
Möglichkeiten und Grenzen des Data Mining in der Strafverfolgung

Mathea Buchholz

Möglichkeiten und Grenzen des Data Mining in der Strafverfolgung

Mathea Buchholz
Rechtswissenschaftliche Fakultät
Universität Münster
Münster, Deutschland

Erster Berichterstatter: Prof. Dr. Mark Deiters
Zweiter Berichterstatter: Prof. Dr. Michael Heghmanns
Dekan: Prof. Dr. Mark Deiters
Tag der mündlichen Prüfung: 20. April 2026

D6

Zugl.: Münster (Westf.), Univ., Diss. der Rechtswissenschaftlichen Fakultät, 2026

ISBN 978-3-658-52410-4 ISBN 978-3-658-52411-1 (eBook)
<https://doi.org/10.1007/978-3-658-52411-1>

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

© Der/die Herausgeber bzw. der/die Autor(en), exklusiv lizenziert an Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2026

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jede Person benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des/der jeweiligen Zeicheninhaber*in sind zu beachten.

Der Verlag, die Autor*innen und die Herausgeber*innen gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag noch die Autor*innen oder die Herausgeber*innen übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Carina Reibold

Springer ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Wenn Sie dieses Produkt entsorgen, geben Sie das Papier bitte zum Recycling.

Vorwort

Diese Arbeit wurde im Wintersemester 2025 von der Rechtswissenschaftlichen Fakultät der Universität Münster als Dissertation angenommen. Rechtsprechung und Literatur wurden bis Januar 2026 berücksichtigt.

Zunächst möchte ich mich bei meinem Doktorvater Herrn Professor Dr. Mark Deiters für seine aufmerksame Betreuung und verständnisvolle Unterstützung und für die, insbesondere angesichts des Umfangs dieser Arbeit, zügige Erstellung des Erstgutachtens bedanken. Weiterhin bedanke ich mich bei Herrn Professor Dr. Michael Heghmanns für die schnelle Erstellung des Zweitgutachtens.

Ein besonderer Dank gebührt meinem langjährigen Partner Felix, der mir stets mit Zuversicht und unerschütterlichem Vertrauen in mein Können zur Seite steht.

Düsseldorf, im April 2026

Mathea Buchholz

Inhaltsverzeichnis

Abbildungsverzeichnis	XIX
Tabellenverzeichnis.....	XIX
Abkürzungen	XIX
A. Einführung.....	1
I. Hintergrund und Ziel der Arbeit.....	1
II. Gang der Untersuchung.....	6
B. Grundlagen des Data Mining	10
I. Technisches Grundverständnis erforderlich.....	10
II. Technische Grundbegriffe.....	10
1. Daten, Informationen, Wissen?.....	10
2. Was ist eigentlich ein Algorithmus?	11
III. Was ist Data Mining?	12
1. Begriff des Data Mining gilt als unscharf: (K)eine Definition des Data Mining.....	12
2. Ablauf und Funktionsweise des Data Mining	23
a) Der Data Mining-Prozess im Überblick.....	23
b) Aller Anfang sind die Daten: Aus welchen Daten kann Data Mining Wissen gewinnen?.....	24
c) Datenvorbereitung.....	26
aa) Bedeutung der Datenvorbereitung	26
bb) Datenselektion: Auswahl der zu analysierenden Daten	26
cc) Datenvorverarbeitung: Datenbereinigung und -reduktion	27
dd) Datentransformation.....	29
d) Analyseschritt: Methoden des Data Mining.....	30
aa) Auswahl der Methode	30
bb) Klassifikation	32
cc) Numerische Vorhersage	34
dd) Clustering	35
ee) Anomalieerkennung	38
ff) Assoziationsanalyse	41
3. Verhältnis zu verwandten Begriffen und Gebieten	44

