

**Gießener Schriften
zum Strafrecht und zur Kriminologie**

55

Amadeus Peters

Smarte Verdachtsgewinnung

Eine strafprozessuale und verfassungsrechtliche Untersuchung
der Verdachtsgewinnung mittels Künstlicher Intelligenz



Nomos

**Gießener Schriften
zum Strafrecht und zur Kriminologie**

mitbegründet von Prof. Dr. Günter Heine (†)

herausgegeben von

Prof. Dr. Britta Bannenberg
Prof. Dr. Dr. h.c. Dr. h.c. Walter Groppe
Prof. Dr. Pierre Hauck
Prof. Dr. Bernd Hecker
Prof. Dr. Bernhard Kretschmer
Prof. Dr. Arthur Kreuzer
Prof. Dr. Thomas Rotsch
Prof. Dr. Gabriele Wolfslast

Band 55

Amadeus Peters

Smarte Verdachtsgewinnung

Eine strafprozessuale und verfassungsrechtliche Untersuchung
der Verdachtsgewinnung mittels Künstlicher Intelligenz



Nomos



Onlineversion
Nomos eLibrary

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Zugl.: Diss., Justus-Liebig-Universität Gießen, Fachbereich Rechtswissenschaft, 2023

ISBN 978-3-7560-1113-1 (Print)

ISBN 978-3-7489-4232-0 (ePDF)

Die Bände 1 – 13 sind erschienen in der Reihe „Nomos Universitätsschriften Recht“

1. Auflage 2023

© Nomos Verlagsgesellschaft, Baden-Baden 2023. Gesamtverantwortung für Druck und Herstellung bei der Nomos Verlagsgesellschaft mbH & Co. KG. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

Meinen Eltern

Vorwort

Diese Arbeit widme ich meinen Eltern Professor Dr. Dr. Uwe H. Peters und Dr. Anna Martini, die mich stets unterstützt haben. Die Widmung erfolgt zugleich in Gedenken an meinen Vater, dem ich meine wissenschaftliche Neugier verdanke.

Diese Untersuchung wäre ohne zahlreiche Denkanstöße, Diskussionen und Unterstützungen nicht möglich gewesen. Zunächst möchte ich meinem Doktorvater Professor Dr. Thomas Rotsch danken. Als ich im Jahr 2016 mit dem Vorschlag für diese Untersuchung an ihn herantrat, war Künstliche Intelligenz noch äußerst selten Untersuchungsgegenstand rechtswissenschaftlicher Arbeiten. Für sein Vertrauen und seine Unterstützung während der Entstehung dieser Arbeit bin ich äußerst dankbar.

Für die freundliche Aufnahme am Information Society Project der Yale Law School danke ich Professor Jack M. Balkin. Für die vielen bereichernden Gespräche während dieses Forschungsaufenthaltes danke ich Assistant Professor Dr. Nikkolos Guggenberger, Liron Shilo und Juniorprofessorin Dr. Lucia Sommerer, denen ich freundschaftlich verbunden bin. Für die finanzielle Unterstützung des Forschungsaufenthaltes danke ich der Deutschen Stiftung für Recht und Informatik.

Ich danke Professor Dr. Dres. h.c. Ingolf Pernice für die Aufnahme als Fellow am Alexander von Humboldt Institut für Internet und Gesellschaft. Für die hervorragende Betreuung in dieser Zeit gilt Dr. Jörg Pohle mein Dank. Ihm und Assistant Professor Dr. Riikka Koulu danke ich zudem für zahlreiche fruchtbare Diskussionen, die teilweise in weiteren wissenschaftlichen Arbeiten außerhalb der vorliegenden Dissertation gemündet sind. In dem Zusammenhang möchte ich auch Professorin Dr. Claudia Müller-Birn für den wertvollen interdisziplinären Austausch zu Diskriminierungsfragen beim Einsatz Künstlicher Intelligenz danken.

Professor Dr. Carsten Momsen und Professor Dr. Franz Reimer danke ich herzlich für die zügige und bereichernde Erstellung des Zweit- bzw. des Drittgutachtens. Für die sehr hilfreiche Durchsicht des Manuskripts danke ich Charlotte Heppner.

Berlin im Mai 2023

Inhaltsübersicht

Inhaltsverzeichnis	11
Abkürzungsverzeichnis	19
Kapitel 1: Einleitung	21
A. Anlass der Untersuchung	21
B. Ziel der Untersuchung	49
C. Gang der Untersuchung	50
Kapitel 2: Funktionsweise und Folgen Künstlicher Intelligenz	53
A. Einleitung	53
B. Maschinelles Lernen	56
C. Tatsächliche Folgen des Einsatzes Künstlicher Intelligenz	72
Kapitel 3: Rechtssystematische Einordnung	89
A. Einleitung	89
B. Rechtssystematische Einordnung als strafprozessualer Verdacht	90
C. Rechtssystematische Einordnung zwischen Gefahrenabwehr und Strafverfolgung	126
D. Rechtssystematische Einordnung innerhalb der Strafverfolgung	140
Kapitel 4: Auswahl von Merkmalen und Verzerrungen	155
A. Einleitung	155
B. Fairness-Debatte	160
C. US-amerikanische Perspektive	163
D. Ungleichbehandlungen und Art. 3 GG	178
Kapitel 5: Begründung von Black-box-Ausgaben	225
A. Einleitung	225

Inhaltsübersicht

B. Funktionen der Begründung	229
C. Verfassungsrechtliche Begründungspflicht	232
D. Begründung des strafprozessualen Verdachts	236
E. Vereinbarkeit der Undurchsichtigkeit mit den Begründungsfunktionen	238
F. Parallelen zum standardisierten Verfahren bei Geschwindigkeitsmessungen	245
G. Fazit	249
 Kapitel 6: Das allgemeine Persönlichkeitsrecht	 253
A. Einleitung	253
B. Das Recht auf informationelle Selbstbestimmung	255
C. Nemo-tenetur-Grundsatz	292
 Kapitel 7: Zusammenfassung und Fazit	 297
 Literaturverzeichnis	 303

Inhaltsverzeichnis

Abkürzungsverzeichnis	19
Kapitel 1: Einleitung	21
A. Anlass der Untersuchung	21
I. Probleme bei der Aufdeckung von Ordnungswidrigkeiten und Straftaten	22
1. Insiderhandel und Marktmanipulation	23
2. Steuerstraftaten	25
3. Ergebnis	27
II. Entwicklung der Künstlichen Intelligenz	28
III. Nutzung Künstlicher Intelligenz zur Ermittlung von Straftaten in der Praxis	33
1. Situation außerhalb der Europäischen Union	33
2. Situation in Staaten der Europäischen Union	36
3. Situation in Deutschland	37
a) Situation in Bezug auf die Ermittlung von Steuerstraftaten	39
aa) Datenaufkommen aus Steuererklärungen	39
bb) Risikomanagementsysteme	40
cc) Verwendete Programme	41
b) Situation in Bezug auf die Ermittlung von Wirtschaftsstraftaten	42
c) Staatliche Datafizierung in Deutschland	44
4. Ergebnis	45
IV. Stand der rechtswissenschaftlichen Forschung	47
V. Zusammenfassung	48
B. Ziel der Untersuchung	49
C. Gang der Untersuchung	50
Kapitel 2: Funktionsweise und Folgen Künstlicher Intelligenz	53
A. Einleitung	53

