatorischen Fähigkeiten deutlich auszubauen, um mit der Dynamik digitaler Finanzkriminalität Schritt halten zu können. OSINT bietet hier ein großes Potenzial – unter der Voraussetzung, dass es strategisch, professionell und rechtssicher weiterentwickelt wird. Dies ist allerdings bereits in finanzieller Hinsicht nur mit politischer Unterstützung möglich.

Inhaltsverzeichnis

1 Einleitung

Die Erwirtschaftung von Gewinnen war schon immer eine der treibenden Kräfte für kriminelles Handeln.[1] Rechtswidrig erlangte Vermögenswerte, beispielsweise durch den Handel mit Betäubungsmitteln, Schwarzarbeit, Prostitution, Cybercrime oder Erpressungstaten, können allerdings nicht direkt genutzt und angelegt werden, ohne dass die Ermittlungsbehörden oder Finanzämter Verdacht schöpfen.[2] Vielmehr bedarf es eines gesonderten Prozesses um den Vermögenswerten einen legalen Anschein zu verleihen und somit die illegale Herkunft zu kaschieren. Diese sogenannte Geldwäsche ist in Deutschland gemäß § 261 Strafgesetzbuch (StGB) unter Strafe gestellt. Bei der Terrorismusfinanzierung geht es auf der anderen Seite um die Generierung und Verteilung von Finanzmitteln für den Terrorismus. So wird gemäß § 89c StGB konkret das Sammeln, Entgegennehmen oder zu Verfügung stellen von Vermögenswerten im Wissen oder in der Absicht, dass sie zur Begehung von bestimmten terroristischen Taten verwendet werden, pönalisiert.[3] Hintergrund ist die Kappung des für die Infrastruktur von Terrororganisationen unabdingbaren kontinuierlichen Zuflusses von Finanzmitteln.[4]

Beide Delikte haben mithin gemein, dass es grundsätzlich um die strukturierte Verschleierung und verdeckte Steuerung von Geldflüssen sowie anderen Werten mit einem dahinterstehenden signifikanten gesamtgesellschaftlichen Gefährdungspotential geht. Staatliche Stellen versuchen deshalb sowohl die Geldwäsche als auch die Terrorismusfinanzierung fortlaufend zu erschweren, beispielsweise durch die zunehmende Regulierung von Bargeldtransaktionen[5] oder die Überwachung des Immobiliensektors[6]. Technologische Innovationen verändern aber nicht nur die Märkte, sondern auch die Methoden krimineller Akteure.[7] Diese nutzen zunehmend digitale Vehikel für die Geldwäsche und Terrorismusfinanzierung, insbesondere die sogenannten

[1] *Suendorf*, Geldwäsche – Eine kriminologische Untersuchung, 2001, S. V.
[2] *Weisser/Bliesener*, NZWiSt 2024, 41 (41).
[3] Hinsichtlich der Methoden vgl. *Teichmann*, NZWiSt 2025, 102ff.
[4] *Weisser*, ZIS 2013, 343 (347).
[5] *Scherrer*, Polizeipraxis 2023/2, 48 (50).
[6] Zu den Auswirkungen der Gelwäsche auf den Immobiliensektor siehe bspw. *Neuenkirch/von Auer/El-Ghazi/Hoffmann/Jansen/Klotz/Seidel/Walz*, Geldwäsche und deren Auswirkungen auf Immobilienpreise in Deutschland, Studie trigeko, 2025.
[7] FIU, Jahresbericht 2024, S. 15.

Kryptowerte.[8] Hinzu tritt der Rückgriff auf im Ausland ansässige Kryptodienstleister.[9] Kryptowerte bieten neben einer hohen Pseudonymität auch den Vorteil einer nahezu grenzenlosen, globalen Nutzungsmöglichkeit ohne Zeitverlust und Reisetätigkeit sowie eine bislang nur geringe Regulierung.[10]

Eingedenk der obigen Tatsachen stellt sich für die Ermittlungsbehörden naturgemäß die Frage, welche Ansätze für das Detektieren und Ermitteln von, mit Kryptowerten als Tatvehikel begangener, Geldwäsche und Terrorismusfinanzierung denkbar sind. Die fortschreitende Digitalisierung eröffnet dabei auch in diesem Bereich neue Wege. In Betracht kommt beispielsweise die sog. Open Source Intelligence (OSINT), also die systematische und gezielte Beschaffung von frei verfügbaren Informationen in den konventionellen Quellen und weltweiten Datennetzen unter Nutzung des gesamten Spektrums der öffentlich zugänglichen Informationskanäle in allen möglichen Sprachen.[11] Die zunehmende Bedeutung dieses Instruments spiegelt sich auch in der aktuellen Forderung der Ständigen Konferenz der Innenminister und -senatoren der Länder wider, welche die alternativen Möglichkeiten zur Bargeldzahlung (u. a. den Einsatz von Kryptowährung) strikter als bisher überwachen und die Analyse verdächtiger Transaktionen durch die Bereitstellung moderner Software weiter verbessern wollen.[12]

2 Ausgangslage

Um die Bedeutung des Themas einzuordnen und mögliche Bewältigungsstrategien in der Praxis und Forschung zu entwickeln, stellt sich zunächst die Frage, welches Ausmaß Geldwäsche und Terrorismusfinanzierung in Deutschland tatsächlich einnehmen und in welchem Umfang bei den Taten Kryptowerte als Vehikel genutzt werden. Darauf aufbauend gilt es die Frage zu beantworten, ob OSINT in diesem Kontext als ein effektives Ermittlungsinstrument einzustufen ist.

[8] https://www.handelsblatt.com/finanzen/banken-versicherungen/geldwaeschebekaempfung-verdaechtige-geschaefte-mit-kryptowaehrungen-steigen-auf-rekordhoch/100134025.html (letzter Aufruf: 01.09.25).
[9] United States Government Accountability Office, Virtual Currencies, in: Report to Congressional Requesters, 2021, S. 11); siehe auch: Mitteilung des Senats zur kleinen Anfrage der Fraktion CDU vom 06.11.24, Bremische Bürgerschaft Drs. 21/924, S. 16.
[10] *Weisser/Bliesener*, NZWiSt 2024, 41 (41).
[11] Wabnitz/Janovsky/Schmitt/*Bär*, Handbuch Wirtschafts- und Steuerstrafrecht, 6. Aufl. 2025, 30. Kap., Rn. 123a.
[12] IMK, 233. Sitzung vom 11. bis 13.06.25, Beschlüsse, TOP 36, Nr. 5.

Schätzungen zum konkreten Umfang der o. g. Straftaten variieren stark und sind mit Vorsicht zu genießen. Hinsichtlich der Geldwäsche wird teilweise von einem jährlichen Volumen von ca. 29 Mrd. € in der Bundesrepublik Deutschland ausgegangen.[13] Andere beziffern es sogar auf ca. 100 Mrd. €.[14] Laut einer Dunkelfeld-Studie aus dem Jahr 2016 ist von einem Betrag i.H.v. 20 bis 30 Mrd. € im Nicht-Finanzsektor und von einem Gesamtgeldwäschevolumen von über 50 Mrd. € bis eher um die 100 Mrd. € auszugehen.[15] Wie sich diese Beträge in den letzten Jahren entwickelt haben könnten, wurde bisher nicht untersucht. Auch heute noch wird allerdings von einem großen Dunkelfeld ausgegangen.[16] Teilweise sehen sich die Ermittlungsbehörden nicht einmal in der Lage, dessen Ausmaß realistisch zu beziffern oder eine fundierte Schätzung vorzunehmen.[17] Hinsichtlich der Frage wie viele Gelder in Deutschland jährlich in die Terrorismusfinanzierung fließen, gibt es auf der anderen Seite nicht einmal belastbare Schätzungen. Als sichere Erkenntnisse liegen ausschließlich die den Ermittlungsbehörden bekannt gewordenen Straftaten vor.[18]

Noch schwieriger gestaltet sich der Überblick über den Einsatz von Kryptowerten als Tatvehikel bei den oben genannten Straftaten. Es ist davon auszugehen, dass neue digitale Zahlungsmittel und technische Weiterentwicklungen immer neue Tatbegehungsweisen ermöglichen.[19] Eine offen zugängliche Datenlage besteht nicht. In der Polizeilichen Kriminalstatistik wird der Einsatz von Kryptowerten zur Tatbegehung nicht ausgewiesen.[20] Es wird allerdings aufgrund der bereits beschriebenen Begünstigungsfaktoren teilweise von einem erheblichen Umfang ausgegangen und angenommen, dass das Volumen illegaler Krypto-Transaktionen bereits im Jahr 2022 den bisherigen Höchstwert von 20,6 Mrd. US-Dollar weltweit erreicht habe.[21] In welchem

[13] University of Utrecht, Project ECOLEF, The Economic and Legal Effectiveness of Anti-Money Laundering and Combating Terrorist Financing Policy, Final Report, 2013, S. 39.
[14] *Bussmann*, Geldwäscheprävention am Markt, 2018, S. 87ff.; ebenso genannt in: BMF, Erste Nationale Risikoanalyse 2018/2019, S. 25.
[15] *Bussmann*, Dunkelfeldstudie über den Umfang der Geldwäsche in Deutschland und über die Geldwäscherisiken in einzelnen Wirtschaftssektoren, 2016, S. 16.
[16] Mitteilung des Senats zur kleinen Anfrage der Fraktion CDU vom 06.11.24, Bremische Bürgerschaft Drs. 21/924, S. 12.
[17] Mitteilung des Senats zur Schriftlichen Kleinen Anfrage vom 25.06.2024, Hamburgische Bürgerschaft Drs. 22/15380, S. 28, 32.
[18] Vgl. dazu unter 5.1.
[19] Mitteilung des Senats zur kleinen Anfrage der Fraktion CDU vom 06.11.24, Bremische Bürgerschaft Drs. 21/924, S. 12.
[20] Die statistische Erfassung von Tatvehikeln ist der PKS dabei nicht fremd, wie man an der Erfassung von Messern als Tatvehikel bei Gewaltdelikten erkennen kann.
[21] Chainalysis, The 2023 Crypto Crime Report, S. 5.

Umfang in Deutschland Kryptowerte bei der Geldwäsche oder Terrorismusfinanzierung tatsächlich genutzt werden, ist bisher nicht abschließend bekannt. Eine belastbare Dunkelfeldforschung fehlt diesbezüglich.

In der ersten nationalen Risikoanalyse stellte das Bundesministerium der Finanzen im Jahr 2019 zudem noch fest, dass keine großumfänglichen Geldwäscheaktivitäten mit Kryptowerten erkennbar gewesen seien, obwohl die erheblichen Begünstigungsfaktoren gleichwohl hervorgehoben wurden.[22] Doch worauf diese Bewertung fußte ist nicht abschließend erkennbar. Gleichzeitig hat das Bundesministerium der Finanzen das Potential von Kryptowerten aber auch hervorgehoben und die Stärkung der Analyse, Aufsicht und Strafverfolgung bei den spezifischen Risiken durch neue Technologien als eine der Grundstrategien der zukünftigen Bekämpfung von Geldwäsche und Terrorismusfinanzierung ausgerufen.[23]

Die Bedeutung scheint seither weiter zuzunehmen. So hat nunmehr auch die Financial Intelligence Unit (FIU)[24] des Zolls in ihrem Jahresbericht 2024 die Geldwäsche unter Verwendung von Kryptowerten als neuen Schwerpunkt klassifiziert.[25] Insgesamt stieg zudem der Anteil der Verdachtsmeldungen mit Kryptowertbezug am Gesamtmeldeaufkommen auf ein Rekordniveau.[26] Ferner legt zukünftig ebenfalls die neu gegründete Anti-Geldwäschebehörde der Europäischen Union AMLA (Anti-Money Laundering Authority)[27] einen Fokus auf neue Technologien, wie Kryptowerte und Künstliche Intelligenz.[28]

Betrachtet man die bekannten Verfahren in Bezug auf die Organisierte Kriminalität (OK) zeichnet sich ebenfalls ein eindeutigeres Bild. So wurden in den geführten OK-Verfahren im Jahr 2022 Investitionen zur Geldwäsche in Kryptowerte i.H.v. ca. 451,4 Mio. € bei

[22] BMF, Erste nationale Risikoanalyse 2018/2019, S. 115.
[23] BMF, Strategie gegen Geldwäsche und Terrorismusfinanzierung, Sicherheit 2019, S. 15.
[24] Die FIU, als Zentralstelle für Finanztransaktionsuntersuchungen, ist eine eigenständige Behörde innerhalb der Generalzolldirektion. Ihre Hauptaufgabe besteht in der Entgegennahme, Analyse und Weiterleitung von Verdachtsmeldungen nach dem Geldwäschegesetz (GwG).
[25] FIU, Jahresbericht 2024, S. 15ff.
[26] FIU, Jahresbericht 2024, S. 20; https://www.handelsblatt.com/finanzen/banken-versicherungen/geldwaeschebekaempfung-verdaechtige-geschaefte-mit-kryptowaehrungen-steigen-auf-rekordhoch/100134025.html (letzter Aufruf: 01.09.25).
[27] The Authority for Anti-Money Laundering and Countering the Financing of Terrorism.
[28] https://www.tagesschau.de/wirtschaft/finanzen/geldwaesche-amla-szego-100.html (letzter Aufruf: 01.09.25).

einem Gesamtvolumen von ca. 1 Mrd. € der kriminellen Erträge verzeichnet.[29] Dies bedeutet, dass fast die Hälfte der gewaschenen Gelder in diesem Jahr in Kryptowerte investiert wurden.[30] Wie schwankend diese Werte allerdings sind, kann schon aus den Zahlen zum Jahr 2023 erkannt werden, wo Kryptowerte nur in einem Umfang von ca. 1,4 Mio. € bei einem Gesamtvolumen von lediglich 166 Mio. € festgestellt werden konnten.[31] Eindeutige Aussagen sind mithin nicht ablesbar. Zumindest deuten die Werte auf ein großes Potential. Nur auf Grundlage eines belastbaren Zahlenmaterials können allerdings Problemfelder erkannt und ggf. für die Zukunft Bewältigungsstrategien erarbeitet werden.

Auch im Bereich der Terrorismusfinanzierung werden Kryptowerte genutzt und spielen teilweise eine entscheidende Rolle für die Aufrechterhaltung von terroristischen Organisationen.[32] So nimmt die Nutzung von Kryptowerten durch Terrororganisationen insgesamt zu, auch in Kombination mit anderen Methoden. Das genaue Ausmaß des Missbrauchs von Kryptowerten zur Terrorismusfinanzierung ist gleichwohl weiterhin schwer zu bestimmen.[33] Die Anzahl der bekannten Fälle von Terrorfinanzierung durch Kryptowerte ist zwar im Vergleich zur Geldwäsche noch begrenzt, es wird aber angenommen, dass sie mit der zunehmenden Akzeptanz der Technik weiter anwächst.[34] Ein Indikator hierfür ist auch der kontinuierliche und signifikante Anstieg der Verdachtsmeldungen in dem Bereich Terrorismusfinanzierung, Staatsschutz und Sanktionen an die FIU[35], wobei ein solcher Anstieg auch mit vielen weiteren Faktoren in Verbindung steht. Konkrete Zahlen oder belastbare Dunkelfeldforschungen gibt es aber nicht.

Neuartige Tatvehikel verlangen neue Ermittlungsinstrumente, damit die Ermittlungsbehörden nicht den Anschluss verlieren. Regelmäßig wird bspw. die Open Source Intelligence angeführt, deren Einsatz auch hinsichtlich der Geldwäsche und Terrorismusfinanzierung ansteigt. Als Beispiel sei nur die strategische Auswertung durch

[29] BKA, Bundeslagebild Organisierte Kriminalität, 2022, S. 2 und 19.
[30] BT-Drs. 20/9730, S. 2.
[31] BKA, Bundeslagebild Organisierte Kriminalität, 2022, S. 2 und 15.
[32] BT-Drs. 20/9730, S. 2.
[33] FATF Report, Comprehensive Update on Terrorist Financing Risks, 2025, S. 66.
[34] https://background.tagesspiegel.de/it-und-cybersicherheit/briefing/terrorfinanzierung-mit-kryptowaehrungen#:~:text=Background%20background,gelang%20israelischen%20Beh%C3%B6rden%20die (letzter Aufruf: 01.09.25).
[35] FIU, Jahresbericht 2024, S. 51.

die FIU genannt.[36] Ob und inwiefern dieses Instrument allerdings in der Praxis zur Ermittlung der Delikte (insbesondere dann, wenn Kryptowerte als Tatvehikel eingesetzt werden) tatsächlich flächendeckend genutzt und welche Bedeutung ihm von der Praxis überhaupt zugesprochen wird, ist derzeit jedenfalls noch nicht erforscht. Belastbare Erhebungen diesbezüglich liegen nicht vor. Auch die Fragen, ob in der Praxis bereits spezielle Anwendungen oder konkrete Schulungen existieren, werden nicht abschließend beantwortet.

3 Das Forschungsprojekt G.E.K.O.

Vor diesen Hintergrund führte die Forschungsgruppe I (Money Laundering and White-Collar Crime) des EU-geförderten Jean Monnet Centre of Excellence Crime Investigations and Criminal Justice (CCICJ) in der Hochschule für Öffentliche Verwaltung Bremen (HfÖV) im Jahr 2025 ein neues Forschungsprojekt mit dem Namen G.E.K.O. (Geldwäsche- und Terrorismusfinanzierung: Ermittlungen bei der Nutzung von Kryptowerte durch OSINT) durch. Ziel war es, bestehende Datenlücken zu schließen, das Ermittlungsinstrument OSINT in dem hiesigen Kontext zu bewerten und Verbesserungsmöglichkeiten aufzuzeigen.

Im Rahmen des Forschungsprojekts sollten die aufgeworfenen Fragestellungen nunmehr durch Zahlen und Einschätzungen aus der Praxis unterlegt werden. Dazu wurde zunächst erhoben, welche Anzahl an Verfahren wegen Geldwäsche und Terrorismusfinanzierung in den Jahren 2023 und 2024 jeweils bei den befragten Behörden geführt wurden. Weiterhin wurde abgefragt, in wie vielen dieser Verfahren Kryptowerte durch die Tatpersonen verwendet wurden. Sofern keine statistische Erfassung erfolgte, wurden die Behörden um eine geschätzte Häufigkeit sowie eine Einschätzung zum Ausmaß des Dunkelfeldes gebeten. Ein weiterer Schwerpunkt lag auf der Frage, ob bei den entsprechenden Ermittlungen OSINT zum Einsatz kam – insbesondere in Fällen mit Bezug zu Kryptowerten. Darüber hinaus sollten die Befragten die Bedeutung dieses Ermittlungsinstruments einschätzen. Zusätzlich war eine Bewertung auf einer Skala von 0 bis 5 vorzunehmen (0 = nicht wichtig, 5 = sehr wichtig). Ergänzend wurde erhoben, auf welcher Rechtsgrundlage OSINT durch die jeweilige

[36] FIU, Jahresbericht 2024, S. 37.

Behörde eingesetzt wird. Gefragt wurde zudem, ob spezielle kommerzielle Anwendungen oder behördeneigene Systeme genutzt werden, ob Schulungen zu konkreten OSINT-Techniken existieren und ob ein Änderungsbedarf im Hinblick auf die Nutzung von OSINT gesehen wird.

Hierfür wurden solche Ermittlungsbehörden der Polizei und des Zolls um Mitwirkung gebeten, von denen auszugehen ist, dass dort besonders komplexe Verfahren der Geldwäsche und/oder Terrorismusfinanzierung geführt werden und sich dabei eine breite Expertise, auch bzgl. der Ermittlungsinstrumente in diesen Bereichen aufgebaut hat.[37] Die Anfragen erstreckten sich deshalb auf das Bundeskriminalamt, das Zollkriminalamt samt dem Zollfahndungsdienst und alle Landeskriminalämter. Erfreulicherweise haben alle angefragten Behörden zugeliefert. Dem Bundeskriminalamt, dem Zollkriminalamt (hat auch für den Zollfahndungsdienst geantwortet) sowie den Landeskriminalämtern Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt, Schleswig-Holstein und Thüringen und der Landespolizeidirektion Saarland gebührt an dieser Stelle großer Dank für ihre umfangreiche Unterstützung des Forschungsprojekts. Ohne diese wäre das Projekt nicht möglich gewesen.

4 Grundlagen und Begrifflichkeiten

Für das grundlegende Verständnis der aufgeworfenen Problemstellungen bedarf es zunächst einer Auseinandersetzung mit den aufgeworfenen Begrifflichkeiten. Aufgrund der Komplexität der jeweiligen Themenbereiche kann an dieser Stelle nur ein kurzer Überblick erfolgen.

4.1 Kryptowerte

Von Kryptowerten wird gesprochen, wenn digitale Werteinheiten auf einer sogenannten Blockchain abgebildet werden.[38] Eine Variante davon stellen Kryptowährungen dar. Bei

[37] Aufgrund der Tatsache, dass sich das Projekt auf die konkrete Ermittlungsarbeit mit OSINT bezieht, erfolgte keine Abfrage bei den Staatsanwaltschaften.
[38] *Bashir*, Mastering Blockchain, 4. Aufl. 2023, S. 469.

diesen handelt es sich um dezentrale Zahlungssysteme, bei deren Abwicklung kryptographische Verfahren zum Einsatz kommen.[39] Der Ursprung dieser Währungen liegt allerdings dabei nicht bei einem Staat oder einer Zentralbank, sondern resultiert aus der Existenz von sogenannten Peer-to-Peer-Netzwerken.[40] Aufgrund der zugrunde liegenden Struktur dieser Netzwerke ist für eine Kryptowährung kein Intermediär erforderlich, d.h. keine zentrale Stelle, welcher die Steuerung und Verwaltung der Währung obliegt.[41] Zur Dokumentation von Zahlungen in diesen Währungen wird stattdessen auf die bereits erwähnte Blockchain-Technologie zurückgegriffen. Hierbei übernimmt die Blockchain die Funktion eines „zentralen Kassenbuchs“ (engl.: Ledger).[42] Im Zuge der Abwicklung von Transaktionen wird diese mit den entsprechenden Transaktionsdaten gefüllt. Durch den Einsatz von kryptografischen Verfahren wird sichergestellt, dass dieses „Kassenbuch“ der entsprechenden Währungen vor Missbrauch und Manipulation geschützt bleibt.[43] Die größte Marktkapitalisierung bei solchen Kryptowährungen weist derzeit die Kryptowährung Bitcoin auf.

