Kapitel I. Einführung

A. Prolog

> „[*Automated Suspicion Algorithms*] *assess individuals based on suspicion of criminal activity in that they engage in probabilistic predictions that rely on patterns detected in imperfect information.* [*They*] *automate the process of identifying suspicious individuals from data: they comb through data for factors that correlate to criminal activity, assess the weight of each factor and how it relates to other factors, use the results to predict criminality from new data, and continuously improve their performance over time.*"
>
> – M. Rich[8]

Stellen Sie sich vor, Sie möchten eine Überweisung tätigen, Ihr Konto wurde jedoch gesperrt. Nach Rückfrage bei Ihrer Bank wird die Überweisung am übernächsten Werktag ausgeführt und die Verzögerung mit technischen Problemen erklärt. Ein halbes Jahr später erhalten Sie wegen eben dieser Überweisung die Mitteilung der Staatsanwaltschaft über die Einleitung eines Ermittlungsverfahrens gegen Sie. Denn Ihre Überweisung wurde durch eine KI als verdächtig identifiziert. Ihre Bank hat daher aufgrund verpflichtender geldwäscherechtlicher Normen bezüglich Ihrer Überweisung eine Verdachtsmeldung gegen Sie erstattet, welche automatisch und ohne genauere Überprüfung an die zuständigen Behörden weitergeleitet wurde. Mit der Überweisung wollten Sie jedoch nur Geld an Ihre Tochter senden, die derzeit ein Auslandsstudium in Südamerika absolviert. Das Zukunftsszenario der KI-gestützten Verdachtsschöpfung mittels „*Automated Suspicion Algorithms*"[9] liegt derzeit weniger fern, als wir heute vielleicht meinen:

---

8 *Rich,* University of Pennsylvania Law Review 2016, 871 (876); der Begriff der *Automated Suspicion Algorithms* wurde für diese Arbeit von dem Aufsatz von *Rich* inspiriert und auf die nationalen Begebenheiten übertragen. Soweit ersichtlich, wurde der Begriff bisher einmalig im deutschen Kontext erwähnt bei: *Golla,* NJW 2021, 667 (672).

9 Näher zur Begriffsdefinition im Kontext dieser Arbeit: Kapitel I.D.V.

B. Einleitung

> *„Die Möglichkeiten, den Umfang der Geldwäscherei zuverlässig zu schätzen, sollten nicht zu hoch bewertet werden.* […]
> *Unsere Kenntnisse auf diesem Gebiet sind vergleichbar mit jenen des Archäologen, der mit Hilfe einiger Tonscherben, einer Speerspitze und eines Kieferreststückes die Wirtschaft einer Steinzeitsiedlung beschreiben muss.“*
> – P. van Duyne[10]

Schätzungen zufolge liegt das jährliche Volumen an gewaschenem Geld nach § 261 StGB allein in Deutschland bei 70-100 Milliarden Euro.[11] Diese Summe repräsentiert zwei bis drei Prozent des jährlichen Bruttoinlandsproduktes.[12] Innerhalb der EU und weltweit liegen die Zahlen Studien zufolge sogar noch deutlich höher.[13] Die Folgen für die Gesellschaft sind gravierend – einige Forschende sprechen von der (Mit-)Zerstörung des Planeten durch diese Art der Wirtschaftskriminalität.[14] In jedem Fall bedroht das

10 *van Duyne*, in: Friedrich-Ebert-Stiftung (Hrsg.), 1993, S. 52.

11 *Bussmann,* Geldwäsche-Prävention im Markt – Funktionen, Chancen und Defizite, 2018, S. 102 ff.; *Bussmann/Veljovic,* NZWiSt 2020, 417 (418); je nach Studie gehen die Schätzungen zum Dunkelfeld der Geldwäsche zwar auseinander, bewegen sich jedoch alle im hohen Milliardenbereich.

12 Diese Prozentzahlen beruhen auf einer Rechnung anhand des Bruttoinlandsproduktes (BIP) des Jahres 2018 nach Angaben des Statistischen Bundesamtes und stimmen mit offiziellen Schätzungen überein. Danach betrug das BIP 2018 3388 Milliarden Euro, *Statistisches Bundesamt*, Bruttoinlandsprodukt 2018 für Deutschland, 15. Januar 2019, (abrufbar: https://perma.cc/8BKN-6PB4, zuletzt abgerufen: 31.08.2024), S. 5. Davon sind 70-100 Milliarden Euro gerundet zwei bis drei Prozent. Da die Schätzungen des Dunkelfeldes bereits einige Jahre alt sind und das BIP (auch durch die Inflation) in den letzten Jahren deutlich angestiegen ist, muss davon ausgegangen werden, dass die tatsächlichen Verluste inzwischen weiter angestiegen sind. 2023 betrug das deutsche BIP beispielsweise 4121 Milliarden Euro, *Statistisches Bundesamt*, Volkswirtschaftliche Gesamtrechnungen, 2024, (abrufbar: https://perma.cc/FQ6N-TUJ7, zuletzt abgerufen: 31.08.2024). Sofern man weiterhin davon ausgeht, dass sich die jährlichen Verluste durch Geldwäsche auf zwei bis drei Prozent des BIP belaufen, würde dies inzwischen einer Summe von 80-120 Milliarden Euro entsprechen.

13 MONEYVAL hat als Komitee des Europarates zur Evaluation von AML-Maßnahmen das Dunkelfeld der Geldwäsche weltweit für 2022 etwa auf 500 Milliarden bis zu einer Billion Euro geschätzt, *MONEYVAL*, Annual Report 2022, (abrufbar: https://perma.cc/G8VJ-6BB4, zuletzt abgerufen: 31.08.2024); *Zuck,* NJW 2002, 1397 (1397).

14 *Boguslavska/Grossmann*, Corruption and money laundering are destroying the planet, (abrufbar: https://perma.cc/6Y5W-RWQX, zuletzt abgerufen: 31.08.2024); *Zypries,* ZRP 2024, 28 (28).

strafrechtliche Phänomen die Integrität unseres Finanzsystems, die Funktionsfähigkeit und Rechtstreue unserer Wirtschaft und den gesellschaftlichen Zusammenhalt insgesamt.[15] Die Methoden und Erscheinungsformen der Geldwäsche sind vielfältig und werden auf Täterseite permanent weiterentwickelt und an neue Bekämpfungsmethoden angepasst.[16] Die rasante internationale Regulierungswelle[17] der letzten Jahrzehnte in der Geldwäschebekämpfung hat ausweislich des nach wie vor hoch geschätzten Dunkelfeldes bisher nicht die erhofften Präventions- und Ermittlungserfolge erzielt. Insbesondere gehen kriminologisch-empirische Forschungen vor allem von einer ungleich verteilten Aufdeckung von Geldwäschetaten aus:[18] kleinere Taten werden aufgedeckt und ermittelt, die wirklich großen Geldwäschefälle laufen aber weiterhin „unter dem Radar".