B. Maschinelles Lernen	56
I. Überwachtes Lernen	57
1. Funktionsweise	57
2. Anwendung zur Ermittlung von Straftaten	61
3. Rechtliche Fragestellungen	62
II. Unüberwachtes Lernen	63
1. Funktionsweise	63
2. Anwendung zur Ermittlung von Straftaten	64
3. Rechtliche Fragestellungen	65
III. Künstliche Neuronale Netze	65
1. Das menschliche Gehirn und der Lernprozess	66
2. Funktionsweise Künstlicher Neuronaler Netzwerke	67
3. Beispiel	70
4. Rechtliche Fragestellungen	72
C. Tatsächliche Folgen des Einsatzes Künstlicher Intelligenz	72
I. Undurchsichtigkeit	72
1. Fehlende Fachkenntnisse	73
2. Schutz vor Kenntnisnahme	73
a) Staatlicher Schutz	74
b) Privatwirtschaftlicher Schutz	74
c) Ergebnis	75
3. Technische Undurchsichtigkeit	75
a) Korrelation	77
b) Black-box	77
c) White box	79
4. Rechtliche Fragestellung	80
a) Verfassungsrechtlicher Begründungszwang	81
b) Recht auf informationelle Selbstbestimmung	81
c) Anfangsverdacht	82
II. Auswahl der Merkmale	82
1. Tatsächliche Fragestellung	82
2. Rechtliche Fragestellung	83
III. Verzerrung der Ergebnisse	84
1. Erhebung der Daten	84
2. Klassifizierung der Trainingsdaten	85
3. Architektur der Algorithmen	86
4. Verhinderung von Verzerrungen und Fehlern	87
5. Ergebnis	87

6. Rechtliche Fragestellungen	88
Kapitel 3: Rechtssystematische Einordnung	89
A. Einleitung	89
B. Rechtssystematische Einordnung als strafprozessualer Verdacht	90
I. Einleitung	90
II. Verdachtsgrundlage	92
III. Verdachtshypothese	94
1. Sachverhalt	95
a) Tatgeschehen	95
b) Begleitumstände	96
2. Rechtliche Würdigung	97
3. Beweisbarkeit	99
4. Prozessvoraussetzungen	99
5. Zusammenspiel der Bestandteile der Verdachtshypothese	100
IV. Verdacht als Wahrscheinlichkeit	100
1. Allgemeine Wahrscheinlichkeitsbegriffe	101
a) Klassischer bzw. mathematischer Wahrscheinlichkeitsbegriff	102
b) Objektive Wahrscheinlichkeitsbegriffe	104
aa) Statistischer Wahrscheinlichkeitsbegriff	104
bb) Logischer Wahrscheinlichkeitsbegriff	105
c) Subjektiver Wahrscheinlichkeitsbegriff	106
2. Der Wahrscheinlichkeitsbegriff in Rechtsprechung und Literatur	107
a) Der Wahrscheinlichkeitsbegriff in der Rechtsprechung	107
b) Der Wahrscheinlichkeitsbegriff in der Literatur zum Verdacht	109
aa) Steinberg	109
bb) Schulz	110
cc) Fincke	110
dd) Lüderssen und Jahn	110
c) Der Wahrscheinlichkeitsbegriff in der straf- und zivilrechtlichen Literatur zum Beweis	111
3. Stellungnahme und Zusammenfassung	114

V. Entstehung des Verdachts	117
1. Einleitung	117
2. Subjektive Wahrscheinlichkeit	118
3. Statistische Wahrscheinlichkeit	119
4. Kenntnis der Künstlichen Intelligenz	119
VI. Zwischenergebnis: Verdacht	120
VII. Die positive Ausgabe der smarten Verdachtsgewinnung als strafprozessualer Verdacht	121
1. Statistischer Wahrscheinlichkeitsbegriff	121
a) Überwachtes Lernen	122
b) Unüberwachtes Lernen	125
2. Subjektiver Wahrscheinlichkeitsbegriff	125
C. Rechtssystematische Einordnung zwischen Gefahrenabwehr und Strafverfolgung	126
I. Relevanz der rechtssystematischen Einordnung	127
II. Strafverfolgung	128
III. Gefahrenabwehr	129
IV. Abgrenzung	130
1. Verwechslung von Strafverfolgung und Strafprozess	131
2. Verfassungsrechtliche Auslegung	132
a) Wortlaut des Art. 74 Abs. 1 Nr. 1 GG	132
b) Die Begrenzung des Strafverfolgungsbegriffs durch die historische Auslegung des Art. 74 Abs. 1 Nr. 1 GG	132
c) Einwände gegen die Argumentation der historischen Auslegung	134
d) Ergebnis	137
3. Vorschriften und Rechtsinstitute aus der Zeit des Grundgesetzes	137
4. Reaktionsfunktion des Anfangsverdachts	138
5. Der Anfangsverdacht als verfassungsrechtliche Rechtmäßigkeitvoraussetzung	139
V. Ergebnis	140
D. Rechtssystematische Einordnung innerhalb der Strafverfolgung	140
I. Kein Verdacht und Vorfeldermittlungen	141
1. Aufdeckung und Ermittlung unbekannter Steuerfälle durch Steuerfahndung	142

2. Überwachung der Einhaltung der Verbote durch die BaFin	143
3. Geldwäsche	145
4. Zwischenergebnis	145
II. Vorverdacht und Vorermittlungen	146
III. Anfangsverdacht und Ermittlungen	147
IV. Weitere Verdachtsgrade	148
V. Quantifizierung des Anfangsverdachts	148
1. Rechtliche Herleitung	149
2. Praxis	150
3. Ergebnis	153
 Kapitel 4: Auswahl von Merkmalen und Verzerrungen	 155
A. Einleitung	155
B. Fairness-Debatte	160
C. US-amerikanische Perspektive	163
I. Equal Protection Clause	164
1. Einleitung und historische Entwicklung	164
2. Der Supreme Court und das Anticlassification Principle	165
3. Die US-amerikanische Literatur und das Antisubordination Principle	168
4. Rechtsprechung	170
a) US Supreme Court	170
b) Gerichte der US-Bundestaaten	172
II. Due Process Clause	173
1. Due Process Dogmatik	173
2. Due Process Rechtsprechung	175
III. Zwischenergebnis	177
D. Ungleichbehandlungen und Art. 3 GG	178
I. Ungleichbehandlung	179
II. Rechtfertigung	181
1. Regelungsgegenstand: Funktionstüchtigkeit der Strafrechtspflege	182
2. Einfluss betroffener Freiheitsrechte	185
3. Differenzierungskriterium	186
a) Verfügbare des Differenzierungskriteriums	187

b) Unmittelbare Anknüpfung an Differenzierungskriterien	188
c) Mehrheit von Differenzierungskriterien	189
aa) Kumulative Differenzierungskriterien	189
bb) Alternative Differenzierungskriterien	190
cc) Intersektionale Differenzierungskriterien	191
d) Mittelbare Diskriminierung	192
e) Zwischenergebnis und Konsequenzen für die smarte Verdachtsgewinnung	195
4. Am Grundsatz der Verhältnismäßigkeit orientierter verfassungsrechtlicher Prüfungsmaßstab	197
a) Differenzierungsziel	199
b) Geeignetes Mittel zur Differenzierung	199
aa) Grundsätzliche Geeignetheit	200
bb) Wirklichkeit	201
cc) Zeitliche Wirklichkeit	201
dd) Soziale Wirklichkeit	202
ee) Individualität vs. Gruppenzugehörigkeit	207
ff) Korrelation und Kausalität	212
gg) Umgang mit wenig verfügbaren Merkmalen	215
c) Erforderlichkeit	218
aa) Smarte Verdachtsgewinnung vs. menschliche Ermittlungsperson	218
bb) Human in the loop	222
cc) Veränderung der Daten	223
d) Angemessenheit	223
Kapitel 5: Begründung von Black-box-Ausgaben	225
A. Einleitung	225
I. Erklärbarkeit vs. Begründung	225
II. Gang der Untersuchung	228
B. Funktionen der Begründung	229
I. Kontrollfunktionen der Begründung	229
1. Selbstkontrolle	229
2. Fachliche Fremdkontrolle	230
3. Öffentliche Kontrolle	231
II. Kommunikationsfunktion der Begründung	231