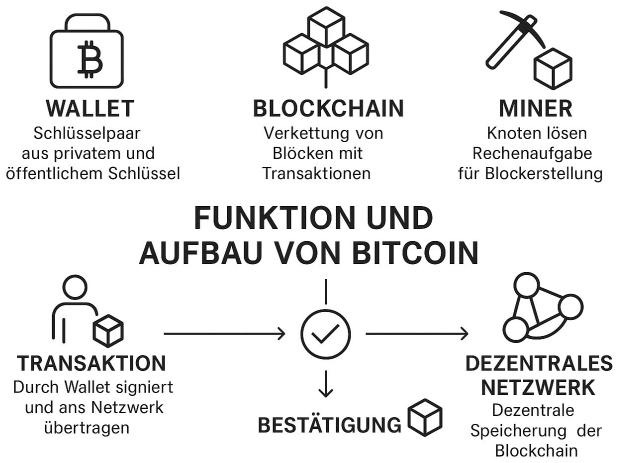

Abb. 1: Schematische Darstellung der Funktion und des Aufbaus von Bitcoin

Die den Kryptowährungen zugrunde liegenden Peer-to-Peer-Netzwerke bestehen aus miteinander verbundenen Rechnern, welche gleichberechtigt und losgelöst von einer

[39] *Böhm*, Der strafrechtliche Schutz der Inhaberschaft von Kryptowährungseinheiten, 2024, S. 38.
[40] *Berentsen/Schär*, Bitcoin, Blockchain und Kryptoassets, 2017, S. 53.
[41] *Koenen*, Auswertung von Blockchain-Inhalten zu Strafverfolgungszwecken, 2023, S. 33.
[42] *Böhm*, Der strafrechtliche Schutz der Inhaberschaft von Kryptowährungseinheiten, 2024, S. 46.
[43] *Bashir*, Mastering Blockchain, 4. Aufl. 2023, S. 11.

zentralen Instanz direkt miteinander kommunizieren.[44] Weil in einem solchen Netzwerk alle teilnehmenden Rechner jeweils eine Kopie der zugrunde liegenden Blockchain vorhalten, wird dies als Distributed-Ledger-Technologie bezeichnet.[45]

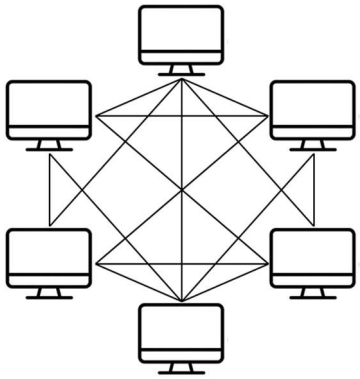

Abb. 2: Schematische Darstellung eines Peer-to-Peer-Netzwerkes

Die Blockchain selbst wiederum kann als kontinuierlich wachsende Datenbank gesehen werden, in welcher die Aktualisierung von Informationen zur Inhaberschaft von Kryptowährungseinheiten erfolgt.[46] Erst die Möglichkeit zur Änderung dieser Inhaberschaft macht Kryptowerte zu einem dezentralen Zahlungssystem: Es gelangt nicht etwa Geld von einem Sender zu einem Empfänger, sondern die Inhaberschaft über Kryptowährungseinheiten, welche einen entsprechenden Tauschwert aufweist und dementsprechend handelbar wird.[47]

Die jeweiligen Aktualisierungen werden im zeitlichen Verlauf unendlich fortgeschrieben und mit Hilfe spezieller Verschlüsselungstechnologien gegen nachträgliche Änderung abgesichert.[48] Sofern eine Veränderung der Inhaberschaft von Kryptowährungseinheiten beabsichtigt wird, ist das zugrunde liegenden Netzwerk darüber zu informieren, wodurch in der Folge die Kopien der Blockchain auf allen teilnehmenden Rechnern entsprechend aktualisiert werden. Dieser Vorgang wird mit Hilfe von verschlüsselten Transaktionsnachrichten angestoßen.[49] Ein „zahlungswilliger“ Netzwerkteilnehmer versendet eine solche Nachricht und signiert bzw. verschlüsselt sie dafür mit Hilfe eines

[44] *Antonopoulos*, Bitcoin & Blockchain, 2. Aufl. 2018, S. 173.
[45] *Bashir*, Mastering Blockchain, 4. Aufl. 2023, S. 23f.
[46] *Bashir*, Mastering Blockchain, 4. Aufl. 2023, S. 11.
[47] *Furneaux*, Investigating Cryptocurrencies, 2018, S. 79.
[48] *Koenen*, Auswertung von Blockchain-Inhalten zu Strafverfolgungszwecken, 2023, S. 50.
[49] *Berentsen/Schär*, Bitcoin, Blockchain und Kryptoassets, 2017, S. 169.

nur ihm bekannten privaten Schlüssels. Die anderen Netzwerkteilnehmer wiederum entschlüsseln diese Nachricht mit Hilfe seines für alle Netzwerkteilnehmer einsehbaren öffentlichen Schlüssels.[50] Für die Erzeugung solcher Schlüsselpaare sowie der Handhabung von Kryptowährungseinheiten ist eine Wallet-Software erforderlich.[51] Eine Wallet wiederum lässt sich grob mit einem Bankkonto vergleichen, wobei im Falle der Blockchain-Technologie eine Verbindung ausschließlich zwischen dem privaten Schlüssel und den Kryptowährungseinheiten besteht, nicht jedoch zwischen einer natürlichen Personen und dem Schlüsselpaar.[52] Auch weist eine Wallet kein Guthaben im engeren Sinne, sondern eine Aggregation zugewiesener Inhaberschafen von Kryptowerteinheiten auf. [53] Kryptowährungen lassen sich über Krypto-Börsen oder spezielle Handelsplattformen handeln. Hierdurch erhalten sie auch final ihren Charakter als Zahlungsmittel bzw. ihren monetären Wert. [54]

Eine weitere Variante von Kryptowerten stellen „Non-Fungible Token“ (NFT) dar.[55] Diese Werteinheiten weisen wiederum eine gewisse Individualität auf und sind im Gegensatz zu Kryptowährungen nicht beliebig gegen andere Werteinheiten austauschbar. Mit NFTs lassen sich beispielsweise digitale Eigentumsrechte auf einer Blockchain abbilden. Die derzeitigen Hauptanwendungsfälle sind sog. „Collectibles“, also digitale Sammlerstücke (bspw. in der Gaming-Industrie zum In-game-Kauf von Zubehör etc.) und insbesondere der digitale Kunsthandel.[56] Exemplarisch sei hier das NFT-Kunstwerk des Künstlers „Beeple“ erwähnt, welches im Jahr 2021 für 57,9 Mio. EUR versteigert wurde.[57]

4.2 Geldwäsche und Terrorismusfinanzierung mit Kryptowerten

Als Geldwäsche wird ein Prozess bezeichnet, bei welchem Gelder aus illegaler Herkunft in den legalen Wirtschaftskreislauf eingeschleust und ihrer Herkunft ein legaler Anschein

[50] *Weisser/Bliesener*, wistra, 2025, 133 (135).
[51] *Antonopoulos*, Bitcoin & Blockchain, 2. Aufl. 2018, S. 57.
[52] *Kipker*, Cybersecurity, 2. Aufl. 2023, S. 906.
[53] *Antonopoulos*, Bitcoin & Blockchain, 2. Aufl. 2018, S. 121.
[54] *Böhm*, Der strafrechtliche Schutz der Inhaberschaft von Kryptowährungseinheiten, 2024, S. 45.
[55] Ausführlich zu Geldwäsche und NFTs: *Weisser/Bliesener* NZWiSt 2024, 41 (43).
[56] BaFinJournal vom 8.3.2023, vgl. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2023/fa_bj_2303_NFT.html (letzter Aufruf: 01.09.25).
[57] *Rapp/Bongers,* DStR 2021, 2178 (2178).

gegeben werden soll. Der Prozess lässt sich klassisch grob in drei Phasen einteilen: Platzierung, Verschleierung und Integration.[58]

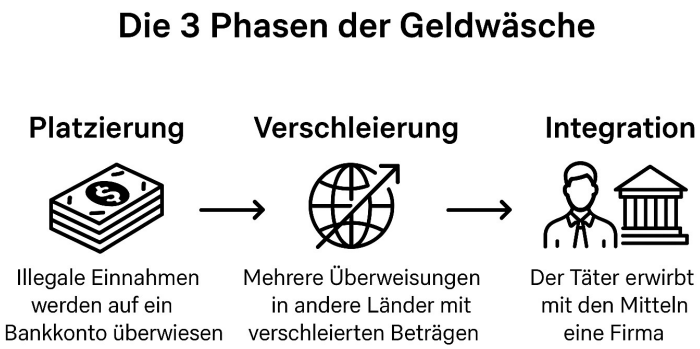

Abb. 3: Beispielhafte Darstellung der Phasen der Geldwäsche

Bei der Bekämpfung der Terrorismusfinanzierung geht es wiederum um die monetäre Austrocknung von terroristischen Organisationen, wobei, im Gegensatz zur Geldwäsche, das eigentliche deliktische Handeln in der Regel in der Zukunft liegt, was zu erhöhten Nachweisproblemen führt.[59]

Abb. 4: Beispielhafte Darstellung der Terrorismusfinanzierung

Kryptowerte als Tatvehikel bieten wiederum vielerlei Möglichkeiten für die Begehung von Geldwäsche- und Terrorismusfinanzierungstaten. Im Falle der Kryptowährungen wären dies beispielsweise Transaktionen, die sich über den klassischen Zahlungsverkehr im

[58] *Spreizer*, VuR 2006, 7 (7).
[59] *Teichmann*, NZWiSt 2025, 102 (102).

Bankwesen nicht ohne Weiteres umsetzen ließen.[60] NFTs wiederum können als Wertespeicher oder auch Spekulationsobjekt genutzt[61] und darüber hinaus im Schutze der Pseudonymität gehandelt werden.[62] Die Kryptowerte werden im Rahmen der Terrorismusfinanzierung auf ganz unterschiedliche Weise genutzt.

Abb. 5: Beispielhafte Darstellung der Nutzungsmöglichkeiten von Kryptowerten[63]

Ein Großteil der Terrorismusfinanzierung mit Kryptowerten erfolgt durch Einzelpersonen, welche um Spenden werben (bspw. im Rahmen von Crowdfunding-Kampagnen oder durch die direkte Veröffentlichung von Wallet-Adressen über Propagandakanäle).[64]

4.2.1 Rechtliche Grundlagen

Der Straftatbestand der Geldwäsche gemäß § 261 StGB stellt den Umgang mit illegalem Vermögen unter Strafe und ist stets in einer Zusammenschau mit dem Geldwäschegesetz und den Einziehungsvorschriften zu sehen.[65] Es handelt sich um ein Anschlussdelikt. Die Gegenstände müssen mithin aus einer anderen rechtswidrigen Tat

[60] *Furneaux*, There's No Such Thing as Crypto Crime, 2025, S. 4.
[61] Elliptic, Preventing Financial Crime in Cryptoassets, 2023, S. 91.
[62] *Furneaux*, There's No Such Thing as Crypto Crime, 2025, S. 46f.
[63] Angelehnt an: FATF Report, Comprehensive Update on Terrorist Financing Risks, 2025, S. 66.
[64] FATF Report, Comprehensive Update on Terrorist Financing Risks, 2025, S. 67.
[65] MüKo/*Neuheuser,* StGB, 4. Aufl. 2021, § 261 Rn. 1.

i.S.v. § 11 Abs. 1 Nr. 5 StGB stammen.[66] Tatobjekt ist jedes Rechtsobjekt mit Vermögenswert[67], mithin also auch Kryptowerte.[68] Seit 2021 kommen zudem alle rechtswidrigen Taten als Vortaten in Betracht (sog. All-Crimes-Ansatz).[69] Dabei muss sich die Vortat nach h.M. lediglich aus den festgestellten Umständen in groben Zügen ergeben.[70]

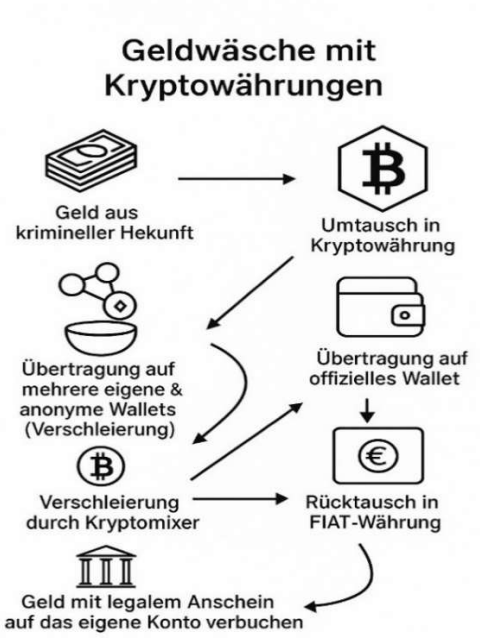

Abb .6: Beispielhafte Darstellung der Geldwäsche mit Kryptowährungen

Die strafbewährten Tathandlungen werden in § 261 Abs. 1 und Abs. 2 StGB enumerativ aufgeführt. Es wird pönalisiert, wer einen der inkriminierten Gegenstände verbirgt, ihn in der Absicht, das Auffinden, die Einziehung oder die Ermittlung der Herkunft zu vereiteln, umtauscht, überträgt oder verbringt, ihn sich oder einem Dritten verschafft oder ihn verwahrt oder für sich oder einen Dritten verwendet, wenn er die Herkunft des Gegenstandes zu dem Zeitpunkt der Erlangung gekannt hat oder Tatsachen, die für das Auffinden, die Einziehung oder die Ermittlung der Herkunft eines Gegenstands von Bedeutung sein können, verheimlicht oder verschleiert.[71] Hervorzuheben ist, dass die Geldwäsche gemäß § 261 Abs. 6 StGB auch leichtfertig begangen werden kann. Dies

[66] *Reisch,* JuS 2023, 207 (208).
[67] BT-Drs. 12/989, S. 27.
[68] BeckOK/*Ruhmannseder*, StGB, 62. Ed. Stand 01.08.2024, § 261 Rn. 9.
[69] Kindhäuser/Neumann/Peffgen/Saliger/*Altenhain,* StGB, 6. Aufl. 2023, § 261, Rn. 4.
[70] BT-Drs. 19/24180, S. 30; BGH, NStZ 2016, 538 (538).
[71] Bzgl. der Definitionen der jeweiligen Tatbestandsmerkmale siehe: Dölling/Duttge/König/Rössner/*Hartmann,* Gesamtes Strafrecht, 5. Aufl. 2022, § 261, Rn. 35 ff.

ist der Fall, wenn sich aufdrängt, dass der Gegenstand aus einer rechtswidrigen Tat stammt und der Täter dies aus grober Unachtsamkeit oder gar besonderer Gleichgültigkeit außer Acht lässt.[72]

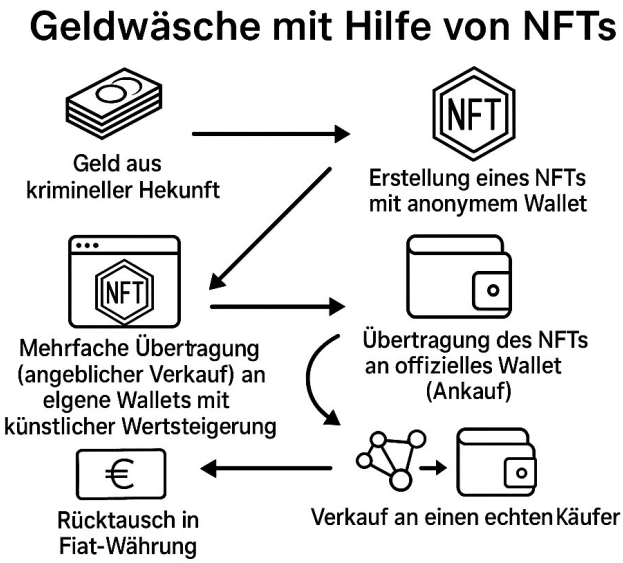

Abb. 7: Beispielhafte Darstellung der Geldwäsche mit Hilfe von NFTs

Die Terrorismusfinanzierung gem. § 89c StGB hat demgegenüber eine andere Stoßrichtung.[73] Hierbei wird das Sammeln, Entgegennehmen oder zu Verfügung stellen von Vermögenswerten im Wissen oder in der Absicht verstanden, dass sie zur Begehung von bestimmten in § 89c Abs. 1 S. 1 Nr. 1 bis 8 StGB (wie z. B. Mord, Verbrechen gegen die Menschlichkeit oder Geiselnahme) aufgeführten terroristischen Taten verwendet werden. Die Strafnorm erfordert auf subjektiver Seite zumindest das Wissen oder sogar die Absicht, dass gesammelte Vermögenswerte von der anderen Person zur Begehung einer der aufgeführten Straftaten, verwendet werden sollen (ein Eventualvorsatz reicht dabei nicht).[74]

[72] BGH NStZ-RR 2019, 145 (146).
[73] *Weisser/Bliesener*, wistra 2025, 133 (138).
[74] BeckOK StGB/*Heintschel-Heinegg*, 65. Ed. Stand 01.05.2025, § 89c, Rn. 12.

4.2.2 Begünstigungsfaktoren

Die bei der Verwendung von Kryptowerten ablaufenden Mechanismen unterscheiden sich vielfach nicht von den bisher bekannten Mustern. Die Zahlungsströme lassen sich jedoch deutlich schwieriger nachvollziehen, da die Transaktionen technisch komplexer gestaltet sind und sich die jeweils wirtschaftlich Berechtigten nicht ohne Weiteres identifizieren lassen, da sie in verborgenen Strukturen agieren.[75] Kryptowerte weisen für die Straftatbestände der Geldwäsche sowie Terrorismusfinanzierung mithin besondere Begünstigungsfaktoren auf. So lässt sich bei Kryptowährungen die Anonymität von Bargeld mit den Vorteilen digitaler Datenübertragung kombinieren.[76] Hieraus resultiert eine für die Täter vorteilhafte Pseudonymität. Zwar sind deren Transaktionen dauerhaft in der Blockchain gespeichert, d.h. einsehbar, können jedoch nicht ohne Weiteres einer konkreten Person zugeordnet werden.[77] Selbst wenn an dieser Stelle noch keine gänzliche Anonymität vorliegt, kann sich dieser durch weitere Maßnahmen inzwischen (bspw. durch die Verwendung von Coin-Mixing-Tools) angenähert werden.[78]

Weiterhin begünstigend wirkt die grenzenlose und globale Nutzungsmöglichkeit ohne Zeitverlust und Reisetätigkeit.[79] So ist der gesamte Handel, wie oben beschrieben, dezentral organisiert und nicht von einem (Finanz-)Intermediär abhängig.[80] Die Möglichkeit von Peer-to-Peer-Verkäufen ohne Regulierung verringert dabei das Risiko der Entdeckung.[81] Zudem werden häufig Länder mit schwacher geldwäscherechtlicher Regulierung[82] und eingeschränkten Rechtshilfebeziehungen mit der Bundesrepublik Deutschland genutzt . Diese Faktoren erschweren den Zugriff und die Entdeckung durch die Ermittlungsbehörden.[83]

[75] FIU, Jahresbericht 2024, S. 15.
[76] *Foley/Karlsen/Putniņš*, Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies, 2019, 1798 (1800).
[77] *Maume/Haffke/Fromberger*, CCZ 2019, 149 (151).
[78] *Ikemeyer/Krimphove,* CB 2022, 432 (435).
[79] *Scherrer,* Polizeipraxis 2023/2, 48 (50).
[80] *Valerius*, RDi 2023, 510 (511).
[81] *Weisser/Bliesener*, NZWiSt 2024, 41 (44).
[82] *Biberacher,* Kryptotoken und Geldwäsche, 2023, S. 177.
[83] *Weisser,* FS A. Hartmann, 2024, S. 315.

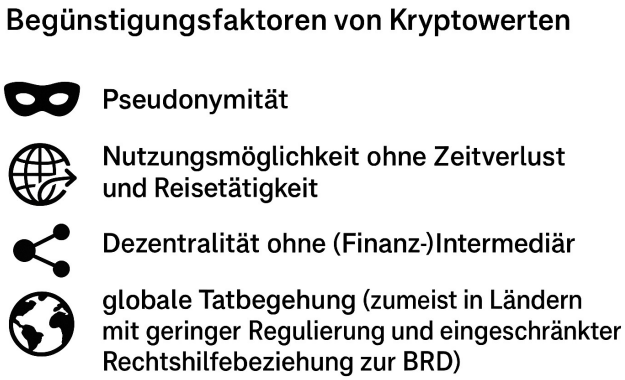

Abb. 8: Schematische Darstellung der Begünstigungsfaktoren von Kryptowerten

Bei NFTs kommen noch weitere Faktoren hinzu. So besteht gerade auf dem Kunstmarkt eine hohe Preisvolatilität. Bei künstlich verknappten Preisen der digitalen Güter lassen sich keine Referenzwerte gegenüberstellen, weshalb Anomalien bei den Marktpreisen nicht sofort ins Auge stechen und hohe Versteigerungserlöse mühelos gerechtfertigt werden können.[84]

4.3 OSINT

Weiterhin gilt es, einen grundlegenden Überblick über die Open Source Intelligence (OSINT) samt deren verfassungs- und strafprozessualen Rahmens sowie deren Potenzial bei der Ermittlung von Geldwäsche- und/oder Terrorismusfinanzierungstaten im Zusammenhang mit Kryptowährungen zu gewähren.

4.3.1 Definition

Der ursprünglich aus der US-nachrichtendienstlichen Arbeit stammende Begriff der Open Source Intelligence (OSINT) umfasst all die Maßnahmen, mit denen ggf. unter Einsatz spezieller Suchwerkzeuge gezielt und systematisch die Beschaffung von frei verfügbaren Informationen in den weltweiten Datennetzen unter Nutzung des gesamten Spektrums der öffentlich zugänglichen Informationskanäle ermöglicht wird und dadurch eine Vielzahl weiterer Informationen und Ermittlungsansätze gewonnen werden

[84] *Weisser/Bliesener*, NZWiSt 2024, 41 (45).

können.[85] Diese Methode hat sich in den letzten Jahren zu einem wichtigen Werkzeug für Strafverfolgungsbehörden entwickelt, insbesondere bei Delikten mit internationaler Dimension und komplexen Verschleierungsmechanismen wie der Geldwäsche.[86]

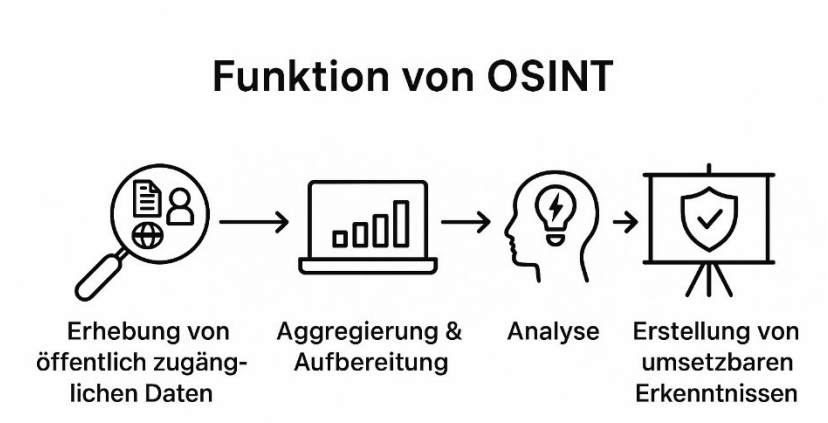

Abb. 9: Schematische Darstellung der Funktionsweise von OSINT

Gleichwohl wirft der Einsatz von OSINT im deutschen Strafverfahren zentrale Rechtsfragen auf, etwa inwieweit diese Informationen durch Ermittlungsbehörden ausgewertet werden dürfen, welche Grenzen in verfassungs- und strafprozessrechtlicher Hinsicht zu beachten sind, aber auch welche besonderen Herausforderungen und Potenziale des OSINT-Einsatzes im Rahmen der Geldwäsche und der Terrorismusfinanzierung bestehen.