a)	Notwendigkeit der Abgrenzung	44
b)	Künstliche Intelligenz und maschinelles Lernen	45
c)	Mathematik, Statistik und statistische Verfahren.....	57
aa)	Rolle der Abgrenzung	57
bb)	Mathematik: <i>Mathematisch</i> -statistische Verfahren?	58
cc)	Statistik und Data Mining: Gemeinsamkeiten und Widersprüche	58
dd)	Statistische Verfahren im Data Mining?	64
(1)	Statistische Verfahren in den Phasen des Data Mining?.....	64
(2)	Statistik in Datenvorbereitung und Evaluation	65
(3)	Statistische Verfahren im Auswerteschritt neben maschinellem Lernen?.....	67
(a)	Ausdrücklich: Statistische Verfahren im Auswerteschritt	67
(b)	Statistische Verfahren abgelöst durch maschinelles Lernen	68
(c)	Begriffsverhältnis zu Verfahren des maschinellen Lernens.....	72
(4)	Zwischenfazit: Abgrenzungsfunktion anders als angenommen.....	79
d)	Regelbasierte Verfahren: Deduktiv vs. Induktiv	79
e)	Data Warehouse und Data Warehousing	82
f)	Online Analytical Processing (OLAP).....	84
g)	Big Data und Big Data-Analysen.....	86
h)	Datenabgleich.....	92
i)	Profiling.....	93
IV.	Fazit: Interdisziplinäres Data Mining ohne klare Abgrenzung	94
C.	Potenzial des Data Mining für die Strafverfolgung	99
I.	Praktische Voraussetzungen für Data Mining in der Strafverfolgung	99
II.	Umfang der potenziellen Datengrundlage für Data Mining zu Strafverfolgungszwecken	99
1.	Daten in der Strafverfolgung als Grundvoraussetzung des Data Mining.....	99
2.	Analoge Daten und Nichtdaten im Strafverfahren als Hürde für Data Mining?	101
3.	Datenerhebungsmaßnahmen der StPO.....	101
a)	Klassische Ermittlungsmaßnahmen und IT-Ermittlungsmaßnahmen.....	101
b)	Datensicherstellung und -beschlagnahme	102
c)	Auskünfte und Datenankauf von privaten Dritten	106
d)	Datenauskünfte: Bestands-, Verkehrs-, und Nutzungsdatenauskunft	107

aa) Daten von Telekommunikationsdiensteanbietern und Anbietern digitaler Dienste.....	108
bb) Bestandsdatenauskunft inklusive Zugangsdaten	109
cc) Verkehrsdatenauskunft von Telekommunikationsdiensteanbietern und Nutzungsdatenauskunft von digitalen Diensten.....	110
e) Stark im Gespann mit §§ 100g ff. StPO: IMSI-Catcher und stille SMS.....	113
f) „Klassische“ heimlich-technische Überwachungsmaßnahmen	115
aa) (Quellen-) Telekommunikationsüberwachung und Online-Durchsuchung	115
bb) Akustische Überwachung, Bildaufnahmen, sonstige technische Mittel	117
g) Fundgrube öffentliche Daten: Internet und soziale Medien.....	118
h) Zugriffsmöglichkeiten auf Datenbestände anderer Behörden.....	121
aa) Auskunftersuchen nach § 161 Abs. 1 StPO bei Behörden und Zugriff auf Register.....	121
bb) Akteneinsicht und Datenübermittlung aus anderen Strafverfahren	123
4. Datenübermittlung und Direktzugriffe auf Daten aus dem Ausland.....	123
5. Nationale und internationale Dateien und Informationssysteme der Strafverfolgungsbehörden	124
a) Umfang und Rolle der Dateien und Datenbanken.....	124
aa) Umfangreiche nationale und internationale Dateien und Datenbanken.....	124
bb) Nationale Dateien und Datenbanken	124
cc) Internationale Dateien und Datenbanken	133
b) Vorgangs- und Fallbearbeitungssysteme: Zwischen Datei und Auswertungswerkzeug	134
6. Zwischenfazit: Vielfältige Quellen und Daten als Grundlage denkbar.....	136
III. Derzeitiger Umgang mit Daten in der Strafverfolgung: Entwicklungstendenzen zur automatisierten Auswertung.....	137
1. Status quo und Entwicklung der Datenauswertung in Deutschland	137
a) Data Mining in der Strafverfolgung: Realistisch?.....	137
b) Manuelle Auswertung und ihre Grenzen	137
c) IT-Forensiker als „Sachverständige“.....	139
d) Massendatenverarbeitung durch Rasterfahndung & Co.....	140
e) Bisher nur theoretisch: Erweiterte Nutzung der Antiterrordatei und Rechtsextremismusdatei.....	146