C. Verfassungsrechtliche Begründungspflicht	232
I. Rechtsstaatsprinzip	233
II. Effektiver Rechtsschutz	234
III. Demokratieprinzip	235
IV. Geheimhaltungsinteresse der Ermittlungsbehörden	235
D. Begründung des strafprozessualen Verdachts	236
I. Grundsatz der Aktenvollständigkeit und -wahrheit	236
II. Verfassungsrechtliche Begründungspflicht	237
E. Vereinbarkeit der Undurchsichtigkeit mit den Begründungsfunktionen	238
I. Vorüberlegung: Gegenstand der Begründung	238
II. Kontrolle von Entscheidungen	242
1. Selbstkontrolle	242
2. Fremdkontrolle	243
III. Kommunikation von Entscheidungen	245
F. Parallelen zum standardisierten Verfahren bei Geschwindigkeitsmessungen	245
G. Fazit	249
I. Technische Undurchsichtigkeit	250
II. Voluntative Undurchsichtigkeit	250
Kapitel 6: Das allgemeine Persönlichkeitsrecht	253
A. Einleitung	253
B. Das Recht auf informationelle Selbstbestimmung	255
I. Einleitung	255
II. Schutzbereich	257
III. Eingriff	260
IV. Rechtfertigung	262
1. Zweck	263
2. Geeignetheit	264
3. Erforderlichkeit	264
4. Angemessenheit	265
a) Verdachtslosigkeit	266
aa) Anlass	267
bb) Eingriffstiefe	269
b) Streubreite	270

c) Potenzielle Einleitung eines Strafverfahrens	271
d) Persönlichkeitsrelevanz der Informationen	272
e) Recht auf Selbstdarstellung	273
aa) Recht auf informationelle Selbstbestimmung	274
bb) Verpönte Merkmale	277
f) Undurchsichtigkeit	278
aa) Undurchsichtige Schlussfolgerungen	278
bb) Undurchsichtige Schlussfolgerung auf zusätzliche Informationen	280
g) Wirksame Strafverfolgung	281
h) Schutz hochrangiger Rechtsgüter/Schwere Straftaten	282
i) Kennzahlen der smarten Verdachtsgewinnung	282
j) Eingriffsbegrenzende Maßnahmen	284
k) Fazit Einsatzphase	286
l) Trainingsphase	287
V. Ermächtigungsgrundlage	287
1. Anforderungen an eine Ermächtigungsgrundlage	287
2. De lege lata	289
C. Nemo-tenetur-Grundsatz	292
I. Inhalt und Reichweite des Nemo-tenetur-Grundsatzes	292
II. Vor der Tatbegehung	293
III. Die Tatbegehung	294
IV. Nach Tatbegehung	294
Kapitel 7: Zusammenfassung und Fazit	297
Literaturverzeichnis	303

Abkürzungsverzeichnis

a.A.	andere Ansicht
Abs.	Absatz
Alt.	Alternative
Art.	Artikel
Bd.	Band
Beschl. v.	Beschluss vom
BGH	Bundesgerichtshof
bspw.	beispielsweise
BT-Drs.	Bundestag-Drucksache
BVerfG	Bundesverfassungsgericht
EMRK	Konvention zum Schutz der Menschenrechte und Grundfreiheiten
et al.	et alii (und andere)
i.S.v.	im Sinne von
i.S.d.	im Sinne des
i.e.S.	im engeren Sinne
f(f).	folgende Seite(n)
FS	Festschrift (auch: Festgabe)
GG	Grundgesetz für die Bundesrepublik Deutschland
Hrsg.	Herausgeber
m.w.N.	mit weiteren Nachweisen
OLG	Oberlandesgericht
S.	Seite; (im Rahmen eines Gesetzeszitats:) Satz
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
u.a.	und andere
Urt. v.	Urteil vom
Var.	Variante
vgl.	vergleiche

Kapitel 1: Einleitung

A. Anlass der Untersuchung

Der deutsche Staat wird digitaler. Immer mehr Aufgaben erledigt er unter Zuhilfenahme von Computern. Dafür speichert er die Informationen, über die er verfügt, als Daten ab. Die Möglichkeiten, diese Daten für sich nutzbar zu machen, erschöpfen sich nicht in der Rationalisierung von Prozessen. Die Auswertungen der Daten mit Methoden der Künstlichen Intelligenz erlauben Rückschlüsse, die unter Verwendung herkömmlicher – analoger – Mechanismen der Datenverarbeitung nicht möglich gewesen wären oder einen unverhältnismäßigen Aufwand bedeutet hätten.

Mögliche Anwendungsbereiche für Künstliche Intelligenz sind das Ordnungswidrigkeitenrecht und das Strafrecht. Künstliche Intelligenz könnte dem Staat dabei helfen, unbekannte Ordnungswidrigkeiten und Straftaten aufzuspüren. Die Künstliche Intelligenz würde hierfür durch die Analyse von Daten Verdachtsmomente generieren, die sich der Staat bei der Verfolgung der Taten zunutze machen könnte. Diese Vorgehensweise soll in der folgenden Untersuchung als „smarte Verdachtsgewinnung“ bezeichnet und an späterer Stelle genauer definiert werden.

Die smarte Verdachtsgewinnung bietet sich bei Straftaten und Ordnungswidrigkeiten an, die ohne eine Überprüfung des zugrundeliegenden Sachverhalts in der Regel unentdeckt bleiben und deren zugrundeliegenden Sachverhalte entweder in einem zu großen Umfang auftreten, um eine manuelle Kontrolle gewährleisten zu können oder die bei einer Kontrolle unter dem Aufdeckungspotential der smarten Verdachtsgewinnung zurückbleiben würden. Wie noch dargestellt werden soll, besteht bei zahlreichen staatlichen Stellen in Deutschland sowie im europäischen und außereuropäischen Ausland ein besonderes Interesse an dem Einsatz einer smarten Verdachtsgewinnung. Dieses Interesse drückt sich entweder durch dessen öffentliche Artikulation oder den bereits stattfindenden Einsatz smarter Verdachtsgewinnung in der Praxis aus.