Die entsprechenden OSINT-Aktivitäten sind dabei keineswegs nur Ermittlungsbehörden oder Nachrichtendiensten vorbehalten. Sie haben sich darüber hinaus auch längst zu einem integralen Bestandteil des geschäftlichen Verkehrs entwickelt, um beispielsweise Wettbewerbsvorteile erzielen zu können.[87]

4.3.2 Verfassungs- und strafprozessrechtlicher Rahmen

Zunächst ist das bloße Sammeln von Informationen aus frei zugänglichen Quellen verfassungsrechtlich grundsätzlich noch kein Eingriff in das informationelle

[85] Erstmalige *Definition aus Sec. 931 lit a) No. 1 des National Defense Authorization Act For Fiscal Year 2006*, siehe aber auch *Ludewig/Epple*, Kriminalistik 2020, 457 (457); *Bazzel*, Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 9. Aufl. 2022; vgl. ferner das Urteil des KG Berlin im Verfahren „Tiergartenmord“ KG Berlin, Urt. v. 15.12.2021 – 2 StE 2/20.
[86] *Seum/Rückert*, KripoZ 2024, 192 (231).
[87] *Hassan/Hijazi*, Open Source Intelligence Methods and Tools, 2018, S. 342.

Selbstbestimmungsrecht.[88] So lässt sich eine, die jeweiligen Grundrechte beeinträchtigende Zwangseinwirkung bei solchen Ermittlungshandlungen nicht feststellen. Dies gilt vor allem deshalb, weil die jeweiligen Betroffenen sich durch das freie Angebot von Informationen selbst mit dem Zugriff auf eigene Daten durch beliebige Dritte einverstanden erklärt haben, indem sie hierzu freien Zugang eröffnen und die jeweiligen Informationen zum Abruf etwa über die weltweiten Datennetze oder auch sonstigen Medien bereithalten. Dies ist bei punktuellen, anlassbezogenen Ermittlungen regelmäßig unproblematisch. Gerade der mit dem Surfen in den Datennetzen verbundene Zugriff auf allgemein zugängliche Informationsquellen, etwa durch das Einwählen in einen offenen Server, das Kontrollieren der Inhalte einer Newsgroup oder eines sonstigen Internet-Angebotes, ist deshalb ohne spezielle Befugnisnorm zulässig.[89] Über Art. 32a der Cybercrime-Konvention des Europarats ist ein Zugriff auf solche frei zugänglichen Daten sogar grenzüberschreitend möglich.

Aber auch die Auswertung frei zugänglicher Daten kann unter Umständen einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) darstellen. Dies gilt insbesondere dann, wenn Informationen systematisch zusammengeführt und personenbezogen ausgewertet werden.[90] Das Bundesverfassungsgericht betont in ständiger Rechtsprechung, dass der Gesetzgeber für derartige Eingriffe eine hinreichend bestimmte Rechtsgrundlage schaffen muss (Gesetzesvorbehalt).[91]

Die Strafprozessordnung enthält bislang keine eigenständige Ermächtigungsnorm für OSINT-Ermittlungen. Eine Nutzung derartiger Techniken fällt schon begrifflich nicht unter §§ 100a ff. StPO, da es sich um offen zugängliche Quellen handelt. Die Norm zur Regulierung der Rasterfahndung § 98a StPO wurde nur für die Erhebung nichtöffentlicher Daten geschaffen, was einem völlig anderen Ermittlungsansatz entspricht. Die Vorschrift des § 98c StPO, der den justiziellen maschinellen Datenabgleich umfasst, regelt auf der anderen Seite den Abgleich von Daten, die bereits erhoben wurden, nicht jedoch die Erhebung von Daten an sich.[92]

[88] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, Rn. 293.
[89] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, ebd. sowie Zöller GA 2000, 568 (568 f.).
[90] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, Rn. 178.
[91] BVerfGE 100, 313 (365).
[92] KK-StPO/*Scheinfeld*, 9. Aufl. 2023, § 98a, Rn. 4 ff.

In der Praxis wird die manuelle Internetrecherche Großteils auf die Generalklauseln der §§ 161, 163 StPO gestützt.[93] Allerdings ist anzunehmen, dass selbst wenn sich eine staatliche Stelle unter einer Legende in eine Kommunikationsbeziehung zu einer betroffenen Person begibt, noch kein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt. Dies ist beispielsweise bei Chats ohne spezielle Zugangsbeschränkungen oder bei der Einsichtnahme von offen sichtbaren Profilen in sozialen Netzwerken der Fall.[94] Lediglich eine gezielte Suche nach Informationen über eine Person bedarf nach h. M. einer Rechtsgrundlage, wobei hier die § 161 Abs. 1, § 163 Abs. 1 StPO als ausreichend gesehen werden.[95] Selbst verdeckte Ermittlungen in sozialen Netzwerken durch nicht offen ermittelnde Polizeibeamte können auf diese Ermittlungsgeneralklausel gestützt werden.[96] Dies gilt auch dann, wenn einem verdeckt operierenden Polizeibeamten oder einer Vertrauensperson (V-Person) von einem Teilnehmer der Zugang zu einem geschlossenen Chat ermöglicht wird.[97] Die Grenze zum Einsatz eines (virtuellen) Verdeckten Ermittlers im Sinne des § 110a StPO ist allerdings stets zu beachten.[98]

Doch auch bei dieser weiten Auslegung stoßen automatisierte Verfahren – etwa Massendatenscreenings oder KI-gestützte Webcrawler – aufgrund ihrer Intensität und Reichweite an die Grenzen dieser Generalklauseln.[99] Insbesondere die Abgrenzung zwischen zulässiger manueller Recherche und genehmigungspflichtiger automatisierter Massenauswertung ist bislang nicht klar konturiert. In diesem Zusammenhang scheint rechtspolitisch dringender Handlungsbedarf gerade im Hinblick auf die Vielzahl sich stellender Abgrenzungsfragen gegeben.

Bis dahin können in Ermangelung nationaler Normen lediglich internationale Leitlinien wie das *Berkeley Protocol on Digital Open Source Investigations*[100] oder die *Leiden*

[93] OLG Hamburg, Beschl. v. 20.05.2015 – 2 Ws 85/15.
[94] BVerfG, Urt. v. 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, Rn. 293.
[95] KK-StPO/*Weingarten*, 9. Aufl. 2023, StPO, § 161 Rn. 12a, krit. *Singelnstein*, NStZ 2012, 593 (600).
[96] *Soiné*, NStZ 2022, 321 (325); 2014, 248 (249); SK-StPO/*Wohlers/Deiters*, 6. Aufl. 2021, § 163 Rn. 17; a.A. HK-StPO/*Zöller*, 7. Aufl. 2023, § 163 Rn. 12.
[97] BVerfG NJW 2008, 822 (835).
[98] Hierzu bspw. Löwe/Rosenberg/*Hauck*, 28. Aufl. 2025, § 110a Rn. 26 f.; *Hertel*, Kriminalistik 2019, 162 (162 f.).
[99] *Seum/Rückert*, KripoZ 2024, 192 (228).
[100] Abrufbar unter: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (letzter Aufruf: 01.09.25).

Guidelines[101] eine Orientierung auch für deutsche Strafverfahren bieten. Diese formulieren allerdings nur Anforderungen an Authentizität, Dokumentation und Nachvollziehbarkeit von OSINT-Ergebnissen und sind somit eher als allgemeines Qualitätsmanagement-Tool zu sehen, denn als ein verbindlicher Rechtsrahmen.

Diese fehlende gesetzliche Regelung führt zu Rechtsunsicherheit, sowohl für Ermittlungsbehörden als auch für Gerichte.[102] So können unrechtmäßig erhobene oder unverlässlich dokumentierte OSINT-Daten einem Beweisverwertungsverbot unterliegen.[103] Dies gilt umso mehr, als OSINT anfällig für Fehlinformationen und Manipulationen ist. Die Überprüfung der Quellen und die Sicherung der Integrität der Daten sind daher essenziell.[104] Dabei ist aber zu beachten, dass selbst rechtmäßig erhobene Daten unter Umständen ausscheiden, wenn ihre Verwendung den Grundsatz des fairen Verfahrens (Art. 6 EMRK) verletzen würde.[105]

4.3.3 Potenzial im Zusammenhang mit Kryptowährungen

In einer globalisierten und digitalisierten Welt, in der Finanzströme oft verschleiert und grenzüberschreitend geführt werden, gewinnt OSINT insbesondere bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung an Bedeutung. Ermittlungsbehörden, Financial Intelligence Units und internationale Organisationen wie die Financial Action Task Force (FATF) setzen OSINT zunehmend ein, um verdächtige Transaktionen aufzudecken, Netzwerke zu identifizieren und Beweise zu sichern.[106] Das Potenzial liegt in der schnellen, grenzüberschreitenden Informationsgewinnung und der kosteneffizienten Ermittlung. Diese Ermittlungsansätze sind besonders dann von Bedeutung, wenn etwa im Darknet[107] die bisherigen technischen Eingriffsbefugnisse nicht zum Erfolg führen.[108]

---

[101] Abrufbar unter: Designed - V3 Guidelines for Open Source Intelligence Organisations.docx (letzter Aufruf: 01.09.25).
[102] *Seum/Rückert*, KripoZ 2024, 192 (234).
[103] BGHSt 51, 285 (292).
[104] *Penlink*, Best Practices for Integrating Open-Source Intelligence (OSINT) into Investigations, Stand 05.08.2025; abrufbar unter: https://www.penlink.com/de/blog/best-practices-for-integrating-osint-into-investigations (letzter Aufruf: 01.09.25).
[105] EGMR, Urt. v. 12.7.1988 – 10862/84 – Schenk vs. Schweiz – Serie A Nr. 140.
[106] FATF, Comprehensive Update on Terrorist Financing Risks, 2025, S. 96, Rn. 196.
[107] Das Darknet ist ein verborgener Teil des Internets, der nicht über herkömmliche Suchmaschinen erreichbar ist und für welchen spezielle Software, wie der Tor-Browser, benötigt wird.
[108] vgl. zu Ermittlungen im Darknet *Fünfsinn/Ungefuk/Krause*, Kriminalistik 2017, 440 (440 f.).

Da – wie auch in Deutschland – die Gewinnung und Verwertung von OSINT-Erkenntnissen vielfach nicht konkret geregelt ist, formuliert die FATF dabei als globaler Standardsetzer für Anti-Money-Laundering (AML) und Countering the Financing of Terrorism (CFT) sogar eigene Empfehlungen, die auch den Einsatz von OSINT betreffen.[109] Die Egmont Group der FIUs veröffentlicht zudem Best Practices, die auf die Integration von OSINT in operative und strategische Analysen abzielen.[110]

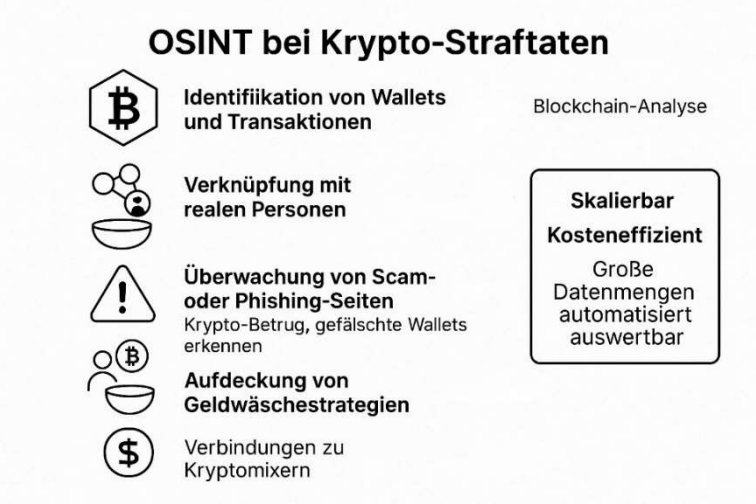

Abb. 10: Schematische Darstellung der Einsatzmöglichkeiten bei Krypto-Straftaten

Bei allen Straftaten im Zusammenhang mit Kryptowährungen besteht die zentrale Problematik hierbei darin, dass zwar öffentliche Blockchains, wie die von Bitcoin, vollständige Transparenz bieten, Privacy-Coins wie Monero oder Zcash die Rückverfolgung von Transaktionen aber erheblich erschweren können. Die Pseudonymität von Wallet-Adressen ermöglicht es Täter:innen, ihre Identität zu verschleiern, während gleichzeitig jede Transaktion dauerhaft auf der Blockchain gespeichert wird.[111]

Diese scheinbare Paradoxie eröffnet OSINT-Spezialisten besondere Chancen, aber auch Herausforderungen: OSINT kann mit frei zugänglichen Blockchain-Explorern

[109] FATF Recommendations, 2023, Empfehlung 29 und 31.
[110] Egmont Group of financial intelligence units principles for information exchange between financial intelligence units, Stand 15. April 2023, S. 4.
[111] FATF, Countering Ransomware Financing (March 2023), Rn. 24.

beginnen, um Transaktionshistorien und -muster zu analysieren.[112] Zudem können Adressen durch Clustering-Methoden, Heuristiken (z. B. gemeinsame Eingaben in Transaktionen) und Korrelation mit externen Daten deanonymisiert werden. Neben On-Chain-Daten bieten Foren, Darknet-Marktplatz-Listings, Social-Media-Posts und GitHub-Repositories wertvolle Hinweise.[113] Beispielsweise können Benutzer, die ihre Wallet-Adressen öffentlich posten, mit spezifischen Transaktionen in Verbindung gebracht werden. Schließlich kann aber auch durch Cross-Referencing mit regulatorischen Meldungen eine Validierung der Daten erreicht werden, um strafprozessuale Risiken zu minimieren.[114]

Damit kann der Einsatz von OSINT im Bereich von Geldwäsche und Terrorismusfinanzierung die Identifizierung komplexer Unternehmens- und Beteiligungsstrukturen, welche zur Verschleierung illegaler Vermögenswerte dienen, erleichtern oder gar erst ermöglichen. Durch die Auswertung von Handelsregistereinträgen, Unternehmenswebsites, Presseartikeln und Social-Media-Profilen sind ferner Verbindungslinien zwischen juristischen Personen und wirtschaftlich Berechtigten herstellbar. In Kombination mit verdächtigen Meldungen nach dem Geldwäschegesetz (GwG) können OSINT-Daten die Hypothesenbildung beschleunigen und die internationale Zusammenarbeit vereinfachen.[115]

Da wegen der vorgeblichen Anonymität gerade terroristische Gruppen zunehmend digitale Plattformen wie Crowdfunding-Websites, Kryptowährungsbörsen oder Zahlungsdienstleister nutzen, um Finanzmittel zu beschaffen[116], kann der Einsatz von OSINT auch durch die Überwachung öffentlicher Blockchain-Explorer, Foren und Social-Media-Kanäle Hinweise auf Transaktionen und Unterstützernetzwerke liefern. So lässt sich zunehmend auch aus der forensischen Ermittlungspraxis beobachten, dass viele Radikalisierungsprozesse und Finanzierungsaufrufe offen oder halböffentlich in Messaging-Diensten, auf Videoplattformen oder in Foren erfolgen. Durch die kontinuierliche Beobachtung und Dokumentation solcher Inhalte lassen sich frühzeitig Risikoprofile erstellen.[117]

[112] Chainalysis, Crypto Crime Report, 2025, S. 27.
[113] *Bazzell*, OSINT Techniques, 9. Aufl. 2021, S. 421.
[114] FinCEN, Advisory on Illicit Activity Involving Convertible Virtual Currency, 2019. S. 10.
[115] FIU Deutschland, Jahresbericht 2024, S. 37.
[116] FATF, Virtual Assets - Red Flag Indicators of Money Laundering and Terrorist Financing, 2020, S. 3.
[117] Europol, Terrorism Situation and Trend Report (TE-SAT), 2024, S. 69.

5 Aktueller Stand bei den Ermittlungsbehörden

Aufbauend auf den dargestellten technischen und rechtlichen Rahmenbedingungen gilt es zu untersuchen, welche Auswirkungen diese Erkenntnisse auf die praktische Umsetzung in der Ermittlungsarbeit haben. Im Zentrum steht die Frage, wie die Bekämpfung von Geldwäsche und Terrorismusfinanzierung (mittels Kryptowerten) gegenwärtig in der polizeilichen Praxis ausgestaltet ist, insbesondere vor dem Hintergrund der bislang begrenzten empirischen Datenlage. Die nachfolgenden Auswertungen basieren maßgeblich auf den im Rahmen des Projektes G.E.K.O. erhobenen Rückmeldungen der teilnehmenden Ermittlungsbehörden sowie auf bestehenden amtlichen Statistiken. Sie erlauben einen differenzierten Blick auf die bisherigen Erkenntnisse zum Umfang und zu den Erscheinungsformen von kryptobasierten Geldwäsche- und Terrorismusfinanzierungstaten. Zudem bieten sie erstmals eine strukturierte Einschätzung zur Nutzung von OSINT als Ermittlungsinstrument in diesem Phänomenbereich.

5.1 Umfang der Geldwäsche und Terrorismusfinanzierung mit Kryptowerten

Um überhaupt die Bedeutung des Themas einschätzen und ggf. aber auch bereits bestimmte Schwachstellen ausmachen zu können, bedarf es zunächst einer Auseinandersetzung mit dem eigentlichen Umfang der Geldwäsche und Terrorismusfinanzierung in Deutschland sowie des Einsatzes von Kryptowerten bei diesen Phänomenbereichen.

5.1.1 Geldwäsche und Terrorismusfinanzierung im Allgemeinen

Die wichtigsten Erkenntnisquellen für die vorliegende Analyse bilden die amtlichen Kriminal- und Justizstatistiken, namentlich die Polizeiliche Kriminalstatistik (PKS), der Kriminalpolizeiliche Meldedienst in Fällen politisch motivierter Kriminalität (KPMD-PMK), die Geschäftsstatistik der Staatsanwaltschaften (StA-Statistik), die Geschäftsstatistik der Strafgerichte (StP-Statistik) sowie die Jahresberichte der Zentralstelle für Finanztransaktionsuntersuchungen (Financial Intelligence Unit - FIU) zur Anzahl der Geldwäscheverdachtsmeldungen (GWVM). Diese Statistiken bilden die Grundlage für

die empirische Bewertung, weisen jedoch jeweils spezifische Erfassungslogiken und Limitationen auf, die bei der Interpretation der Ergebnisse zu berücksichtigen sind.

Zusätzlich zu dem statistischen Datenmaterial der Polizei und Justiz fließen Angaben aus der durchgeführten Erhebung ein. Zu berücksichtigen ist, dass die amtlichen Statistiken keine reelle Kriminalitätswirklichkeit messen können, sondern primär Tätigkeitsnachweise der erstellenden Stellen abbilden. Es handelt sich bei den zugrundeliegenden Daten um Hellfeldstatistiken, die auf angezeigten und verfolgten Fällen basieren und somit das Dunkelfeld strukturell unberücksichtigt lassen. In Zusammenschau mit der durchgeführten Befragung stellen die Daten dennoch eine empirische Grundlage für eine Bewertung der betrachteten Kriminalitätslage zu.

5.1.1.1 Fälle der Geldwäsche nach der PKS und der Zolljahresstatistik

Bei der im Bundeskriminalamt (BKA) geführten Polizeilichen Kriminalstatistik (PKS) handelt es sich um eine sogenannte Ausgangsstatistik. Das bedeutet, dass die statistische Erfassung eines Falles nicht bei Eingang einer Strafanzeige, sondern erst mit Abschluss aller polizeilichen Ermittlungen durch die für die Endbearbeitung zuständige Dienststelle bei endgültiger Abgabe der entstandenen Ermittlungsvorgänge bzw. des Schlussberichts an die Staatsanwaltschaft erfolgt. In der PKS wird ein Fall in dem Monat gezählt, in dem er erfasst wurde. Die Tatzeit bleibt dabei unberücksichtigt und wird nicht ausgewertet. Somit sind in der PKS eines Kalenderjahres regelmäßig Straftaten enthalten, die ein oder mehrere Jahre zuvor begangen wurden, während Straftaten mit Tatzeit aus dem aktuellen Kalenderjahr aufgrund der laufenden Ermittlungen noch nicht erfasst wurden.[118] Insoweit können bei den Ermittlungsbehörden entstandene Bearbeitungsrückstände in Abhängigkeit des Zeitpunktes ihrer Bearbeitung zu Verzerrungen in der Statistik führen.

Geldwäsche bzw. die Verschleierung unrechtmäßiger Vermögenswerte (§ 261 StGB) wird unter der PKS-Schlüsselnummer 633000 erfasst. In der PKS nicht enthalten sind allerdings Staatsschutzdelikte, mithin auch die Terrorismusfinanzierung, sowie

[118] Zur Bedeutung, Inhalt, Aussagekraft der PKS vgl. https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/bedeutungInhaltAussagekraft.html?nn=46948 (letzter Aufruf: 01.09.25). https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/PKS2023/Interpretationshilfen/interpretationshilfen_node.html (letzter Aufruf: 01.09.25).

Straftaten, die außerhalb der Bundesrepublik Deutschland begangen wurden. Eine Auflistung des jeweils bekannt gewordenen Schadens der Geldwäsche ist in der PKS ebenso nicht einsehbar.

Bei der Interpretation der Daten ist ferner zu berücksichtigen, dass sich die in der PKS abgebildeten Fälle jeweils nur auf das Delikt mit der höchsten Strafandrohung beziehen. Aufgrund der Vortaterfordernis bei der Geldwäschestrafbarkeit ist somit davon auszugehen, dass nicht alle geführten Geldwäscheverfahren einen Eingang in die PKS finden. Ferner ist zu beachten, dass die jüngste Reformierung des § 261 StGB, durch den Wegfall des Vortatenkataloges und dem nunmehr eingeführten sog. All-Crimes-Ansatz, dazu führte, dass eine Strafbarkeit wegen Geldwäsche deutlich häufiger in Betracht kommt.[119] Zu berücksichtigen ist ebenfalls, dass das Ausleitungsverhalten der FIU wesentliche Auswirkungen auf die erfassten Fallzahlen der Geldwäsche hat.[120] Auch diesbezüglich dürfte die jüngste Reform des § 261 StGB ein Treiber gewesen sein, da eine Anpassung des Meldeverhaltens der Verpflichteten nach dem Geldwäschegesetz (GwG) sowie verschiedene weitere gesetzliche Änderungen der jüngeren Vergangenheit erfolgten (wie z.B. Einstufung des Kryptoverwahrgeschäfts als erlaubnispflichtige Dienstleistung). So werden in der Ermittlungspraxis der Strafverfolgungsbehörden Geldwäscheverfahren maßgeblich entweder auf Basis der Verdachtsmeldungen nach dem GwG[121] eingeleitet oder in Form verfahrensintegrierter Ermittlungen als Bestandteil laufender Verfahren geführt.

Die Anzahl der in Deutschland geführten Verfahren aus den Jahren 2023 (bundesweite Gesamtzahl 32.573) und 2024 (bundesweite Gesamtzahl 37.663 Fälle) kann der nachfolgenden Abbildung entnommen werden:

[119] Kindhäuser/Neumann/Peffgen/Saliger/*Altenhain,* StGB, 6. Aufl. 2023, § 261, Rn. 4.
[120] Mitteilung des Senats zur Schriftlichen Kleinen Anfrage der Fraktion CDU vom 01.08.2023, Hamburgische Bürgerschaft Drs. 22/12447, S. 3-5.
[121] Anlass für verfahrensunabhängige Ermittlungen sind überwiegend Geldwäscheverdachtsmeldungen der Verpflichteten (GWVM) oder Bargeldfeststellungen des Zolls. Das Geldwäschegesetz (GwG) definiert den Kreis der Verpflichteten. Sowohl die GWVM als auch die Bargeldfeststellungsverfahren der Zollverwaltung stellen eine Maßnahme zur Geldwäschebekämpfung dar (§ 12a ZollVG). Die Verpflichteten übermitteln ihre Verdachtsmeldungen an die administrativ ausgerichtete Zentralstelle Financial Intelligence Unit (FIU).

