AI Generated Money Laundering Alerts as Probable Cause in Criminal Law?

Lena Leffer[1] & Lucia Sommerer[2]

It is estimated that between $ 500 billion to $ 1 trillion are laundered every year,[3] with serious implications for society – as money laundering threatens the integrity of the global financial system, a law-abiding economy and social cohesion as a whole.[4]

Against this backdrop "big data and artificial intelligence for the financial sector" are the buzzwords of the hour[5]: In the field of money laundering, the use of machine learning could revolutionize law enforcement and (semi-)automate the detection of suspicious behavior.[6]

Such automation is at the heart of the German government-funded research project "Machine Learning for the Efficient Identification of Conspicuous Financial Transactions" (MaLeFiz) conducted by the authors of this papers in cooperation with among others computer scientists from the Fraunhofer Institute for Secure Information Technology.

A central question that arises when using AI systems for money laundering detection is to what extent the labeling of a transaction as suspicious by an AI based on complex statistical-empirical knowledge is sufficient to represent probable cause in criminal law and to legitimize follow-up measures such as search warrants and wiretapping.

---

[1] The author is PhD student and research assistant at the Martin Luther University Halle-Wittenberg (Germany). Research on an anti-money laundering AI is the subject of the author's ongoing doctoral thesis.

[2] The author is Assistant Professor of Criminology, Criminal Compliance, Risk Management and Criminal Law at Martin Luther University Halle-Wittenberg (Germany) and Affiliate Fellow of the Information Society Project at Yale Law School (USA).

[3] This figure is based on surveys conducted by the Council of Europe by MONEYVAL, Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), Annual Report for 2022 (accessible at: https://perma.cc/A8EG-6N6L, last accessed: Jan. 2024), p. 8.

[4] See former FATF-President *Pleyer,* FAZ of 30.6.2021, p. 27; *Blaeschke*, Geldwäscheaufsicht über Notarinnen und Notare, DNotZ 2022, 827 (827); *Heger,* in: Lackner/Kühl/Heger, StGB, 30th ed. 2023, § 261, mn. 2.

[5] See e.g. *Schulz,* in: Gola/Heckmann, DSGVO BDSG, 3rd ed. 2022, Art. 6 GDPR, mn. 153 et seq.; *Dreisigacker/Hornung/Ritter-Döring,* Die BaFin-Prinzipien zum Einsatz von Algorithmen und KI in der Finanzwirtschaft – ein Überblick, RDi 2021, 580 (580); *Dieckmann,* in: Chibanguza/Kuß/Steege, KI, § 5, I., mn. 37 et seq.

[6] *Bertrand/Maxwell/Vamparys,* Do AI-based anti-money laundering (AML) systems violate European fundamental rights?, International Data Privacy Law 2021, 276 (276).

The paper at hand addresses this question with regard to German and U.S. law (5.). First, however, the status quo of anti-money laundering (1.) including its three-stage-model (2.) will be summarized, and the technological background (3.) as well as possible institutional loci for the application of an AI-system outlined (4.).

1. Failure of Traditional Anti-Money Laundering Approaches

Across the globe the financial sector´s compliance obligations and the governmental organizational setup for combating money laundering are very similarly structured due to globally recognized FATF standards.[7] However, obligated private sector entities such as banks are often quite overwhelmed with the preparation of suspicious activity reports (SARs) regarding transactions of their customers.[8] The obligation to make such reports rests on FATF Rec. 20 (implemented in Germany in § 43 (1) of the German Money Laundering Act (G-AMLA), in the U.S. inter alia in 12 CFR § 21.11). At the same time, the Financial Intelligence Units (FIUs; cf. FATF Rec. 29[9]) often pile up unprocessed suspicious activity reports.[10] The German FIU for example only forwards about 15% of all SARs to the public prosecutor's offices and only 0.5% of all SARs actually lead to criminal law consequences.[11] A total of 3.6 SARs were generated in

[7] *FATF*, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations, updated February 2023 (accessible at: https://perma.cc/YZR2-4YDU, last accessed: Jan. 2024).

[8] For Germany: *Kanning*, Kampf gegen Geldwäsche überfordert Banken, FAZ v. 09.10.2019 (accessible at: https://perma.cc/FGA7-7GGQ, last accessed: Jan. 2024); for the U.S.: FinCen Files – Easy Game for Money Launderers, SZ of 20.09.2020 (accessible at: https://perma.cc/K7RY-VKQZ, last accessed: Jan. 2024).

[9] In the U.S. called Financial Crimes Enforcement Network (FinCen), in France Intelligence Processing and Action against Illicit Financial Networks Unit (TRACFIN), in Italy Financial Intelligence Unit of Italy (UIF), in Germany simply Financial Intelligence Unit (FIU).

[10] For Germany: *Lenk*, Zu den Ermittlungen gegen Verantwortliche der Financial Intelligence Unit (FIU) wegen des Verdachts der Strafvereitelung im Amt, ZWH 2021, 353 (353); The FATF Country Report Germany also comments on the lack of effectiveness of the FIU: FATF, Anti-money laundering and counter-terrorist financing measures Germany – Mutual Evaluation Report, August 2022, et al. pp. 4, 9; due to the lack of or slow forwarding of suspicious activity reports to law enforcement authorities, the public prosecutor's office in the German city of Osnabrück even conducted a criminal investigation against the FIU*, Diehl/Siemens,* Ermittler gehen gegen Zoll-Spezialeinheit vor, Spiegel of 14.07.2020 (accessible at: https://perma.cc/JE9R-V7EY, last accessed: Jan. 2024). The investigation has since been discontinued, Staatsanwaltschaft Osnabrück, Press Release of 31.05.2023 (accessible at: https://perma.cc/J422-U3AH, last accessed: Jan. 2024); see also *El-Ghazi/Jansen,* Anwendung des risikobasierten Ansatzes durch die FIU als Strafvereitelung?, NZWiSt 2022, 465 (472).

[11] These percentages are based on FIU, Jahresbericht 2022 (accessible at: https://perma.cc/LV9N-ZB4S, last accessed: Jan. 2024) according to which the obligated parties submitted a total of approx. 340,000 suspicious activity reports (p. 16), the FIU passed on approx. 52,000 suspicious activity reports to the public prosecutor's offices (p. 19) and on the basis of this data there were approx. 1,100 judgments or indictments on the part of the law enforcement authorities (p. 21).

the U.S. in 2022.[12] In contrast to Germany, however, no figures are published on the extent to which the reports have led to relevant convictions.[13]

The low success numbers from Germany are consistent with international scholarship, which assumes a false-positive rate of up to 99% for SARs[14] (the term "false-positive" referring to those reports that did not suffice for a criminal indictment). This means that the German anti-money laundering-approach today is hardly any more successful than it was seven years ago. This is surprising since an improvement was expected after a restructuring of the FIU and the whole suspicious activity reporting in 2017, which was intended to increase the efficiency of the anti-money laundering process.[15] Despite all efforts in recent years, only an estimated one percent of all crimes annually related to money laundering are uncovered in Germany as well as worldwide.[16] This fact was recently criticized by the FATF, especially with regard to Germany.[17] Not least because of this inadequate mode of law enforcement, money laundering remains highly attractive for perpetrators worldwide.[18]

2. Three Stages of Anti-Money Laundering

In order to better understand the possible institutional loci for AI solutions to address these problems of law enforcement, the three-stage[19] anti-money laundering system

[12] A table with all SARs from 2022 can be generated on the FinCEN website: https://perma.cc/DB2R-L6KE (last accessed: Jan. 2024).