Gegenstand der vorliegenden Untersuchung ist die rechtliche Einordnung sowie die rechtlichen Grenzen der smarten Verdachtsgewinnung. Konkret soll untersucht werden, wie die Gewinnung von Verdachtsmomenten hinsichtlich Straftaten und Ordnungswidrigkeiten durch die Analyse

von Daten mit Hilfe Künstlicher Intelligenz rechtssystematisch zu fassen sowie ob und unter welchen Voraussetzungen dieses Vorgehen verfassungskonform möglich ist.

In das Thema soll wie folgt eingeführt werden: Erstens soll dargestellt werden, warum die Entdeckung von Straftaten und Ordnungswidrigkeiten in den vorgenannten Konstellationen, in denen sich eine smarte Verdachtsgewinnung anbietet, den Staat bisher vor eine Herausforderung stellt. Zweitens soll die Entwicklung der Künstlichen Intelligenz und der „Datafizierung“ erläutert werden. Drittens soll der Einsatz Künstlicher Intelligenz zur Verdachtsgewinnung weltweit und in Deutschland beschrieben werden. Viertens soll ein Überblick über den Stand der rechtswissenschaftlichen Forschung zum Untersuchungsgegenstand gegeben werden.

I. Probleme bei der Aufdeckung von Ordnungswidrigkeiten und Straftaten

Probleme bei der Aufdeckung von Ordnungswidrigkeiten und Straftaten lassen sich in vielen verschiedenen Lebensbereichen aufzeigen. Besonders instruktiv und von praktischer Bedeutung für die smarte Verdachtsgewinnung sind Beispiele aus dem Wirtschaftsleben und der Steuerverwaltung, auf die hier exemplarisch sogleich näher eingegangen werden soll.

Aus dem Wirtschafts- und Steuerstrafrecht ist bekannt, dass viele Straftaten häufig erst aufgrund von Kontrollen entdeckt werden (sog. Kontrolldelikte).¹ Ein Grund hierfür ist das Fehlen eines individualisierbaren Opfers, das die Straftat anzeigen könnte. Gehen bei allgemeinen Straftaten ca. 85-98% der eingeleiteten Ermittlungsverfahren auf Anzeigen zurück,² sind es bei Wirtschafts- und Steuerstrafaten nur ca. 10%.³

Erschwerend kommt hinzu, dass bei Straftaten, die sich auf arglistigem Verhalten gründen – wie dies bei Wirtschafts- und Steuerstrafaten häufig der Fall ist – die Begehungsformen sich fortlaufend verändern.⁴ Die Straftäter, die wiederholt Wirtschafts- oder Steuerstrafaten begehen, werden versuchen, bestehende Lücken in Überwachungsmechanismen zu entdecken und für sich zu nutzen.

1 Kudlich/Oğlakcioğlu, Wirtschaftsstrafrecht, S. 7 f.

2 Eisenberg/Conen, NJW 1998, 2241 (2243); Lange, Vorermittlungen, S. 78 m.w.N. Kühne, Strafprozessrecht, S. 215 m.w.N.

3 Kudlich/Oğlakcioğlu, Wirtschaftsstrafrecht, S. 7.

4 Baesens/Van Vlasselaer/Verbeke, Fraud analytics, S. 19.

1. Insiderhandel und Marktmanipulation

Die Problematik fehlender Anzeigenerstatter wird am Beispiel des Insiderhandels deutlich. Beim Insiderhandel verschafft sich der Täter beim Handel mit Finanzinstrumenten einen Vorteil gegenüber den anderen Marktteilnehmern, indem er über Informationen verfügt, die nicht öffentlich sind und deren Bekanntwerden einen Einfluss auf den Marktpreis des Finanzinstruments haben.⁵ Durch die Nutzung der Informationen – bspw. durch den Kauf eines Finanzinstruments – erhält der Täter einen unlauteren Vorteil gegenüber anderen Handelsteilnehmern und macht sich strafbar. Der Handel kann vom Täter mit Hilfe von Strohmannern – beispielsweise durch den Einsatz ausländischer Briefkastenfirmen – vollkommen anonym betrieben werden.⁶

Man stelle sich den folgenden Fall vor. Ein Täter kauft Aktien, bevor die Aktiengesellschaft Ankündigungen macht, die den Aktienkurs positiv beeinflussen. Kannte der Täter die Ankündigung vor ihrer Veröffentlichung und kaufte er daraufhin die Aktien, dann hat er sich durch den Kauf der Aktien strafbar gemacht. Für den Verkäufer der Aktien ist jedoch weder vor noch nach der Ankündigung ersichtlich, dass der Käufer seiner Aktien sich strafbar gemacht hat. Denn nach außen hin handelt es sich um einen normalen und insofern unauffälligen Handelsvorgang.⁷ Dies gilt auch dann, wenn die Transaktion in einer sehr engen zeitlichen Nähe zur Ankündigung der Aktiengesellschaft erfolgt. Denn bei den geläufigen Handelsvolumina dürfte der Kauf der Aktien – auch in großem Umfang – unmittelbar vor einer wichtigen Ankündigung nicht auffällig sein. So beträgt beispielsweise die Zahl der im Durchschnitt an einem Handelstag gehandelten Siemens-Aktien am Referenzmarkt Xetra mehr als zwei Millionen Aktien.⁸ Allenfalls könnte beim Handel mit Aktien durch prominente Führungskräfte der Aktiengesellschaft, bei denen Insiderkenntnisse zu erwarten sind, ein Verdacht auf Insiderhandel aufkommen. Jedoch könnte in einem solchen Fall ein Strohmann als Käufer eingesetzt werden. Der Verkäufer der Aktien wird somit in der Regel keinen Verdacht schöpfen und sich nicht veranlasst sehen, eine Anzeige zu erstatten. Hieran dürfte auch nichts ändern, dass

5 *Nestler*, Bank- und Kapitalmarktstrafrecht, S. 251 ff.

6 *Nestler*, Bank- und Kapitalmarktstrafrecht, S. 244.

7 *Koch*, Ermittlung und Verfolgung von strafbarem Insiderhandel, S. 61.

8 Aktienkennzahlen Siemens, http://www.siemens.com/investor/de/siemens_aktie/aktiekennzahlen.htm, abgerufen am: 27.6.2020.

Führungskräfte sowie „in enger Beziehung zu ihnen stehende Personen“ nach Art. 19 MAR (Marktmissbrauchsverordnung⁹) verpflichtet sind, ihre eigenen Geschäfte zu melden. Es ist nicht zu erwarten, dass ein vorsätzlich handelnder Täter dieser Pflicht nachkommt.

Zu den fehlenden Anzeigen kommt beim Insiderhandel noch erschwerend hinzu, dass auf Grund der Masse an potenziellen Tathandlungen – nämlich jeder einzelnen Transaktion – eine überwältigende Menge an Handlungen kontrolliert werden muss. Das Handelssystem Xetra der deutschen Börse in Frankfurt a.M. bearbeitet beispielsweise bis zu 136 Millionen Transaktionen am Tag.¹⁰ Eine Auswertung aller Transaktionen kann offensichtlich nicht analog erfolgen.