f)	Automationsgestützte Risikomanagementsysteme der AO	148
g)	Praktischer Einsatz eigener Datenanalysesoftware in Ermittlungsverfahren.....	150
aa)	Mittel der Strafverfolgungsbehörden über Rasterfahndung & Co. hinaus.	150
bb)	Stand und Entwicklung bei den Datenverarbeitungsanwendungen des Bundes	151
(1)	Frühe Tuchföhlung mit Data Mining: Marktbeobachtungen des BKA .	151
(2)	Softwareunterstützung von Bundesbehörden: (Kein) Data Mining?	152
(3)	KI-Einsatz durch Bundesbehörden im Bereich der Strafverfolgung.....	165
cc)	Datenverarbeitungsanwendungen der Länder: Status quo und Ausblick...	167
(1)	Status quo der Länder.....	167
(2)	Unternehmensangaben: Polizeibehörden der Länder als Kunden von <i>Intrafind</i>	183
(3)	Data Mining mit Palantir-Software in Hessen, NRW, Bayern und bald auch bundesweit?	184
(a)	Wirbel um Anschaffung: Gotham von Palantir	184
(b)	VeRA in Bayern.....	187
(c)	HessenData in Hessen	190
(d)	DAR in NRW	194
(e)	Palantir bald bundesweit im Einsatz?	198
dd)	Forschungsprojekte von Bund und Ländern	204
(1)	KI gegen Kinderpornografie: Aus der Forschung in die Praxis.....	204
(2)	Weitere Forschungsprojekte zu KI in der Strafverfolgung	207
h)	Zwischenfazit und Ausblick: Deutliche Tendenz Richtung Data Mining in Deutschland.....	209
2.	Internationaler Einsatz und Entwicklung hin zu Data Mining zu Strafverfolgungszwecken	216
a)	Die EU und Data Mining	216
aa)	Entwicklung hin zur automatisierte Datenauswertung in der EU	216
bb)	Einsatz von Data Mining durch Europol.....	216
cc)	EU fördert Forschungsprojekte zu Data Mining in der Strafverfolgung ...	220
b)	Einsatz von Data Mining im Ausland durch nationale Behörden.....	231
aa)	Data Mining in der Strafverfolgung: Gegenwart statt <i>Science Fiction</i>	231
bb)	New York: <i>Domain Awareness System</i> und <i>Patternizr</i>	232

cc)	USA: Aufspüren von Tätern im Bereich Kindesmissbrauch	237
dd)	Italien: Data Mining mit <i>Redditometro</i>	238
ee)	Niederlande: Data Mining mit <i>iColumbo</i>	239
c)	Zwischenfazit: Internationaler Einsatz von Data Mining als Vorbild für Deutschland?	239
IV.	Wert und Anwendungsbeispiele des Data Mining in der Strafverfolgung	240
1.	Data Mining: Wie nützlich ist es wirklich für die Strafverfolgung?	240
2.	Mögliche Lösung für große Datenmengen und unerschlossene Schätze	241
a)	Kapazitätsgrenzen der Strafverfolgungsbehörden angesichts Big Data	241
b)	Lösungsoptionen ohne Data Mining ausreichend?	248
c)	Fähigkeiten des Data Mining im Umgang mit Big Data in der Strafverfolgung.....	250
3.	Begrenzende Aspekte des Potenzials: Technische Grenzen und praktische Erwägungen.....	254
a)	Hält Data Mining, was es verspricht?	254
b)	Grenzen und Schwächen des Data Mining	255
aa)	Von Wahrscheinlichkeit und Fakten, Korrelation und Kausalität	255
bb)	Richtigkeit und Objektivität: Berechtigte Hoffnung auf Rationalisierung?	262
(1)	Algorithmen und Fehler: <i>garbage in – garbage out</i>	262
(2)	Algorithmen und Bias: Objektivität?	271
(a)	Bias und Diskriminierung	271
(b)	Bias speziell bei Anwendungen in der Strafverfolgung.....	276
(c)	Lösungen für Bias als Chance für Rationalisierung.....	283
cc)	Nachvollziehbarkeit: Nicht nur Black Box-Problem	285
(1)	Schwarz, weiß, grau?	285
(2)	Praktische Konsequenzen für Data Mining in der Strafverfolgung	296
c)	Grundvoraussetzungen für erfolgreiches Data Mining in der Praxis schaffen ..	299
aa)	Objektive und verlässliche Ergebnisse ermöglichen.....	299
bb)	Verständnis und notwendige Fähigkeiten der Anwender ausbauen.....	300
d)	Beschaffung: Eigen- oder Fremdentwicklung?.....	304
e)	Zwischenfazit: Nicht nur kein Wundermittel.....	306
4.	Vom abstrakten Potenzial zu konkreten Anwendungsbeispielen.....	307