[13] *Anthony*, Reporting FinCEN's Suspicious Activity, Cato Institute 2022 (accessible at: https://perma.cc/M7JA-TMZN, last accessed: Jan. 2024).

[14] *Schmuck,* Künstliche Intelligenz im Geldwäsche-Transaktionsmonitoring – Umsetzungsimplikationen für eine ethische künstliche Intelligenz (KI) in der Geldwäscheprävention, ZRFC 2023, 55 (56); *Fruth,* Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states, Reuters, 14.03.2018 (accessible at: https://perma.cc/9CXA-DXP, last accessed: Jan. 2024).

[15] *Lenk,* Zu den Ermittlungen gegen Verantwortliche der Financial Intelligence Unit (FIU) wegen des Verdachts der Strafvereitelung im Amt, ZWH 2021, 353 (356). For details of the restructuring: *Bülte,* Die Risiken des Risikobasierten Ansatzes – Zu den Pflichten der FIU nach §§ 30, 32 GwG, NVwZ 2022, 378 (379).

[16] *Heuser*, in: Chan/Ennuschat/Lee/Lin/Storr, Künstliche Intelligenz als Ressource im Kampf gegen Geldwäsche?, Künstliche Intelligenz und Öffentliches Wirtschaftsrecht, 2022, p. 138.

[17] FATF, Anti-money laundering and counter-terrorist financing measures Germany – Mutual Evaluation Report, August 2022, et al. p. 3 et seqq.; *Wegner*, Der FATF-Deutschlandbericht im Überblick, GuR, 2022, 117 (117).

[18] *Heuser,* in: Chan/Ennuschat/Lee/Lin/Storr, (fn. 16), p. 138 with further references in fn. 4; see also *Berner*, Geldwäsche-Prävention: Cloud & Künstliche Intelligenz ist die einzige Chance, IT-Finanzmagazin.de of 21.10.2019 (accessible at: https://perma.cc/5K4S-UVHM, last accessed: Jan. 2024); *Bussmann/Veljovic,* Die hybride strafrechtliche Verfolgung der Geldwäsche – Schlussfolgerungen aus den Ergebnissen einer bundesweiten Studie, NZWiSt 2020, 417 (425) stress that Germany is a "money laundering paradise".

[19] The three-stage system is expected to gain a fourth stage at the European level in the future. In July 2021, the European Commission proposed the creation of a new authority in the form of a European Anti-Money Laundering and Countering the Financing of Terrorism Agency (AMLA). For further details, see: *Neumann,* Das Sanktionenrecht der vorgeschlagenen EU-Agentur für die Bekämpfung von Geldwäsche und Terrorismusfinanzierung (AMLA), NZWiSt 2021, 449 (449).

will first be described in more detail with regard to a) obligated private sector entities, b) FIUs, and c) law enforcement authorities.

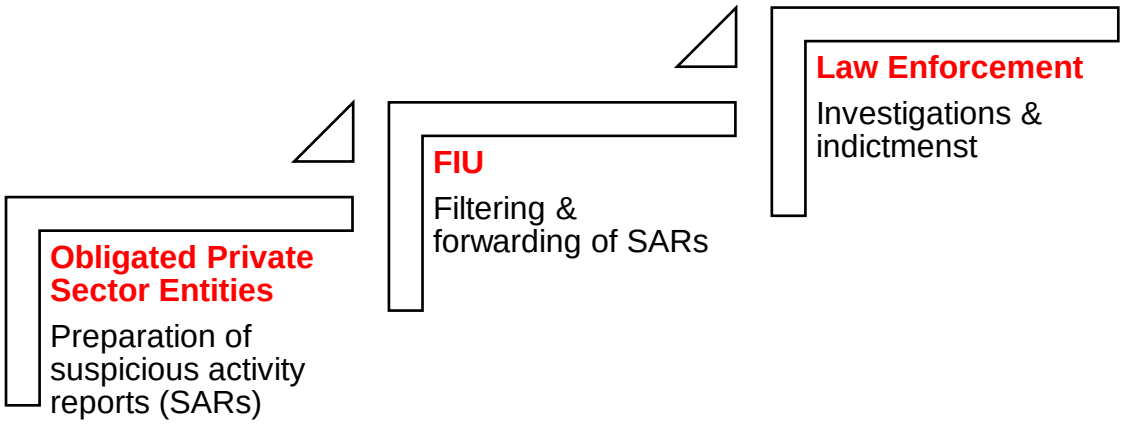

Fig. 1: Three-stage anti-money laundering system

a) Obligated Private Sector Entities

In its 40 recommendations, the FATF sets out which private sector groups are addressees of the obligations to combat money laundering: they include financial institutions[20] as well as designated non-financial businesses and professions, such as real estate agents, notaries, and lawyers.[21]

These are the so-called non-state “obligated entities” in the fight against money laundering; *Thompson* aptly chooses the term “White-Collar Police Force” due to the outsourcing of core crime prevention and prosecution tasks to them.[22]

For obliged entities, the FATF recommends the so-called risk-based approach.[23] This means that obliged entities must identify and assess money laundering risks in order to take countermeasures appropriate to the identified risks.[24] Interwoven with each other, the FATF recommendations include obligations aimed at both prevention and detection and, in this sense, represent a "two-sided coin".[25] On the one side of the

[20] FATF Rec. 10 et seqq.; FATF, International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation: The FATF Recommendations, updated February 2023, p. 126 (Glossary) (accessible at: https://perma.cc/YZR2-4YDU, last accessed: Jan. 2024).
[21] FATF Rec. 22; for Germany § 2 (1) G-AMLA; for the U.S. inter alia 12 CFR § 21.1.
[22] *Thompson*, The White-Collar Police Force: “Duty to Report” Statutes in Criminal Law Theory, Wm. & Mary Bill Rts. J. 11 (2002), p. 3.
[23] FATF Rec. 1; for Germany § 3a G-AMLA; for the U.S. inter alia 31 CFR § 1020.220; 31 CFR § 1020.210; 31 U.S.C. § 5321 (i, h).
[24] *Müller,* in: BeckOK GwG, 13th ed., 2023, § 3a, mn. 13.
[25] For Germany see BMI, Was ist Geldwäsche? (accessible: https://perma.cc/F3AN-DC8M, last accessed: Jan. 2024).

coin, obligated entities must preventively carry out risk management in accordance with FATF Rec. 10 (in Germany § 4 G-AMLA; in the U.S., inter alia 31 CFR § 1010.620; 31 U.S.C. § 5321 (i, h)), so that money laundering crimes do not occur in the future. On the other side of the coin lies the detection-focused obligation[26] to prepare SARs to the FIU in accordance with FATF Rec. 20 (in Germany § 43 (1) G-AMLA; USA 12 CFR § 21.11) to single out money laundering acts that have already been committed.