Ebenso wie der Insiderhandel ist auch die Marktmanipulation eine unauffällige Straftat, die schwer greifbar und inmitten ebenso zahlreicher Transaktionen „versteckt“ ist.¹¹ Dies gilt besonders für die sog. handelsgestützte Marktmanipulation. Bei dieser Form der Marktmanipulation wird, allein durch das Verhalten am Markt, versucht, die Preisbildung zu lenken – bspw. durch die Aufgabe von Kauf- oder Verkaufsangeboten, die später wieder storniert werden sollen.¹² Das Erkennen von handelsgestützter Marktmanipulation wird zusätzlich dadurch erschwert, dass zahlreiche Manipulationsvarianten im automatisierten Hochfrequenzhandel zum Tragen kommen.¹³

Bereits die große Menge an Transaktionen lässt eine computerbasierte Auswertung der Transaktionen als notwendig erscheinen. Jedoch wird durch die bisherigen computerbasierten Systeme keine effektive Abhilfe geschaffen. Die Financial Industry Regulatory Authority (FINRA), eine unter anderem mit der Aufdeckung von Insiderhandel und Marktmanipulation

9 Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission.

10 Xetra - Regulierter Markt für hochliquiden Handel, Deutsche Börse AG, <http://www.deutsche-boerse-cash-market.com/blob/2647824/342a232ab55d65762c938646b526ecb7/data/Broschuere--Regulierter-Markt-fuer-hochliquiden-Handel.pdf>, abgerufen am: 19.4.2017, S. 16.

11 Blumenberg, Marktmanipulation und Compliance, S. 22 f.

12 Nestler, Bank- und Kapitalmarktstrafrecht, S. 267; Blumenberg, Marktmanipulation und Compliance, S. 39 ff.

13 Näher hierzu Kasiske, WM 2014, 1933 (1934 ff.).

in der US-amerikanischen Wertpapierbranche betraute Stelle,¹⁴ überwacht beispielsweise täglich durchschnittlich 66,7 Milliarden Transaktionen.¹⁵ Ein Prozent dieser Transaktionen werden mit herkömmlichen computerbasierten Überwachungssystemen als verdächtig markiert.¹⁶ Dies entspricht 667 Millionen verdächtigen Transaktionen am Tag. Übertragen auf die Transaktionen des Handelssystems Xetra ergibt ein Prozent der Transaktionen bis zu 1,36 Millionen verdächtige Transaktionen am Tag. Diese Zahl an verdächtigen Transaktionen ist offensichtlich zu groß, um effektiv überprüft werden zu können.

Angesichts dieser Schwierigkeiten verwundert es nicht, dass von hohen Dunkelziffern bei Insiderhandel und Marktmanipulation ausgegangen wird.¹⁷ Belege gibt es hierfür – was in der Natur der Sache liegen dürfte – nicht. Jedoch erscheint es angesichts der dargestellten Schwierigkeiten äußerst plausibel, dass Insiderhandel und Marktmanipulation häufig unentdeckt bleiben.

2. Steuerstraftaten

Gemessen an der vergleichsweise großen Zahl von Verurteilungen kommt Straftaten gegenüber dem Fiskus in Deutschland eine besondere gesellschaftliche Relevanz zu. Beispielsweise erfolgten 2015 11.539 Verurteilungen auf Grundlage von Straftatbeständen nach der Abgabenordnung.¹⁸ Im Vergleich hierzu betrug im selben Jahr die Zahl der Verurteilungen nach dem Wertpapierhandelsgesetz – wozu auch die Tatbestände des Insiderhan-

14 Scholz, Selbst- und Fremdregulierung von Wertpapierbörsen, S. 95 f.; *Halfpap*, Kapitalmarktaufsicht in Europa und den USA, S. 123; Koch, Ermittlung und Verfolgung von strafbarem Insiderhandel, S. 63 f.

15 FINRA Processes Billions of Transactions Per Day, FINRA, <https://www.finra.org/about/technology>, abgerufen am: 27.6.2020.

16 So noch Tom Gira (executive vice president for market regulation von FINRA) im Mai 2016: Market surveillance a constant challenge: FINRA, Reuters, <http://www.reuters.com/article/us-finance-summit-finra-idUSKCN0Y82GL>, abgerufen am: 27.6.2020.

17 Koch, Ermittlung und Verfolgung von strafbarem Insiderhandel, S. 62; Lenk, Neuer Markt - Das Scheitern eines Kapitalmarktexperimentes?, S. 69; Blumenberg, Marktmanipulation und Compliance, S. 23; Beim Insiderhandel sind die Ermittler oft hilflos, Süddeutsche Zeitung, <http://www.sueddeutsche.de/wirtschaft/kommentar-insiderhandel-die-unsichtbare-straftat-1.3367628>, abgerufen am: 26.6.2020.

18 Statistisches Bundesamt, Fachserie 10, Reihe 3, 2015, (Strafverfolgung), S. 53.

dels und der Marktmanipulation gehören – lediglich 14.¹⁹ Trotz der hohen Zahl an Verurteilungen und der kontinuierlichen Kontrollen durch die Steuerämter kennt auch der Fiskus das Problem nicht entdeckter Steuerstraftaten. Wie hoch die Dunkelziffer ist, lässt sich nur schwer ermitteln. Man geht jedoch auch hier davon aus, dass die Dunkelziffer hoch ist.²⁰

Einen Anhaltspunkt für das Gewicht der nicht entdeckten Steuerstraftaten bieten die Schätzungen zu Schäden durch Steuerstraftaten. Die Schätzungen zur Höhe der jährlich entstehenden Schäden durch Straftaten gegenüber dem Fiskus gehen zwar stark auseinander. Alle Schätzungen gehen jedoch von signifikanten Schäden aus: Die Steuerausfälle in Deutschland aufgrund der Schattenwirtschaft wurden für das Jahr 2011 von *Schneider* auf 83 Milliarden Euro²¹ bzw. von *Murphy* auf 166 Milliarden Euro²² geschätzt. Anderen Schätzungen zufolge sollen jährlich 50-100 Milliarden Euro Steuern hinterzogen werden.²³ Spezifischere Schätzungen gibt es für sog. Umsatzsteuerkarusselle, deren verursachter Schaden einen Großteil der jährlichen Umsatzsteuerbeträge in Höhe von 14-15 Milliarden Euro in Deutschland ausmachen soll.²⁴ Die Steuerausfälle durch die bisherige Manipulierung von Kassensystemen werden auf 5 bis 10 Milliarden Euro jährlich geschätzt.²⁵

Die Begehung von Steuerstraftaten kann, ebenso wie beim Insiderhandel und der Marktmanipulation, unauffällig sein. Die Steuerhinterziehung nach § 370 Abs.1 AO beispielsweise kann durch die Angabe unrichtiger oder unvollständiger steuerlich erheblicher Tatsachen sowie das Unterlassen, solche Angaben zu machen, begangen werden. Weder muss die Unrichtigkeit oder Unvollständigkeit der Angaben, noch muss das vollständige Fehlen von Angaben aus sich heraus erkennbar sein.

19 Statistisches Bundesamt, Fachserie 10, Reihe 3, 2015, (Strafverfolgung), S. 57.

20 *Peter/Kramer*, Steuerstrafrecht, S. 117; *Kudlich/Oğlakcioğlu*, Wirtschaftsstrafrecht, S. 71.

21 *Schneider*, Turkish Economic Review 2016, 1 (10).

22 *Murphy*, The Cost of Tax Abuse, S. 10.

23 *Herbertz*, HRRS 2012, 318 (318).

24 *Ott*, Die EU - eine Goldgrube für Betrüger, <http://www.sueddeutsche.de/wirtschaft/umsatzsteuertricksereien-die-eu-eine-goldgrube-fuer-betrueger-1.1730226>, abgerufen am: 27.6.2020.