Finanzinstitute (und andere sog. Verpflichtete nach § 2 GwG) sind häufig mit der Erstellung von Geldwäscheverdachtsmeldungen bezüglich potenziell verdächtiger Transaktionen ihrer Kunden überfordert.[19] Die Verpflichtung zur Abgabe dieser Verdachtsmeldungen ergibt sich aus § 43 Abs. 1 GwG. Gleichzeitig stapeln sich bei der Financial Intelligence Unit (FIU) zum allgemeinen medialen Empören unbearbeitete Verdachtsmeldungen, viele Verdachtsmeldungen werden auch aus der Unsicherheit der Verpflichteten heraus abgegeben, wann eine Meldung überhaupt zu erstatten ist.[20]

---

15 So auch der ehemalige Präsident der FATF: *Pleyer*, Geldwäsche geht uns alle an – Digitalisierung ist im Kampf gegen Geldwäsche bedeutend, FAZ v. 30.05.2021, S. 27; *Blaeschke,* DNotZ 2022, 827 (827); *Heger,* in: Lackner/Kühl/Heger (Hrsg.), 30. Aufl. 2023, § 261 Rn. 2.

16 *Diergarten/Barreto Da Rosa*, Praxiswissen Geldwäscheprävention – Aktuelle Anforderungen und Umsetzung in der Praxis, 2. Aufl. 2021, S. 6.

17 Kapitel II.B.II.

18 *Bussmann/Veljovic*, NZWiSt 2020, 417 (418); *Geng*, in: Dünkel/Fahl/Hardtke/Harrendorf/Regge/Sowada, S. 221 ff.; *Transparency International Deutschland e.V.*, Geldwäschebekämpfung in Deutschland – Probleme, Lösungsvorschläge und Beispielfälle, 2021, (abrufbar: https://perma.cc/MQ62-7SDE, zuletzt abgerufen: 31.08.2024), Zusammenfassung.

19 *Kanning*, Kampf gegen Geldwäsche überfordert Banken, FAZ, 09.10.2019, (abrufbar: https://perma.cc/FGA7-7GGQ, zuletzt abgerufen: 31.08.2024).

20 *Lenk,* ZWH 2021, 353 (353); auch der FATF Länderbericht Deutschland äußert sich zur fehlenden Effektivität der FIU: *FATF*, Anti-money laundering and counter-terrorist financing measures Germany – Mutual Evaluation Report, August 2022, (abrufbar: https://perma.cc/6QSV-R5AL, zuletzt abgerufen: 31.08.2024) u. a. S. 4, 9; aufgrund der fehlenden oder langsamen Weitergabe von Verdachtsmeldungen an die Strafverfolgungsbehörden leitete die Staatsanwaltschaft Osnabrück im Sommer 2020 sogar Ermittlungen gegen Verantwortliche der FIU ein, *Diehl/Siemens*, Ermittler gehen gegen Zoll-Spezialeinheit vor, Spiegel, 2020, (abrufbar: https://perma.cc/J

Bei den Staatsanwaltschaften schließlich kommen durch die Weiterleitung über die FIU 15,3 Prozent aller Geldwäscheverdachtsmeldungen an, lediglich 0,3 Prozent der Verdachtsmeldungen führen jedoch überhaupt zu strafrechtlichen Konsequenzen.[21]

Es überrascht daher nicht, dass die politischen und rechtlichen Bemühungen derzeit dahin gehen, die Digitalisierung zur Bekämpfung der Geldwäsche nutzen zu wollen – was bisher nach Experteneinschätzung zu wenig geschieht.[22] Ein schwieriges Problem zur Nutzung der Digitalisierung ist die rechtskonforme Auswertung von Massendaten – nicht nur im Bereich der Geldwäsche.[23] Als revolutionäres Detektionsmittel wird seit einiger Zeit die Nutzung von Künstlicher Intelligenz (KI) gehandelt. Ausgangspunkt ist die Aufdeckung von Geldwäsche-Mustern und Vortaten i. S. d. § 261 StGB mit Hilfe einer KI. Diese wird primär durch die Verpflichteten des GwG, z. B. Banken, nutzbar sein. Die Erkenntnisse sollen nachgelagert jedoch auch für die Zentralstelle zur Auswertung von Geldwäscheverdachtsmeldungen, die FIU und die Strafverfolgungsbehörden nutzbar gemacht werden.[24] Die Auswertung von Massendaten – auch „Big Data" genannt – mittels KI soll Rückschlüsse erlauben, die durch analoge Mechanismen nicht möglich gewesen wären oder einen unverhältnismäßigen Aufwand bedeutet hätten.[25] Ausgehend von dieser Idee wurde das durch das Bundesministerium für Bildung und Forschung (BMBF) geförderte Forschungs-

---

E9R-V7EY, zuletzt abgerufen: 31.08.2024). Diese Ermittlungen wurden inzwischen eingestellt, da das risikobasierte Vorgehen bei der operativen Analyse der Geldwäscheverdachtsmeldungen nicht mit den Vorgaben des GwG vereinbar sei und für die Mitarbeiter der FIU daher ein unvermeidbarer Verbotsirrtum nahegelegen habe, *Staatsanwaltschaft Osnabrück*, 31.05.2023, Pressemitteilung, (abrufbar: https://perma.cc/J422-U3AH, zuletzt abgerufen: 31.08.2024); auch *El-Ghazi/Jansen* sehen in der aktuellen Arbeitsweise der FIU sogar ggf. strafrechtlich relevantes Fehlverhalten, NZWiSt 2022, 465 (472).

21 Diese Prozentzahlen stützen sich auf eine rechnerische Auswertung des FIU-Jahresberichtes 2022, wonach die Verpflichteten insgesamt ca. 340.000 Verdachtsmeldungen abgegeben haben (S. 14), die FIU davon ca. 51.700 Verdachtsmeldungen an die Staatsanwaltschaften weitergegeben hat (S. 19) und es auf Basis dieser Daten auf Seiten der Strafverfolgungsbehörden zu ca. 1.058 Urteilen oder Anklagen (S. 21) kam.

22 *Seehafer,* GWuR 2022, 74 (76).

23 *Burkhardt,* Kriminalistik 2020, 336 (337).

24 Zu den Begrifflichkeiten des Geldwäscherechts siehe unten Kapitel II.B.III.

25 *Peters*, Smarte Verdachtsgewinnung – Eine strafprozessuale und verfassungsrechtliche Untersuchung der Verdachtsgewinnung mittels Künstlicher Intelligenz, 2023, S. 21.

projekt „MaLeFiz“ gegründet.[26] Das Akronym „MaLeFiz“ steht für „Maschinelles Lernen zur effizienten Identifikation auffälliger Finanztransaktionen“. Innerhalb dieses Forschungsvorhabens wird die Forschungsidee interdisziplinär unter Mitwirkung der Autorin praktisch umgesetzt und der Demonstrator einer KI zu genau diesem Vorhaben – der Detektion von Geldwäsche – durch die Computerwissenschaftler des Fraunhofer Instituts für Sichere Informationstechnologie entwickelt. Aufgrund der starken gesetzgeberischen Verzahnung der Geldwäsche mit der Terrorismusfinanzierung werden diese Delikte heute immer in einem Atemzug genannt. Ziel dieser Arbeit ist jedoch spezifisch die Detektion von Geldwäsche durch KI.