Preventive risk management includes a risk analysis tailored to the respective business area and subsequent internal security measures, such as the appointment of a money laundering officer and the ongoing schooling of employees regarding new money laundering typologies. Depending on the risk profile, risk management results in due diligence obligations on the part of obliged entities with regard to the screening of their customers.[27] According to § 10 G-AMLA as well as 31 CFR § 1020.220, 31 CFR § 1010.620, 31 U.S.C. § 5321 (k) the base level of due diligence requirement for *every* customer is their identification, also known as KYC (know your customer) principle.[28] In addition, in the event of certain circumstances – for example, in the case of a particularly complex and unusual transaction – increased due diligence obligations may apply, according to which, among other things, the transaction must be investigated further.[29] These due diligence obligations are often summed up under the headline of transaction monitoring.[30]

In the past, AI has rarely been applied for such monitoring, rather what most banks relied on were so called “rule-based” systems.[31] This refers to IT systems that execute rules that have been precisely programmed into the system beforehand by humans (e.g. transactions over $ 50,000 are generally coded as suspicious).[32] In the event of suspicious transactions, an alert is triggered, which leads to human employees taking

[26] For Germany see: *Barreto da Rosa,* in: Herzog, GwG, 5th ed. 2023, § 43, mn. 16 et seq.
[27] *Figura,* in: Herzog, (fn. 26), § 10, mn. 38 et seq.
[28] *Kaetzler*, in: Möslein/Omlor, 2nd ed. 2021, Part 1, Chapter 4, § 18, mn. 142.
[29] *Achtelik,* in: Herzog, (fn. 26), § 15, mn. 34.
[30] *Faust,* in: Ellenberger/Bunte, Bankrechts-Handbuch, 6th ed. 2022, § 89, mn. 175.
[31] *Bafin*, Big Data und künstliche Intelligenz: Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen, 15.06.2021 (accessible: https://perma.cc/U6P4-NRTC, last accessed: Jan. 2024); see also *Nink,* Justiz und Algorithmen – Über die Schwächen menschlicher Entscheidungsfindung und die Möglichkeit neuer Technologien in der Rechtsprechung, 2021, p. 325.
[32] *Heuser,* in: Chan/Ennuschat/Lee/Lin/Storr, (fn. 16), p. 145 et seq.

a closer look at the labeled transaction and deciding whether to submit a SAR ("human in the loop" decision support system[33]).

According to German case law, suspicious activity is present if "objectively recognizable facts indicate that a transaction is intended to remove illegal funds from the access of law enforcement authorities or to conceal the origin of illegal assets and if criminal origins of the funds cannot be ruled out".[34] According to U.S. case law, suspicious activity similarly is based on the evaluation of a combination of factors such as the person of the customer, their behavior, the nature and context of the transaction carried out and the question of whether it is an unusual transaction or not.[35]

It is these objectively recognizable facts (e.g. unusually high transaction; transactions with a high-risk country), which in the past have been programmed into rule-based IT systems.

This overview has already made it apparent that anti-money laundering requirements are oftentimes rather abstract and that their fulfillment can present obligated entities with difficult decisions requiring the weighing of risk and interest.[36] For violating anti-money laundering requirements obligated entities face fines of up to 5 million Euros or 10% of their total revenue in Germany (§ 56 G-AMLA),[37] and fines of up to $1,000,000. (31 U.S.C. 5321 (7)) in the U.S.

In view of such impending penalties, it is not surprising that SARs to FIUs are increasing worldwide. In Germany, reports have increased from just 60,000 in 2017 to almost 340,000 annual reports in 2021;[38] In the U.S. from 100,000 reports in 2000 to 3.6 million in 2022.[39]

---

[33] On the other hand, it would be decision replacement (so-called "human out of the loop") if an alarm from the system automatically led to the submission of the SAR. This is currently not taking place. For more information on the definition, see *Sommerer*, Self-imposed Algorithmic Thoughtlessness and the Automation of Crime Control – A study of person-based predictive policing and the algorithmic turn, 2022, p. 146 et seqq.

[34] Federal Constitutional Court of Germany (BVerfG), dec. of 11.03.2020, 2 BvL 5/17, NZWiSt 2020, 276 (281); see also OLG Frankfurt, dec. of 17.12.2012, 19 U 210/12, juris, mn. 25.

[35] *Lamba/Glazier/Cámara/Schmerl/Garlan/Pfeffer,* Model-based cluster analysis for identifying suspicious activity sequences in software, Proceedings of the 3rd ACM International Workshop on Security and Privacy Analytics, 2017, 17 (17); *Ping*, The suspicious transactions reporting system, Journal of Money Laundering Control, 8(3), 2005, 252 (254).

[36] *Krais,* in: BeckOK GwG, (fn. 24), § 10, mn. 38.

[37] *Barreto da Rosa,* in: Herzog, (fn. 26), § 56, mn. 111 et seq.

[38] FIU, Jahresbericht 2022, (fn. 11), p. 16; FIU, Jahresbericht 2017 (accessible at: https://perma.cc/LV9N-ZB4S, last accessed: Jan. 2024), p. 6.

[39] Financial Crimes Enforcement Network (2000), "The SAR activity review – trends, tips and issues", FINCEN Report, p. 2; U.S. Department of the Treasury (2023), "Financial crimes enforcement network: congressional budget justification and annual performance plan and report FY2023", Report, p. 13; already quoted in *Pavlidis*, Deploying artificial intelligence for anti-money laundering and asset

This increase clearly seems to be causing problems for the authorities responsible for evaluating submitted SARs: the FIUs.[40]

b) Financial Intelligence Unit (FIU)

According to FATF Rec. 20 (in Germany § 27 (1) G-AMLA; in the US 12 CFR § 21.11) the Financial Intelligence Unit, respectively in the U.S. the Financial Crimes Enforcement Network, has the function of collecting and analyzing information related to money laundering and passing it on to the law enforcement agencies. It receives and evaluates SARs submitted by obligated private sector entities. It is important to note that – at least in principle – according to German law the FIU must carry out its own examination of each and every SAR.[41] However, as its resources are limited, the German FIU has recently moved towards a risk-based approach, i.e. not every single SAR is examined by the FIU, but only certain reports with special risk characteristics.[42] Criteria relevant to the decision are in particular the maturity and complexity of case.[43] However, there are serious concerns about such a risk-based approach chosen by the FIU itself – which must not be confused with the risk-based approach of obliged entities recommended by the FATF and enshrined in law.[44] If the German FIU is no longer checking each and every SAR actual money laundering cases could remain unnoticed by law enforcement.[45]

c) Law Enforcement Agencies

When it comes to combating money laundering, law enforcement agencies (FATF Rec. 30) are only at the very end of an extensively regulated chain of action. Law enforcement agencies will receive the results of the FIU's analysis of individual SARs. They then evaluate the information provided by the FIU, carry out further investigations

---

recovery: the dawn of a new era, Journal of Money Laundering Control 2023, Vol. 26 No. 7, pp. 155-166.