25 BT-Drs. 18/10667, S. 2; ARD-KONTRASTE: Bundesrechnungshof schätzt Steuerhinterziehung durch manipulierte Ladenkassen auf 10 Milliarden Euro Schäuble gegen Sofortmaßnahmen, <http://www.presseportal.de/pm/110520/3082870#null>, abgerufen am: 27.6.2020.

Als weitere Herausforderung für die Steuerämter kommt die Zahl der zu bearbeitenden Steuerfälle hinzu. Im Jahr 2012 waren ca. 40 Millionen Steuerfälle zu bearbeiten.²⁶ Dem standen (2013) insgesamt 100.901 Mitarbeiter des einfachen Dienstes bis zum höheren Dienst gegenüber.²⁷ Hiervon dürften nach eigener Schätzung höchstens ca. 4.160 Mitarbeiter Steuerfahnder sein.²⁸

3. Ergebnis

Zusammenfassend lässt sich für die genannten Straftaten feststellen, dass von einer bedeutenden Dunkelziffer an nicht entdeckten Straftaten auszugehen ist und die Straftaten im Einzelfall oder als gesamtes Phänomen zu erheblichen wirtschaftlichen Schäden führen. Als Grund für die Probleme bei der Verfolgung dieser Straftaten wurde die Schwierigkeit identifiziert, auf die Straftaten überhaupt aufmerksam zu werden. Die Herausforderung liegt somit nicht in der Aufklärung, sondern in der Entdeckung der Straftaten.

Als besonders anspruchsvoll erweist sich diese Aufgabe vor allem durch zwei Faktoren. Einerseits ist es schwierig, des strafbaren Verhaltens habhaft zu werden. Um alle Tatbestandsmerkmale und somit die Straftat erkennen zu können, ist häufig Wissen notwendig, über das nur der Täter verfügt – bspw. beim Insiderhandel. In Fällen, in denen dies nicht notwendig ist, kann der Sachverhalt so unübersichtlich und schwer zugänglich sein, dass es eine besondere Leistung ist die Straftat darin zu erkennen – bspw. bei

26 Die Steuerverwaltung in Deutschland, http://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2014-09-10-die-steuerverwaltung-in-deutschland.html, abgerufen am: 19.4.2017, S. 16.

27 Die Steuerverwaltung in Deutschland, http://www.bundesfinanzministerium.de/Content/DE/Downloads/Broschueren_Bestellservice/2014-09-10-die-steuerverwaltung-in-deutschland.html, abgerufen am: 19.4.2017, S. 13.

28 Die Zahl wird wie folgt geschätzt. Aus Antworten auf Anfragen der Partei Bündnis 90 / Die Grünen in mehreren Bundesländern geht hervor, dass auf eine Millionen Einwohner die folgende Anzahl an Steuerfahndern im Jahr 2010 entfiel: 27 in Bayern, 32 in Niedersachsen, 35 in Nordrhein-Westfalen, 40 in Sachsen, 42 in Schleswig-Holstein, 47 in Berlin und 52 in Hamburg (vgl. Der Spiegel, Nr. 46, 15.11.2010, S. 17; zitiert nach Statista). Nach dem Statistischen Bundesamt umfasste die Bevölkerung in Deutschland im Jahr 2011 ca. 80 Millionen Menschen (Statistisches Bundesamt, Ausgangsdaten der Bevölkerungsfortschreibung aus dem Zensus 2011, S. 7). Die Multiplikation der höchsten Zahl an Steuerfahndern pro eine Millionen Einwohner (52) mit der Zahl der in Deutschland lebenden Menschen in Millionen (80) ergibt 4.160 Steuerfahnder in ganz Deutschland.

der handelsgestützten Marktmanipulation. Andererseits ist die Zahl der Sachverhalte, die geprüft werden müssen, so hoch, dass eine gründliche Prüfung jedes Einzelfalls nicht möglich ist.

Während – wie noch gezeigt werden soll – sich die meisten aktuellen Anwendungsbeispiele einer smarten Verdachtsgewinnung im Kontext der Wirtschaftsaufsicht und der staatlichen Leistungs- und Steuerverwaltung aufzeigen lassen, bestehen die zugrundeliegenden Aufklärungsprobleme bei der Verfolgung von Straftaten in anderen Kriminalitätsbereichen ebenfalls. Zu denken ist hier beispielsweise an Menschenhandel- und Ausbeutungsdelikte, Geldwäsche sowie Drogenhandel, bei denen ebenfalls aufgrund fehlender Anzeigen von einem großen Dunkelfeld ausgegangen wird.²⁹ Auch Straftaten in diesen Bereichen lassen sich häufig nur durch Kontrollen entdecken. Daher bietet sich der Einsatz einer smarten Verdachtsgewinnung auch hier grundsätzlich ebenso an.

II. Entwicklung der Künstlichen Intelligenz

Mit dem Begriff „Künstliche Intelligenz“ (KI) werden häufig Science-Fiction und Zukunftsszenarien verbunden. Die historischen Anfänge dieses Forschungsgebiets reichen jedoch bis in die Mitte des 20. Jahrhunderts zurück und bilden bis heute dessen Grundlage.³⁰ Was Gegenstand der KI-Forschung ist, bleibt bis heute umstritten,³¹ kann aber für die hiesige Un-

29 *Bundeskriminalamt*, Menschenhandel und Ausbeutung - Bundeslagebild 2019, S. 34; *Bussmann/Vockrodt*, CB 2016, 138 (138 ff.) gehen von einem Dunkelfeld von ca. 100 Milliarden Euro bei Geldwäsche im Nicht-Finanzsektor aus; *Bundeskriminalamt*, Rauschgiftkriminalität – Bundeslagebild 2019, S. 18 geht von einem hohen Dunkelfeld beim Drogenhandel über das Internet aus.

30 Als Beginn der Forschung über Künstliche Intelligenz werden unterschiedliche Zeitpunkte angenommen: *Russell/Norvig*, Künstliche Intelligenz, S. 39 geht aufgrund einer Arbeit von McCulloch und Pitts zu künstlichen Neuronen von dem Jahr 1943 aus; *Mainzer*, Künstliche Intelligenz, S. 10 geht aufgrund des Aufsatzes „Computing Machinery and Intelligence“ von Turing hingegen von dem Jahr 1950 aus; für *Ertel*, Grundkurs Künstliche Intelligenz, S. 9 ist das Aufkommen „programmierbarer Rechenmaschinen“ in den 50er Jahren entscheidend.