a)	Data Mining-Anwendungen zwischen Gefahrenabwehr und Strafverfolgung ..	307
b)	Data Mining in der Strafverfolgung: Phasen der Einsatzmöglichkeiten	308
aa)	Data Mining im Ermittlungsverfahren	308
bb)	Predictive Policing: (K)ein Anwendungsbereich des Data Mining in der Strafverfolgung?	310
cc)	Strategische Erkenntnisse und Lagebilder	313
dd)	Strukturermittlungen und Verdachtsgewinnung mittels Data Mining als strafprozessuale Ermittlungsmaßnahme?	314
	(1) Anwendungsszenarien in der repressiven Kriminalitätsbekämpfung	314
	(2) Data Mining zur tatbezogenen Verdachtsgenerierung	314
	(3) Data Mining für Strukturermittlungen	332
	(4) Fazit zur Verdachtsgenerierung und Strukturermittlung	348
ee)	Zwischenfazit: Grat zwischen präventivem und repressivem Recht im Angesicht von Data Mining	348
c)	Mögliche konkrete Einsatzgebiete von Data Mining im strafprozessualen Ermittlungsverfahren	349
aa)	(Zu) Vielfältige Anwendungsszenarien	349
bb)	Reduzierung von Massendaten: Suche nach der Nadel im Heuhaufen	352
cc)	Unterstützung der Operativen Fallanalyse (OFA)	356
	(1) Herkömmliche Operative Fallanalyse	356
	(2) Serienstraftaten identifizieren mit Hilfe von Data Mining	358
	(3) Täterprofilbildung mit Data Mining	360
	(a) Mögliche Eigenschaften des Täters ermitteln	360
	(b) Geographic Profiling	365
	(4) Kommunikationsanalyse mit Data Mining	366
	(5) Zwischenfazit zu Data Mining in der OFA	367
dd)	Tatverdächtige aus Daten ermitteln	368
	(1) Kreis von Tatverdächtigen identifizieren: Rasterfahndung 2.0 u. a.	368
	(2) Digitale Spurenverfolgung: Täter identifizieren und/oder aufspüren	374
	(3) Täterverdacht automatisch generieren möglich?	378
ee)	Social Network Analysis und Profile von bekannten Verdächtigen	379
d)	Zwischenfazit: Zahlreiche Anwendungsszenarien mit Potenzial	381