[40] With a vivid list of the failures of the German FIU that have come to light in the past: *Lüneborg,* Geldwäsche-Compliance bei Güterhändlern – überbordend?, NZG 2022, 825 (825).

[41] *El-Ghazi/Jansen,* Anwendung des risikobasierten Ansatzes durch die FIU als Strafvereitelung?, NZWiSt 2022, 465 (466); *Barreto da Rosa,* in: Herzog, (fn. 26), § 28, mn. 4 et seq.

[42] See also BT-Drs. 20/5125, p. 3 et seq.

[43] BT-Drs. 20/5125, p. 9.

[44] *El-Ghazi/Jansen*, Anwendung des risikobasierten Ansatzes durch die FIU als Strafvereitelung?, NZWiSt 2022, 465 (470); see also *Beres*, FIU-Ermittlung "Rechtlich äußerst fraglich", tagesschau.de of 20.9.2021 (accessible: https://perma.cc/6DPE-9786, last accessed: Jan. 2024); see also Staatsanwaltschaft Osnabrück, press release of 31.05.2023 (accessible: https://perma.cc/J422-U3AH, last accessed: Jan. 2024).

[45] *Lenk,* Zu den Ermittlungen gegen Verantwortliche der Financial Intelligence Unit (FIU) wegen des Verdachts der Strafvereitelung im Amt, ZWH 2021, 353 (356).

and decide whether to discontinue the investigation or initiate criminal proceedings. The final assessment of whether there is probable cause in criminal law terms is up to law enforcement authorities.[46]

So far, the status quo of the current three-stage anti money laundering system.
This status quo combined with the largely untapped mountains of "Big Data" in banking[47] provides the breeding ground for the ongoing discussion of the use of AI systems.[48] In particular, it seems promising to develop AI solutions not only based on national but also on international transaction data, since money laundering is regularly a cross-border crime.
In the following, first, the term AI will be explained in more detail before three application scenarios of AI are discussed.

3. AI Terminology

To understand the euphoria surrounding the use of AI to combat money laundering, it is first necessary to clarify the term. Due to the self-learning character of advanced AI systems, the ideal scenario is that new money laundering typologies can be recognized and continuously adapted in detection programs.[49] However, the term "AI solution" must always be critically questioned – in all areas, not just those of anti-money laundering. AI has been a dazzling buzzword for decades, used to better market technical solutions. However, technology labeled as AI on the surface often lacks true AI in substance.
The exact definition of AI is controversial in both legal and computer science.[50] In 2021, for example, the German Federal Financial Supervisory Authority (BaFin), which is responsible for all banking supervision, provided [51] only a very vague[52] definition in its "Principles for the Use of Algorithms in Decision-Making Processes". According to BaFin AI is the combination of big data, computing resources and machine learning.

[46] BT-Drs. 18/11555, p. 144.
[47] Cf. *Götz,* Big Data und der Schutz von Datenbanken – Überblick und Grenzen, ZD 2014, 563 (563); *Momsen,* in: Chibanguza/Kuß/Steege, (fn. 5), § 2, G., mn. 18.
[48] *Dreisigacker/Hornung/Ritter-Döring,* Die BaFin-Prinzipien zum Einsatz von Algorithmen und KI in der Finanzwirtschaft – ein Überblick, RDi 2021, 580 (580).
[49] *Heuser,* in: Chan/Ennuschat/Lee/Lin/Storr, (fn. 16), p. 146.
[50] Cf. *Santos*, Nicht besser als nichts – Ein Kommentar zum KI-Verordnungsentwurf, ZfDR 2023, 23 (25).
[51] *Bafin*, Big Data und künstliche Intelligenz: Prinzipien für den Einsatz von Algorithmen in Entscheidungsprozessen, 15.06.2021 (accessible: https://perma.cc/U6P4-NRTC, last accessed: Jan. 2024).
[52] *Steinrötter/Stamenov,* in: Möslein/Omlor, (fn. 28), Part 1, Chapter 3, § 11, mn. 8.

The draft EU AI Act[53] understands AI – similarly vague – as software that has been developed with one or more of the techniques and concepts listed in Annex I of the Act (including machine learning) and that generates certain outputs (content, predictions, recommendations or decisions) to enact humanly specified goals, Art. 3 No. 1 EU AI Act.[54] At the beginning of December, an agreement was reached within the EU on the definition of AI based on the OECD definition.[55] However, the final version of the text is not yet available.

The AI definition relied upon in this paper is more concrete and based on a synopsis of the definitions of *Niederée/Nejdl* and *Sommerer*: AI is the algorithm-based automation of intelligent behavior, which is executed by a computer and evaluates data sets to achieve certain results based on predefined properties.[56] *Jiang et al.* summarize it particularly succinctly: "the core of AI is widely believed to be the research theories, methods, technologies, and applications for simulating, extending, and expanding human intelligence".[57] The goal of developing AI understood in this sense is to enable machines to solve tasks "intelligently".[58] An important subcategory of AI is the aforementioned machine learning.[59] It aims to generate knowledge from experience by using algorithms to develop complex patterns and models from large volumes of training data (e.g. a large number of images in the case of image recognition algorithms, a large number of transactions in the case of money laundering detection).[60] After a machine learning model has been "trained", it can be shown new – previously unknown – data for identification, classification or evaluation (e.g. a new photo, a new transaction).[61] This type of learning enables – especially in the financial

[53] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union acts, COM(2021) 206 final of 21.04.2021.
[54] *Santos*, Nicht besser als nichts – Ein Kommentar zum KI-Verordnungsentwurf, ZfDR 2023, 23 (25 et seq.).
[55] *Council of the EU*, Press release, "Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world", 09.12.2023 (accessible: https://perma.cc/A538-2NU8, last accessed: Jan. 2024).
[56] *Niederée/Nejdl,* in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 2020, § 2, mn. 3; *Sommerer*, Self-imposed Algorithmic Thoughtlessness and the Automation of Crime Control – A study of person-based predictive policing and the algorithmic turn, 2022, p. 52.
[57] *Jiang/Li/Luo/Yin/Kaynak*, Quo vadis artificial intelligence?, Discover Artificial Intelligence 2, 4, 2022 (accessible: https://perma.cc/24NU-W5TA, last accessed: Jan. 2024).
[58] *Fraunhofer Gesellschaft*, Maschinelles Lernen: Eine Analyse zu Kompetenzen, Forschung und Anwendung, p. 8 (accessible: https://perma.cc/AE3E-PRZV, last accessed: Jan. 2024).
[59] SAP, Maschinelles Lernen und KI: Wo liegt der Unterschied? (accessible: https://perma.cc/L4N5-72ET, last accessed: Jan. 2024).
[60] *Fraunhofer Gesellschaft*, Maschinelles Lernen: Eine Analyse zu Kompetenzen, Forschung und Anwendung, p. 8 (accessible: https://perma.cc/AE3E-PRZV, last accessed: Jan. 2024).
[61] Ibid.

sector and in the field of money laundering – the creation of automated results from data collections by recognizing learned patterns.[62] Machine learning, in turn, can be further subdivided into numerous subcategories – for example, decision trees,[63] clustering, or neural networks[64] (also called deep learning[65]). The latter is considered particularly non-transparent and hard to comprehend for human experts in ex post analyses of AI behavior.[66] These different models of machine learning each arrive at the same goal in different ways – creating automated results from learned patterns.