Dabei ist der Gedanke des Einsatzes von KI zur Geldwäschebekämpfung nicht neu. Schon Ende der 1990er-Jahre – vor über 20 Jahren – äußerte sich ein UN-Bericht zu einer solchen Einsatzmöglichkeit.[27] Dieser Bericht gab jedoch bereits damals zu bedenken, dass KI nicht als „Allheilmittel“ zur Geldwäsche-Detektion gehandelt werden dürfe.[28] Auch diesen Zweifeln will die Arbeit nachgehen. Daher liegt auch ein Schwerpunkt der Ausführungen auf der Auslagerung zentraler Bestandteile der Geldwäschebekämpfung an die GwG-Verpflichteten, wie z. B. Banken, und an die FIU. Analysiert wird mithin im Schwerpunkt die Automatisierung dieser Auslagerung mit Blick auf den Einsatz von KI im Bereich des sog. Transaktionsmonitorings und die Weiterleitung von Geldwäscheverdachtsmeldungen durch einzelne Institute an die FIU. Nicht Gegenstand dieser Arbeit ist die Bewertung eines Datenaustausches zwischen verschiedenen Finanzinstituten zur gebündelten Weiterleitung von Informationen an die FIU.

Der Blick der Arbeit wird außerdem sowohl auf die Rechtsprechung des Bundesverfassungsgerichts (BVerfG) als auch des Europäischen Gerichtshofs (EuGH) der letzten Jahre gerichtet. Diese haben immer wieder aufgezeigt, in welcher Form tiefgreifende (staatliche) Grundrechtseingriffe bei der (automatisierten) Auswertung von Daten unzulässig sind. Sicher ist jedenfalls, dass das Potenzial der Verfügbarkeit und Vernetzung wachsender Datenmengen mit Hilfe von KI ungeahnte Analysemöglichkeiten eröffnet.[29]

---

26 Forschungsprojekt „Maschinelles Lernen zur effizienten Identifikation auffälliger Finanztransaktionen“ (MaLeFiz), gefördert vom BMBF im Rahmen des Programms „Künstliche Intelligenz in der zivilen Sicherheitsforschung II“ unter Koordination des Fraunhofer SIT (Förderkennzahl 13N16306).

27 *UNODC*, Financial havens, banking secrecy and money laundering, 1998, (abrufbar: https://perma.cc/6EUB-D6HM, zuletzt abgerufen: 31.08.2024), S. 25.

28 Ebenda.

29 *Seehafer*, GWuR 2022, 74 (76); *Bock/Höffler,* KriPoZ 2022, 257 (263).

Denn die Möglichkeit der Ausschöpfung von schier unermesslichen Datenbeständen stellt sowohl eine der größten Chancen als auch technischen und rechtlichen Herausforderungen für die Strafverfolgung und die Gesellschaft insgesamt dar.

C. Gang der Untersuchung

Die vorliegende Arbeit ist insgesamt in sieben Kapitel unterteilt:

Kapitel I. erläutert in einem ersten Schritt die verständnisnotwendigen Terminologien und bietet einen Problemaufriss an. Zugleich wird ein Oberbegriff für die Masse algorithmenbasierter Systeme eingeführt und eine Abgrenzung der im Rahmen dieser Arbeit beschriebenen *Automated Suspicion Algorithms* vom Predictive Policing vollzogen. Die von der Autorin entwickelten Begriffe Verdachtshöhe und Verdachtsstufe, mit denen diese Arbeit dem Leser eine Orientierungshilfe anbieten möchte, werden eingeführt. Sodann wird die Forschungsfrage dargestellt und der Forschungszuschnitt begründet.

Im Kapitel II. werden die supranationale Entwicklung der Geldwäschebekämpfung und die zahlreichen Regularien des hier als Verdachtsschöpfungssystem bezeichneten Geldwäscherechtes dargestellt. Es erfolgt eine Nachzeichnung der wichtigsten Meilensteine der internationalen und europäischen Entwicklung mit ihren Auswirkungen auf das nationale Anti-Geldwäscherecht und die Verdachtsstufen der Geldwäschebekämpfung in Deutschland. Das Kapitel schließt mit einem Ausblick auf die ausstehenden europäischen Regelungen der nächsten Jahre. Mit einer Darstellung (inter)nationaler Kritik an der Geldwäschebekämpfung, die in Empfehlungen für eine Technisierung des Geldwäschemeldesystems mündet, wird zu den computerwissenschaftlichen Aspekten im dritten Kapitel übergeleitet.

Im Kapitel III. erfolgt eine Auseinandersetzung mit den technischen Grundlagen von KI, den Möglichkeiten, die durch die verschiedenen Arten des maschinellen Lernens bestehen und den derzeit existierenden technischen Grenzen. Dazu wird der Begriff KI definiert und in die am 14.03.2024 verabschiedete Verordnung der EU zur Harmonisierung der Vorschriften zu KI[30] (EU-KI-Verordnung) eingeordnet.

30 Die Einigung wurde im Dezember 2023 erzielt, siehe *Europäische Kommission*, Kommission begrüßt politische Einigung über das Gesetz über künstliche Intelligenz, Pressemitteilung, 09.12.2023, (abrufbar: https://perma.cc/CVG3-SVSW, zuletzt abge-

Im Kapitel IV. werden die rechtlichen Grenzen des Einsatzes von KI durch Finanzinstitute erläutert, die von dieser Arbeit als erste Verdachtsstufe der Geldwäschebekämpfung eingeordnet werden. Als Grundlage dieser Verdachtsstufe erfolgt eine – für den weiteren Fortgang der Arbeit zentrale – Einordnung der Rechtsnatur der Meldepflicht nach dem GwG und einer Bestimmung der erforderlichen Verdachtshöhe für das Auslösen dieser Meldepflicht. Die Einordnung der Rechtsnatur ist unerlässlich für die in den nachfolgenden Kapiteln daraus abgeleiteten Entwicklungs-, Einsatz- und Kontrollmodalitäten, ohne die Projekte einer Geldwäsche-Detektions-KI[31] nicht in Angriff genommen werden sollten. Diese Art von KI soll zum Aufspüren von Geldwäscheverdachtsfällen in der Lage sein. Der gewählte Begriff der Verdachtshöhe veranschaulicht die Schwelle hin zu einem automatisiert generierten Alarm – einem sog. KI-Alert[32] – und die Rechtsfolgen eines solchen Alerts.