5. EncroChat: Ein konkreter Beispielanwendungsfall zur Veranschaulichung	382
V. Fazit: Großes Potenzial mit großen praktischen Hürden	386
D. Rechtliche Vorgaben für Data Mining in der Strafverfolgung	391
I. Leitlinien für den Gesetzgeber sowie zur Einordnung künftiger Gesetze.....	391
II. Mindeststandards aus Grundrechtecharta der Europäischen Union (GRC) und Europäischer Menschenrechtskonvention (EMRK).....	392
III. Verfassungsrechtliche Anforderungen	394
1. Betroffene Grundrechte durch Data Mining	394
a) Szenario: Auswertung rechtmäßig erhobener Daten mittels Data Mining	394
b) Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.....	394
aa) Schutzbereich des Rechts auf informationelle Selbstbestimmung.....	394
bb) Eingriff des Data Mining in das Recht auf informationelle Selbstbestimmung	397
(1) Einigkeit in Rechtsprechung und Literatur	397
(2) Differenzierung: Verschiedene Datenverarbeitungsschritte und - modalitäten und Data Mining.....	399
(a) Data Mining: auch rechtlich ein Datenverarbeitungsprozess.....	399
(b) Eigenständiger Eingriff des Data Mining nicht nur bei Datenweiterverwendung.....	401
(c) Doppelnatur des Data Mining: Datenauswertung und -erhebung.....	410
(d) Eingriff auch bezüglich Nichttreffern bei Data Mining-Auswertung	412
(e) Eingriff durch Verwendung von Daten als Trainingsdaten für Data Mining	413
(f) Mit Data Mining einhergehende Grundrechtseingriffe: Eingriffe durch Vor- und nachgelagerte Datenverarbeitungsschritte	415
c) Eingriff in spezielle Datenschutzgarantien durch Auswertung: Telekommunikationsgeheimnis und Wohnungsgrundrecht.....	416
aa) Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG und Art. 13 Abs. 1 GG durch Data Mining-Auswertung.....	416
bb) Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG (IT- Grundrecht)	427
d) Betroffene Grundrechte abseits des Datenschutzes	430

aa)	Nicht nur Datenschutzgrundrechte zu beachten.....	430
bb)	Eingriff in die Meinungsfreiheit aus Art. 5 Abs. 1 GG bzw. die Glaubens- und Gewissensfreiheit aus Art. 4 Abs. 1, Abs. 2 GG.....	431
cc)	Ungleichbehandlung und Diskriminierung: Art. 3 GG.....	436
(1)	Stiefmütterliche Behandlung des Gleichheitsgrundsatzes	436
(2)	Verbotene Diskriminierung nach Art. 3 Abs. 3 GG.....	437
(3)	Ungleichbehandlung nach Art. 3 Abs. 1 GG	443
2.	Rechtfertigungsanforderungen für Eingriffe in Datenschutzgrundrechte durch Data Mining	445
a)	Anforderungen an eine Rechtsgrundlage für Data Mining	445
aa)	Allgemeine Anforderungen an Datenverarbeitungen und spezielle Anforderungen an Data Mining	445
bb)	Einheitliche Rechtfertigungsanforderungen unabhängig von betroffenen Datengrundrechten	445
b)	Eingriffsintensität der Auswertung mittels Data Mining	450
aa)	Eingriffsintensität des Data Mining in der Literatur	450
bb)	Keine pauschale Beurteilung möglich.....	452
cc)	Relevante Eingriffsintensitätsfaktoren aus Literatur und Rechtsprechung 455	
(1)	Generelle Intensitätskriterien für Dateneingriffe: Allein ausreichend? .	455
(2)	Zweistufige Prüfung der Eingriffsintensität nach BVerfG, Urt. v. 26.2.2023 - 1 BvR 1547/19, 1 BvR 2634/20, BVerfGE 165, 363 – Automatisierte Datenanalyse	457
(a)	Rolle der Erhebungsintensität für Datenweiterverwendungen und eigenständige Eingriffsintensität der Auswertung	457
(b)	Kritik an zweistufiger Prüfung: Intensität der Erhebung und Anforderungen der Zweckbindung überflüssig?.....	464
(3)	Ergänzung des Ansatzes des Bundesverfassungsgerichts und Anwendung auf Data Mining	469
(a)	Weitere Intensitätskriterien bzw. Ausdifferenzierung erforderlich	469
(b)	Eingeschränkte Anwendbarkeit der Kriterien zur Bestimmung der Eingriffsintensität nach Methode: Statistik, selbstlernende Verfahren, Künstliche Intelligenz?.....	470
(c)	Ergänzung und Ausgestaltung der Kriterien zur Bestimmung der Eingriffsintensität nach <i>Rückert</i>	473
dd)	Bestimmung der Eingriffsintensität des Data Mining.....	475