The benefits expected from the use of AI systems in contrast to the "conventional" rule-based systems in the field of money laundering detection is that AI might uncover previously unknown money laundering indicators and, above all, lead to an increase in effectiveness: a reduction of the large number – up to 99.5% as mentioned above – of "false positive" SARs.[67]

4. Application Scenarios

Based on the three-stage system of anti-money laundering described above (Fig. 1) and the understanding of AI just described, there are three possible application scenarios for a money laundering detection AI: a) within the obligated entities, b) within the FIUs, or c) within law enforcement agencies.

a) AI within Obligated Entities

The promise AI holds for obliged entities is to fulfill the legal requirements of national anti-money laundering law more efficiently for transaction monitoring,[68] i.e. to better identify money laundering patterns that trigger SARs to the FIU. The AI would here be used to "recognize meaningful connections in the noise of unsuspicious everyday transactions".[69] It is this scenario that makes the use of AI in the field of anti-money

[62] Ibid.
[63] *Knuth,* Lernende Entscheidungsbäume – Überholtes Verfahren oder vielseitige KI-Methode?, Informatik Spektrum 2021, 364 (364).
[64] *Brühl,* Big Data, Data Mining, Machine Learning und Predictive Analytics – ein konzeptioneller Überblick, CFS Working Paper Series, 2019, No. 617, p. 6.
[65] SAP, Maschinelles Lernen und KI: Wo liegt der Unterschied? (accessible: https://perma.cc/L4N5-72ET, last accessed: Jan. 2024).
[66] *Andrae*, Geldwäsche und Maschinelles Lernen – ein Strukturierungsrahmen bank und markt 2019, 73 (73).
[67] *Heuser,* in: Chan/Ennuschat/Lee/Lin/Storr, (fn. 16), p. 146.
[68] *Andrae*, Geldwäsche und Maschinelles Lernen – ein Strukturierungsrahmen, bank und markt 2019, 73 (73).
[69] *Baur,* Maschinen führen die Aufsicht – Offene Fragen der Kriminalprävention durch digitale Überwachungsagenten, ZIS 2020, 275 (278).

laundering so attractive, as money laundering is often disguised by linking many small, unsuspicious actions on the perpetrator side (so-called layering) that are hard to uncover for the human eye.[70] An AI, however, could function like a "tracking dog", so to speak, which reveals connection between individual red flags and "sounds the alarm".

There are various options for application:

In a first step, an AI solution could be used *on top* of tradition rule-based systems to reduce false alarms. Second, an AI solution could be used *next to* a traditional rule-based system for anomaly detection, i.e. to detect when perpetrators deliberately circumvent rule-based filters.[71] And third, AI could be used *instead* of traditional rule-based systems, replacing the old approach altogether.

Further, an AI system could be designed as decision-supporting ("human in the loop") or as a decision-replacing ("human out of the loop").[72]

Private companies who already today aim to offer such AI solutions to the financial sector include e.g. HawkAI,[73] SAS Institute,[74] InvestGlass,[75] and even Google.[76]

However, when evaluating the application of such automation technologies, there are numerous unresolved legal questions – from data protection to criminal procedural law and constitutional law.

In particular, the use of AI by obligated entities appears problematic to the extent that it is *private parties* (e.g. banks) that use this technology to identify criminal conduct, whereby the technology in turn was produced by *another* private party (software companies). Thus, these private actors are centrally involved in an inherently government task: law enforcement. The growing shift of government tasks to private parties in the context of law enforcement and criminal justice must be examined critically.[77]

---

[70] Ibid.

[71] *Schmuck,* Künstliche Intelligenz im Geldwäsche-Transaktionsmonitoring – Umsetzungsimplikationen für eine ethische künstliche Intelligenz (KI) in der Geldwäscheprävention, ZRFC 2023, 55 (56).

[72] See fn. 33.

[73] HawkAI, accessible: https://perma.cc/VCF7-J9YG (last accessed: Jan. 2024).

[74] SAS Institute, accessible: https://perma.cc/5QMW-HEV4 (last accessed: Jan. 2024).

[75] InvestGlass, accessible: www.investglass.com/de/automation-transaction (last accessed: Jan. 2024).

[76] Google AML AI, accessible: https://perma.cc/JT2R-U7N9 (last accessed: Jan. 2024).

[77] *Beukelmann,* Outsourcing bei Polizei und Strafjustiz, NJW-Spezial 2008, 280; *Böse,* Aufsichtsrechtliche Vorermittlungen in der Grauzone zwischen Strafverfolgung und Gefahrenabwehr, ZStW 2007, 847 (864 et seq.); *Lenk,* Sanktionsbewehrte Melde- und Anzeigepflichten – Zu den materiell-rechtlichen Problemen einer privatisierten Kriminalitätsbekämpfung, JR 2020, 103 (106, 111).

b) AI within the FIUs

On the other hand, an AI solution could be used within the FIU to automate the analysis of all incoming SARs and make the analysis more efficient.

In Germany the FIU is using – as mentioned above – a risk-based approach whereby not every report is examined[78] but only those appearing the most promising.[79] According to the FIU, this is done by using filter methods that prioritize incoming SARs that contain certain "trigger characteristics".[80] Since 2020, this risk-based approach has been largely automated, the German FIU claims.[81] According to the German government, this automation is enabled by a system called "FIU Analytics" and described as containing AI.[82] Within this system it is alleged that SARs are automatically compared with certain data stocks and pre-filtered semi-automatically on the basis of pre-defined risk focal points.[83] Reports that do not trigger an alarm within the "FIU Analytics" system will remain untouched by human analysis in the so-called "information pool" but will be continuously automatically compared with newly incoming information.[84] It is unclear, however, to what extent "FIU Analytics" is truly an AI solution. In the latest FATF report, the software is described more as a kind of trial software or field test.[85]

In the U.S., the Financial Crimes Enforcement Network AI System (FAIS) has been used at the FIU-level since the 90s.[86] It, too, however, appears to not yet be a full fledges artificial intelligence system in the modern machine learning sense, but rather