Im Kapitel V. wird dargestellt, was die in Kapitel IV. erarbeiteten rechtlichen Grenzen für die Arbeit der FIU bedeuten und die Auswirkungen des KI-Einsatzes auf Ebene der Verpflichteten für den weiteren Prozess der Geldwäsche-Verdachtskette bei der FIU werden diskutiert. Dazu erfolgt insbesondere eine kritische Betrachtung des für die Geldwäschebekämpfung seit Langem propagierten sog. risikobasierten Ansatzes aus rechtlicher und aus technischer Sicht.

Im Kapitel VI. erfolgt ein Ausblick auf die möglichen Folgen der automatisierten Vorauswertung für die Arbeit der Staatsanwaltschaften und die besondere Stellung dieser im Bereich der Geldwäschebekämpfung.

Die Arbeit schließt mit Kapitel VII., welches die Folgen der betrachteten Automatisierung mit einem Blick auf die Einordnung des „gesunden Menschenverstandes" resümiert. Zusammenfassend mit den Thesen dieser Arbeit werden die Chancen zur Verbesserung der Strafverfolgung mit den Risiken der von dieser Arbeit eingeführten Begrifflichkeit einer *„blinden automatisierten Navigation"* abgewogen.

---

rufen: 31.08.2024); Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

31 Engl. zuweilen auch als AML-AI bezeichnet.

32 Zum Begriff Kapitel I.D.VI.

D. Terminologie

Der KI-Einsatz im Bereich des Strafrechts wird häufig in einem Sammelbecken aus den Begriffen KI-gestützte Kriminalitätsvorbeugung, Kriminalitätskontrolle oder Kriminalitätsverfolgung ohne nähere Differenzierung zum Oberbegriff des Predictive Policing zusammengefasst. Daneben treten weitere technische Grundbegriffe, die ebenfalls nicht näher eingegrenzt werden und lediglich unter dem Buzzword KI firmieren. Die klare begriffliche Trennung der verschiedenen Arten des KI-Einsatzes und die Abgrenzung von anderen Einsatzarten von Algorithmen ist wichtig, um die verschiedenen (grundrechtlichen) Eingriffsintensitäten und rechtlichen Anforderungen beurteilen zu können.

I. Algorithmus

Das Wort „Algorithmus" wird heute im Kontext des Technikeinsatzes völlig selbstverständlich benutzt. Die Eingangszeichnung vor Kapitel I. hat bereits verdeutlicht, dass Algorithmen seit vielen Jahrhunderten ursprünglich zur einfachen Beschreibung von einer Reihe von Schritt-für-Schritt Anweisungen genutzt wurden, die – mechanisch ausgeführt – zu einem bestimmten Ergebnis führen.[33] Im Laufe der Zeit wandelte sich der Begriffsinhalt dann zur automatischen Abfolge dieser Schritte (Computeralgorithmus).[34] Inzwischen wird der Begriff – fälschlicherweise – oft mit KI gleichgesetzt. Es gibt auch heute noch zahlreiche Computeralgorithmen, die keine KI sind. Der Algorithmus ist lediglich ein Grundbaustein technisch weiterentwickelter Systeme.

II. Big Data

Der Begriff „Big Data" wird insbesondere zur Umschreibung der Herausforderungen um die technologischen Möglichkeiten für die Erhebung, Sammlung, Verarbeitung, Analyse und Nutzung schnell wachsender Daten-

33 *Chabert/Barbin/Borowczyk/Guillemot/Michel-Pajus*, 1999, S. 1.

34 Siehe auch *Martini*, Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, 2019, S. 18. Soweit diese Arbeit von Algorithmus spricht, meint sie das automatisierte Begriffsverständnis davon.

mengen herangezogen.[35] Diese Datenmengen sind zu einer Grundlage des großen Fortschritts bei der Entwicklung von KI-Systemen geworden, wobei die Datenmengen durch verschiedene Arten von maschinell-lernenden Algorithmen in hoher Geschwindigkeit ausgewertet und verarbeitet werden können.[36] Zusätzlich sind diese Datenmassen auch für das Training mit einigen Lernverfahren dieser Systeme notwendig.[37]

Teilweise fällt in einem Atemzug mit Big Data auch der Begriff des „Data Mining". Diesen hat beispielsweise das BVerfG u. a. in seinem Beschluss vom 10.11.2020 zum Antiterrordateigesetz verwendet. Das Gericht versteht darunter die komplexe Auswertung von großen Datenbeständen, um dadurch neue Erkenntnisse für Strafverfolgung, Gefahrenabwehr und nachrichtendienstliche Aufgaben zu erlangen.[38] Bei der Verwendung dieser Begrifflichkeit erfolgt mithin noch keine Unterscheidung, zu welchen späteren Zwecken (z. B. präventiv oder repressiv) die Datenauswertung durchgeführt wird. Mithin stellt das Data Mining zumindest nach dem Verständnis des BVerfG bereits eine deutlich spezifischere Auswertung von Datenbeständen dar, als mit dem Oberbegriff Big Data gemeint ist.

III. Künstliche Intelligenz (KI)

Sowohl in der Rechts- als auch in der Computerwissenschaft existiert bis heute keine allgemeingültige Definition von KI.[39] Seit 2021 versuchte die EU, sich in dem Entwurf eines „Gesetzes für Künstliche Intelligenz" auf eine Begriffsbestimmung zu einigen. Inzwischen hat sie sich in der verabschiedeten Fassung auf die bereits von der Organisation for Economic Cooperation and Development (OECD) erarbeitete Definition von KI ver-

35 *Götz,* ZD 2014, 563 (563); *Momsen*, in: Chibanguza/Kuß/Steege (Hrsg.), 2022, § 2, G., Rn. 18.

36 *Brüning*, in: Rotsch, 2021, S. 63 f.; *Bock/Höffler*, KriPoZ 2022, 257 (263).

37 *Leffer/Leicht*, in: Schweighofer/Kummer/Saarenpää/Eder/Hanke/Zanol/Schmautzer, 2022, S. 89.

38 BVerfG, Beschl. v. 10.11.2020, 1 BvR 3214/15, ZD 2021, 205, (207); *Golla*, NJW 2021, 667 (667).

39 Mit dieser Einschätzung auch: *Steinrötter/Stamenov*, in: Möslein/Omlor (Hrsg.), 2. Aufl. 2021, § 11 Rn. 2.; m. w. N. *Santos,* ZfDR 2023, 23 (25); *Lang*, Methoden des bestärkenden Lernens für die Produktionsablaufplanung, 2023, S. 42; *Rückert,* GA 2023, 361 (362).

ständigt.[40] Nach der OECD ist ein KI-System ein maschinengestütztes System, das für explizite oder implizite Ziele aus den empfangenen Eingaben ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können. Verschiedene KI-Systeme unterscheiden sich in ihrem Grad an Autonomie und Anpassungsfähigkeit nach dem Einsatz.[41] Diese Definition und die existierenden Unterformen von KI werden in Kapitel III. ausführlich erläutert.