(1)	Intensität der Erhebung als Ausgangspunkt	475
(2)	Datengrundlage des Data Mining im Ermittlungsverfahren	476
(3)	Intensität der Data Mining-Verfahren	481
(a)	Intensivierung üblicher Faktoren durch Automatisierung mittels Data Mining	481
(b)	Fehleranfälligkeit: Risiko insbesondere von <i>false positives</i> durch Data Mining	487
(c)	Diskriminierungsrisiken des Data Mining	490
(d)	Nachvollziehbarkeit: Verfahrensabhängig	492
(4)	Zusätzliche Faktoren gegenüber BVerfG, Urt. v. 26.2.2023 - 1 BvR 1547/19, 1 BvR 2634/20, BVerfGE 165, 363 – Automatisierte Datenanalyse..	499
(a)	Dauer der Maßnahme nach <i>Rückert</i>	499
(b)	Heimlichkeit der Maßnahme	499
ce)	Zwischenfazit: Eingriff mit Eigengewicht mit regelmäßig hoher Intensität	500
c)	Eigenständige Rechtfertigung nur bei Übermittlung bzw. Zweckänderung erforderlich?	501
d)	Bestimmtheit, Normenklarheit und Parlamentsvorbehalt: Anforderungen an Data Mining	504
e)	Zweckbindungsgrundsatz und Data Mining	513
aa)	Zweckbindungsgrundsatz und Doppelnatur des Data Mining	513
bb)	Anforderungen aus dem Zweckbindungsgrundsatz für Data Mining	518
(1)	Zweckändernde und zweckwahrende Weiterverwendung im strafprozessualen Ermittlungsverfahren	518
(2)	Korrespondierende Mindestanforderungen aus dem Zweckbindungsgrundsatz	520
f)	Absolute Grenzen: Kernbereich, Totalüberwachung, Persönlichkeitsprofile	521
aa)	Kernbereich: Eingriff erst durch Data Mining?	521
bb)	Verbot umfassender Persönlichkeitsprofile und Verbot der Totalüberwachung	523
g)	Verhältnismäßigkeit des Data Mining	526
aa)	Zentrale Anforderungen folgen aus dem Verhältnismäßigkeitsgrundsatz.	526
bb)	Legitimer Zweck	526
cc)	Geeignetheit	527

(1) Anwendungsszenarien als solche nicht ausreichend zur Beurteilung der Geeignetheit	527
(2) Data Mining-Ergebnis als Beweismittel oder nur Spurenansatz.....	527
(3) Data Mining-Ergebnis als Grundlage eines täterbezogenen Verdachts .	532
(4) Data Mining-Ergebnis als Grundlage eines hinreichenden Tatverdachts nach § 170 Abs. 1 StPO	542
dd) Erforderlichkeit	542
(1) Erforderlichkeit des Data Mining regelmäßig gegeben	542
(2) Vorgaben in einer Rechtsgrundlage, um die Erforderlichkeit zu sichern	542
ee) Angemessenheit	545
(1) Ausgewogenheit zwischen Eingriffsintensität und Zweck	545
(2) Verdachtsanforderungen und Straftatenkatalog	546
(a) Übertragbarkeit der Vorgaben aus BVerfGE 165, 363 – Automatisierte Datenanalyse für die Anforderungen an Data Mining?.....	546
(b) Relevanz der Anforderungen aus BVerfGE 156, 11 – Antiterrordateigesetz II	548
(c) Verdachtsgrad	550
(d) Straftatenkatalog	554
(3) Qualitätsanforderungen und besondere Verfahrenssicherungen für Richtigkeit und Fairness.....	560
(a) Keine konkreten Vorgaben aus BVerfGE 165, 363 – Automatisierte Datenanalyse	560
(b) Qualität und Fairness – Hand in Hand	561
(c) Anforderungen an die Anwendungs- und Ergebnisqualität	562
(d) Anforderungen an die Datenqualität	564
(e) Vorgabe für den Einsatz: Human in the Loop-Vorgaben	565
(f) Verpflichtende regelmäßige Qualitätskontrollen erforderlich	567
(g) Spezielle Anforderungen mit Blick auf Diskriminierungsrisiken.....	568
(h) Trotz Vorgaben bleibt Risiko und damit eine hohe Eingriffsintensität .	574
(4) Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle	574
(a) Anforderungen abhängig vom Eingriffsgewicht.....	574