[78] Critical *El-Ghazi/Jansen,* Anwendung des risikobasierten Ansatzes durch die FIU als Strafvereitelung?, NZWiSt 2022, 465 (467 et seq.).
[79] FIU, Jahresbericht 2019 (accessible at: https://perma.cc/LV9N-ZB4S, last accessed: Jan. 2024), pp. 10, 12.
[80] FIU, Jahresbericht 2019, (fn. 79), pp. 10, 12; in this respect, *Lenk* speaks of a "rather superficial initial assessment", which should probably lead to a strong reduction in the number of unprocessed SARs due to the risk-based approach, *Lenk,* Zu den Ermittlungen gegen Verantwortliche der Financial Intelligence Unit (FIU) wegen des Verdachts der Strafvereitelung im Amt, ZWH 2021, 353 (355).
[81] BT-Drs. 20/5125, p. 12.
[82] Ibid.
[83] Ibid.
[84] *Barreto da Rosa,* in: Herzog, (fn. 26), section 5, preliminary remarks, mn. 25.
[85] FATF, Anti-money laundering and counter-terrorist financing measures Germany – Mutual Evaluation Report, August 2022, p. 67; see also BT-Drs. 20/5125, p. 10 et seq.; *Adamek,* Millionenvorhaben zur Geldwäschebekämpfung gestoppt, tagesschau.de (accessible: https://perma.cc/2R5J-BJM4, last accessed: Jan. 2024).
[86] *Senator/Goldberg/Wooton/Cottini/Khan/Klinger/Llamas/Marrone/Wong*, Financial crimes enforcement network AI system (FAIS) identifying potential money laundering from reports of large cash transaction, AI Magazine 1995, Volume 16, Number 4, pp. 21-39: "It is a complex system incorporating several aspects of AI technology, including rule-based reasoning and a blackboard. FAIS consists of an underlying database (that functions as a black-board), a graphic user interface, and several pre-processing and analysis modules."

a rule-based data analysis system focusing inter alia on the visualization of connections (link analysis).[87]

Regardless of whether AI solutions are already being used within FIUs today or will be used in the future, it will be important to think through whether FIUs may base AI-analyses on their existing legal regulatory framework or whether new regulation delineating basic rule of law requirements for such AI may be necessary.

The German legislator understands the FIU as a purely administrative entity that is not to be equated with law enforcement authorities in any way, so that laws and regulations of digital and automated data processing found in the German Code of Criminal Procedure or Police Laws do not directly apply the FIU.[88] The German Data Protection Commissioner recently pointed out, in his view, currently, there is no statutory basis for the FIU's automated evaluation of suspicious activity reports, the FIU's analyses are thus unconstitutional in Germany.[89]

c) AI within the Law Enforcement Agencies

It is theoretically possible to locate an AI for money laundering detection within law enforcement agencies. In practice, the use of AI is, however, the least interesting at this location, as it is the very end of the "chain of suspicion", so to speak. The relevant data for the investigations have already been collected and pre-processed elsewhere (step one and two of the three-stage anti-money laundering regime).

Currently no laws addressing the mass automated analysis of all (transactional) data transmitted by the FIU exists in the German Code of Criminal Procedure. If the German government would still decide to use AI at this stage a new statutory foundation would have to be enacted to address this issue. Without statutory foundation governmental data processing in Germany is unconstitutional.

A recent decision by the Federal Constitutional Court on automated data analysis in a different area, namely in preventive predictive policing, points towards strict limitation also on such statutory foundation in crime detection.[90] As does a recent ruling by the

[87] *Alexandre/Balsa*, Incorporating machine learning and a risk-based strategy in an anti-money laundering multiagent system, Expert Systems With Applications 2023, 1 (1).
[88] BT-Drs. 20/5125, p. 7.
[89] BfDI, Activity Report 2020 – 29th Activity Report on Data Protection and Freedom of Information, 2020, p. 63 et seq.
[90] BVerfG, decision of 16.02.2023, 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1196).

European Court of Justice that prohibited the use of "self-learning AI systems" for flight passenger data pattern recognition to detect and predict criminal behavior.[91]

The three-stage system of anti-money laundering shows once again that law enforcement today is only one component in an overall security concept of prevention and detection.[92] This makes the factual and legal demarcation between the two on the one hand and the permissible information acquisition and processing on the other hand considerably challenging.[93]

5. AI Alert as Reasonable Suspicion?

Finally, regardless of the place of application, the question appears as to what quality should be ascribed to AI-generated alerts in criminal law. This question arises both if the law enforcement authorities themselves were to use AI and if an AI alert generated by third parties (obligated entities) were passed through to them by the FIU: Do AI alerts equal probable cause (grounded in Germany in § 152 (2) of the Code of Criminal Procedure; in the U.S. in the 4th Amendment)?

Case law and literature on the (non-)admissibility of purely empirical-statistical findings as basis for criminal justice decision-making have existed for quite some time.[94] In the mid 1990s, this question was discussed avidly for the first time in Germany with regard to statistical recidivism prediction.[95] It must now be determined, however, to what extent these predominantly critical considerations can be transferred to AI, which is also based on – albeit very complex – empirical-statistical models.

[91] ECJ, decision of 21.06.2022, C-817/19.
[92] *Zöller*, Die zweckändernde Nutzung von personenbezogenen Daten im Strafverfahren – Gegenwart und Zukunft von § 161 StPO, StV 2019, 419 (419).
[93] Recently, the BVerfG once again ruled on automated data evaluation, BVerfG decision of 16.02.2023, 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 et seqq.
[94] For the resonable suspicion *Bach*, Der Verdacht im Strafverfahren – abstrakt –, JURA 2007, 12, (13 et seq.); for preventive detention based on statistical data BGH, decision of 25.03.2009, 5 StR 7/09, NStZ 2009, 499 (499); also *Boetticher/Dittmann/Nedopil/Nowara/Wolf,* Zum richtigen Umgang mit Prognoseinstrumenten durch psychiatrische und psychologische Sachverständige und Gerichte*,* NStZ 2009, 478 (480 et seq.); on resonable suspicion in tax law, *Peters*, Der strafrechtliche Anfangsverdacht im Steuerrecht Kooperative Vorermittlungen in Grenzfällen, DStR 2015, 2583 (2586); cf. also *Schenke,* Police and Regulatory Law, 10th ed., 2018, p. 43, mn. 77; *Leisner*, Die polizeiliche Gefahr zwischen Eintrittswahrscheinlichkeit und Schadenshöhe, DÖV 2002, 326 (326, 333).
[95] *Steinke,* Der Beweiswert forensischer Gutachten*,* NStZ 1994, 16 (17 f.).

If an AI alert is equivalent to probable cause, law enforcement personnel could immediately order certain measures such as a search warrant when receiving an alert. If an AI alert is, however, not equivalent to a probable cause, law enforcement agencies would first have to collect further information using less intrusive methods.