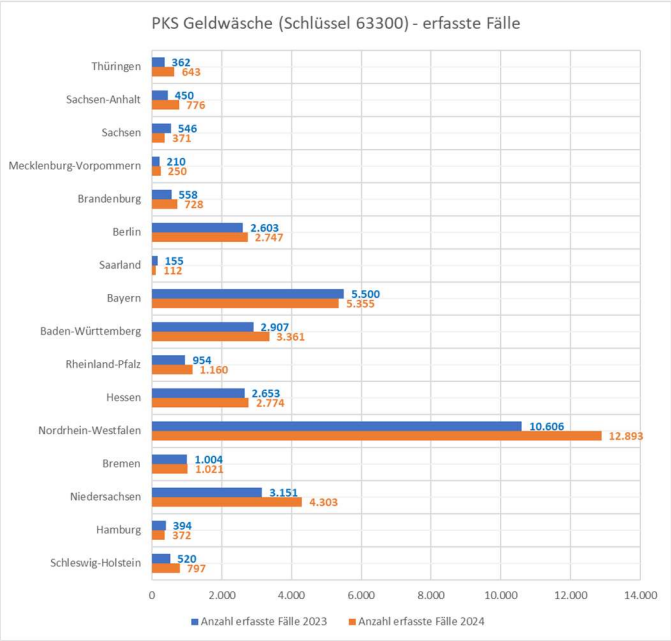

Abb. 11: Erfasste Fälle der Geldwäsche (Summenschlüssel 63300) in der PKS je Bundesland[122]

Vergleicht man dabei den prozentualen Anteil der Fälle der Geldwäsche zu dem PKS-Gesamtfallaufkommen in den Ländern, ergibt sich folgende Verteilung:

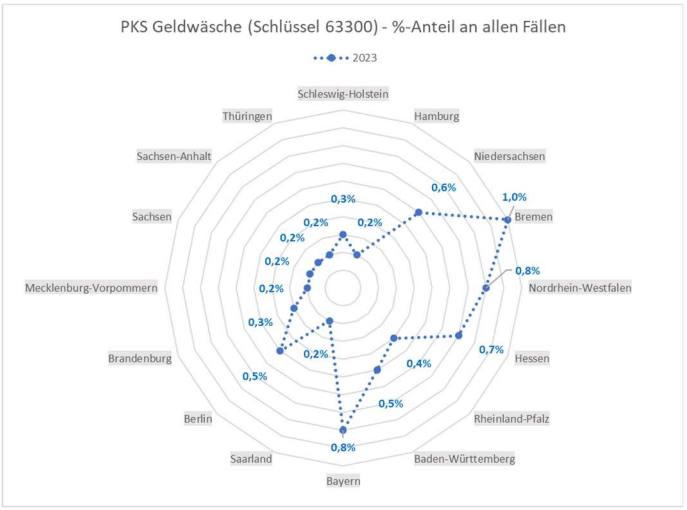

Abb. 12: Prozentualer Anteil am Gesamtfallaufkommen im Jahr 2023

[122] BKA, PKS T01 Grundtabelle - Fallentwicklung - Länder (V1.0), Schlüssel 633000.

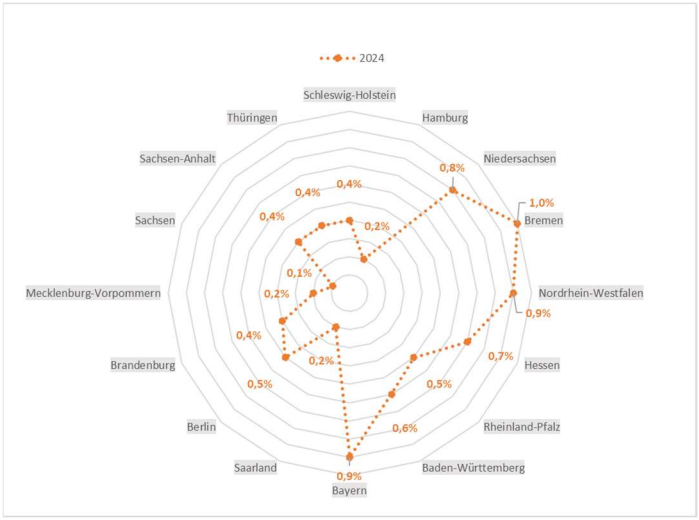

Abb. 13: Prozentualer Anteil am Gesamtfallaufkommen im Jahr 2024

Erwartungsgemäß weisen bevölkerungsreiche Flächenländer wie Bayern und Nordrhein-Westfalen die höchsten absoluten Fallzahlen auf. Auffällig ist aber, dass auch bei einigen kleineren Bundesländern, wie Bremen oder dem Saarland, signifikante Unterschiede in der prozentualen Verteilung auszumachen sind. Diese Unterschiede können sowohl auf die tatsächliche Kriminalitätsbelastung als auch auf unterschiedliche Ermittlungs- und Erfassungspraxen zurückzuführen sein. Eine belastbare Bewertung der Ursachen ist aufgrund der heterogenen Datenlage jedoch nicht möglich und bedürfte einer detaillierten Untersuchung.

Bei Betrachtung des prozentualen Anteils der Geldwäschefälle am Gesamtfallaufkommen der PKS für die Jahre 2023 und 2024 fällt auf, dass insbesondere Bremen, Bayern und Nordrhein-Westfalen einen überdurchschnittlichen Anteil an Geldwäschefällen im Vergleich zum Gesamtfallaufkommen aufweisen. Dies kann auf eine gezielte Schwerpunktsetzung der Ermittlungsbehörden, eine hohe Sensibilisierung für das Thema oder auf regionale Kriminalitätsstrukturen zurückzuführen sein. Demgegenüber liegen andere Bundesländer, wie Hamburg und Sachsen unter dem Bundesdurchschnitt. Hier könnte eine geringere Priorisierung des Deliktsfeldes, eine andere Kriminalitätsstruktur oder auch eine zurückhaltendere Erfassungspraxis eine Rolle spielen. Der Vergleich der prozentualen Anteile zwischen 2023 und 2024 zeigt zudem, dass die relativen Unterschiede zwischen den Bundesländern weitgehend stabil bleiben. In einzelnen Ländern sind leichte Verschiebungen zu beobachten, die jedoch

nicht auf grundlegende Veränderungen, sondern eher auf Schwankungen im Erfassungsverhalten oder auf Einzelfälle zurückzuführen sein dürften.

Der Zoll wiederum hat im Bereich der Organisierten Kriminalität im Jahr 2023 insgesamt zehn[123] und im Jahr 2024 insgesamt vier[124] Geldwäscheverfahren geführt.

Insgesamt zeigen die statistischen Daten, dass Geldwäsche als Deliktsfeld regional sehr unterschiedlich ausgeprägt ist und in einigen Bundesländern eine deutlich größere Rolle im polizeilichen Alltag spielt als in anderen.

5.1.1.2 Fälle der Terrorismusfinanzierung nach dem KPMD-PMK

Wie bereits beschrieben sind Straftaten der politisch motivierten Kriminalität (PMK) - Staatsschutzdelikte - wie die Terrorismusfinanzierung, nicht in der PKS enthalten. Sie werden vielmehr im bundeseinheitlichen Kriminalpolizeilichen Meldedienst politisch motivierte Kriminalität (KPMD-PMK)[125] und – anders als Straftaten in der PKS – grundsätzlich bereits zu Beginn des Verfahrens zugeordnet (Eingangsstatistik). Fälle der Terrorismusfinanzierung gemäß § 89c StGB werden in dem KPMD-PMK innerhalb des Phänomens Terrorismus als Staatsschutzdelikte statistisch festgehalten. Da die PMK-Fälle sogenannten Themenfeldern zugeordnet werden, enthält der durch das BKA jährlich veröffentlichte Bericht mit den Darstellungen der bundesweiten Fallzahlen keine gesondert aufbereiteten Daten zu Fällen nach § 89c StGB. Daher können aus den veröffentlichten BKA-Aufbereitungen der KPMD-PMK-Daten keine weiteren Daten für die vorliegende Befassung herangezogen werden.

Im Rahmen des Forschungsprojekts erfolgte aus diesem Grund eine gesonderte Abfrage der jeweils in den Behörden geführten Fälle. Die Anzahl kann der folgenden Tabelle entnommen werden:

[123] Generalzolldirektion, Zolljahresstatistik 2023, S. 19.
[124] Generalzolldirektion, Zolljahresstatistik 2024, S. 19.
[125] Zur Definition, Beschreibung und Deliktsbereiche der KPMD-PMK vgl. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/PMK/PMKrechts/PMKrechts_node.html#doc121714bodyText1 (letzter Aufruf: 01.09.25).

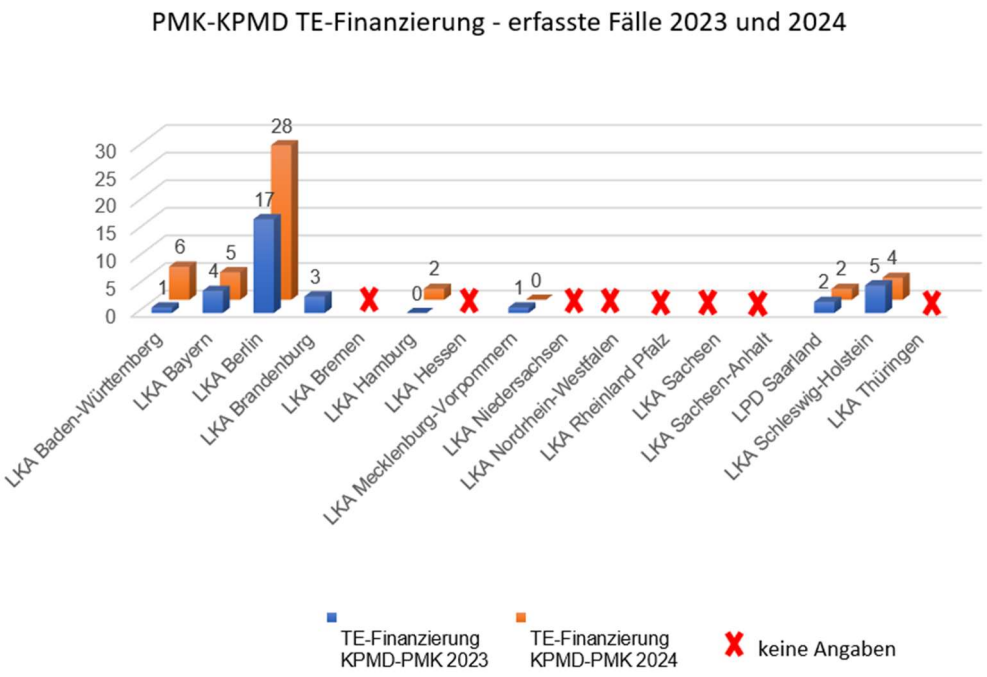

Abb. 14: Erfasste Fälle der Terrorismusfinanzierung im KPMD-PMK je Bundesland[126]

Die niedrigen Fallzahlen und die starke Streuung zwischen den Ländern verdeutlichen, dass die polizeiliche Hellfeldstatistik im Bereich der Terrorismusfinanzierung nur einen sehr kleinen Ausschnitt des tatsächlichen Geschehens abbildet. Die fehlenden Angaben aus mehreren Bundesländern stellen zudem eine erhebliche Limitation für die bundesweite Bewertung dar. Zudem ist von einem erheblichen Dunkelfeld auszugehen, da viele Finanzierungsströme verdeckt und international verschleiert ablaufen.

5.1.1.3 Fälle nach der StA-Statistik

Weitere Anhaltspunkte liefert die StA-Statistik, in welcher die staatsanwaltschaftliche Tätigkeit erfasst wird. In diese werden die bei den Staatsanwaltschaften geführten Ermittlungsverfahren nach der bundeseinheitlichen Anordnung für die StA-Statistik des Ausschusses für Justizstatistik der Justizministerkonferenz aufgenommen. Diese erfolgt anhand von Deliktsbereichen (sog. Sachgebietsgliederung). Für die hiesige Untersuchung relevant sind dabei das Sachgebiet Staatsschutzsachen[127] und das

[126] Im Rahmen der Beantwortung haben (aus ermittlungstaktischen Gründen) das LKA Bremen, Hessen, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen und Sachsen-Anhalt keine Angaben zu den im KPMD-PMK erfassten Fälle der Terrorismusfinanzierung gemacht. Mangels Zuständigkeit erfolgte diesbezüglich ebenfalls keine Mitteilung durch das ZKA bzw. den ZFD.
[127] Sachgebiet Nr. 10.

Sachgebiet Geldwäschedelikte nach § 261 StGB[128]. Es gilt zu beachten, dass es sich wiederum um eine Verfahrensstatistik handelt, sodass die Daten der StA-Statistik den Daten der Personenstatistik PKS nicht ohne Verzerrungen gegenübergestellt werden können.

Die Anzahl der in Deutschland im Jahr 2023 (bundesweite Gesamtzahl 136.650) und im Jahr 2024 (bundesweite Gesamtzahl 144.353) erledigten Geldwäscheverfahren und der im Jahr 2023 (bundesweite Gesamtzahl 1.590) und im Jahr 2024 (bundesweite Gesamtzahl 1.478) erledigten Staatsschutzsachen können den nachfolgenden Abbildungen entnommen werden:

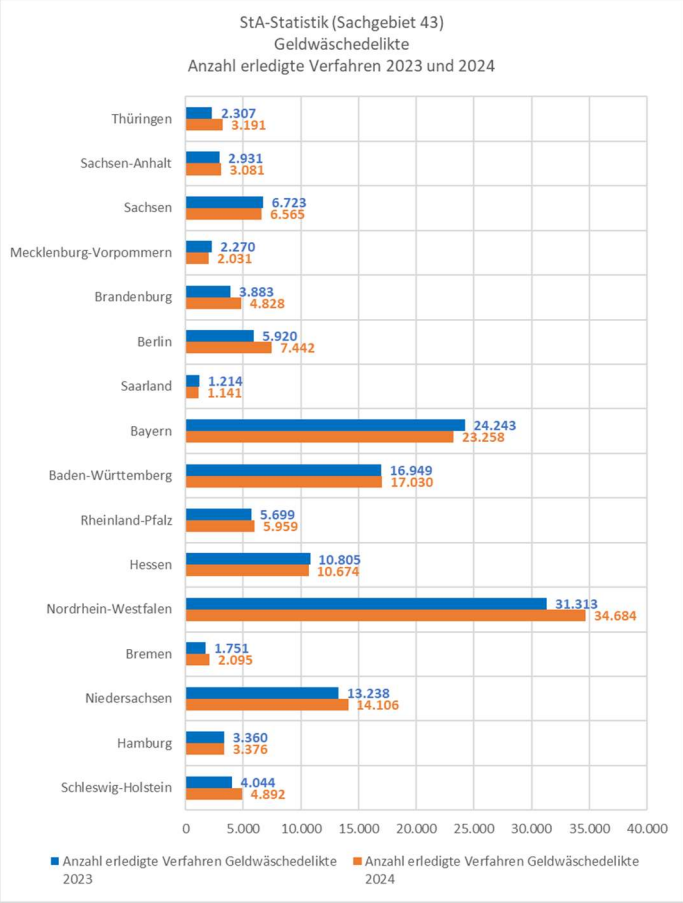

Abb. 15: Anzahl der erledigten Verfahren (Sachgebiet 43) je Bundesland [129]

[128] Sachgebiet Nr. 43.
[129] Statistische Berichte – Staatsanwaltschaften 2023 und 2024, EVAS-Nummer 24211, Tabelle 24211-07, siehe veröffentlicht durch Statistisches Bundesamt, siehe: https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Gerichte/statistischer-bericht-staatsanwaltschaften-2100260237005.html (letzter Aufruf: 01.09.25) bzw.

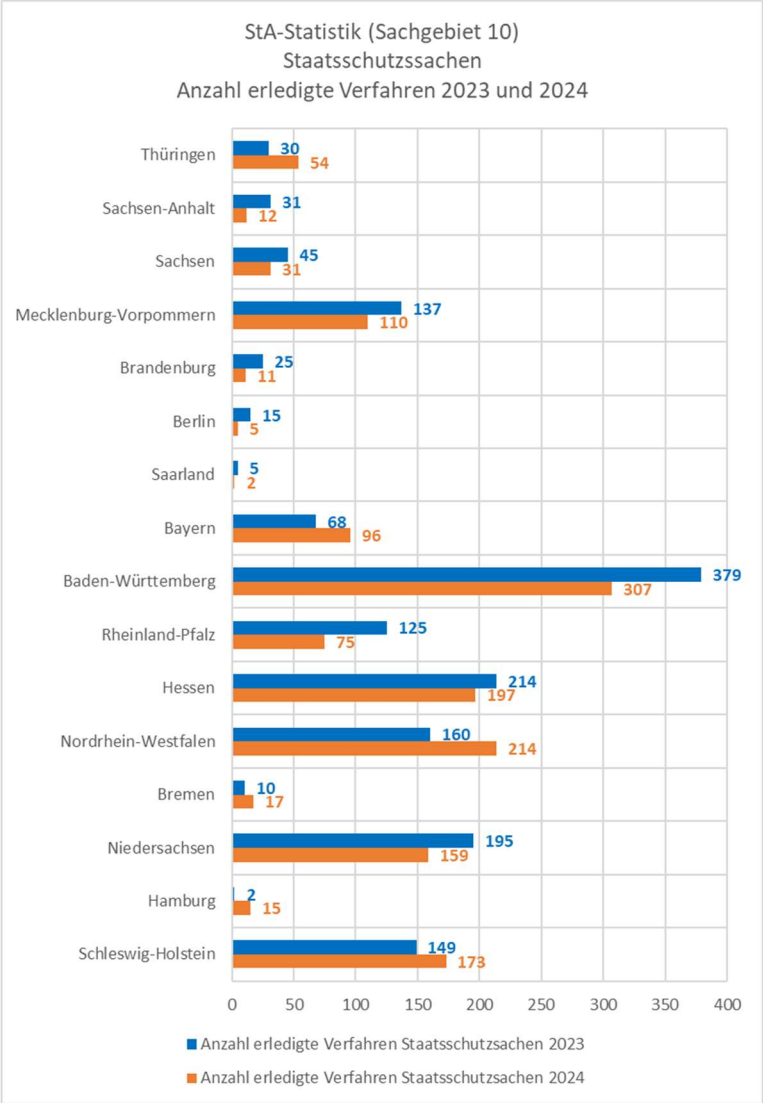

Abb. 16: Anzahl der erledigten Verfahren (Sachgebiet 10) je Bundesland [130]

Innerhalb der Kategorie der erledigten Staatsschutzsachen differenziert die StA-Statistik nicht nach einzelnen Straftatbeständen. Eine spezifische Aussage zur Anzahl der

durch Eingabe der Codes 24211-0001 und 24211-0010 in das Suchfenster der Datenbank GENESIS-Online.

[130] Statistische Berichte – Staatsanwaltschaften 2023 und 2024, EVAS-Nummer 24211, Tabelle 24211-07, siehe veröffentlicht durch Statistisches Bundesamt, siehe: https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Gerichte/statistischer-bericht-staatsanwaltschaften-2100260237005.html (letzter Aufruf: 01.09.25) . bzw. durch Eingabe der Codes 24211-0001 und 24211-0010 in das Suchfenster der Datenbank GENESIS-Online.

Verfahren wegen Terrorismusfinanzierung gemäß § 89c StGB ist daher auf Basis der vorliegenden Daten erneut nicht möglich.

Vergleicht man den prozentualen Anteil der bei den Staatsanwaltschaften erledigten Geldwäscheverfahren zu dem Gesamtfallaufkommen bei den jeweiligen Staatsanwaltschaften in den Ländern, ergibt sich folgende Verteilung:

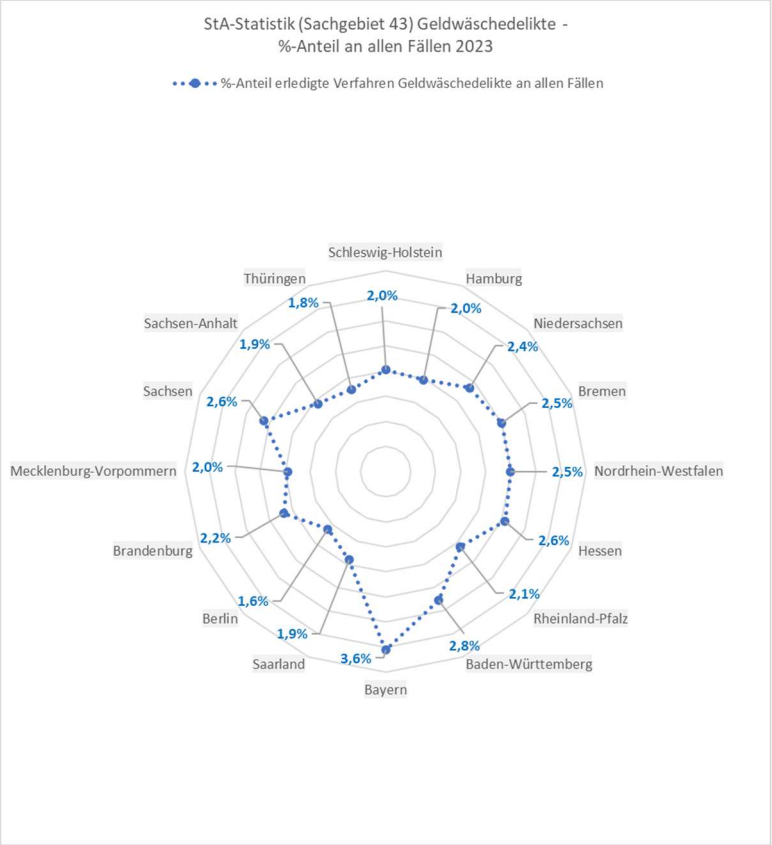

Abb. 17: Prozentualer Anteil am Gesamtfallaufkommen im Jahr 2023

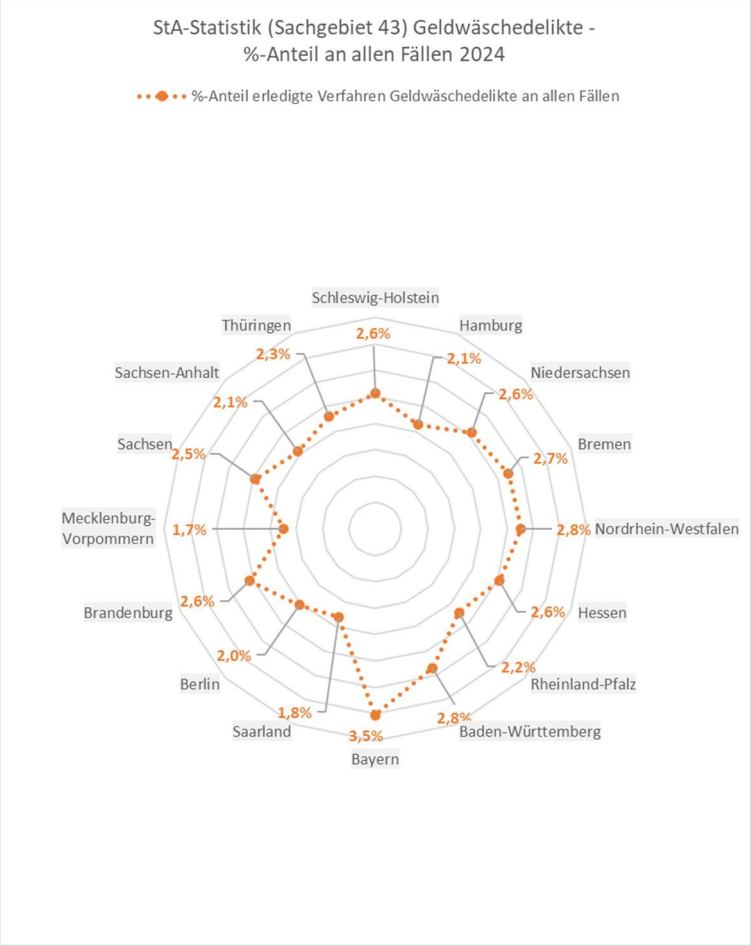

Abb. 188: Prozentualer Anteil am Gesamtfallaufkommen im Jahr 2024

Ergänzend liefert die StA-Statistik[131] einen Überblick über die Verfahrensausgänge in Geldwäschefällen. Für Fälle der Terrorismusfinanzierung liefert die StA-Statistik keine auswertbaren Daten. Die nachstehende Tabelle zeigt die Erledigungsarten dieser Verfahren im Jahr 2023[132]:

[131] Statistischer Bericht – Staatsanwaltschaften 2023, EVAS-Nummer 24211, Tabellen 24211-30, 24211-31 veröffentlicht durch Statistisches Bundesamt, siehe: https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Gerichte/statistischer-bericht-staatsanwaltschaften-2100260237005.html (letzter Aufruf: 01.09.25).
[132] Die nach Erledigungsart aufgeschlüsselten Daten für das Jahr 2024 waren zum Zeitpunkt der Berichtsfinalisierung noch nicht veröffentlicht.