(b)	Verfassungsrechtliche Transparenzanforderungen an Data Mining	574
(c)	Kontrolle und Aufsicht.....	585
(d)	Anforderungen an die Datensicherheit.....	590
(e)	Protokollierungs-, Kennzeichnungs- und Löschpflichten.....	590
3.	Auswirkungen von Data Mining-Anwendungen auf die Intensität anderer Datenverarbeitungseingriffe.....	592
a)	Wechselwirkung der Datenverarbeitungsschritte?	592
b)	Auswirkung auf Datenerhebungsmaßnahmen durch mögliches Data Mining?	594
c)	Auswirkung auf Übermittlungs- und Datenweiterverwendungsregelungen?	599
d)	Auswirkung auf Regelungen für die Speicherung erhobener Daten im Vorfeld des Data Mining?	600
4.	Rechtfertigung für Eingriffe in Art. 4 Abs. 1, Abs. 2 GG, Art. 5 Abs. 1 GG und Art. 3 Abs. 1, Abs. 3 GG durch Data Mining	602
a)	Sonderkonstellation im Überblick: Eingriffe in Art. 4, 5 GG	602
b)	Rechtfertigung einer Ungleichbehandlung nach Art. 3 GG	603
IV.	Vorgaben aus dem einfachgesetzlichen Datenschutzrecht: JI-Richtlinie und BDSG 603	
1.	Richtlinie (EU) 2016/680 (JI-Richtlinie) und §§ 45 ff. BDSG: Beachtung de lege lata und de lege ferenda.....	603
2.	Geltung der §§ 45 ff. Bundesdatenschutzgesetz (BDSG) im Strafverfahren.....	605
3.	Regelungen des BDSG: Vorgaben de lege lata und de lege ferenda	606
a)	Unmittelbar für Anwender geltende Regelungen der §§ 45 ff. BDSG	606
aa)	Klarstellender Verweis über Geltung empfehlenswert	606
bb)	Grundsätze für die Verarbeitung von Daten, §§ 47 ff. BDSG	607
(1)	Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten, § 47 BDSG	607
(2)	Verarbeitung zu anderen Zwecken, § 49 S. 1 BDSG	609
(3)	Verarbeitung besonderer Kategorien personenbezogener Daten nach § 48 Abs. 1 BDSG	609
(4)	Verbot diskriminierenden Profilings aus § 54 Abs. 3 BDSG	612
(5)	Verpflichtung auf das Datengeheimnis, § 53 BDSG	614
cc)	Pflichten der Verantwortlichen und Auftragsverarbeiter, §§ 62-77 BDSG.....	614
dd)	Erweiterung der Betroffenenrechte aus dem BDSG	618
b)	Vorgaben für (zu schaffende) Regelungen aus §§ 45 ff. BDSG.....	620