IV. Algorithmic-Decision-Making-System (ADM-System)

Als Oberbegriff für Software-Lösungen, welche algorithmenbasiert arbeiten und auf der Grundlage einer Reihe von Eingabevariablen eine einzige Aussage erzeugen, dient der Begriff des ADM-Systems.[42] Dabei kann die algorithmische Komponente einen statischen Algorithmus enthalten, der z. B. auf den Entscheidungsregeln von Experten auf dem Gebiet basiert und auf dieser Grundlage ein Ergebnis generiert.[43] Alternativ nutzt der Algorithmus Daten zum Training eines sog. Modells, mit welchem er im Anschluss arbeitet.[44] Dabei können die Entscheidungsregeln ebenfalls vorgegeben werden, müssen sie jedoch nicht.[45] Im deutschen Sprachkontext werden ADM-Systeme häufig auch als algorithmengestütztes (Entscheidungs-)System bezeichnet.[46]

40 Ausführlich zu einer Definition von KI und den zugehörigen Unterkategorien siehe unten Kapitel III.; *Rat der EU*, Gesetz über künstliche Intelligenz: Rat und Parlament einigen sich über weltweit erste Regelung von KI, Pressemitteilung, 09.12.2023, (abrufbar: https://perma.cc/3SPM-AL63, zuletzt abgerufen: 31.08.2024).

41 *OECD*, OECD AI Principles overview, (abrufbar: https://perma.cc/J8HA-MNWR, zuletzt abgerufen: 31.08.2024).

42 *Zweig/Wenzelburger/Krafft,* Minds and Machines 2019, 555 (559); vgl. im Kontext der Impfpriorisierung durch ADM-Systeme in der Covid-19-Pandemie *Ruschemeier,* NVwZ 2021, 750 (750 ff.).

43 Ebenda.

44 Ebenda.

45 Zu den genauen Möglichkeiten der technischen Ausgestaltung eines solchen Systems siehe Kapitel III.

46 *Sommerer*, Personenbezogenes Predictive Policing – Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose, 2020, S. 34.

V. Predictive Policing, Automated Suspicion Algorithms, Data Mining

Innerhalb des Oberbegriffs der ADM-Systeme sind verschiedene Arten des Predictive Policing[47] von den in dieser Arbeit näher betrachteten *Automated Suspicion Algorithms*[48] zu unterscheiden. Unter Predictive Policing versteht man allein die Verwendung von algorithmengestützten Systemen zur Straftatprognose in der präventiven Polizeiarbeit, d. h. in der Gefahrenabwehr.[49] Predictive Policing wird mithin eingesetzt, um eine noch nicht eingetretene Gefahr für ein Rechtsgut abzuwenden und erfolgt zur Prognose sowie möglichst anschließender Vermeidung eines Rechtsverstoßes.[50] Demgegenüber dienen *Automated Suspicion Algorithms* der repressiven Verbrechensbekämpfung.[51] Ziel ist mithin nicht mehr der Schutz des Rechtsguts vor Beeinträchtigung, sondern die Ermöglichung der Sanktionierung der Beeinträchtigung.[52] Diese Arbeit untersucht daher, ob der Einsatz von KI zur Detektion von Geldwäsche einen solchen *Automated Suspicion Algorithm* darstellt und wie die vor allem mit einer solchen Technologie bezweckte Erhöhung des Aufdeckungsrisikos von Straftaten für die Täter rechtlich zu beurteilen ist. Mithin wird ein *Automated Suspicion Algorithm* in dieser Arbeit als automatisierte Verdachtsgewinnung mittels KI verstanden.[53]

VI. KI-Alert

Ein KI-Alert (dt.: Alarm) ist die Markierung eines Prozesses oder im Falle der Geldwäsche-Detektion einer Transaktion oder eines Geschäftsvorganges als auffällig. Das bedeutet, ein technisches System[54] markiert

47 Zur genauen Terminologie innerhalb des Predictive Policing ausführlich *Sommerer*, 2020, S. 36 ff.

48 Dieser Begriff wurde von den Autoren *Rich*, University of Pennsylvania Law Review 2016, 871 (871 ff.) und *Golla*, NJW 2021, 667 (672) inspiriert und übernommen.

49 *Sommerer*, 2020, S. 34.

50 Ebenda.

51 Die Gründe für die Zuordnung einer KI zur Detektion von Geldwäschefällen zu den *Automated Suspicion Algorithms* werden ausführlich in Kapitel IV. und V. dargestellt.

52 Teilweise werden diese Algorithmen auch als Retrospective Policing Systems bezeichnet, *Sommerer*, 2020, S. 244.

53 *Rademacher* spricht ebenfalls von „automatisierter Verdachtsgewinnung": *Rademacher*, in: Zimmer, 2021, S. 231.

54 Zu den Ausgestaltungsmöglichkeiten siehe unten Kapitel III.

riskante Transaktionen für eine weitergehende Analyse.[55] Sowohl für den Automatisierungsgrad des KI-Alerts als auch für die anschließende weitergehende (menschliche) Analyse sind unterschiedliche Automatisierungsgrade denkbar.[56] An einen solchen Alarm schließen sich Validierungs- bzw. Untersuchungsprozesse an, die eine Bewertung in unterschiedliche Treffer-Arten ermöglichen. Dies wird im betreffenden Kontext unter dem folgenden Gliederungspunkt VII. zu false-positive Treffern dargestellt.

VII. False-positive Treffer

Besonders wichtig bei KI-Modellen ist die jeweilige Klassifizierung des Treffers und die Untersuchung der Fehlerrate des KI-Systems. Diese Fehlerrate ergibt sich maßgeblich aus dem Entwicklungsprozess des Systems.[57] Jedem technischen Modell wohnt eine solche Fehlerrate inne, denn wie der Mensch kann sich auch das technische System „irren".[58] Um zumindest ansatzweise eine Vergleichbarkeit und die Konsequenzen aus dem Einsatz eines solchen KI-Systems einzuschätzen, wird die Analyse dieser Fehlerrate so bedeutend. Es existieren zwei mögliche Fehlerarten, die technische Systeme produzieren können: „false-positive"-Treffer (dt.: falsch-positiv) und „false-negative"-Treffer (dt.: falsch-negativ).[59] Alle anderen Treffer sind folglich „right-positive" Treffer (dt.: richtig-positiv) oder „right-negative" Treffer (dt.: „richtig-negativ). Die Fehlerraten von KI-Systemen sind technisch so aneinandergekoppelt, dass false-positive Treffer nicht reduziert werden können, ohne gleichzeitig false-negative Treffer zu erhöhen.[60] Dieses technische Phänomen wird auch als „Asymmetric Cost Ratio" bezeichnet.[61] In Abb. 2: Trefferarten eines KI-Systems ist die Klassifizierung in diese vier Unterkategorien, wovon zwei Arten als Fehler des Systems einzuordnen sind, kurz dargestellt:

55 *Schmuck,* ZRFC 2023, 409 (409).
56 Ausführlich zu den unterschiedlichen Optionen in Kapitel III.
57 *Sommerer*, 2020, S. 50 f.; *Lehr/Ohm,* U.C. Davis Law Review 2017, 653 (691 f.); *Kang/Wu,* Journal of Experimental Criminology 2023, 919 (920).
58 *Sommerer*, 2020, S. 50 f.; *Lehr/Ohm*, U.C. Davis Law Review 2017, 653 (691 f.)
59 *Kang/Wu*, Journal of Experimental Criminology 2023, 919 (920); *Sommerer*, 2020, S. 50 f.
60 *Lehr/Ohm*, U.C. Davis Law Review 2017, 653 (691 f.); *Sommerer*, 2020, S. 50 f.; für eine visuelle Darstellung dieser technischen Koppelung siehe *Grossenbacher/Zehr*, Polizei-Software verdächtigt zwei von drei Personen falsch, SRF, 05.04.2018, (abrufbar: https://perma.cc/7ZY8-6HCS, zuletzt abgerufen: 31.08.2024).
61 *Sommerer*, 2020, S. 113 f.; *Lehr/Ohm*, U.C. Davis Law Review 2017, 653 (691 f.).

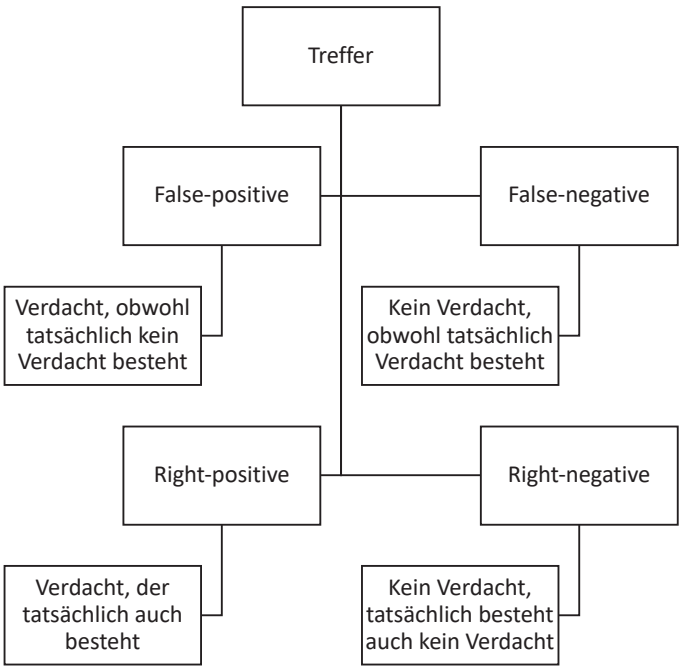

Abb. 2: Trefferarten eines KI-Systems

Nach technischer Definition liegt ein false-positive Treffer vor, wenn ein technisches Modell ein Ergebnis als richtig anzeigt, welches sich als falsch entpuppt.[62] An diesem Punkt stellt sich daher die Frage, wann in der Geldwäschebekämpfung ein KI-Alert richtig und wann falsch ist. Grundsätzlich ist es im Rahmen der Detektion von Geldwäsche durch *Automated Suspicion Algorithms* nämlich möglich, die false-positive Treffer eines KI-Systems auf zwei unterschiedliche Arten festzulegen. Die Ursache dafür liegt in den unterschiedlichen rechtlichen Verdachtsstufen der Geldwäschebekämpfung, die für eine Befassung auf der jeweiligen Ebene eine Verdachtshöhe erfordern, die sich von der nächsten Stufe unterscheidet.[63]

Die erste Möglichkeit ist somit, einen false-positive Treffer abhängig von der jeweiligen Verdachtsstufe zu definieren. Im Wesentlichen ist die erste

62 *Taulli*, Grundlagen der Künstlichen Intelligenz – Eine nichttechnische Einführung, 2022, S. 76.

63 Zu den Verdachtsstufen siehe Abb. 7: Verdachtsstufen der Geldwäschebekämpfung in Deutschland.

Verdachtsstufe die Weiterreichung eines bestimmten Verdachtes von den Banken an die FIU, § 43 Abs. 1 Nr. 1 GwG. Auf dieser Stufe würde ein false-positive Treffer bedeuten, dass ein Mitarbeitender auf der ersten Ebene der GwG-Verpflichteten (z. B. Finanzinstitute) sich nach der (menschlichen) Befassung mit einem KI-Alert bereits gegen die Abgabe einer Verdachtsmeldung an die FIU entscheidet, da der dafür erforderliche Sachverhalt nach § 43 Abs. 1 Nr. 1 GwG nicht gegeben ist.

Die zweite Verdachtsstufe ist die Weiterreichung eines bestimmten Verdachtes von der FIU an die Staatsanwaltschaft, § 32 Abs. 1 Satz 1 GwG. Hier liegt demgemäß ein false-positive Treffer vor, wenn die von der FIU im Rahmen ihrer operativen Analyse weitergehenden Untersuchungen nicht in eine Weiterleitung der Verdachtsmeldung an die dritte Ebene der Staatsanwaltschaft münden.

Als dritte und letzte Verdachtsstufe steht dann die Überprüfung der durch die FIU übermittelten Meldung durch die Staatsanwaltschaft. Hier läge dann ein false-positive Treffer vor, wenn der durch die FIU übermittelte Sachverhalt nur zu einer Einstellung und nicht zur Anklageerhebung bzw. später zu einer Verurteilung führt.

Die zweite Möglichkeit, einen false-positive Treffer zu definieren, besteht in einer Gesamtbetrachtung. Nach dieser wird die Zahl der in einem Jahr abgegebenen Verdachtsmeldungen mit der Zahl der in einem Jahr ergangenen Verurteilungen und Strafbefehle nach § 261 StGB verglichen und daraus direkt abgeleitet, wie hoch die Fehlerrate ist. Mithin ist dann jeder Fall ein false-positive Treffer, der sich im Ergebnis als nicht-geldwäscherelevant herausgestellt hat. Als nicht-geldwäscherelevant gilt ein Treffer konkret, wenn in der Realität tatsächlich keine Geldwäschetat begangen wurde oder wenn die jeweilige Institution zu dem Ergebnis kommt, dem Alarm nicht weiter nachzugehen. Diese Einordnung wird hier absolut, d. h. unabhängig von der Verdachtsstufe, auf der das Verfahren beendet wurde, vorgenommen.