(1) Status Quo in Germany: Statistical Findings *not* as Probable Cause

In Germany, discussions on the admissibility of statistical findings as basis for individualized criminal justice decisions date back to the mid 1990s and the early 2000s and occurred in the context of the use of statistical prognosis tools to determine the need for preventive detention by courts.[96] In Germany, preventive detention is a so-called "measure of improvement and security", it takes effect *after* particularly dangerous offenders have served their prison sentence in full and would actually have to be released into freedom if the court had not ordered subsequent preventive detention. The measure is therefore not intended to punish the perpetrator, but rather to protect the public from ongoing danger from repeat offenders. Regarding such decisions, the German Federal Supreme Court (BGH) concluded that judges should not be guided solely by statistical information when ordering the preventive detention, but that statistical information can be one of several decision-making factors.[97] The judge must take *all* aspects of an offender's personality, behavior, and environment into account (totality of circumstances) and make an individualized decision.

Similar statements have been made in German legal scholarship regarding reasonable suspicion. *Bach*, for example, argues very aptly against the use of statistical findings to substantiate probable cause, as this would lead to a decision based merely on the "suspicion of suspicion".[98]

Böse even goes so far as to call data collection by BaFin on the basis of statistical likelihood for the monitoring of securities trading (inter alia for the investigation of criminal offences under the German Securities Trading Act – WpHG) to be generally unconstitutional.[99]

[96] See *Volckart*, Zur Bedeutung der Basisrate in der Kriminalprognose – Was zum Teufel ist eine Basisrate?, Recht & Psychatrie 2002, 105 (110).
[97] BGH, decision of 27.07.2000, 1 StR 263/00, NJW 2000, 3015 (3015); *Best,* in: Dölling/Duttge/König/Rössner, Gesamtes Strafrecht, 5th ed. 2022, § 66 StGB, mn. 1.
[98] *Bach,* Der Verdacht im Strafverfahren – abstrakt –, JURA 2007, 12 (13).
[99] *Böse*, Aufsichtsrechtliche Vorermittlungen in der Grauzone zwischen Strafverfolgung und Gefahrenabwehr, ZStW 2007, 848 (854).

For probable cause – just as for preventive detention – it is necessary to take a totally of circumstances view of a situation and to make an individualized decision – both aspects are precluded by purely generalized, statistical calculation.

(2) Status Quo in U.S.: Statistical Findings *not* as Probable Cause

Classifying statistical results in the legal system is an universal challenge. In the U.S. according to the 4th Amendment, which guarantees protection against state encroachment, probable cause is required for e.g. a search warrant.[100] Probable cause must be focused on an individualized person in a certain place.[101] The factual basis for probable cause must be well founded.[102] This means that the police must have evidence sufficient to conclude that a suspect is probably guilty or that they probably have evidence of a crime hidden inside their home.[103] The U.S. Supreme Court has held that the determination of probable cause and reasonable suspicion ultimately depends on reason,[104] "common sense"[105] and police experience.[106] The Court has also made it clear that individual suspicion is ultimately a matter of "probabilities", although it has also stated that these probabilities "are not technical".[107]

In U.S. American scientific discourse, too, the sole use of statistical data for the substantiation of probable cause within criminal proceedings is viewed critically.[108]

[100] *Ferguson*, Big Data and Predictive Reasonable Suspicion, University of Pennsylvania Law Review 2015, 327 (329).
[101] Ibid.
[102] *Brennan-Marquez*, "Plausible Cause": Explanatory Standards in the Age of Powerful Machines, Vanderbilt Law Review 2017, 1249 (1249).
[103] *Colb*, Probabilities in Probable Cause and Beyond: Statistical Versus Concrete Harms, Cornell Law Library 2010, 69 (71).
[104] See Terry v. Ohio (1968) 392 U.S. 1, 21 ("the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion"); *Rich*, Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment, University of Pennsylvania Law Review 2016, 871 (877).
[105] See Illinois v. Gates, (1983) 462 U.S. 213, 244; *Rich*, Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment, University of Pennsylvania Law Review 2016, 871 (877).
[106] See United States v. Cortez (1981) 449 U.S. 411, 418; *Rich*, Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment, University of Pennsylvania Law Review 2016, 871 (877).
[107] See United States v. Cortez (1981) 449 U.S. 411, 418 ("The process does not deal with hard certainties, but with probabilities"); Brinegar v. United States (1949) 338 U.S. 160, 175 ("In dealing with probable cause, however, as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act").
[108] *Rich*, Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment, University of Pennsylvania Law Review 2016, 871 (879); *Goldberg*, Getting Beyond Intuition in the Probable Cause Inquiry, Lewis & Clark Law Review 2013, 789 (808 et seqq.).

While it is often assumed that a sufficient statistical probability of at least 51% is required for the probable cause, since one cannot assume a "sufficient" probability below this value,[109] the U.S. Supreme Court has stressed that the meaning of "probable" should be interpreted differently within the reasoning of probable cause.[110] In particular, probable cause does not require a preponderance of evidence, nor proof that the belief is more likely to be right than wrong.[111] Only a reasonable probability is required, but not a probability in the statistical sense.[112]

As in German law, U.S. law also focuses on the totality of the circumstance's aspect of probable cause decisions, which, as the U.S. Supreme Court emphasizes, cannot be guaranteed by statistics alone.[113] Further, U.S. scholars such as *Gardiner* are generally critical of basing *any* individualized decision in the justice system purely on statistics.[114]

We can pause at this point and recognize: the German and U.S. legal systems are generally skeptical to the use of purely statistical knowledge as basis for probable cause.

Does the same critical assessments apply to AI models, which, too, are essentially based on statistical calculations?

(3) Status Futurus: AI as Probable Cause?

Against AI as Probable Cause

There are three main arguments against the fact that AI should be treated differently from statistical methods and thus for the fact that AI cannot generate probable cause: the required totality of circumstances evaluation in individualized decisions, the inability of AI to give reason and the hollowing out of probable cause.

[109] *Colb*, Probabilities in Probable Cause and Beyond: Statistical Versus Concrete Harms, Cornell Law Library 2010, 69 (71); *Alvarez*, LibreTexts Workforce (accessible: https://perma.cc/XM34-WRAK, last accessed: Jan. 2024).
[110] Texas v. Brown (1983) 460 U.S. 730, 742; also see People v. Carrington (2009) 47 Cal.4th 145, 163.
[111] Ibid.
[112] See Illinois v. Gates (1983) 462 U.S. 213, 238; Safford Unified School District v. Redding (2009) 557 U.S. 364, 371.
[113] Illinois v. Gates (1983) 462 U.S. 213, 231; also see United States v. Cortez (1981) 449 U.S. 411, 418.
[114] *Gardiner*, in: Chase/Coady (eds.), The Routledge Handbook of Applied Epistemology, 2018.

Totality of Circumstances in Individualized Decisions

The issue of lack of a totality of circumstances perspective is often raised against algorithmic decisions, including decisions in criminal justice such as predictive policing.[115] An algorithm can only "see" what it has been trained by people to see. This become obvious with many facial recognition programs, which often deliver unreliable results for minorities due to their training with "non-diverse" faces.[116] In this sense, *Wittgenstein's* famous saying "the limits of my language are the limits of my world"[117] applies to AI. What is not quantifiable in the code language of the algorithm and what is not inscribed into the algorithm does not exist in the world of the AI. A machine learning AI cannot independently identify new relevant categories of information that are outside of its predefined input variables and training data set.