Erledigte Verfahren bundesweit insgesamt:	**136.650**	
davon beendet…		Anteil
durch Anklage:	1.833	1,34 %
durch Antrag auf Erlass eines Strafbefehls:	2.079	1,52 %
durch Einstellung mit Auflage § 153a StPO:	2.045	1,50 %
durch Einstellung wegen Geringfügigkeit (§ 153 Abs.1 StPO):	3.771	2,76 %
durch Einstellung bei Auslandstat (§ 153c StPO):	2.446	1,80 %
durch Einstellung bei unwesentlicher Nebenstraftat (§ 154 Abs. 1 StPO):	4.145	3,03 %
durch Einstellung wegen Abwesenheit des Beschuldigten oder wegen eines anderen in seiner Person liegenden Hindernisses (§ 154f StPO):	6.153	4,50 %
durch Einstellung nach § 170 Abs. 2 StPO:	54.251	39,70 %
Übrige Verfahrensausgänge (ohne nähere Zuordnung)	59.927	43,85 %

Abb. 19: StA-Statistik, aufgeschlüsselt nach Erledigungsart

Die durchschnittliche Verfahrensdauer dieser Fallgruppe beträgt bundesweit neun Monate.[133]

Im Jahr 2023 wurden bundesweit insgesamt 5.503.431 und im Jahr 2024 bundesweit insgesamt 5.464.278 Verfahren bei den Staatsanwaltschaften erledigt. Davon entfielen im Jahr 2023 insgesamt 136.650 Verfahren und im Jahr 2024 insgesamt 144.353 Verfahren auf Geldwäschedelikte, was einem Anteil von rund 2,5 % (im Jahr 2023) bzw. 2,6 % (im Jahr 2024) an allen erledigten Verfahren entspricht. Die höchste relative Verfahrenslast im Bereich Geldwäsche wiesen dabei die Bundesländer Bayern (3,6 % in 2023 und 3,5 % in 2024), Baden-Württemberg (2,8 % in 2023 und 2024), Hessen (2,6 % in 2023 und 2024) und Sachsen (2,6 % in 2023 und 2024) auf. Im Gegensatz dazu lagen Berlin (1,6 % in 2023 und 2,0 % in 2024), Thüringen (1,8 % in 2023 und 2,3 % in 2024) sowie das Saarland (1,9 % in 2023 und 1,8 % in 2024) und Sachsen-Anhalt (1,9 % in 2023 und 2,1 % in 2024) unter dem Bundesdurchschnitt. Eine belastbare Bewertung dieser Abweichungen setzt jedoch vertiefte regionale Kontextanalysen voraus, etwa hinsichtlich der Ermittlungsressourcen, regionalen Kriminalitätslage oder institutionellen Schwerpunktsetzungen. Dies bedarf einer eigenständigen Aufarbeitung.

[133] Vgl. Statistischer Bericht – Staatsanwaltschaften 2023, EVAS-Nummer 24211, Tabellen 24211-30, 24211-31 veröffentlicht durch Statistisches Bundesamt, siehe: https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Gerichte/statistischer-bericht-staatsanwaltschaften-2100260237005.html (letzter Aufruf: 01.09.25); Verfahrensdauer vom Tag des Eingangs bei der Staatsanwaltschaft bis zur Erledigung durch die Staatsanwaltschaft.

Im Jahr 2023 wurden zudem bundesweit 1.590 und im Jahr 2024 bundesweit 1.478 Verfahren im Bereich der Staatsschutzsachen bei den Staatsanwaltschaften erledigt. Dabei zeigt sich eine deutliche Streuung der Fallzahlen zwischen den einzelnen Bundesländern.

Die höchsten Fallzahlen verzeichneten Baden-Württemberg (379 Verfahren in 2023 und 307 Verfahren in 2024), Hessen (214 Verfahren in 2023 und 197 Verfahren in 2024), Niedersachsen (195 Verfahren in 2023 und 159 Verfahren in 2024) sowie Schleswig-Holstein (149 Verfahren in 2023 und 173 Verfahren in 2024). Auffällig ist, dass sich diese Bundesländer sowohl hinsichtlich ihrer Größe als auch ihrer Sicherheitslage unterscheiden, was auf unterschiedliche Ermittlungsansätze, regionale Schwerpunkte oder spezifische Fallkonstellationen schließen lässt. Demgegenüber wurden in anderen Bundesländern vergleichsweise wenige Staatsschutzverfahren abgeschlossen. So meldeten etwa Hamburg (2 Verfahren in 2023 und 15 Verfahren in 2024), Berlin (15 Verfahren in 2023 und 5 Verfahren in 2024) und Saarland (5 Verfahren in 2023 und 2 Verfahren in 2024) nur sehr geringe Fallzahlen.

Die erheblichen Unterschiede in den absoluten Zahlen können erneut verschiedene Ursachen haben. Neben tatsächlichen Unterschieden in der Kriminalitätsbelastung spielen auch organisatorische Faktoren eine Rolle, etwa die Konzentration besonderer Verfahren bei Schwerpunktstaatsanwaltschaften. Auch hier bedürfte es einer weiteren Forschung.

Aus der StA-Statistik geht zudem hervor, dass ein sehr hoher Anteil der Geldwäscheverfahren im Wege der Einstellung mangels hinreichendem Tatverdacht (§ 170 Abs. 2 StPO) erledigt werden. Über die Gründe ist nur zu mutmaßen. Ein Grund könnte sein, dass der kausale Zusammenhang zwischen Geldwäschehandlung und Vortat oftmals nicht erbracht werden kann. Zudem dürften aufgrund spezifischer Fallkonstellationen - z.B. in den Fallkonstellationen der sog. Finanzagenten[134] - kein hinreichender Tatverdacht für eine Strafbarkeit der jeweiligen Kontoinhaber wegen Geldwäsche begründet werden und zudem keine erfolgversprechenden Ermittlungsansätze zur Ermittlung der Hintermänner vorliegen. Diese Ursache, aber

[134] In dieser Fallkonstellation stellen die sog. Finanzagenten unwissentlich ihr privates Konto zur Entgegennahme und Weiterleitung betrügerisch erlangter Zahlungen zur Verfügung.

auch die geringe Anklagequote sowie die sehr hohe Zahl der übrigen Verfahrensausgänge bedürfen einer weiteren intensiven Forschung.

5.1.1.4 Fälle nach der StP-Statistik

Die Statistik der Strafgerichte (StP-Statistik) orientiert sich hinsichtlich der Sachgebietseinteilung an denselben Kategorien wie die Statistik der Staatsanwaltschaften. Dadurch ist eine vergleichbare Auswertung der gerichtlichen Bearbeitung von Geldwäscheverfahren (Sachgebiet 43) auf Länderebene möglich. Die StP-Statistik erfasst sämtliche bei den Strafgerichten erledigten Verfahren und ermöglicht so einen Einblick in die gerichtliche Praxis. Durch die gemeinsame Betrachtung der PKS/KPMD-PMK sowie der StA- und StP-Statistik kann ein Überblick über alle Verfahrensstadien gewonnen werden. Im Bereich der Staatsschutzdelikte (Sachgebiet 10) ist jedoch zu beachten, dass diese in der StP-Statistik nicht isoliert, sondern gemeinsam mit weiteren Verfahrenskategorien (Sachgebiete 11 bis 13) ausgewiesen werden. Eine spezifische Auswertung der Staatsschutzsachen und damit auch der Terrorismusfinanzierung auf Ebene der Strafgerichte ist daher erneut nicht möglich. Die nachfolgenden Abbildungen geben einen Überblick über die Verteilung und Bedeutung der Geldwäscheverfahren vor den Strafgerichten in den einzelnen Bundesländern und beleuchten die damit verbundenen methodischen Limitationen.

Die Anzahl der in Deutschland von den Strafgerichten erledigten Geldwäscheverfahren im Jahr 2023 (bundesweite Gesamtzahl 2.514) und im Jahr 2024 (bundesweite Gesamtzahl 3.742) kann der nachfolgenden Abbildung entnommen werden:

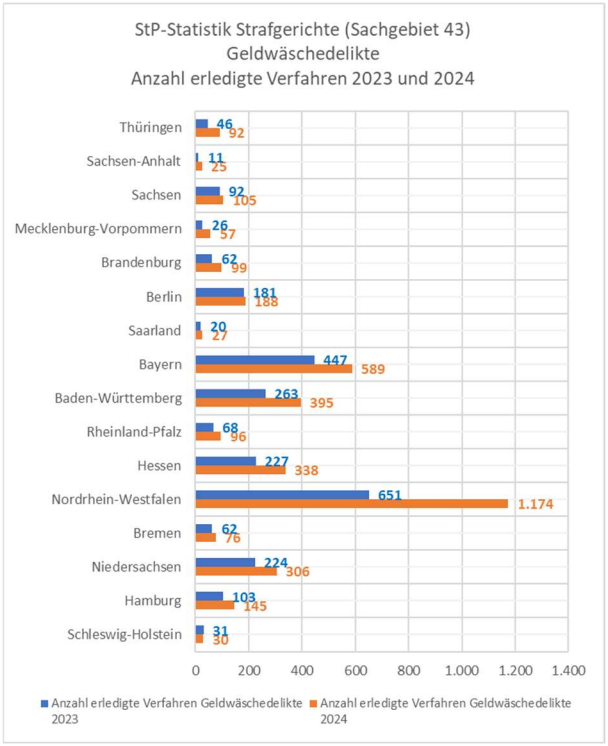

Abb. 20: Anzahl bei den Strafgerichten erledigte Verfahren der Geldwäsche (Sachgebiet 43) je Bundesland

Vergleicht man den prozentualen Anteil der bei den Strafgerichten erledigten Geldwäscheverfahren zu dem Gesamtfallaufkommen bei den jeweiligen Strafgerichtsbarkeiten der Länder, ergibt sich folgende Verteilung:

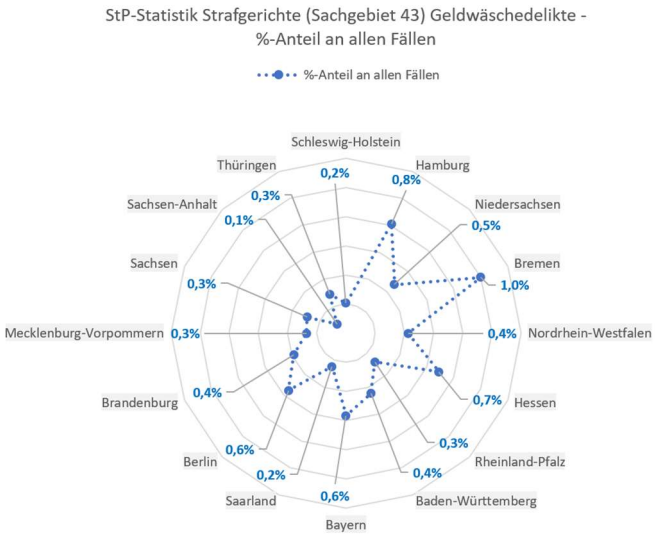

Abb. 20: Prozentualer Anteil am Gesamtfallaufkommen im Jahr 2023

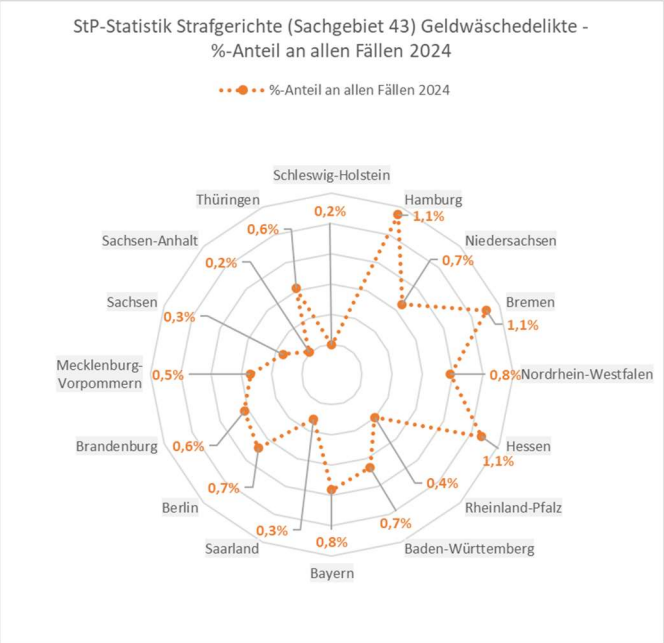

Abb. 21: Prozentualer Anteil am Gesamtfallaufkommen im Jahr 2024

Hinsichtlich der Verteilung der erledigten Geldwäscheverfahren auf die einzelnen Bundesländer zeichnet sich in der StP-Statistik ein ähnliches Bild wie bereits bei der StA-Statistik ab. Diese Parallelen deuten darauf hin, dass sich die regionalen Unterschiede in der Bearbeitung von Geldwäscheverfahren durchgängig entlang der gesamten Verfahrenskette – von der staatsanwaltschaftlichen Erledigung bis zur gerichtlichen Entscheidung – widerspiegeln. Die StP-Statistik ist, genauso wie die StA-Statistik, eine Verfahrensstatistik und zeigt lediglich die Tätigkeit der Strafgerichte auf, nicht aber die tatsächliche Kriminalitätsbelastung. Die Unterschiede zwischen den Bundesländern können daher auch auf organisatorische Faktoren, wie die Konzentration besonderer Verfahren bei Schwerpunktgerichten, zurückzuführen sein. Zudem ist zu beachten, dass die StP-Statistik keine differenzierte Auswertung nach einzelnen Straftatbeständen innerhalb der Staatsschutzsachen zulässt.

5.1.1.5 Verdachtsmeldungen nach den FIU-Jahresberichten

Die FIU nimmt gemäß § 27 Abs. 1 Geldwäschegesetz (GwG) die Rolle der nationalen Zentralstelle für die Verhinderung, Aufdeckung und Unterstützung bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung wahr. Sie nimmt

Geldwäscheverdachtsmeldungen (GWVM) entgegen und führt im Vorfeld eines strafrechtlichen Anfangsverdachts Finanzanalysen durch.

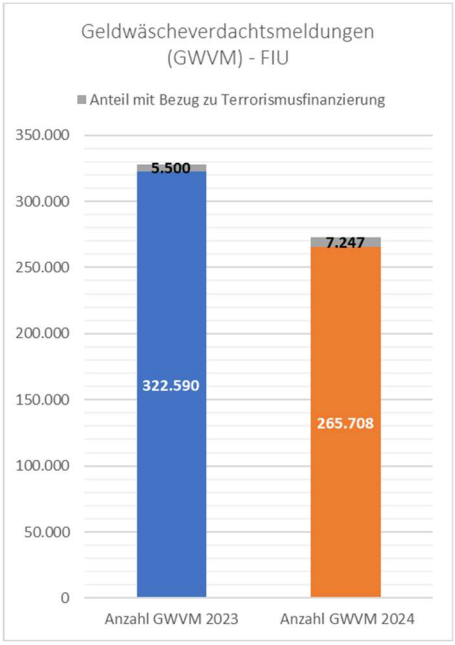

Abb. 22: Angaben aus den FIU-Jahresberichten der Jahre 2023 und 2024

Aus dem FIU-Jahresbericht für 2023 ergibt sich, dass im Berichtsjahr 2023 insgesamt 5.500 Verdachtsmeldungen mit potentiellem Bezug zu Terrorismusfinanzierung, sonstiger staatsschutzrelevanter Kriminalität oder Sanktionen eingingen, was 2 % am Gesamtaufkommen der Verdachtsmeldungen ausmacht.[135] Im Gegensatz zur rückläufigen Gesamtentwicklung des Verdachtsmeldeaufkommens zeichnet sich im Jahr 2024 ein deutlicher Anstieg der Verdachtsmeldungen mit Bezug zu Terrorismusfinanzierung, Staatsschutz und Sanktionen ab.[136] So gingen im Berichtsjahr 2024 rund 7.200 Verdachtsmeldungen mit potentiellem Bezug zu Terrorismusfinanzierung sonstiger staatsschutzrelevanter Kriminalität oder Sanktionen, mithin also ein Anteil von 3%, ein. Die FIU führt dies auf die Zunahme von Verdachtsmeldungen im Zusammenhang mit mutmaßlichen Verstößen gegen EU-Sanktionen sowie auf eine Zunahme von Verdachtsmeldungen zu politisch motivierter Kriminalität zurück.[137]

[135] FIU, Jahresbericht 2023, S. 15.
[136] FIU, Jahresbericht 2024, S. 50-51.
[137] FIU, Jahresbericht 2024, S. 50-51.

5.1.1.6 Zwischenbewertung

Die Auswertung der verfügbaren amtlichen Statistiken zu Geldwäsche und Terrorismusfinanzierung zeigt, dass die aufsichtsrechtlich, polizeilich und justiziell erfassten Fallzahlen nur einen Bruchteil des mutmaßlichen tatsächlichen Geschehens abbilden können. Während die Schätzungen von einem jährlichen Geldwäschevolumen in Deutschland zwischen 29 und bis zu 100 Milliarden Euro ausgehen (vgl. Erläuterungen unter 2.) und Szenekenntnisse aus der Organisierten Kriminalität sowie aus der Finanzkriminalität diese Annahme noch unterstreichen, spiegeln die aufsichtsrechtlich von der FIU, polizeilich in der PKS und dem KPMD-PMK sowie justiziell in der StA-Statistik und der StP-Statistik erfassten Fälle diese Größenordnung (bereits mit Blick auf die Anzahl der Fälle) bei weitem nicht wider. Die erhebliche Diskrepanz zwischen den in der Literatur geschätzten volkswirtschaftlichen Schäden durch Geldwäsche und den tatsächlich polizeilichen und justiziell erfassten Fällen verdeutlicht das Ausmaß des Dunkelfelds in diesem Deliktsbereich. Die Bewertung wird auch dadurch erschwert, dass in den bekannten Fällen der Schaden nicht konsequent erfasst wird.

Die Statistiken sind wegen unterschiedlicher Erfassungsgrundsätze, -daten und -Zeitpunkte nicht vergleichbar.[138] Die Fallzahlen variieren zudem auch zwischen den Bundesländern, welche grundsätzlich hinsichtlich der Bevölkerungsdichte vergleichbar sind, erheblich, was sowohl auf unterschiedliche Kriminalitätsbelastungen als auch auf divergierende Ermittlungs- und Erfassungspraxen zurückzuführen sein könnte.

Zusammenfassend lassen sich anhand der vorliegenden Daten keine realistischen Einschätzungen dazu ableiten, wie viele Straftaten tatsächlich in den betrachteten Jahren begangen wurden und auch keine belastbaren Schlüsse über das Dunkelfeld ziehen. Die einbezogenen statistischen Daten basieren auf unterschiedlichen Erfassungsmodellen. Dies führt dazu, dass dieselbe Straftat unter Umständen in

[138] Daten im Aufgabenspektrum der Bundespolizei werden in der Polizeilichen Eingangsstatistik der Bundespolizei (PES) erfasst. Diese statistischen Daten werden auf im Gegensatz zur PKS auf Grundlage des Feststellungsprinzips (Meldeprinzips) erhoben, weswegen auch diese Daten aufgrund der unterschiedlichen Erfassungskriterien nicht vergleichbar sind. Im vorliegenden Kontext liegen keine auswertbaren Daten der Bundespolizei vor.

mehreren Statistiken auftauchen kann oder sogar unberücksichtigt bleibt, je nachdem, wie das Verfahren geführt wird.

Es kann primär Folgendes festgehalten werden,

- Die Datenlage ist insgesamt heterogen und lückenhaft. Aufgrund der unterschiedlichen Erfassungsarten der geführten Statistiken ist eine einheitliche Bewertung sowie ein Vergleich nur schwerlich möglich.
- Die erfassten Fälle der Geldwäsche und Terrorismusfinanzierung spiegeln wohl nicht den angenommenen gesamtgesellschaftlichen Umfang wider. Dies deutet auf ein sehr großes Dunkelfeld hin, so dass eine dezidierte Dunkelfeldforschung notwendig wäre.
- Es bedürfte einer einheitlichen Erfassung aller Geldwäsche- und Terrorismusfinanzierungstaten. Dies gilt selbst dann, wenn die Taten nur im Zusammenhang mit anderen Taten aufgetreten sind.
- Es bedürfte zudem einer flächendeckenden Erfassung des jeweiligen Schadens durch die einzelnen Taten.

5.1.2 Geldwäsche und Terrorismusfinanzierung bei Nutzung von Kryptowerten

Seit der verstärkten öffentlichen Aufmerksamkeit für Kryptowerte steht naturgemäß auch deren kriminelle Nutzungen im Fokus von Praxis und Forschung. Ein zentraler Untersuchungsaspekt war deshalb die Frage, in welchem Umfang Kryptowerte als Tatmittel in Verfahren der Geldwäsche und Terrorismusfinanzierung überhaupt eingesetzt werden. So kann, aufgrund der beschriebenen Begünstigungsfaktoren, ggf. von einem erheblichen Umfang ausgegangen werden. Genau aus diesem Grund wurde die Stärkung der Analyse, Aufsicht und Strafverfolgung bei den spezifischen Risiken durch neue Technologien als eine der Grundstrategien zur zukünftigen Bekämpfung der Geldwäsche und Terrorismusfinanzierung ausgerufen.[139] Nicht ohne Grund klassifiziert auch die FIU, wie besehen, die Geldwäsche unter Verwendung von Kryptowerten als neuen Schwerpunkt.[140]

[139] BMF, Strategie gegen Geldwäsche und Terrorismusfinanzierung, Sicherheit 2019, S. 15.
[140] FIU, Jahresbericht 2024, S. 15ff.

In den bestehenden Statistiksystemen erfolgt allerdings keine systematische Erfassung des Krypto-Bezugs bei Straftaten. Eine fundierte Datenlage liegt mithin nicht vor, ist allerdings für die Entwicklung von Bewältigungsstrategien unabdingbar.

5.1.2.1 Statistische Erhebung bei den Ermittlungsbehörden

Aus diesem Grund erfolgte im Rahmen des Forschungsprojekts eine Erhebung bei den Ermittlungsbehörden selbst. Allerdings konnte die Mehrheit der angefragten Behörden ebenfalls keine belastbaren statistischen Angaben zum Einsatz von Kryptowerten als Tatmittel machen, weil dies zum großen Teil intern nicht erfasst wird.