aa) Bestimmtheit und Normenklarheit, § 47 Nr. 2 BDSG, Art. 8 Abs. 2 JI-Richtlinie	620
bb) Keine automatisierte Einzelentscheidung, § 54 Abs. 1, Abs. 2 BDSG	620
V. Ausblick: KI-Verordnung und Data Mining	623
1. Geltung der KI-Verordnung (größtenteils) ab 2026	623
2. Relevanz für Data Mining	623
a) Data Mining als Künstliche Intelligenz im Sinne der Verordnung	623
b) Verbotene KI, Art. 5 KI-VO	627
c) Hochrisiko-KI nach Art. 6 Abs. 2 i. V. m. Anhang III	628
d) Anforderungen an Hochrisiko-KI nach Art. 8 ff. KI-VO	630
3. Zwischenfazit: Nationaler Regelungsbedarf für Data Mining bleibt bestehen	631
VI. Fazit: Regelungsbedarf mit hohen Anforderungen	632
E. Rechtsgrundlagen de lege lata für Data Mining	643
I. Bestehende Rechtsgrundlagen der StPO ausreichend?	643
II. Implizite Regelung in Datenerhebungsgrundlage bzw. Annexkompetenz und Verwendungsregelungen nicht ausreichend	645
III. Kein Data Mining auf Grundlage der §§ 98a, 98c StPO	646
IV. Kein Data Mining auf Grundlage der §§ 483 ff. StPO	651
V. Ermittlungsgeneralklausel aus §§ 161 Abs. 1, 163 Abs. 1 StPO für Data Mining nicht ausreichend	653
VI. Rechtsgrundlagen aus anderen Gesetzen als der StPO	655
1. Datenschutzrecht: BDSG	655
2. Normen des ATDG und RED-G	656
VII. Verfahrenssicherungen de lege lata für Data Mining?	656
VIII. Fazit: Keine Rechtsgrundlage de lege lata	658
F. Optionen und Hürden für eine Rechtsgrundlage de lege ferenda	659
I. Offene Fragen für eine Rechtsgrundlage de lege ferenda	659
II. Data Mining-Rechtsgrundlage als unzulässige Gesetzgebung auf Vorrat?	659
III. Standort einer Rechtsgrundlage de lege ferenda	661
IV. Eingriffsintensität nach den Kriterien des Bundesverfassungsgerichts verringern? ..	662
1. Bedürfnis nach Verringerung der Eingriffsintensität	662
2. Regulatorische Optionen zur Einschränkung der Datengrundlage	662

a) Auswirkungen auf die Datenqualität durch rechtliche Beschränkung der Datengrundlage	662
b) Einschränkung der Datengrundlage ohne Auswirkung auf die Datenqualität ...	664
c) Zwischenfazit: Datenqualität kann, aber muss nicht leiden	665
3. Regulatorische Optionen zur Einschränkung der Methode.....	666
a) Vorschläge des Bundesverfassungsgerichts zur Beschränkung der Methode begrenzt anwendbar.....	666
b) Beschränkung auf statische Modelle erforderlich	667
c) Differenzierung nach statistischen Verfahren und solchen des maschinellen Lernens?	667
d) Unterscheidung nach Transparenzgraden	669
e) Zwischenfazit: Flexible Stufung nach Transparenz möglich	672
4. Parlamentsvorbehalt, Bestimmtheit und Normenklarheit für Beschränkungen.....	672
V. Praktische Erfüllbarkeit der rechtlichen Anforderungen?.....	674
1. Datenqualitätsanforderungen im Strafverfahren erfüllbar?.....	674
2. Unerfüllbare Vorgaben: Transparenz und Qualität?	674
3. Unerfüllbare Vorgaben: Diskriminierungsschutz?.....	675
4. Zwischenfazit: Zahlreiche praktische Hürden durch technische Grenzen, insbesondere sog. trade-offs	677
VI. Fazit: Eine Rechtsgrundlage de lege ferenda muss technische Voraussetzungen des Data Mining einbeziehen	678
G. Bewertung des § 16a BKAG-E aus dem Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung vom 9.9.2024	680
H. Zusammenfassung in Thesen	686
I. Literaturverzeichnis.....	703

Abbildungsverzeichnis

Abbildung 1: Interdisziplinarität des Data Mining, entnommen aus Cleve/Lämmel, Data Mining	15
Abbildung 2: Schlechtes und gutes Clustering, entnommen aus Cleve/Lämmel, Data Mining	37

Tabellenverzeichnis

Tabelle 1: Auswahl von Definitionen aus der Informatik/Data Science	16
Tabelle 2: Auswahl von Definitionen aus der Rechtswissenschaft	18
Tabelle 3: EU-geförderte Projekte im Überblick	221

Abkürzungen

Hinsichtlich der verwendeten Abkürzungen wird auf *Kirchner*, Abkürzungsverzeichnis der Rechtssprache, 11. Aufl. 2024 verwiesen.