Die stufenabhängige Fehlerrate und die Gesamtbetrachtung können daher jeweils eine unterschiedliche Fehlerrate aufweisen. Beide Berechnungsmöglichkeiten sind aufgrund des hohen Dunkelfeldes der Geldwäsche und den oft fehlenden Rückmeldungen sowohl durch die FIU als auch durch die Staatsanwaltschaften mit erheblichen Tücken verbunden.

In dieser Arbeit wird die stufenabhängige Definition eines false-positive Treffers gewählt. Insbesondere mit Blick auf die – in Umsetzung der EU-Geldwäsche-Richtlinien – im GwG vorgesehenen Rückmeldungspflichten ist es zielführend, den Begriff so zu wählen. Nach § 41 Abs. 2 Satz 1 GwG

ist die FIU verpflichtet, den GwG-Verpflichteten eine Rückmeldung zur Relevanz der jeweiligen Verdachtsmeldung zu geben. Diese Daten sollen die GwG-Verpflichteten zur Verbesserung ihres jeweiligen Risikomanagements – also zur Verbesserung ihrer Verdachtsmeldungen – nutzen, § 41 Abs. 2 Satz 2 GwG. Ebenso müssen die Staatsanwaltschaften der FIU Rückmeldung erstatten, ob öffentliche Klage erhoben wurde und wie das Verfahren ausgegangen ist – inklusive Übermittlung aller Einstellungsentscheidungen, § 42 Abs. 1 Satz 1, 2 GwG.

Außerdem würde die Definition eines false-positive Treffers nach der Maßgabe der Gesamtbetrachtung den Eindruck erwecken, die Banken müssten zwingend sichere Fälle der Geldwäsche detektieren.[64] Dies suggeriert, dass nur eine höhere Verurteilungsrate zu einer effektiven Geldwäschebekämpfung führen könnte. Ziel muss aber die Aufdeckung der schwerwiegenden Geldwäschefälle des Dunkelfeldes sein – dies korrespondiert nicht *zwingend* mit einer höheren Verurteilungsrate.

Die stufenabhängige Definition bedeutet daher nicht unbedingt, dass an der prozentualen Zahl der false-positive Treffer eine Änderung erzielt werden muss, um die Effektivität des gesamten Systems zu erhöhen. Vielmehr ist es so, dass gerade aus false-positive Treffern Anhaltspunkte für zukünftige technische Verfeinerungen des Systems gewonnen werden können. Dies hängt mit der in diesem Abschnitt erwähnten Asymmetric-Cost-Ratio zusammen. Richtigerweise können daher aus der generellen Anzahl von false-positive Treffern nicht zwingend Rückschlüsse auf die Effektivität des Systems geschlossen werden.

64 Zu den an die Banken zu stellenden Anforderungen: Kapitel IV.C.

Die stufenabhängige Definition eines false-positive Treffers wird in der folgenden Abb. 3 dargestellt:

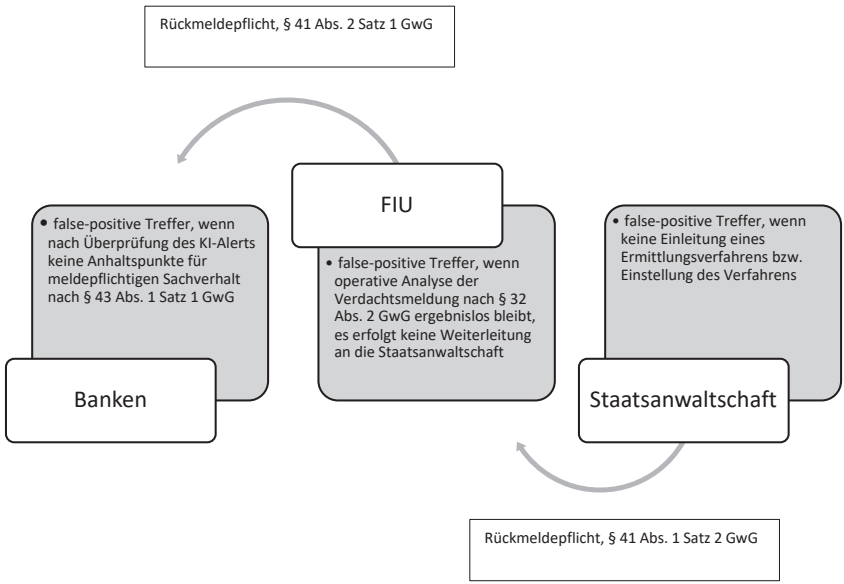

Abb. 3: Definition eines false-positive Treffers anhand der Verdachtsstufen der Geldwäschebekämpfung

Der Frage, ab wann das Verdachtsmeldesystem als effektiv eingestuft werden kann, soll in Kapitel IV. nachgegangen werden.

E. Forschungsfrage

Die Detektion von Kriminalität mittels KI ist vielgestaltig und wirft grundlegende rechtliche und technische Fragen auf. Daher muss eine Eingrenzung der Forschungsfrage erfolgen.

Die Ausführungen dieser Arbeit beschränken sich auf den Einsatz der oben definierten *Automated Suspicion Algorithms*[65] durch Finanzinstitute am Beispiel der Geldwäsche im Rahmen des sog. Transaktionsmonito-

65 Kapitel I.D.V.

rings[66] und die rechtlichen Konsequenzen der dortigen Ergebnisse für die Arbeit der FIU und der Staatsanwaltschaften. Dazu liegt der Fokus auf der Automatisierung der Verdachtsmeldungen der Finanzinstitute durch KI. Mithin erfolgt zunächst eine historische Einordnung der Geldwäsche und eine Analyse der Rechtsquellen, um daraus die Rechtsnatur der Verdachtsmeldung und die Konsequenzen der Automatisierung zu analysieren.

Dieser Forschungszuschnitt basiert auf Überlegungen zur Aktualität der Thematik (I.) sowie ihres besonderen transformativen Potenzials für die Gesellschaft (II.). Außerdem ist diese Forschung relevant für die Kriminalitätsverfolgung als Ganzes (II.) mit Blick auf die „Regulierungsflut" im Geldwäschebereich und die mit einer Automatisierung verbundenen tiefgreifenden Grundrechtseingriffe (III.). All dies führt zu einer hier in besonderem Maße bestehenden Forschungslücke (IV.).