Eine Ausnahme hiervon bilden das LKA Niedersachen, welches in den Deliktsbereichen der Geldwäsche und der Terrorismusfinanzierung den Anteil der Fälle mit Bezug zu Kryptowerten festhält.[141] Das LKA Schleswig-Holstein auf der anderen Seite erfasst das Tatmittel nur bei den Fällen der Terrorismusfinanzierung[142], das BKA wiederum nur bei den Geldwäscheverfahren. So wurden im BKA in den Jahren 2023 und 2024 insgesamt sechs Ermittlungsverfahren wegen des Verdachts der Geldwäsche gemäß § 261 StGB bearbeitet, bei denen durch die beschuldigten Personen (auch) Kryptowährungen genutzt wurden. Das LKA Mecklenburg-Vorpommern erfasst nur die Sachverhalte der Geldwäscheverdachtsanzeigen, bei denen Kryptowerte als Tatmittel eingesetzt werden. Das LKA Mecklenburg-Vorpommern hat im Jahr 2023 ganze 28 Sachverhalte von insgesamt 1.127 GWVM und im Jahr 2024 wiederum 35 Sachverhalte von insgesamt 1.071 GWVM erfasst, bei denen Kryptowerte als Tatmittel zum Einsatz kamen.[143] Das LKA Hessen hält auf der anderen Seite lediglich eine Erfassung basierend auf den Ersuchen mit Kryptowährungsbezug vor. Hiernach konnten im Jahr 2023 in mindestens 17 Fällen der Geldwäsche und in mindestens drei Fällen der Terrorismusfinanzierung und im Jahr 2024 in mindestens 37 Fällen der Geldwäsche und in mindestens vier Fällen der Terrorismusfinanzierung entsprechende Bezüge festgestellt werden.

[141] Das LKA Niedersachsen gab in seiner Antwort auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. dazu allerdings – aus ermittlungstaktischen Gründen – keine konkreten Fallzahlen an, benannte den Anteil aber als vergleichsweise gering.
[142] Eine Mitteilung der konkreten Zahlen erfolgte allerdings nicht.
[143] Antwort auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch das LKA Mecklenburg-Vorpommern.

5.1.2.2 Einschätzungen der Ermittlungsbehörden

Mangels einer durchgehenden statistischen Erhebung wurden die angefragten Behörden um eine fundierte Einschätzung dahingehend gebeten, in welchem Umfang Kryptowerte für die Geldwäsche und/oder Terrorismusfinanzierung genutzt werden.

Eine solche Bewertung war vielen Behörden nicht möglich.[144] Die getätigten Auskünfte sind zudem nicht homogen: Die Spannweite reicht dabei von 10 bis 30%[145] über ein Drittel[146], bis hin zu „einer Vielzahl von Fällen“[147]. Ein Dunkelfeld wird bspw. durch das LKA Bremen und Mecklenburg-Vorpommern angenommen. Das LKA Hamburg geht wiederum von einem erhöhten, das LKA Hessen sowie das BKA von einem hohen und das LKA Nordrhein-Westfalen sogar von einem erheblichen Dunkelfeld aus. Hinsichtlich der Terrorismusfinanzierung wird durch das LKA Hessen nur von einem moderaten Dunkelfeld ausgegangen.

Insgesamt ist ein erhebliches Problem durch die mangelhafte Erfassung in den Behörden erkennbar. Die Heterogenität zeigt zudem, dass selbst die Ermittlungsbehörden derzeit keine genaue Kenntnis über diesen Phänomenbereich haben, hierzu aber in die Lage versetzt werden müssten.

5.1.2.3 Einschätzung der FIU

Im aktuellen FIU-Jahresbericht[148] wurde das Thema „Kryptowerte“ als Schwerpunktthema einer Sonderauswertung behandelt. Die FIU stellt fest, dass die Anzahl der Verdachtsmeldungen mit Bezug zu Kryptowerten in den letzten Jahren signifikant angestiegen ist. Dieser Trend spiegelt die zunehmende Relevanz digitaler Vermögenswerte im Bereich der Geldwäsche und Terrorismusfinanzierung wider. Die FIU unterstreicht die wachsende Bedeutung von OSINT für die Aufklärung und Verfolgung von Geldwäsche- und Terrorismusfinanzierungsfällen mit Krypto-Bezug.

[144] Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch die LKÄ Berlin, Rheinland-Pfalz, Sachsen, Sachsen-Anhalt, Thüringen und die LPD Saarland sowie das ZKA samt ZFD.
[145] Antwort auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch das LKA Bayern
[146] Antwort auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch das LKA Schleswig-Holstein.
[147] Antwort auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch das LKA Brandenburg.
[148] Vgl. FIU, Jahresbericht 2024, S. 16-23.

Ein zentrales Ergebnis der FIU-Sonderauswertung ist, dass die Erkennung und Bearbeitung von krypto-bezogenen Geldwäscheverdachtsfällen besondere analytische und technische Kompetenzen erfordert. Die FIU empfiehlt daher, die Erfassung von Krypto-Bezug in den Meldesystemen zu standardisieren und die Auswertungskapazitäten – insbesondere im Bereich OSINT und Blockchain-Analyse – weiter auszubauen. Zudem sieht die FIU einen erheblichen Entwicklungsbedarf bei der OSINT-Kompetenz der Ermittlungsbehörden und empfiehlt, sowohl die technische Infrastruktur als auch die Aus- und Fortbildung in diesem Bereich gezielt zu stärken. Die FIU betont zudem, dass die Zusammenarbeit mit anderen Behörden und internationalen Partnern im Bereich Kryptowerte intensiviert werden muss, um grenzüberschreitende Geldwäsche- und Terrorismusfinanzierungsstrukturen wirksam zu bekämpfen.

5.1.2.4 Zwischenbewertung

Die unterschiedlichen Datenquellen verdeutlichen die fehlende Standardisierung der statistischen Erhebung und erschweren jede valide Vergleichbarkeit. Aufgrund der niedrigen Fallzahlen in den jeweiligen Deliktsfeldern und der gleichwohl bestehenden Einschätzung der Praxis, ist davon auszugehen, dass viele relevante Finanzierungsströme unerkannt bleiben. Denn das Erkennen ebendieser erfordert spezialisierte technische und analytische Kompetenzen im Bereich der Blockchain-Analyse.

Geldwäsche ist ein vielschichtiges Phänomen und tritt in den verschiedensten Erscheinungsformen auf. Der Modus Operandi wird an die sich stetig ändernden wirtschaftlichen und rechtlichen Rahmenbedingungen angepasst. So ist es deliktsimmanent, dass die Vermögenswerte häufig über unterschiedliche Wege verschleiert und in den legalen Wirtschaftskreislauf zurückgeführt werden. „Klassische“ bekannte Wege sind das Waschen mit Hilfe von sog. Bargeldkurieren, im Rahmen von Immobiliengeschäften[149] im In- und Ausland oder über Finanzagenten. Für die Arbeit der Strafverfolgungsbehörden stellt der Einsatz von Kryptowerten aber eine besondere Herausforderung dar. So ergibt sich aus der Erhebung, dass zahlreiche Ermittlungsbehörden davon ausgehen, dass der Einsatz von Kryptowerten im Kontext

[149] Zu den Auswirkungen der Gelwäsche auf den Immobiliensektor siehe bspw. *Neuenkirch/von Auer/El-Ghazi/Hoffmann/Jansen/Klotz/Seidel/Walz*, Geldwäsche und deren Auswirkungen auf Immobilienpreise in Deutschland, Studie trigeko, 2025.

der Geldwäsche zunehmen und weiter an Bedeutung gewinnen oder gar eine zentrale Tatbegehungsweise darstellen wird.[150]

Bei der Betrachtung der Terrorismusfinanzierung müssen sich die Strafverfolgungsbehörden zudem mit den Typologien und Indikatoren, welche auf eine Finanzierung terroristischer Organisationen hindeuten, befassen. Dies kann demnach die direkte Unterstützung von Terrorismus (wie die Finanzierung von Anschlägen) als auch die indirekte Unterstützung (bspw. Propaganda, Rekrutierung, Ausbildung und Reisen) umfassen. Zudem können die Mittel sowohl aus illegalen als auch aus legalen Quellen stammen, durch verschiedene Kanäle bewegt werden und für verschiedene Zwecke wie Ausbildung, Materialien oder den Kauf von Ausrüstung Verwendung finden.[151]

Genau diese Faktoren machen die Ermittlungen der Geldwäsche und der Terrorismusfinanzierung so anspruchsvoll. So gibt es nicht das einzelne „Alarmzeichen“ (Red Flag) für illegale Aktivitäten. Es gilt vielmehr eine Vielzahl von Entitäten zu berücksichtigen, einschließlich der finanziellen Geschichte einzelner Akteure und des Kontexts von analysierten Transaktionen, bevor feststellbar ist, ob ein Verhalten oder eine Transaktion verdächtig erscheint.

Obwohl die Ermittlungskompetenzen und personellen Ressourcen im Bereich der digitalen Finanzermittlungen stetig ausgebaut werden, bleiben zudem die Herausforderungen für die Strafverfolgungsbehörden vor dem Hintergrund der täterseitigen Anpassung an die technischen Entwicklungen des Kryptomarktes auf einem hohen Niveau. Die beschriebenen Begünstigungsfaktoren machen Kryptowerte weiterhin zu einem lukrativen Vehikel für die Geldwäsche und Terrorismusfinanzierung.

Es können primär drei Dinge festgehalten werden:

- Die Datenlage ist insgesamt heterogen und lückenhaft. Ein zentrales Problem stellt die fehlende systematische Erfassung des Krypto-Bezugs in bestehenden Statistiksystemen dar. Nur wenige Polizeibehörden führen eigenständige

[150] Entsprechende Ausführungen erfolgten in den Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch das LKA Niedersachen und durch das Zollkriminalamt.
[151] Siehe zur Bedeutung der Bekämpfung der Finanzierung des Terrorismus: *Weisser*, ZIS 2013, 343ff.

Erhebungen durch, andere beschränken sich auf Schätzwerte oder können gar keine Angaben machen. Hierdurch wird der Phänomenbereich durch die Praxis nur unzureichend erfasst.

- Gerade vor dem Hintergrund der anzunehmenden, steigenden Relevanz von Kryptowerten im Kontext krimineller Finanztransaktionen zeigt sich ein struktureller Reformbedarf in der statistischen Erfassung. Ansonsten besteht das Risiko, dass operativ wichtige Entwicklungen nicht oder zu spät erkannt werden.
- Das Dunkelfeld des Einsatzes von Kryptowerten in den genannten Deliktsfeldern ist wohl erheblich, wie von mehreren Behörden explizit betont wird. Allerdings bedarf es einer weiteren Erforschung der Dunkelfeldentwicklung in den letzten Jahren.

5.2 Einsatz von OSINT im Rahmen der Ermittlungen

Trotz der bereits genannten Begünstigungsfaktoren bieten Kryptowerte der Strafverfolgung aber auch neue Ansatzpunkte. Die meisten öffentlichen Blockchains fungieren als transparente, dezentrale Buchungssysteme, in denen alle Transaktionen dauerhaft gespeichert sind. Im Gegensatz zu Bargeldflüssen, die sich nur schwer zurückverfolgen lassen, sind Krypto-Transaktionen – wie beschrieben – zwar pseudonym, grundsätzlich aber in der Blockchain nachvollziehbar. Hier bietet die Open Source Intelligence vielversprechende Ermittlungsansätze. So können beispielsweise von der Auswertung öffentlich einsehbarer Transaktionsdaten bis hin zu Social-Media-Profilen wertvolle Hinweise gewonnen werden, um die Kryptowerte realen Personen zuzuordnen.

Aufgrund der potenziellen Einsatzmöglichkeiten in der Ermittlungsarbeit galt es zu untersuchen, ob und wenn ja in welchem Umfang die Ermittlungsbehörden dieses Vehikel bereits in der Praxis nutzen.

Im Rahmen der durchgeführten Untersuchung stellte sich heraus, dass ein Großteil der teilnehmenden Ermittlungsbehörden OSINT als Ermittlungsinstrument bei Geldwäsche- und Terrorismusfinanzierungsverfahren grundsätzlich einsetzt. Dies gilt insbesondere für den Bereich der Terrorismusfinanzierung, wo OSINT mittlerweile als etabliertes

Standardinstrument betrachtet wird.[152] Auch bei Geldwäscheermittlungen wird OSINT vielfach als bewährtes Werkzeug angesehen[153], wenngleich einige Behörden betonen, dass der Einsatz vor allem bei „werthaltigen“ oder komplexeren Sachverhalten erfolge.[154]

Mit Blick auf Sachverhalte, in denen Kryptowerte verwendet wurden, zeigt sich ein differenzierteres Bild: Einige Landeskriminalämter berichteten von einer Einbindung spezialisierter OSINT-Verfahren unter Nutzung blockchainanalytischer Werkzeuge.[155] Die Anwendung erfolgt hier teilweise durch spezialisierte Fachdienststellen.[156] Andere Behörden beschränken sich derzeit auf frei zugängliche OSINT-Tools, ohne dass eine systematische Nutzung im Bereich kryptobasierter Straftaten etabliert ist.[157] Einzig das Bundeskriminalamt machte aus ermittlungstaktischen Gründen keine Angaben.

Die Rückmeldungen lassen insgesamt auf eine breite, aber unterschiedlich intensiv ausgeprägte Nutzung von OSINT im Kontext finanzbezogener Ermittlungen schließen, wobei insbesondere die Kombination aus OSINT und Kryptoanalyse an Relevanz gewinnt. Wie und insbesondere in welchem Umfang OSINT eingesetzt wird, ist dabei bei den Ermittlungsbehörden in Deutschland vollkommen unterschiedlich ausgestaltet.

5.3 Strategische Bedeutung von OSINT als Ermittlungsinstrument

Zur Einordnung der strategischen Relevanz von OSINT in der Praxis wurden die Ermittlungsbehörden gebeten, die Bedeutung dieses Instruments auf einer Skala von 0 bis 5 zu bewerten. Die Einschätzungen sind in der nachstehenden Übersicht zusammengefasst:

[152] Beispielsweise Antwort auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch das LKA Berlin: OSINT wird regelmäßig im Bereich der Terrorismusfinanzierung eingesetzt; ist in diesem Bereich „Standard“.
[153] Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch LKA Berlin, LKA Bayern, LKA Hessen, LKA Niedersachsen, LPD Saarland, LKA Schleswig-Holstein, LKA Thüringen und Zollkriminalamt.
[154] Antwort auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch das LKA Baden-Württemberg: OSINT-Nutzung bei werthaltigen Sachverhalten; bei Geldwäsche nur selten.
[155] Antwort auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch das LKA Hessen: Bei OSINT mit Krypto-Bezug werden spezialisierte Blockchain-Analystetools genutzt.
[156] Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch das LKA Berlin und das LKA Sachsen-Anhalt: Hinweis auf spezialisierte Fachdienststellen bei Verwendung von Kryptowerten.
[157] Antwort auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch das LKA Brandenburg: Nur Nutzung von frei zugänglichen OSINT-Tools; jedoch keine grundsätzliche Nutzung.

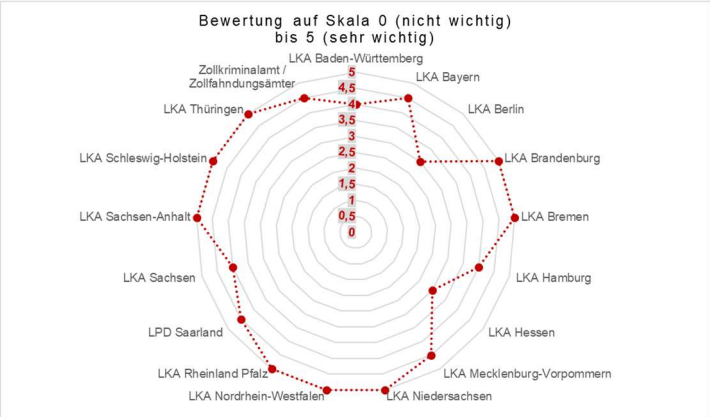

Abb. 23: Bewertung des Instruments OSINT[158]

Die Bewertung von OSINT als Ermittlungsinstrument fällt mithin durchweg positiv aus. Mit einem Mittelwert von 4,5 auf einer Skala von 0 bis 5 ist klar: OSINT hat sich als unverzichtbares Werkzeug etabliert, insbesondere in Fällen mit Krypto-Bezug.

Begrüßenswert ist, dass OSINT bereits bei allen Ermittlungsbehörden als Ermittlungsinstrument Einzug gehalten hat, die Bedeutung als besonders signifikant eingeschätzt wird und erste Schritte hinsichtlich einer Spezialisierung unternommen werden. Trotz dieser positiven Entwicklung gibt es aber auch Herausforderungen. Die Nutzung von Kryptowerten im Bereich der Geldwäsche und Terrorismusfinanzierung (z.B. die Nutzung von „no-KYC crypto exchanges[159]“) stellt eine besondere Erschwernis für OSINT-Ermittlungen dar. Kryptowerte und pseudonyme Transaktionen können es sehr schwierig machen, die Quellen und Ziele von illegalen Finanzströmen zu ermitteln. OSINT-Ermittler müssen spezialisierte Tools und Techniken entwickeln, um digitale Assets in einer Weise zu verfolgen, die über klassische öffentlich zugängliche Quellen hinausgehen, etwa durch technische Blockchain-Analyse oder die Auswertung von Darknet-Inhalten. Die Nutzung unregulierter Kryptobörsen, die keine KYC-Anforderungen haben, stellt OSINT-Ermittler zudem vor zusätzliche Herausforderungen, da diese Plattformen es Nutzern ermöglichen, nahezu anonym zu handeln. OSINT-Analysten müssen sich mit der Identifizierung solcher Plattformen und deren Benutzer befassen und gegebenenfalls alternative Quellen wie Blockchain-Explorer und Darknet-

[158] Das BKA hat aus ermittlungstaktischen Gründen keine Bewertung abgegeben und wurde daher nicht berücksichtigt.
[159] No-KYC-Crypto-Exchanges sind Kryptowährungsbörsen, die es Nutzern ermöglichen, Kryptowährungen zu handeln, ohne eine Identitätsprüfung (Know Your Customer, KYC) durchlaufen zu müssen.

Quellen hinzuziehen. Änderungen in der Gesetzgebung und Regulierung, wie z.B. die Verschärfung der Vorschriften für die Kryptoverwahrung oder neue Meldepflichten, könnten dazu führen, dass bestimmte Informationen leichter zugänglich werden. Für OSINT-Ermittler bedeutet dies, dass sie sich ständig über gesetzliche Änderungen auf dem Laufenden halten müssen, um ihre Suchstrategien und Datenquellen anzupassen. Zudem müssen sie in einem zunehmend komplexer werdenden Umfeld arbeiten, in dem die klassische Quellenanalyse nicht mehr ausreicht. Dies erfordert den Zugriff auf digitale und oft schwer nachvollziehbare Daten sowie den Einsatz von neuen Technologien (wie Blockchain-Analysewerkzeugen) und die Anpassung ihrer Methoden an die sich schnell ändernden Rahmenbedingungen.

Ein weiterer entscheidender Aspekt ist die Aufbereitung der Ergebnisse aus OSINT-Ermittlungen. Diese muss so gestaltet sein, dass sowohl staatsanwaltschaftliche Dezernentinnen und Dezernenten als auch die Gerichte die gewonnenen Erkenntnisse nachvollziehen und in den Kontext der jeweiligen Ermittlungsverfahren einordnen können. Nur wenn die Analyse klar, verständlich und transparent präsentiert wird, kann OSINT seine volle Wirksamkeit entfalten und zur rechtssicheren Entscheidungsfindung beitragen.

Es kann mithin festgehalten werden, dass OSINT seitens der Ermittlungsbehörden als Ermittlungsvehikel als signifikant wichtig eingestuft wird. Die Wirksamkeit hängt aber stark von der technischen und personellen Ausstattung sowie von der internen Organisation ab.

5.4 Nutzung spezialisierter OSINT-Werkzeuge und Ressourcen

Um ein genaueres Bild über den Einsatz von OSINT als Ermittlungsvehikel zu erhalten, ist es von besonderer Bedeutung auch einen Blick auf die vorhandene OSINT-Infrastruktur zu werfen. Denn eine effektive Nutzung ist nur möglich, wenn auch die technischen Gegebenheiten vorliegen. Aus diesem Grund wurde erhoben, ob die Ermittlungsbehörden frei verfügbare, eingekaufte oder eigens entwickelte Systeme verwenden.

Die Befragung zeigt, dass die Nutzung spezieller OSINT-Anwendungen bei den Ermittlungsbehörden verbreitet ist. Frei verfügbare Anwendungen kommen bei einem Großteil der teilnehmenden Landeskriminalämter zum Einsatz.[160] Einige Behörden nutzen zusätzlich oder ausschließlich eigens entwickelte, polizeiinterne Systeme mit speziellen Funktionalitäten für polizeiliche Anforderungen, beispielsweise die sogenannte „OSINT-Box“, die eine Kombination aus frei verfügbaren und polizeiinternen Tools darstellt.[161] Auch kommerzielle, eingekaufte OSINT-Anwendungen kommen bei mehreren Behörden zum Einsatz, wobei diese häufig ergänzend zu weiteren frei verfügbaren Tools eingesetzt werden.[162] Nur vereinzelt wurden derartige Anwendungen gar nicht verschafft.[163] Hinzu kommt, dass ein paar wenige Behörden aus ermittlungstaktischen Gründen keine Angaben machen konnten.[164]

Insgesamt kann festgehalten werden, dass die Nutzung spezieller Systeme und Anwendungen für OSINT grundsätzlich gegeben, aber sehr inkonsistent ist. Dabei lässt sich die Tendenz erkennen, dass frei verfügbare Tools weit verbreitet sind, aber naturgemäß nur begrenzte Funktionalitäten bieten. Eingekaufte Anwendungen wiederum kommen vor allem in größeren Bundesländern oder beim Zoll zum Einsatz.

Vielmehr erscheint es allerdings von besonderer Bedeutung deutschlandweit einheitliche oder zumindest vergleichbare Standards – etwa in Form eines zentralen Werkzeugkatalogs oder Mindestvorgaben für Schulungsinhalte – einzuführen. Dies könnte zu einer besseren Angleichung der behördlichen Fähigkeiten beitragen. Die vom BKA bereitgestellte OSINT-Box stellt grundsätzlich einen Schritt in die richtige Richtung dar, da sie zentrale Werkzeuge und standardisierte Rechercheumgebungen bündelt.

[160] Laut den Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. werden frei verfügbare Anwendungen genutzt durch: LKA Bayern, LKA Brandenburg, LKA Bremen, LKA Hamburg (OSINT-Box), LKA Hessen, LKA Mecklenburg-Vorpommern, LKA Nordrhein-Westfalen, LPD Saarland, LKA Sachsen (OSINT-Box), LKA Schleswig-Holstein, LKA Thüringen.
[161] Laut den Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. werden polizeiinterne Systeme (z.B. OSINT-Box) genutzt durch: LKA Hamburg, LKA Hessen, LKA Nordrhein-Westfalen, LKA Sachsen, LKA Sachsen-Anhalt, LKA Schleswig-Holstein, Zollkriminalamt/Zollfahndungsämter.
[162] Laut den Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. werden wiederum eingekaufte Anwendungen genutzt durch: LKA Baden-Württemberg, LKA Bayern, LKA Bremen, LKA Mecklenburg-Vorpommern, LKA Nordrhein-Westfalen, LKA Sachsen, LKA Sachsen-Anhalt, LKA Schleswig-Holstein, Zollkriminalamt/Zollfahndungsämter.
[163] Laut den Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. werden keine Systeme genutzt oder eine Antwort verneint durch: LKA Brandenburg (keine eingekauften Anwendungen, keine polizeiinternen Systeme), LKA Mecklenburg-Vorpommern (keine polizeiinternen Systeme).
[164] Durch das LKA Niedersachsen, die LPD Saarland und das Bundeskriminalamt wurden (aus ermittlungstaktischen Gründen) keine oder nur eingeschränkte Angaben gemacht.