31 Es werden im wesentlichen vier Ansichten zu der Frage vertreten, was Gegenstand der Künstlichen Intelligenz ist: Eine erste Ansicht versteht unter Künstlicher Intelligenz Maschinen, die wie Menschen denken. Eine zweite Ansicht versteht unter Künstlicher Intelligenz Maschinen, die wie Menschen handeln. Eine dritte Ansicht versteht unter Künstlicher Intelligenz die formell mathematische Abbildung von Intelligenz. Ein vierte Ansicht versteht unter Künstlicher Intelligenz, eine Aufgabe

tersuchung offenbleiben. Von Interesse sind vorliegend die Methoden, die im Forschungsgebiet der Künstlichen Intelligenz entwickelt wurden und in der Praxis verwendet werden. Vor diesem Hintergrund orientiert sich diese Arbeit an der Definition von *Mainzer*. Danach lässt sich Künstliche Intelligenz als System bezeichnen, das teilweise oder vollständig Fragestellungen selbstständig lösen kann.³² „Der Grad der Intelligenz hängt vom Grad der Selbstständigkeit, dem Grad der Komplexität des Problems und dem Grad der Effizienz des Problemlösungsverfahrens ab.“³³

Die Methoden, die im Bereich der Künstlichen Intelligenz zum Tragen kommen, sind vielfältig. Unter den verwendeten Methoden sind es besonders die Methoden des Maschinellen Lernens, die in jüngster Zeit erhebliche Durchbrüche gefeiert haben und zugleich viele rechtliche Fragen aufwerfen. Dabei handelt es sich um unterschiedliche Ansätze, deren Ziel es ist, Wissen aus Beispielen (insbesondere Big Data) zu extrahieren und zu nutzen.³⁴ Deshalb soll das Maschinelle Lernen auch im Mittelpunkt dieser Arbeit stehen. Soweit andere Methoden der KI im Kontext des Aufspürens von Straftaten rechtliche Fragen aufwerfen, dürften sich diese ebenso beim Maschinellen Lernen stellen. Deshalb sollen in dieser Arbeit alle problematischen Aspekte der Künstlichen Intelligenz allein anhand des Maschinellen Lernens besprochen werden und auf eine separate Darstellung für andere Methoden der Künstlichen Intelligenz verzichtet werden. Dennoch lohnt sich ein Blick auf die Entwicklung der KI, um sich der Thematik anzunähern und einen ersten Einblick in die Ansätze und Potentiale der KI zu erhalten.

In den Anfängen zielte die KI-Forschung auf das Erschaffen von autonomen und universell einsetzbaren Maschinen.³⁵ Die Hoffnungen, dieses Ziel zu erreichen, waren hoch und wurden von schnellen Erfolgen getragen.³⁶ Ein erster öffentlich-wirksamer Erfolg der KI war ein von Arthur Samuel 1956 vorgestelltes Programm, welches das Brettspiel Dame zu spielen lernte und im Laufe der Spiele besser wurde als sein Erfinder.³⁷ Der Versuch jedoch, die entwickelten Ansätze auch komplexere Aufgaben lösen zu lassen,

mit dem bestmöglichen Ergebnis zu lösen. Vgl. *Russell/Norvig*, Künstliche Intelligenz, S. 22 ff.

32 *Mainzer*, Künstliche Intelligenz, S. 2.

33 *Mainzer*, Künstliche Intelligenz, S. 3.

34 *Alpaydin*, Introduction to machine learning, S. 2.

35 *Russell/Norvig*, Künstliche Intelligenz, S. 40 f.

36 *Ertel*, Grundkurs Künstliche Intelligenz, S. 9.

37 *Russell/Norvig*, Künstliche Intelligenz, S. 42.

scheiterte. Die Gründe hierfür waren begrenzte Rechen- und Speicherkapazitäten, fehlendes digitalisiertes Wissen sowie Begrenzungen, die aus der Gestaltung der Systeme resultierten.³⁸

Die Forschung konzentrierte sich in der nachfolgenden Zeit auf die Lösung spezifischer Anwendungsfälle. Mit unterschiedlichen Methoden wurde versucht, Wissen und menschliche Entscheidungsmechanismen – Logik – mathematisch zu repräsentieren und zur Aufgabenlösung zu nutzen.³⁹ Teilweise wurde auch versucht, unterschiedliche Ansätze miteinander zu kombinieren. Einer der Ansätze war die Programmierung sog. wissensbasierter Expertensysteme.⁴⁰ Dabei handelt es sich um Programme, die dergestalt programmiert werden, dass Wissen in Spezialgebieten in Form von Regeln (bspw. „wenn X, dann Y“) und Fakten gespeichert wird.⁴¹ Das Wissen kann sowohl aus wissenschaftlicher Literatur als auch aus menschlicher Erfahrung stammen und muss von einem Menschen identifiziert und in das Expertensystem eingepflegt werden. Die dadurch entstehende sog. Wissensbasis kann dann mit Hilfe eines Ableitungssystems genutzt werden. Ein Beispiel hierfür ist das Programm MYCIN aus dem Jahr 1976, das mit Hilfe von ca. 450 Regeln im Durchschnitt Infektionskrankheiten besser diagnostizierte als angehende Ärzte.⁴² Expertensysteme verbreiteten sich in der Folgezeit in der Industrie erfolgreich, blieben aber dennoch hinter den Erwartungen zurück.⁴³

Systeme, die auf einer programmierten Logik und/oder Wissensbasis beruhen, stoßen dann an Grenzen, wenn ihre Programmierung durch Menschen nicht mehr möglich oder sinnvoll ist. Hierfür kommen unterschiedliche Gründe in Betracht. Sachverhalte können für eine Übersetzung in eine Programmiersprache zu komplex sein. Sei es, weil ein Programmierer nicht weiß, wie er eine Aufgabe ausdrücken soll oder sei es, weil selbst die avanciertesten Computersprachen eine entsprechende Ausdrucksweise

38 *Russell/Norvig*, Künstliche Intelligenz, S. 42, 44, 45; *Mainzer*, Künstliche Intelligenz, S. 11 f.

39 *Mainzer*, Künstliche Intelligenz, S. 12; *Russell/Norvig*, Künstliche Intelligenz, S. 46 ff.

40 *Russell/Norvig*, Künstliche Intelligenz, S. 46 ff.; *Mainzer*, Künstliche Intelligenz, S. 12.

41 *Mainzer*, Künstliche Intelligenz, S. 43 ff.

42 *Russell/Norvig*, Künstliche Intelligenz, S. 47; *Ertel*, Grundkurs Künstliche Intelligenz, S. 10, 138.

43 *Russell/Norvig*, Künstliche Intelligenz, S. 48.

nicht erlauben.⁴⁴ Weiterhin kann ein Programmierer nicht immer alle Eventualitäten bedenken, die auftreten können.⁴⁵

Beispiel: In der Praxis wird für E-Mail-Spamfilter auf Maschinelles Lernen zurückgegriffen. Einerseits kann zwar der Benutzer einer E-Mail-Adresse ohne weiteres eine E-Mail als Spam-E-Mail identifizieren, jedoch fällt es äußerst schwer bzw. ist unmöglich, Spam anhand konkreter programmierbarer Merkmale zu bestimmen.⁴⁶ Insbesondere ist es schwer, konkrete Wenn-Dann-Regeln aufzustellen. Andererseits ändert sich mit der Zeit auch die Form des Spams, um die Spamfilter zu umgehen. Dann ist es sinnvoll, einen sich von selbst anpassenden Algorithmus zu verwenden.⁴⁷

Ein Zweig der KI hat deshalb parallel zu den vorgehend dargestellten Ansätzen das Maschinelle Lernen vorangetrieben. Beim Maschinellen Lernen wird das Wissen nicht von einem Menschen programmiert, sondern durch das System selbstständig anhand von Beispielsfällen erworben. Dadurch entfallen die vorgehend dargestellten Defizite. Das System passt sich beim Maschinellen Lernen von selbst an die Fragestellung an und kann sich auf der Grundlage neuer Daten dynamisch weiterentwickeln. Ein darüber hinausgehender Vorteil des Maschinellen Lernens ist es, dass in den Daten nach Wissen gesucht werden kann, das noch nicht bekannt ist – insofern wird auch von Data Mining gesprochen.⁴⁸ Dies kommt in solchen Fällen in Betracht, in denen die Menge an Daten zu groß oder unübersichtlich ist, um sinnvoll von Menschen ausgewertet zu werden.⁴⁹

Seit Anfang des 21. Jahrhunderts wächst die Erkenntnis, dass bessere Ergebnisse häufig nicht durch eine Optimierung der verwendeten Algorithmen erzielt werden, sondern durch die Erweiterung der verwendeten Datenmengen.⁵⁰ Im Standardlehrbuch der Künstlichen Intelligenz von *Russell/Norvig* heißt es in Bezug auf Übersetzungsprogramme: „Ein mittelmäßiger Algorithmus mit 100 Millionen Wörtern von nicht kommentierten

44 *Ertel*, Grundkurs Künstliche Intelligenz, S. 191; *Russell/Norvig*, Künstliche Intelligenz, S. 809; vgl. auch *Rich*, University of Pennsylvania Law Review 2016, 871 (874 f.).