I. Aktualität

Im aktuellen Sog des KI-Hypes und der sich ständig im Fluss befindlichen nationalen sowie internationalen Anti-Geldwäschegesetzgebung beschränken sich die Ausführungen zur Aktualität dieses Themas auf die wichtigsten Meilensteine. Die automatisierte Verarbeitung umfangreicher Datenmengen zur Gefahrenabwehr,[67] das Profiling durch die Schufa[68] und die Auswertung von Fluggastdaten[69] waren alle bereits Gegenstand weitreichender Entscheidungen sowohl des BVerfG als auch des EuGH. Auch diese Entscheidungen und die Einordnung der hiesigen Technik in den Kontext der nach dreijähriger Verhandlungsphase erst 2024 final verabschiedeten EU-KI-Verordnung[70] sind Gegenstand dieser Arbeit. Der Einsatz von *Automated Suspicion Algorithms* erfolgt bereits zu unterschiedlichen Zwecken von Finanzkriminalität. Es existieren – wie in Kapitel III. ausführlich ge-

66 Zum Begriff unten Kapitel II.B.III.1.
67 BVerfG, Urt. v. 16.02.2023, 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1196 ff.).
68 EuGH, Urt. v. 07.12.2023, C-634/21, BKR 2024, 70 (70 ff.).
69 EuGH, Urt. v. 21.06.2022, C-817/19, ZD 2022, 553 (553 ff.).
70 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).

zeigt werden wird – schon heute mindestens sieben kommerzielle computergestützte Geldwäscheerkennungsprogramme, die mit dem Einsatz von KI werben.[71] Es steht zu befürchten, dass eine weitere Entwicklung solcher KI-Systeme ohne zentrale Einbeziehung von Juristen erfolgen wird, wenn nicht frühzeitig Regularien als Richtpfeiler für die weitere Entwicklung, den weiteren Einsatz und die zukünftige Kontrolle vorgegeben werden. Auch im eingangs beschriebenen Forschungsprojekt MaLeFiz wird bereits dieser Ansatz einer technikbegleitenden juristischen Einschätzung verfolgt. Dabei geht es nicht nur darum, für den jetzigen Moment die Rechtskonformität dieser Technologie sicherzustellen, sondern um eine generelle und rechtzeitige Diskussion, wie wir unser Rechtssystem zukünftig ausgestalten wollen. Sicher ist, dass der aktuelle technische Prozess und die damit verbundene Fortentwicklung des Rechtssystems nicht aufgehalten werden können und sollen, sondern juristisch mitgedacht und mitgestaltet werden müssen.

II. Transformation der Gesellschaft

Es ist unbestritten, dass die Digitalisierung die Gesellschaft transformiert hat und weiter stetig transformieren wird. KI-Systeme haben erst still und leise (etwa mit den Tools zur Analyse des Kaufverhaltens auf Amazon oder durch die Bewertung der Kreditwürdigkeit potenzieller Hauskäufer) Einzug in das tägliche Leben gefunden. Spätestens seit der umfassenden Nutzung von generativer KI[72] wie ChatGPT erlebt diese Technologie einen echten Höhenflug und beschäftigt neben allen anderen Branchen auch die Rechtsanwender. Es liegt auf der Hand, dass fortgeschrittene technische Lösungsmöglichkeiten sowohl zur Begehung von Straftaten genutzt als auch als smartes Ermittlungstool eingesetzt werden können. Mithin wird KI sowohl aufseiten der Straftatbegehung als auch aufseiten der Strafverfolgung Einfluss auf die Gesellschaft nehmen. Es ist Aufgabe dieser Arbeit, Rahmenbedingungen für den Einsatz von KI als Ermittlungstool in Gestalt eines *Automated Suspicion Algorithm* vorzunehmen.

71 Siehe unten Kapitel III.E.I.
72 Begriffserläuterung siehe Kapitel III.

III. Regulierungsflut und tiefgreifende Grundrechtseingriffe

Der politische Handlungswille, man muss nahezu von einer Regulierungsflut im Bereich der Geldwäsche sprechen, ist – wie in Kapitel II. dargelegt wird – ungebremst. Neben den zahlreichen europäischen Vorgaben, die das deutsche Recht stark beeinflussen, startet auch der nationale Gesetzgeber fortlaufend eigene Vorhaben zur Verbesserung der Geldwäschebekämpfung. Diese Vorhaben sind gerade im Bereich der Geldwäsche teilweise erstmalig auch mit rechtlichen Normen verbunden, die den Einsatz von KI zu Zwecken der Ermittlungsarbeit sogar ausdrücklich vorsehen. Naturgemäß ist die automatisierte Erhebung, Verarbeitung und Speicherung von Datenbeständen mit tiefgreifenden Grundrechtseingriffen verbunden, die es in dieser Arbeit in Kapitel IV. und V. zu analysieren und zu bewerten gilt.

IV. Forschungslücke

Zwar gibt es bereits zahlreiche Arbeiten, die sich allgemein der Geldwäsche oder einzelnen Begriffen aus dem Geldwäscherecht widmen.[73] Auch nimmt die Zahl von Arbeiten, die sich mit der Automatisierung im Bereich der Kriminalitätsprävention und -aufdeckung beschäftigen, stetig zu.[74] Die Schnittstelle beider Perspektiven ist in der deutschsprachigen juristischen Literatur jedoch bis heute noch nicht monografisch beleuchtet worden. Zu dieser Problematik existieren nur wenige Beiträge in Aufsatzform, häufig nicht von Juristen, sondern von Computerwissenschaftlern verfasst.[75] In

73 Siehe nur zuletzt die Monografien von *Tsakalis*, Die Verflechtung zwischen Geldwäsche und Steuerhinterziehung – Zugleich eine Darstellung der historischen Entwicklung des strafrechtlichen Geldwäschebegriffs im internationalen und europäischen Raum, 2022, insb. S. 34 ff.; *Gürkan*, Der risikoorientierte Ansatz zur Geldwäscheprävention und seine Folgen – Geldwäschegesetz und Kreditwesengesetz im Lichte von Rechtsdogmatik und Rechtsökonomie, 2019, zum risikobasierten Ansatz auf Ebene der Verpflichteten; *Wende*, Die Verdachtsmeldung als Mittel zur Bekämpfung der Geldwäsche am Beispiel der Kreditinstitute, 2024, mit Fokus auf der Verdachtsmeldung.

74 Jüngst etwa: *Peters*, 2023, allerdings anders als in dieser Arbeit vor allem auf den strafprozessualen Anfangsverdacht im Kontext der Marktmanipulation bezogen.

75 Siehe etwa *Chen/Khoa/Teoh/Nazir/Karuppiah/Lam,* Knowledge and Information Systems 2016, 245 ff.; *Lamba/Glazier/Cámara/Schmerl/Garlan/Pfeffer,* IWSPA '17: Proceedings of the 3rd ACM on International Workshop on Security And Privacy Analytics 2017, 17 ff.

der internationalen Literatur hat das Thema zwar etwas mehr Aufmerksamkeit erfahren,[76] dort fehlen jedoch Bezüge zu Besonderheiten des deutschen Rechts.

Es herrscht damit an der Schnittstelle von Geldwäsche und KI eine Forschungslücke, welche zu erhellen sich die vorliegende Arbeit zur Aufgabe gemacht hat.

76 Siehe etwa *Rich*, University of Pennsylvania Law Review 2016, 871 ff.; *Bertrand/Maxwell/Vamparys,* International Data Privacy Law 2021, 276 ff.; *Pavlidis,* Journal of Money Laundering Control 2023, 155 ff.