Allerdings wird das Potenzial dieser zentralen Lösung derzeit von vielen Landesbehörden nur unzureichend ausgeschöpft. Stattdessen dominiert vielfach ein föderal geprägter individueller Ansatz, was zu einer fragmentierten OSINT-Infrastruktur führt. Diese Uneinheitlichkeit verhindert Synergien, erschwert den Wissenstransfer und steht der notwendigen Professionalisierung im Bereich digitaler Ermittlungen entgegen. Gegebenenfalls ist auch in diesem Fall neben einer föderalen Homogenisierung zumindest ein intensiver Austausch auf europäischer Ebene von besonderer Bedeutung. In einem dynamischen, grenzüberschreitenden Feld wie dem der Krypto-Kriminalität kann ein solches Nebeneinander lokaler Lösungen langfristig keine wirksamen Ergebnisse erzielen.

5.5 OSINT-Schulungen: Bestandsaufnahme, Professionalisierung und Entwicklungsbedarf

Ein weiterer Untersuchungsaspekt des Projekts betraf die Fortbildungspraxis bzgl. des Ermittlungsvehikels OSINT. Der Einsatz von neuartigen Ermittlungsmethoden bedarf einer effizienten und kontinuierlichen Schulung.

Bei der Untersuchung zeigte sich, dass die meisten Landeskriminalämter bereits eigene Fortbildungsangebote zu OSINT-Techniken etabliert haben und interne Schulungen durchführen.[165] Viele Behörden nutzen ergänzend die Fortbildungsangebote des Bundeskriminalamts, was auf eine koordinierte und standardisierte Qualifizierungsstrategie im Bundesgebiet hinweist.[166] Einige Behörden planen zudem, den Nutzerkreis der Schulungen zu erweitern oder neue Angebote zu implementieren.[167] Nicht alle Behörden verfügen allerdings über ein eigenes Fortbildungsangebot; vereinzelt greifen diese ausschließlich auf externe Schulungen zurück oder planen

[165] Laut den Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. bestehen eigene Fortbildungsangebote bzw. interne Schulungen bei: LKA Baden-Württemberg, LKA Bayern, LKA Berlin, LKA Brandenburg, LKA Bremen, LKA Hamburg, LKA Hessen, LKA Mecklenburg-Vorpommern, LKA Rheinland-Pfalz, LPD Saarland, LKA Sachsen, LKA Sachsen-Anhalt, LKA Schleswig-Holstein, LKA Thüringen.
[166] Laut den Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. werden die Fortbildungsangebote des BKA genutzt durch: LKA Bayern, LKA Berlin, LKA Brandenburg, LKA Bremen, LKA Hamburg, LKA Hessen, LKA Mecklenburg-Vorpommern, LKA Nordrhein-Westfalen, LPD Saarland, LKA Schleswig-Holstein.
[167] Laut den Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. werden Erweiterungen oder neue Angebote geplant durch: LKA Berlin (Erweiterung Nutzerkreis), Zollkriminalamt (interne Schulungen geplant).

diese, wie etwa das Zollkriminalamt, das aktuell externe Fortbildungen nutzt und interne Schulungen in Planung hat.[168]

Insgesamt verdeutlichen die Rückmeldungen, dass OSINT-Schulungen sowohl intern als auch extern verankert sind, jedoch hinsichtlich des Umfangs und Detaillierungsgrads variieren. Somit ist positiv hervorzuheben, dass bereits ein gewisser Professionalisierungsgrad besteht, jedoch auch ein klarer Bedarf an Koordination, Standardisierung und Ressourcenangleichung. Einheitliche Standards (z.B. Mindestumfang an Tools, Schulungsinhalte, zentrale Trainingszentren) könnten helfen, eine bundesweit gleichwertige Ermittlungsqualität sicherzustellen.

5.6 Rechtsrahmen und Anpassungswünsche zur Nutzung von OSINT in der Strafverfolgung

Vor dem Hintergrund des rechtlichen Rahmens des Einsatzes von OSINT wurden die Einschätzungen der Ermittlungsbehörden zum Änderungsbedarf bei der Nutzung von OSINT abgefragt. Die Ergebnisse zeigen ein vielschichtiges Bild, welches die aktuellen Herausforderungen und den Anpassungsbedarf in verschiedenen Bereichen verdeutlicht.

Eine Mehrheit der Behörden sieht in rechtlicher Hinsicht aktuell zumindest keinen akuten Änderungsbedarf.[169] Diese Position reflektiert offenbar die Einschätzung, dass die bestehenden rechtlichen Rahmenbedingungen und Eingriffsnormen ausreichend sind, um OSINT zweckmäßig und rechtssicher einzusetzen. Demgegenüber formulieren wiederum andere Behörden konkrete Anpassungswünsche oder -forderungen. So betont das LKA Bayern den Bedarf, die Beweiskraft von OSINT-Erkenntnissen in Strafverfahren zu stärken und schlägt die Abschaffung des Richtervorbehalts bei Datenanfragen nach § 100k StPO vor. Zudem wird eine generelle Flexibilisierung der rechtlichen Grundlagen gefordert, um mit den dynamischen Entwicklungen und grenzüberschreitenden Herausforderungen des Internets besser umgehen zu können.

[168] Laut den Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. haben kein eigenes Fortbildungsangebot oder ausschließlich externe Schulungen: LKA Nordrhein-Westfalen, Zollkriminalamt/Zollfahndungsämter.
[169] So die Antworten auf die Forschungsanfrage im Rahmen des Projekts G.E.K.O. durch: LKA Baden-Württemberg, LKA Brandenburg, LKA Hamburg, LKA Hessen, LKA Rheinland-Pfalz, LKA Sachsen-Anhalt, LPD Saarland, LKA Thüringen sowie das Zollkriminalamt samt Zollfahndungsdienst.

Das LKA Berlin und das LKA Nordrhein-Westfalen unterstreichen die Notwendigkeit, insbesondere die Mindestspeicherfrist für IP-Adressen im Bereich der Verkehrsdatenerhebung verbindlich umzusetzen. Dies spiegelt einen Fokus auf die Sicherung und Verwertbarkeit von digitalen Spuren im Rahmen der OSINT-Nutzung wider und wurde politisch aktuell bereits durch das BMI aufgegriffen, welches die zeitnahe Einführung einer Speicherpflicht für IP-Adressen plant.[170] Das LKA Bremen wünscht hingegen Anpassungen bei Abfragen von Benutzer- und Verkehrsdaten, um eine eindeutigere Verifizierung von OSINT-Informationen zu gewährleisten. Das LKA Mecklenburg-Vorpommern hebt den Änderungsbedarf bei der Identifikation von Pseudonymen in sozialen Netzwerken sowie bei Eingriffsnormen im Zusammenhang mit dem Einsatz ermittlungsunterstützender Künstlicher Intelligenz (KI) hervor. Auf der anderen Seite spricht sich das LKA Schleswig-Holstein für eine spezielle Eingriffsnorm für OSINT-Recherchen aus, um mehr Handlungssicherheit zu schaffen und fordert eine zentrale rechtliche Bewertung und Akkreditierung von OSINT-Tools.

Insgesamt lässt sich feststellen, dass der Änderungsbedarf vor allem an den Schnittstellen zu Beweiskraft, Datenspeicherung, Identifikation und der Integration neuer Technologien (wie KI) gesehen wird. Während viele Behörden mit den bestehenden Normen zufrieden sind, mahnen einige eine Modernisierung und Flexibilisierung an, um den rechtlichen Rahmen an die technische und taktische Entwicklung der OSINT-Praxis anzupassen.

6 Verbesserungsmöglichkeiten

Die Analyse der aktuellen OSINT-Nutzung und Krypto-Ermittlungen offenbart, neben den soeben aufgeführten Anregungen der abgefragten Behörden, deutlichen Optimierungsbedarf sowohl bei der Infrastruktur als auch bei der rechtlichen und organisatorischen Einbindung. Die nachfolgenden Empfehlungen richten sich auf konkrete Handlungsfelder, um die Ermittlungsfähigkeit in diesem dynamischen Kriminalitätsfeld nachhaltig zu stärken, können gleichwohl aber nur beispielhafter Natur sein.

[170] https://www.handelsblatt.com/politik/deutschland/internetkriminalitaet-dobrindt-will-ip-adressenspeicherung-zeitnah-einfuehren/100149656.html (letzter Aufruf 01.09.25).

6.1 Lagebild

Um die Erfassung der Nutzung von Kryptowerten in Geldwäsche- und Terrorismusfinanzierungsverfahren deutlich zu verbessern, sollten bestehende Strukturen gezielt erweitert werden, mit möglichst geringem Mehraufwand für die Behörden. Dabei empfehlen sich folgende Maßnahmen:

6.1.1 Einheitliches Zusatzmerkmal „Krypto-Bezug“ in Vorgangsbearbeitungssystemen und Statistikmeldungen

In allen relevanten Vorgängen – unabhängig vom Delikt – sollte ein einziges, bundesweit einheitliches Merkmalsfeld „Krypto-Bezug vorhanden: Ja/Nein“ ergänzt werden. Dieses sollte bei der Erfassung im Vorgangssystem (z. B. Fallanlage bei Polizei oder Justiz) gesetzt und möglichst per Schnittstelle bei der Statistikmeldung automatisch übernommen werden.[171] In der Polizeilichen Kriminalstatistik wird beispielsweise – wie besehen – derzeit der Einsatz von Kryptowerten zur Tatbegehung noch nicht ausgewiesen. Dabei ist die statistische Erfassung von Tatvehikeln der PKS nicht fremd, wie man an der Erfassung von Messern als Tatvehikel bei Gewaltdelikten erkennen kann. Mit einem einheitlichen Merkmalsfeld ließe sich eine einfache und vergleichbare Datenbasis schaffen, ohne tiefgreifende Systemumstellungen oder neue Datenbanken einzuführen. In diesem Zusammenhang ist die generelle Aussagekraft der polizeilichen und justiziellen Statistiken zu verbessern.

6.1.2 Aufnahme der politischen Straftaten in die PKS

Wie oben dargestellt, erscheint eine vergleichbare statistische Erfassung von relevanten und vergleichbaren Themenfeldern für die Beurteilung eines Phänomenbereichs elementar notwendig. Dabei erscheint es widersinnig, dass Staatsschutzdelikte – und für die hiesige Betrachtung insbesondere die Terrorismusfinanzierung – aus der Polizeilichen Kriminalstatistik herausgenommen wurden. Vielmehr sollten einheitliche

[171] Dieser muss allerdings im Verlaufe des Verfahrens noch abgeändert werden können, da sich der Krypto-Bezug ggf. erst im späteren Verlauf des Verfahrens herausstellt.

Erfassungsvoraussetzungen existieren, was auch eine Vergleichbarkeit untereinander vereinfachen würde.

6.1.3 Zentrale Erfassungs- und Lagekompetenz bündeln

Für eine bessere Übersicht über den Phänomenbereich erscheint auch eine Bündelung der Erfassung- und Lagekompetenzen sinnvoll zu sein. Statt paralleler Einzelauswertungen sollte das BKA dauerhaft mit der konsolidierten Lagebildführung zum Thema „Krypto und illegale Finanztransaktionen“ betraut werden. Die Landesbehörden würden relevante Merkmale melden, das Lagebild entstünde zentral und könnte jährlich veröffentlicht werden, ähnlich dem Cybercrime-Lagebild.

6.1.4 Zunahme der europäischen Kooperation samt dem Aufbau eines föderal oder ggf. europäisch koordinierten Frühwarnsystems

Zudem bedarf es einer zunehmenden föderalen und europäischen Kooperation. So bestehen derzeit in jedem Bundesland sowie aber auch in jedem Mitgliedsstaat unterschiedliche Systeme zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung. Vielmehr bedürfte es aber einer Vereinheitlichung der Arbeitsweisen der einschlägigen Behörden, um bestehende Lücken zu schließen.[172] Dabei scheint insbesondere der Austausch sowie die Verschmelzung von präventiv- und repressiv arbeitenden Behörden von zunehmender Bedeutung. Die Schaffung der neuen europäischen Anti-Geldwäschebehörde AMLA war dabei ein bedeutender Schritt in die richtige Richtung.

Zu der erforderlichen Harmonisierung gehört ferner aber auch die Einführung eines effektiven Frühwarnsystems. Neue Entwicklungen – z. B. der Einsatz bestimmter Coins, Mixing-Dienste oder „no-KYC“-Börsen – müssen erkannt und bewertet werden. Ein mindestens föderal, am besten aber europaweit, koordiniertes Frühwarnsystem sollte Trends aus verschiedenen Quellen (OSINT, Blockchain-Analytik, Verdachtsmeldungen, Ermittlungsverfahren) bündeln. Hierzu sollte ein Austauschformat unter Federführung

[172] https://www.tagesschau.de/wirtschaft/finanzen/geldwaesche-amla-szego-100.html (letzter Aufruf: 01.09.25).

des BKA bzw. der AMLA eingerichtet werden, in dem relevante Beobachtungen regelmäßig strukturiert zusammengetragen und an die anderen Ermittlungsbehörden multipliziert werden. Beispielsweise sollte erfasst werden, ob bekannte oder neuartige Vehikel oder Vorgehensweisen genutzt wurden. Dadurch wird zum einen die Quantität erfasst, aber zugleich auch ein Hinweis auf technologische Weiterentwicklung oder Neuerungen gegeben.

6.2 OSINT-Infrastruktur

Die Analyse zeigt zudem deutliche strukturelle Schwächen in der OSINT-Infrastruktur der Ermittlungsbehörden. Um der zunehmenden Relevanz von Open Source Intelligence insbesondere im Kontext digitaler und kryptobasierter Finanzermittlungen gerecht zu werden, sind zahlreiche Verbesserungsmaßnahmen zu erwägen.

6.2.1 Zentralisierung und Standardisierung

Die föderal zersplitterte Werkzeuglandschaft sollte durch einheitliche, bundesweit nutzbare OSINT-Standards – insbesondere solcher mit erweiterten Funktionen für Blockchain- und Kryptoanalyse – ergänzt werden. Die OSINT-Box des BKA ist hierfür ein sinnvoller Ausgangspunkt, der jedoch vermehrt in die Praxis der Länderbehörden integriert werden sollte. Dies impliziert einen PDCA-Zyklus[173], denn Tools und Vorgehensweisen sind angesichts der Innovationsgeschwindigkeit praktisch fortwährend hinsichtlich Eignung und Wirksamkeit zu hinterfragen.

6.2.2 Ausbau interoperabler Schulungskonzepte

Wie besehen, ist auch der Fortbildungsstand je nach Behörde sehr unterschiedlich. Es sollten bundesweit einheitliche Mindest-Schulungsstandards etabliert werden, ggf. im Rahmen eines Basiszertifikats für OSINT-Ermittler. Kooperationsformate wie länderübergreifende Trainingszentren könnten zusätzlich Synergieeffekte schaffen.

[173] PDCA-Zyklus: Ein kontinuierlicher Verbesserungsprozess bestehend aus den Phasen Plan (Planen), Do (Umsetzen), Check (Überprüfen) und Act (Handeln), der sicherstellt, dass Methoden und Werkzeuge fortlaufend auf ihre Eignung und Wirksamkeit überprüft und angepasst werden.

Ferner bedarf es aber einer statistischen Grundlage, aus welcher sich das Ausmaß ergibt. Dabei muss festgestellt werden, ob die derzeitigen Voraussetzungen zur Bewältigung der Herausforderungen überhaupt ausreichend sind. Erst im Anschluss stellt sich die Frage nach Kompetenzerweiterungen.

6.2.3 Förderung eines bundesweiten Krypto/OSINT-Netzwerks

Angeregt wird zudem der Aufbau eines bundesweiten und gegebenenfalls europaweiten Krypto/OSINT-Netzwerks. Eine vernetzte OSINT-Community innerhalb der Strafverfolgung – vergleichbar mit bestehenden Cybercrime-Zentren – könnte den informellen Austausch fördern, Fachwissen bündeln und Innovation beschleunigen. So besteht durch rein föderale Strukturen das Risiko der Ermittlungsredundanz, also womöglich zeitgleiche Ermittlungen bei gleichen Sachverhalten, wobei im ungünstigsten Fall dann die ohnehin unveränderlichen Daten einer Blockchain mehrfach analysiert bzw. ausgewertet werden. Geldwäsche und Terrorismusfinanzierung erfolgen im Kryptobereich zumeist länderübergreifend. Mithin können unterschiedliche Ermittlungsbehörden auf die gleiche Tätergruppierung oder womöglich wiederkehrende Wallets aufmerksam werden. Da im Kryptobereich insbesondere in der Anfangsphase der Ermittlungen häufig keine konkreten Personen bekannt sind, erscheint ein Rückgriff auf tradierte Systeme wenig hilfreich, da in diesen nur die Tatbeteiligten, nicht aber Strukturen abfragbar sind. Aus diesem Grund bedarf es eines detaillierten Austausches in einem Krypto/OSINT-Netzwerks, um auf gegebenenfalls längst vorhandene Daten und Erkenntnisse kurzfristig zugreifen zu können und etwaig vorhandene Zusammenhänge kontinuierlich zu ermitteln. Dabei bestehen in Deutschland bereits umfangreiche Strukturen und Kenntnisse, bspw. durch die Einheit „Sharks“[174] der FIU, welche ausgebaut und breiter zugänglich gemacht werden müssten.

6.2.4 Bessere Integration privater Analysewerkzeuge inkl. Austausch

Schlussendlich erscheint insbesondere die bessere Integration von privaten Analysewerkzeugen sinnvoll. Die enge Zusammenarbeit mit spezialisierten Anbietern

[174] Die Sharks sind eine Einheit der FIU und arbeiten auf Grundlage des Follow-the-Money-Ansatzes. Sie analysieren komplexe, häufig grenzüberschreitende Geldwäschestrukturen. Ihr Fokus liegt auf Mustern, Netzwerkverbindungen und neuen Begehungsformen, vgl. FIU, Jahresbericht 2024, S. 38.

(z. B. Blockchain-Analytics-Firmen) sollte strategisch geplant und finanziell unterstützt werden, um technische Innovationssprünge nicht zu verpassen.

Darüber hinaus ist eine intensivere Vernetzung mit der Wirtschaft, insbesondere mit Compliance-Officern, von zentraler Bedeutung. Diese Fachkräfte bilden die erste Verteidigungslinie gegen Geldwäsche und Terrorismusfinanzierung, indem sie in Unternehmen präventive Maßnahmen etablieren und verdächtige Aktivitäten frühzeitig erkennen können. Aus Compliance-Sicht stellen die unternehmensinternen Compliance-Regeln – die von der Unternehmensleitung verantwortet und meist delegiert werden – wichtige „Auffangparagrafen“ dar, um Vermögen zu schützen und einen ordnungsgemäßen Geschäftsbetrieb sicherzustellen.

Im Gegensatz zu Strafverfolgungsbehörden unterliegen Unternehmen bei der Nutzung von OSINT weniger restriktiven rechtlichen Vorgaben, da hier etwaige Einschränkungen durch die Strafprozessordnung nicht greifen. Dies ermöglicht flexiblere und schnellere Analyseprozesse. Durch den gezielten Informationsaustausch zwischen Behörden, Compliance-Abteilungen und spezialisierten Anbietern können Auffälligkeiten besser identifiziert und Straftaten bereits im Vorfeld erschwert oder sogar verhindert werden. Die Förderung dieser Kooperationen ist somit ein wesentlicher Baustein einer effektiven Bekämpfung von Geldwäsche und Terrorismusfinanzierung im Kryptobereich.

6.3 Finanzierungsoptionen und strukturelle Lösungen für den Einsatz kostenintensiver OSINT-Tools

Die Finanzierung leistungsfähiger Blockchain-Analysetools stellt insbesondere kleinere Bundesländer vor große Herausforderungen. Zur Lösung dieses Problems sind zentralisierte Lizenzmodelle, der Aufbau überregionaler Analysezentren sowie die gezielte Nutzung europäischer Fördermittel geeignete Wege, um Effizienz und Gleichbehandlung im Zugang zu hochpreisigen Spezialtools sicherzustellen.

So würde sich eine Zentrale Beschaffung durch den Bund (BKA/BMI bzw. ZKA/BMF) anbieten. Um Kosten zu senken und überzählige Lizenzen zu vermeiden, sollte der Bund diese für besonders teure Tools (z.B. Blockchain-Analysetools) zentral beschaffen und bedarfsgerecht an die Polizeibehörden der Länder oder Schwerpunktdienststellen

weitergeben. Ähnlich wie bei anderen zentralen IT-Infrastrukturen kann das über bestehende Rahmenverträge gesteuert werden. Aus ökonomischer Sicht könnte aber auch beim Thema Kryptowerte hinterfragt werden, ob es betriebswirtschaftlich nicht geboten wäre, die Aufträge an private Dienstleister fremd zu vergeben. Auch wenn dies bezüglich einzelner Projekte tatsächlich kostengünstiger wäre, fehlt es allerdings häufig an der notwendigen Flexibilität. So ist es, insbesondere für komplexe Ermittlungsverfahren, von besonderer Bedeutung, dass die ermittelnden Personen sowie die technischen Unterstützungskräfte in einen stetigen Austausch eintreten. Die Erweiterung und Anpassung des jeweiligen Ermittlungsziels sowie die notwendige Fokussierung können am besten nur innerhalb fester Strukturen erfolgen.

Alternativ könnten zentrale Analyse-Hubs mit Zugriff auf kostenintensive Tools eingerichtet werden (z.B. in Form eines Kompetenzzentrums Digitalfinanzermittlungen beim BKA oder bei LKA-Zentralstellen). Länderbehörden reichen dort besonders komplexe Krypto-Cases ein, ähnlich wie bei bestehenden technischen Diensten. Das würde auch die Qualifikation und Nutzung der Tools konzentrieren und Qualitätsverluste vermeiden. Die Finanzierung wiederum könnte u. a. auch über die zahlreichen Förderprogramme der EU zur digitalen Kriminalitätsbekämpfung erfolgen (z. B. Internal Security Fund). Deutsche Behörden würden dabei gezielt Fördermittel abrufen, um den Aufbau einer nationalen Plattform für Blockchain-Forensik mitzufinanzieren, inklusive Lizenzen, Schulungen und Tool-Konsolidierung.

6.4 Koordination und Aufgabenbündelung

Der föderale Aufbau der Sicherheitsarchitektur führt derzeit dazu, dass jede Landespolizei ihre eigene OSINT-Infrastruktur, Tools und Ermittlungsstrategien entwickelt – mit dem Effekt fragmentierter Kompetenzen und reduzierter Schlagkraft in besonders komplexen Krypto-Fällen. Vor dem Hintergrund begrenzter Ressourcen und hoher technischer Anforderungen könnte daher ein Umdenken im Sinne arbeitsteiliger Schwerpunktbildung sinnvoll sein. Daneben erscheint die, bereits angesprochene, verstärkte Koordination sowie ein besserer Austausch auf EU-Ebene denkbar.