Even with a large number of input variables, it is impossible for humans to exhaustively foresee all potentially relevant influences on every conceivable future individual case and then write an algorithm for it, respectively train an AI for each individual case by including it in the training data set. Unlike humans, who can respond spontaneously to new influences of a situation, an algorithm is never able to take a true totality of circumstances view.

It is important to note that although the (partial) automation of individualized *administrative* decisions is already permitted elsewhere in German law, it is precisely not permitted in criminal law. And even in administrative law it is only permitted if there is neither discretion nor scope for assessment, i.e. only in the case of simply structured, schematical decisions.[118] However, the decision on a probable cause in criminal law does not fall into this category of simply structured decisions.

Although *Rich* admits that AI could certainly take a human-*like* overall view: "The novelty of an [AI] is its potential to step into the shoes of that human being by analyzing groups of disparate facts together and drawing conclusions about the probability of an individual's guilt."[119] He still concludes that this mere *likeness* is not sufficient to

[115] *Sommerer*, Self-imposed Algorithmic Thoughtlessness and the Automation of Crime Control – A study of person-based predictive policing and the algorithmic turn, 2022, pp. 84 et seqq.
[116] *Benedict,* The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest, HeinOnline (accessible: https://perma.cc/L2FG-JLNT, last accessed Jan. 2024).
[117] *Wittgenstein,* Tractatus Logico-Philosophicus – Logisch-Philosophische Abhandlung, 1963, sentence 5.6.
[118] Cf. *Wischmeyer,* in: Ebers/Heinze/Krügel/Steinrötter, (fn. 56), § 20, mn. 65.
[119] *Rich*, Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment, University of Pennsylvania Law Review 2016, 871 (892).

automatically trigger probable cause. According to *Rich,* only a human can take a comprehensive overall view; an AI alert can only be a piece of information to be considered by a human along with other pieces of information on the path towards the cause.[120]

Inability of AI to Give Reason – Right to Explanation

Wischmeyer[121] in Germany and *Brennan-Marquez* in the U.S. complement this perspective by emphasizing the central role of the obligation to give reason as part of the rule of law. AI cannot justify itself, cannot give reason to itself when questioned[122] – this is especially true for the most promising forms of AI, such as particularly opaque neural networks. Making a serious decision, such as probable cause, without the ability of citizens to question this decision and demand a reason and an explanation undermines core aspects of the rule of law.

Hollowing out Probable Cause

Finally, automation of probable cause by AI could undermine the core task of probable cause that is to act as a partition wall between a space in society that the state may encroach upon and a space that is free of state interference and criminal justice suspicions. The dissolution of this partition wall threatens to lead us into surveillance state-like conditions. In principle, as can be seen in various Criminal Procedure Code norms for digital data collection in Germany[123] and the 4th Amendment in the U.S., probable cause is required *before* large amounts of data may be combed through to look for potential criminal activities. In the case of AI-based automated data analysis that is conducted not because of pre-existing probable cause but to create probable cause – even if it is only for the narrowly defined area of anti-money laundering – this principle would be turned upside down.[124]

---

[120] Ibid p. 901 et seqq.; 923: “First, courts must recognize that an ASA’s [Automated Suspicion Algorithm] prediction, like any prediction of criminality, is only a part of the totality-of-the-circumstances analysis, and litigants must be prepared to educate courts about the importance of facts other than an ASA’s numerical prediction in determining the existence of individualized suspicion”.

[121] Not on probable cause but more generally on AI decision-making *Wischmeyer*, Regulierung intelligenter Systeme, AöR 2018, 1 (55).

[122] *Brennan-Marquez*, "Plausible Cause": Explanatory Standards in the Age of Powerful Machines, Vanderbilt Law Review 2017, 1249 (1249; 1253): “[…] and judges must have an opportunity to scrutinize that explanation: to test its overall intelligibility; to weigh it against the best innocent account on the other side; and to evaluate its consistency with background values, flowing from the Constitution, from general legality principles, and from other sources of positive law”.

[123] E.g. dragnet investigations § 98a German Criminal Procedure Code.

[124] Cf. also for predictive policing: BVerfG, decision of 16.02.2023, 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 (1196).

Pro AI as Probable Cause

However, there could be two arguments in favor of the fact that AI should be treated differently from simple statistical outputs – and thus by all means generate an initial suspicion: On the one hand, the larger amounts of data that are processed by AI compared to simple statistical models, and on the other hand, a human-like nature of data processing due to the higher degree of complexity processed.

It could be argued that the totality of circumstances required by law, which traditional statistical calculations are unable to provide, is precisely what AI is good at achieving. This is because the inclusion of immense amounts of data ("Big Data") and the complexity of the considered interrelated data points. Depending on the perspective, one could say that AI – as admitted by *Rich* above – at least carries out a human-*like* process of considering, and an *almost* totality of circumstances. Or one could say that an AI may even be able to perform a totality of circumstances analysis that is superior to humans, since the AI may be able to recognize patterns and contexts that remain hidden from the human eye. This perspective assumes that AI can see *more* than humans.

However, only one scholar – *Peters* based in Germany – has so far expressly spoken out in favor of the assumption of probable cause being triggered by an AI money laundering alert.[125]

We can sum up at this point: according to the current state of legal scholarship, AI does not yet seem to generate probable cause in and of itself in money laundering cases. At the same time, however, especially in the U.S. literature a certain pragmatism can be noticed when authors, despite their criticism, seem to assume that the automation of the criminal justice system is a development that can hardly be stopped.

[125] *Peters*, Smarte Verdachtsgewinnung – Eine strafprozessuale und verfassungsrechtliche Untersuchung der Verdachtsgewinnung mittels Künstlicher Intelligenz, 2023, p. 149 et seq.

In the meantime, scholarship's critical stance does, however, not mean that AI is meaningless in the fight against money laundering. AI has its role as one element of an overall assessment to be carried out by humans.

6. Conclusion

When using AI for money laundering detection, it will depend crucially on the adaptation of the legal framework and the place and time of use. One of the most likely application scenarios is the use of automation techniques right at the beginning of anti-money laundering at banks. This approach is promising in order to ensure an efficient and resource-saving subsequent state-based anti-money laundering process. This is because the application of AI solutions at an early anti-money laundering stage could make SARs submitted to the FIUs much more substantive, thereby simplify the work of FIUs and subsequent investigations by law enforcement authorities.

One thing is clear: It is to be expected that in the near or far future, investigations by law enforcement authorities will no longer be just the result of coincidental reports and accidental whistleblowers, but rather the result of the automated search for criminal conduct.[126]

It remains to be seen whether AI alerts will only support human evaluation processes of probable cause in the future or whether and when the human decision-maker will be replaced by a fully automated system of anti-money laundering.

[126] *Baur,* Maschinen führen die Aufsicht – Offene Fragen der Kriminalprävention durch digitale Überwachungsagenten, ZIS 2020, 275 (276).