45 *Russell/Norvig*, Künstliche Intelligenz, S. 809.

46 *Burrell*, Big Data & Society 2016, 1 (7); *Alpaydin*, Introduction to machine learning, S. 2; *Brunton*, Spam, S. 200.

47 *Russell/Norvig*, Künstliche Intelligenz, S. 53.

48 *Ertel*, Grundkurs Künstliche Intelligenz, S. 11.

49 *Murphy*, Machine learning, S. 1.

50 *Russell/Norvig*, Künstliche Intelligenz, S. 52; vgl. auch *Stiemerling*, CR 2015, 762 (764).

Trainingsdaten übertrifft den besten bekannten Algorithmus mit 1 Million Wörtern.“⁵¹

Parallel zur Entwicklung der KI entsteht das Phänomen der *Datafizierung* – der immer weiterreichenden Erfassung unserer Umwelt in Form von Daten.⁵² Dabei werden nicht nur analog verfügbare Informationen in Daten durch die Digitalisierung transformiert, sondern auch solche Umstände in Form von Daten festgehalten, die vormals nicht erfasst wurden. PKWs beispielsweise speichern heutzutage umfangreich Daten über deren Nutzung, aber auch über das Verhalten von Bauteilen (z.B. zur Reaktion des Airbag-Mechanismus bei Unfällen).⁵³

Die Datafizierung wird durch die nunmehr kostengünstige Erhebung und Speicherung der Daten ermöglicht und den daraus ziehbaren Nutzen motiviert.⁵⁴ Künstliche Intelligenz bzw. Maschinelles Lernen funktioniert wiederum um so besser, je größer die Menge an vorhandenen Daten ist.⁵⁵ Datafizierung und KI lassen somit eine sich wechselseitig begünstigende Ausbreitung und Verwendung erwarten.⁵⁶ In der Wirtschaft ist dies bereits heute der Fall. Künstliche Intelligenz kommt in zahlreichen und alltäglichen Situationen zur Anwendung. Dazu zählen Suchanfragen mit Hilfe von Google, der Schutz des eigenen E-Mail-Postfaches vor Spam, Kaufempfehlungen im Internet und die automatische Identifizierung von Kreditkartenbetrug.⁵⁷

Die soeben dargestellte Geschichte der Künstlichen Intelligenz verdeutlicht drei Aspekte des Maschinellen Lernens. Erstens hat das Maschinelle Lernen den Vorteil gegenüber anderen Methoden der Künstlichen Intelligenz, dass es nicht die Aufstellung konkreter Wenn-Dann-Regeln erfordert. Der auf Maschinellern Lernen beruhende Algorithmus extrahiert selbstständig aus historischen Beispielfällen eine „Logik“. Die automatisierte und wirtschaftliche Bearbeitung komplexer Aufgaben wird durch Maschi-

51 *Russell/Norvig*, Künstliche Intelligenz, S. 52.

52 *Cukier/Mayer-Schoenberger*, *Foreign Affairs* May/June 2013, 28 (29, 35); *Hill*, *DÖV* 2014, 213 (213).

53 Wo Ihr Auto überall Daten speichert, ADAC, https://www.adac.de/infotestrat/adac-im-einsatz/motorwelt/daten_auto_spion.aspx, abgerufen am: 17.5.2017.

54 *Cukier/Mayer-Schoenberger*, *Foreign Affairs* May/June 2013, 28 (29 ff., 35).

55 *Russell/Norvig*, Künstliche Intelligenz, S. 52.

56 Vgl. *Jordan/Mitchell*, *Science* (Issue 6245) 2015, 255 (256 f.).

57 *Görz/Schneeberger/Schmid*, *Handbuch der Künstlichen Intelligenz*, S. 407 m.w.N.; Zur Datafizierung und Verwendung von Künstlicher Intelligenz durch den Staat noch unter III. 3.

nelles Lernen ermöglicht. Zweitens erfordert die erfolgreiche Anwendung des Maschinellen Lernens hinreichende Mengen an Beispielfällen, die in Form von Daten bereitgestellt werden müssen („Big Data“)⁵⁸. Diese Anforderung ist zugleich auch ein Vorteil des Maschinellen Lernens. Das Maschinelle Lernen erlaubt es, besonders umfangreiche Mengen an Daten zu verarbeiten. Drittens führt die zunehmende Datafizierung dazu, dass über immer mehr Lebenssachverhalte Daten vorhanden sind. Deshalb erlaubt letztlich erst die Datafizierung den sinnvollen Einsatz Maschinellen Lernens.

III. Nutzung Künstlicher Intelligenz zur Ermittlung von Straftaten in der Praxis

Über die Verwendung Künstlicher Intelligenz zur gezielten Aufdeckung von Straftaten durch staatliche Stellen in Deutschland liegen keine konkreten Informationen vor. Hingegen sind solche Praktiken aus anderen Staaten bekannt. Im Folgenden soll deshalb zunächst ein Überblick über die Situation außerhalb der Europäischen Union sowie in dessen Mitgliedstaaten gegeben werden. Dies soll die Zwecke umfassen, zu denen Künstliche Intelligenz verwendet wird, sowie die Erfahrungen, die bei der Verwendung Künstlicher Intelligenz gesammelt wurden. Anschließend sollen die Indizien vorgestellt werden, die für eine Verwendung oder zumindest eine in Zukunft gewünschte Verwendung Künstlicher Intelligenz in Deutschland sprechen. Von zentraler Bedeutung sind dabei die Tätigkeiten der Finanzämter und der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

1. Situation außerhalb der Europäischen Union

In den USA wird die Überwachung des Kapitalmarktes durch eine unabhängige Aufsichtsbehörde, der Securities and Exchange Commission (SEC), sowie in Teilbereichen von Selbstregulierungsorganisationen wahrgenommen.⁵⁹ Zu den Selbstregulierungsorganisationen gehören auch von den Börsen betriebene Organisationen, die das gesetzestreue Verhalten der

58 Siehe hierzu Kapitel 2 A.

59 Scholz, Selbst- und Fremddregulierung von Wertpapierbörsen, S. 95 f.; *Halfpap*, Kapitalmarktaufsicht in Europa und den USA, S. 123; Koch, Ermittlung und Verfolgung von strafbarem Insiderhandel, S. 63 f.