Eine Möglichkeit bestünde darin, dass sich die Länder innerhalb eines koordinierten Mechanismus auf bestimmte fachliche Schwerpunkte verständigen. So können

insbesondere kleinere Bundesländer von der Bereitstellung ganzer Ermittlungsteams (samt dem Aufbau von tiefgreifendem Know-how) sowie von der Anschaffung umfangreicher Hard- und Software befreit werden. Dies könnte durch eine Bildung von Schwerpunktabteilungen und im Wege einer bundeslandübergreifenden Verteilung, rechtlich flankiert durch die Schließung von Staatsverträgen erreicht werden. Die finanziellen Zuwendungen an diejenigen Länder, welche die Ermittlungen übernehmen, könnten zu einer weiteren Spezialisierung verwendet werden, während die zahlenden Länder finanziell insgesamt eher entlastet würden, da keine vollständige personelle und materielle Doppelstruktur mehr vorgehalten werden muss.

Sinnvoll wäre es, einen solchen strukturierten Zuständigkeitsverbund durch eine übergeordnete Koordinierungsebene – etwa über das BKA – zu begleiten. Notwendig ist dafür aber auch eine gewisse Flexibilisierung der bislang stark auf territoriale Zuständigkeit ausgerichteten Fallbearbeitung. So stößt die bisher übliche enge Fallzuständigkeit einzelner Landesbehörden bei transnationalen Krypto-Strukturen an ihre Grenzen und verhindert eine effiziente Bündelung von Expertise und Ressourcen.

Besonders umfangreiche Krypto-Ermittlungen (bspw. bei komplexen, internationalen Geldwäschenetzwerken) verlangen nach einer funktionalen anstatt einer strikt geografischen Zuständigkeit. Bund und Länder sollten daher aktiv neue Modelle arbeitsteiliger Schwerpunktbildung und kooperativer Ermittlungseinheiten prüfen.

6.5 Nutzung von Künstlicher Intelligenz im Rahmen von OSINT

Der Einsatz von Künstlicher Intelligenz (KI) samt deren gesamtgesellschaftlichen Auswirkungen und Gefahren bildet eine der größten Herausforderungen der Gegenwart. Die Ermittlungsbehörden sehen in ihr teilweise die Möglichkeit in neue Dimensionen der Ermittlungsarbeit vorzudringen und gleichzeitig aber auch die Möglichkeit, die auflaufenden Massendaten überhaupt noch abarbeiten zu können. Exemplarisch sei an dieser Stelle darauf hingewiesen, dass mit den aktuell vorhandenen, globalen Rechnerkapazitäten nicht einmal ein Echtzeit-Monitoring der Bitcoin-Blockchain möglich ist.[175] Der Einsatz von KI ist naturgemäß auch im Rahmen von OSINT-Tools verlockend

[175] *Aldridge*, Synthetic KYC: Detecting Irregularities and Money Laundering on Blockchains, https://dx.doi.org/10.2139/ssrn.4857706 (letzter Aufruf: 01.09.25).

und würde dazu führen, dass viele Ermittlungstätigkeiten durch Software, sogar zeitlich schneller, übernommen werden könnten.

Der Einsatz von Künstlicher Intelligenz zur Ermittlungsunterstützung in Strafverfahren eröffnet aber auch viele Problemstellungen. So stellten sich die Fragen, ob es einer gesonderten Ermächtigungsgrundlage bedarf, wie die menschliche Kontrolle auszusehen hat, welche Fehlertoleranz akzeptabel ist, welche datenschutzrechtlichen und europarechtlichen (bspw. KI-VO) Anforderungen zu erfüllen sind, wie der Anlernprozess ausgestaltet wird und woher die Daten stammen.[176] Insbesondere muss ein „racial bias“[177] verhindert oder zumindest bestmöglich reduziert werden.

Die Einführung von KI im Rahmen von OSINT-Ermittlungen wird unausweichlich sein, bedarf allerdings einer weiteren intensiven Forschung. Die Bundesrepublik Deutschland als demokratischer Rechtsstaat darf aber nicht nur die Potentiale, sondern muss auch die Risiken der Künstlichen Intelligenz berücksichtigen und die rechtsstaatlichen Grenzen wahren.[178]

6.6 Proaktive und disruptive Strafverfolgung als strategisches Leitbild

Die vorliegenden Untersuchungsergebnisse legen offen, dass klassische Ermittlungsstrukturen mit den dynamischen, international organisierten Erscheinungsformen digitaler Finanzkriminalität zunehmend an ihre Grenzen stoßen. Wie besehen, müssen die Ermittlungsbehörden deshalb rechtlich, personell, materiell und taktisch so ausgestattet werden, dass eine effektive Strafverfolgung auch bei stetig komplexer werdenden Verfahren mit regelmäßig bestehendem, internationalem Bezug möglich bleibt. Dabei erscheint es nicht mehr alleine ausreichend zu sein, neu auftretende Phänomenbereiche erst nach deren Entstehen zu bewerten und dann Bewältigungsstrategien zu entwickeln. Vielmehr ist es erforderlich, dass sich die Strafverfolgung vom reinen Reagieren hin zum Agieren bewegt. Dies umfasst zwei Teilbereiche.

[176] *Weisser,* FS A. Hartmann, 2024, S. 318.
[177] *Döbel/Leis/Molina Vogelsang/Neustroev/Petzka/Riemer/Rüping/Voß/Wegele/Welz*, Maschinelles Lernen. Eine Analyse zu Kompetenzen, Forschung und Anwendung, 2018, S. 48.
[178] *Ibold*, GSZ 2024, 10 (18).

Zum einen erscheint eine proaktive Strafverfolgung unabdingbar. So müssen die Behörden mit ministerieller bzw. senatorischer Begleitung regelmäßig aktiv die Frage aufwerfen, welche Bedrohungsszenarien in Zukunft zu erwarten sind sowie welche Ausstattung erforderlich erscheint, um den anstehenden Phänomenen zu begegnen, auch damit eine langfristige Anschaffungs- und Schulungsphase abgemildert werden kann.[179] Dies beinhaltet zunächst eine frühzeitige Bewertung zukünftiger Kriminalitätsfelder und zukünftiger Tatvehikel, u. a. durch einen fundierten Austausch mit anderen Ermittlungsbehörden und der Wirtschaft auf nationaler wie internationaler Ebene. Im Anschluss müssen Bewältigungsstrategien entwickelt und abgearbeitet werden.[180] Sollten rechtliche Lücken bestehen, ist bereits frühzeitig darauf hinzuwirken, dass diese geschlossen werden. Aufgrund der notwendigen Finanzmittel handelt es sich um eine politische Entscheidung. Anders als bei konventioneller Kriminalität besteht allerdings ansonsten das Risiko, dass neuartige Vehikel der Geldwäsche sowie Terrorismusfinanzierung derart komplex werden, dass eine immer länger werdende Reaktionsphase, ohne effektive Strafverfolgung, entstehen könnte.

Ferner erscheint das – ursprünglich für die Bekämpfung von Cybercrime – entwickelte Leitbild einer disruptiven Strafverfolgung auch für die Bekämpfung der Geldwäsche und Terrorismusfinanzierung mit Kryptowerten sinnvoll.[181] Gemeint ist ein Ansatz, der über die rein reaktive Verfolgung von Tatverdächtigen hinausgeht und gezielt auf die parallele, strukturelle Zerschlagung krimineller Infrastrukturen (sog. Infrastrukturansatz) und Finanzierungen (sog. Finanzansatz) abzielt.[182] Dies kann bspw. durch die Abschaltung illegaler (Krypto-)Plattformen sowie durch eine gezielte Kommunikationsstrategie zur Abschreckung in der Szene erfolgen. Die disruptive Strafverfolgung bedeutet damit nicht eine Abkehr vom Legalitätsprinzip, sondern eine zusätzliche Fokussierung auf proaktive, koordinierte und strukturorientierte Maßnahmen, um strafrechtlich schwer fassbare Tatkomplexe im digitalen Raum effektiv zu bekämpfen. Als konzeptioneller Rahmen für

[179] *Weisser,* FS A. Hartmann, 2024, S. 318.
[180] Naturgemäß kann es auch einmal dazu kommen, dass vermeintlich erkannte neue Kriminalitätsfelder oder Tatvehikel nicht erstarken und bereits Gelder investiert wurden. Dieses Risiko ist allerdings durch eine fundierte Bewertung reduzierbar. Zudem geht es zunächst um die Erstellung von Konzepten. Die tatsächliche Anschaffung von teurem Material oder die Aufstockung von Personal wird dann natürlich nur der letzte Schritt sein können. Derzeit vergeht in der Praxis allerdings bereits eine lange Zeit bevor neue Problemfelder erkannt und geeignete Konzepte entwickelt werden, so dass die Umsetzung der dann entwickelten Strategie noch weiter in den Hintergrund rückt.
[181] Bspw. entwickelt für die Bekämpfung von Cybercrime, aber inhaltlich übertragbar: BKA, Bundeslagebild Cybercrime 2024, S. 32ff.
[182] BKA, Bundeslagebild Cybercrime 2024, S. 32ff.

Folgeforschung und organisationsstrategische Weiterentwicklung sollte dieses Leitbild zunehmend mit Leben gefüllt werden.

Dies korrespondiert mit den Erkenntnissen aus dem vorliegenden Forschungsprojekt, insbesondere der Notwendigkeit, frühzeitig relevante Informationen aus offenen Quellen (OSINT) zu aggregieren, auszuwerten und strategisch nutzbar zu machen. Der Aufbau vernetzter OSINT-Strukturen innerhalb der Ermittlungsbehörden – etwa in Form einer nationalen Community mit interoperablen Werkzeugstandards – kann ein Baustein disruptiver Strafverfolgung sein, sofern er gezielt auf operative Wirksamkeit ausgerichtet ist.

7 Fazit / Ausblick

Zusammenfassend kann insgesamt festgehalten werden, dass Geldwäsche und Terrorismusfinanzierung mit Kryptowerten die Ermittlungsbehörden vor neuartige Herausforderungen stellen. So bieten Kryptowerte besondere Verschleierungsmöglichkeiten, da die Transaktionen grenzüberschreitend, pseudonym, dezentral und unter nur teilweiser Regulierung erfolgen. Gleichzeitig liefern sie aber auch selbst die Werkzeuge, um diese Problemstellungen anzugehen.

Die Ergebnisse des Forschungsprojekts zeigen, dass die bestehende Datenlage eklatant lückenhaft ist. Die derzeit bekannten Fälle der Geldwäsche und Terrorismusfinanzierung spiegeln wohl nicht den geschätzten Gesamtumfang dieser Deliktsfelder wider, so dass von einem erheblichen Dunkelfeld ausgegangen werden muss. Der Einsatz von Kryptowerten wird zudem in keiner amtlichen Statistik systematisch erfasst. Es hat sich herausgestellt, dass nur wenige Behörden eigene Erhebungen durchführen. Mithin haben die Ermittlungsbehörden über den Umfang und die Ausprägung der Phänomenbereiche nur sehr eingeschränkte Kenntnisse, was auch zu teilweise gänzlich unterschiedlichen Bewertungen führt. Die Spannbreite der Rückmeldungen – von „keine Angaben möglich“ bis zu Schätzungen von über 30% – belegt ein erhebliches Defizit an Standardisierung. Besonders kritisch ist das als mindestens hoch angenommene Dunkelfeld, auf welches fast alle Behörden hinweisen (vor allem in Bezug auf „no-KYC crypto exchanges“ und andere Verschleierungsmechanismen). Der tatsächliche Umfang illegaler Finanzströme bleibt

dadurch vielfach unerkannt. Die Ermittlungsarbeit ist mithin auf technisch spezialisierte Teams angewiesen, die jedoch vielerorts (noch) fehlen.

Die Befragungsergebnisse und ergänzenden Analysen zeigen allerdings insgesamt deutlich: Kryptowerte gewinnen als Tatmittel im Bereich der Geldwäsche und Terrorismusfinanzierung an praktischer Relevanz. Es muss von einem sehr hohen Dunkelfeld der Geldwäsche- und Terrorismusfinanzierung unter Verwendung von Kryptowerten ausgegangen werden.

Kryptowerte bieten aber auch ganz neue Ermittlungsansätze. So hat das Forschungsprojekt ferner ergeben, dass OSINT bereits in vielen Behörden zur Ermittlung eingesetzt wird, insbesondere im Bereich der Terrorismusfinanzierung. Aber auch bei Geldwäschefällen – v. a. in komplexeren Verfahren – kommt OSINT zunehmend zum Einsatz. Die Bewertung des Instruments fiel mit einem Durchschnittswert von 4,5 (auf einer Skala von 0 bis 5) sehr positiv aus. Gleichwohl zeigen sich strukturelle Defizite. So ist die Verfolgung von Straftaten im Zusammenhang mit Kryptowerten insbesondere technisch anspruchsvoll und erfordert spezialisierte Werkzeuge, wie beispielsweise Blockchain-Analyse-Tools und eine funktionierende internationale Zusammenarbeit.[183]

Derzeit sind die eingesetzten Tools, Schulungsangebote und rechtlichen Rahmenbedingungen aber teilweise uneinheitlich oder unzureichend standardisiert. Ein bundesweites OSINT-Netzwerk mit interoperabler Infrastruktur fehlt bisher. Die Wirksamkeit dieses Ermittlungsvehikels hängt stark von der technischen und personellen Ausstattung sowie der internen Organisation ab. Viele Behörden nutzen deshalb inzwischen eigene oder eingekaufte Anwendungen, teils über zentrale Angebote wie die vom BKA bereitgestellte „OSINT-Box“. Es zeigt sich jedoch eine starke Fragmentierung der eingesetzten Werkzeuge. Das Prinzip „jeder macht seins“ verhindert Synergien und schwächt die bundesweite Schlagkraft. Gleiches gilt für Fortbildungsangebote: Während viele Länderpolizeien interne Schulungen anbieten und BKA-Angebote nutzen, fehlt ein bundesweiter Mindeststandard für Inhalte, Tools und Methodik.

[183] Mitteilung des Senats zur kleinen Anfrage der Fraktion CDU vom 06.11.24, Bremische Bürgerschaft Drs. 21/924, S. 17.

Im Rahmen des Forschungsprojekts konnten ferner zahlreiche Empfehlungen erarbeitet werden. So sind beispielsweise die Einführung eines bundesweit einheitlichen Merkmals „Krypto-Bezug“ in polizeilichen und justiziellen Statistiken; die Bündelung der Lagebildkompetenz, die Einführung von flächendeckenden Schulungsstandards und Fortbildungsangeboten für OSINT-Ermittler; eine Koordinierung auf bundes- oder europarechtlicher Ebene, der Aufbau zentraler Analyse-Hubs oder lizenzfinanzierten Schwerpunktstellen für ressourcenintensive Tools sowie der Einsatz von künstlicher Intelligenz in OSINT-Verfahren denkbar.

Langfristig stellt sich zudem die Frage wie Strafverfolgung im digitalen Raum strategisch weiterentwickelt werden kann. Die Ansätze der proaktiven und disruptiven Strafverfolgung bieten hier ein mögliches Leitbild: Statt allein auf Einzelfälle zu reagieren, geht es darum, frühzeitig zu evaluieren, welche Bedrohungsszenarien in Zukunft auftreten werden und zudem kriminelle Infrastrukturen proaktiv zu stören, Kommunikationsräume zu schließen und technische Voraussetzungen gezielt zu schwächen. Eine effektive OSINT-Strategie kann hierfür ein zentrales Element sein, vorausgesetzt, sie wird institutionell, personell und rechtlich entsprechend verankert.

Die kriminalistische Realität digitaler Finanzdelikte fordert insgesamt ein Umdenken: Weg von isolierten Zuständigkeiten hin zu arbeitsteiliger Spezialisierung, moderner Technik und strategisch koordiniertem Vorgehen. Es besteht aber weiterer Investitionsbedarf in spezialisierte Schulungen, Werkzeuge und Kooperationen mit privaten Anbietern von Blockchain-Analyse-Tools und eines Aufbaus einer flächendeckenden OSINT-Community innerhalb der Ermittlungsbehörden.

Auch die rechtlichen Grundlagen der Einziehung bedürfen einer Weiterentwicklung, da die strafrechtliche Verfolgung stets im Zusammenspiel mit dem Geldwäschegesetz und den Einziehungsvorschriften zu sehen ist.[184] Diesbezüglich ist auch die aktuelle Forderung der Ständigen Konferenz der Innenminister und -senatoren der Länder sinnvoll, den Wortlaut der §§ 111c, 111f StPO sowie des § 73c StGB anzupassen, um trotz fehlenden privaten Schlüssels (Private Key) die Wertersatzeinziehung bei illegal erlangten Kryptowerten durchführen zu können.[185] Auch Verbesserungen in der

[184] MüKo/*Neuheuser* StGB, 4. Aufl. 2021, § 261 Rn. 1.
[185] IMK, 233. Sitzung vom 11. bis 13.06.25, Beschlüsse, TOP 36, Nr. 6.

Rechtshilfe sind unausweichlich. Der neue Entwurf zum Gesetz zur Umsetzung der Richtlinie (EU) 2023/1544 und zur Durchführung der Verordnung (EU) 2023/1543 über die grenzüberschreitende Sicherung und Herausgabe elektronischer Beweismittel in Strafverfahren innerhalb der Europäischen Union ist dabei ein Schritt in die richtige Richtung.

Trotz rechtlicher Nachschärfungen bleibt die effektive Umsetzung eine große Herausforderung. Dies gilt nicht nur wegen technischer und personeller Defizite, sondern vor allem auch wegen der professionellen und grenzüberschreitenden Natur geldwäsche- und terrorismusfinanzierungsrelevanter Kriminalität. Eine konsequente Bekämpfung erfordert nicht nur neue Gesetze, sondern ein funktionierendes Zusammenspiel aus präventiver Überwachung, datenbasierter Aufklärung und internationaler Kooperation. Eine weitere Säule stellt deshalb die Regulierung und Aufsicht dar. So muss bspw. die Koordination und Zentralisierung der Aufsichtsbehörden zur Bekämpfung von Geldwäsche im Nichtfinanzsektor verbessert werden.[186]

Zudem bedarf es in vielen Bereichen weiterhin einer dezidierten Forschung. Ein zentrales Forschungsdesiderat betrifft (neben dem Dunkelfeld) die Evaluierung bestehender OSINT-Werkzeuge und –Methoden in Bezug auf die Ermittlungen von Geldwäsche und Terrorismusfinanzierung mit Hilfe von Kryptowerten. In der Praxis zeigt sich eine erhebliche Heterogenität hinsichtlich der eingesetzten Tools, Analyseansätze und technischen Infrastrukturen. Viele Behörden greifen auf individuell entwickelte oder kommerziell zugekaufte Lösungen zurück, ohne dass bislang eine systematische Bewertung ihrer Wirksamkeit, Interoperabilität oder rechtlichen Belastbarkeit erfolgt ist. Gerade vor dem Hintergrund begrenzter Ressourcen und steigender technischer Anforderungen wäre es sinnvoll, in einer vergleichenden Analyse die Stärken und Schwächen gängiger OSINT-Werkzeuge unter realen Einsatzbedingungen zu untersuchen. Ziel sollte es sein, evidenzbasierte Standards zu entwickeln, die eine bessere Vergleichbarkeit, Austauschbarkeit und Skalierbarkeit ermöglichen, auch im Sinne einer bundesweit konsistenten Ermittlungsstrategie.

Ein weiterer Forschungsansatz liegt im Bereich der forensischen Analyse und digitalen Beweisführung bei Kryptowerten. Aufgrund der speziellen technischen Eigenschaften

[186] IMK, 233. Sitzung vom 11. bis 13.06.25, Beschlüsse, TOP 36, Nr. 4.

von Kryptowährungen – etwa der kryptografischen Absicherung und der dezentralen Struktur der Blockchain – stellen sich besondere Herausforderungen bei der gerichtsfesten Dokumentation und Verwertung von Beweismitteln. Es bedarf der Entwicklung und Etablierung von standardisierten Verfahren und technischen Protokollen, die sicherstellen, dass digitale Spuren nachvollziehbar, manipulationssicher und juristisch belastbar sind. Darüber hinaus sollten Untersuchungen klären, wie forensische Erkenntnisse aus Blockchain-Analysen im Prozess effektiv vermittelt und von Gerichten bewertet werden können, um Rechtssicherheit und Akzeptanz zu gewährleisten.

Ein letzter wichtiger Forschungsbereich betrifft die Vernetzung zwischen Strafverfolgungsbehörden und der Wirtschaft, insbesondere Compliance-Abteilungen. Unternehmen spielen eine zentrale Rolle bei der Prävention und Erschwernis von Geldwäsche- und Terrorismusfinanzierungshandlungen. Die effektive Einbindung privater Akteure in die OSINT-gestützte Ermittlungsarbeit erfordert jedoch klare rechtliche Rahmenbedingungen, vertrauensbildende Kooperationen sowie datenschutzkonforme Modelle des Informationsaustauschs. Forschungsbedarf besteht deshalb dahingehend, wie eine solche institutionalisierte Zusammenarbeit gestaltet werden kann, welche gesetzlichen Anreize oder Verpflichtungen zielführend sind und wie private Analysewerkzeuge und Ressourcen effizient genutzt werden können, ohne dabei die Unabhängigkeit und Integrität der Ermittlungen zu gefährden.

Insgesamt ist anzumerken, dass es eines Paradigmenwechsels in der Bekämpfung der Geldwäsche und Terrorismusfinanzierung mit Krypowerten bedarf. So drohen die Aufsichts- und Ermittlungsbehörden, trotz ihres erheblichen Einsatzes, zunehmend den Anschluss an neue digitale Entwicklungen zu verlieren, insbesondere, weil finanzielle Mittel nur eingeschränkt zur Verfügung stehen. Es muss verhindert werden, dass die Strafverfahren – aufgrund der enormen Datenmengen und komplexeren Strukturen – nicht mehr handhabbar werden. Ansonsten könnte es zu nicht mehr hinnehmbaren Verfahrensdauern kommen, was wiederum die Strafzwecke nihilieren könnte.[187]

[187] *Niemz*, Komplexitätsbewältigung in Großverfahren des Wirtschaftsstrafrechts, 2020, S. 13.

Impressum:

Jean Monnet Centre of Excellence
Crime Investigations and Criminal Justice (CCICJ)
an der Hochschule für Öffentliche Verwaltung Bremen
Doventorscontrescarpe 172 C / 28195 Bremen
Internet: https://www.hfoev.bremen.de/ccicj
Kontakt: Niclas.Weisser@hfoev.bremen.de

Über das CCICJ:

Das Jean Monnet Centre of Excellence Crime Investigations and Criminal Justice (CCICJ) ist ein Institut in der Hochschule für Öffentliche Verwaltung Bremen (HfÖV). Sein Ziel ist es, Wissen und Erkenntnisse zur Unterstützung der EU-Politikgestaltung zu generieren und die Rolle der EU in Europa und in einer globalisierten Welt zu stärken. Das CCICJ betreibt praxisorientierte Forschung insbesondere in den Bereichen Geldwäsche & Wirtschaftskriminalität, Opferschutz, Compliance, Steuern & Steuerkriminalität sowie innovative Technologien & Strategien.

Das EU-Programm Erasmus+ unterstützt Ausbildung, Bildung, Jugend und Sport in Europa. Die Erasmus+: Die Jean-Monnet-Exzellenzzentren sind Kompetenz- und Wissenszentren zu Themen der Europäischen Union. Sie bündeln die Expertise und Kompetenzen hochrangiger Expertinnen und Experten mit dem Ziel, Synergien zwischen den verschiedenen Disziplinen und Ressourcen der European Studies zu entwickeln.

Finanziert von der Europäischen Union