

Lucia M. Sommerer

Personenbezogenes Predictive Policing

Kriminalwissenschaftliche Untersuchung über
die Automatisierung der Kriminalprognose



Nomos

Schriften zur Kriminologie

herausgegeben von

Prof. Dr. Katrin Höffler, Georg-August-Universität Göttingen

Prof. Dr. Johannes Kaspar, Universität Augsburg

Prof. Dr. Jörg Kinzig, Eberhard Karls Universität Tübingen

Prof. Dr. Ralf Kölbel, Ludwig-Maximilians-Universität München

Band 19

Lucia M. Sommerer

Personenbezogenes Predictive Policing

Kriminalwissenschaftliche Untersuchung über
die Automatisierung der Kriminalprognose



Nomos

Gedruckt mit Unterstützung des Förderungsfonds Wissenschaft der VG WORT.

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

Zugl.: Göttingen, Univ., Diss., 2019

ISBN 978-3-8487-6233-0 (Print)

ISBN 978-3-7489-0348-2 (ePDF)



Onlineversion
Nomos eLibrary

1. Auflage 2020

© Nomos Verlagsgesellschaft, Baden-Baden 2020. Gedruckt in Deutschland. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.



Quelle: *Petrarch*, des *Remèdes de l'une et l'autre fortune prospère et adverse*, Paris, 1524; Mit freundlicher Genehmigung der Bibliothèque Nationale, Paris.

Fortuna, die römische Schicksalsgöttin (links), und die Göttin der Weisheit und Wissenschaft Sapientia (rechts) sind in dieser Abbildung im traditionellen Gegensatz dargestellt. Fortunas Rad lässt das Schicksal der Menschen scheinbar zufällig steigen und fallen, während die Wissenschaft Sicherheit verspricht. Die Untersuchung der „Zähmung des Zufalls“ und dadurch der spezifisch modernen Vereinigung der Erzrivalen Fortuna und Sapientia durch algorithmengestützte Vorhersagen bildet den Kern der vorliegenden Arbeit.¹

1 Abbildung bereits bei *Gigerenzer* 1997, xiii, xviii; *Ders.* 2015, 22. (“By ‘taming chance’ in Ian Hacking’s evocative phrase (*Hacking* 1990), probability and statistics had reconciled Scientia to her archrival Fortuna.”)

Danksagung

*“A scholar is just a library’s way of making another library.”
– Daniel Dennett*

Eine wissenschaftliche Arbeit ist nie das Werk einer einzelnen Person. Deshalb gilt mein Dank all denjenigen, die mich in den vergangenen Jahren persönlich unterstützt und mir die Erstellung meiner Dissertation ermöglicht haben, aber auch denjenigen Autorinnen und Autoren, deren Bibliothek an Werken Grundlage und Inspirationsquelle für diese Arbeit war – dazu zählen insbesondere die Arbeiten von Mireille Hildebrandt, Bernard E. Harcourt, Tobias Singelstein und Lucia Zedner.

Ganz besonderer Dank gebührt jedoch meiner Doktormutter Professorin Dr. Katrin Höffler für die herausragende und unkomplizierte Betreuung und die Freiheit, die mir während der Anfertigung der vorliegenden Arbeit gelassen wurde. Interessiert und stets ermutigend hat sie mich auf meinem Weg begleitet, viel Vertrauen in mich gesetzt und mich die Kunst der Wissenschaft gelehrt. Sie ist mir die denkbar beste Mentorin gewesen. Ihre Liebe und Leidenschaft für Strafrecht, Kriminologie und Rechtssoziologie ist wahrlich ansteckend.

Bedanken möchte ich mich zudem für die Unterstützung und Erstkorrektur durch Professor Dr. Johannes Kaspar und bei Professor Dr. Dr. h. c. Jörg-Martin Jehle für die Zweitkorrektur dieser Arbeit.

Zu tiefem Dank verpflichtet bin ich darüber hinaus Eva Marguerite Herzog, Maximiliane Berger und Elena Rittinghausen, ohne deren Zuspruch und Unterstützung diese Arbeit nicht hätte realisiert werden können, sowie Felix Butz und Henrike Kruse für die sehr großzügige Spende ihrer Zeit.

Meine Dankbarkeit gilt auch der Yale Law School, insbesondere dem dortigen Information Society Project, das mir während meines LL.M.-Studiums die Möglichkeit der Vertiefung der internationalen Perspektive auf diese Arbeit geboten hat. Für den anregenden Austausch und das hilfreiche Feedback, besonders von Professor Jack Balkin und Professor Tom Tyler, möchte ich mich ganz herzlich bedanken.

Ich danke zudem den Mitarbeiterinnen und Mitarbeitern des Graduiertenprogramms der Yale Law School, insbesondere Maria Dino, Allegra Di Buenaventura und Gordon Silverstein, sowie den herausragenden Bibliothekaren der Law School, insbesondere Lucie Olejnikova.

Danksagung

Mein Dank gilt schließlich der Studienstiftung des deutschen Volkes für die Finanzierung meiner Forschung, insbesondere Professor Dr. Florian Jacoby und Professor Dr. Henning Ernst Müller, die durch ihre Gutachten schon zu Beginn meiner Doktorarbeit ihr Vertrauen in mich gesetzt haben.

Die Kernideen für diese Arbeit haben sich – fern der Zwänge des Alltags – im Sommer 2017 auf der Insel Gozo herauskristallisiert. Dem Eigentümer des einsamen Strandhauses in der Bucht von Ghajn Barrani möchte ich ebenfalls ganz herzlich für seine Gastfreundschaft danken.

Die Arbeit berücksichtigt Literatur und Rechtsprechung bis einschließlich Dezember 2019.

Inhaltsübersicht

Abbildungsverzeichnis	25
Tabellenverzeichnis	27
Danksagung	7
Kapitel I. Grundlagen des personenbezogenen Predictive Policing	29
A. Einführung	29
B. Gang der Untersuchung	32
C. Terminologie und Abgrenzung	34
I. Arten des Predictive Policing	36
II. Abgrenzung zum Einsatz von Algorithmen im Strafverfahren, Strafvollzug und Ermittlungsverfahren	40
D. Forschungszuschnitt	41
E. Technologischer Hintergrund	45
I. Traditionelle statistische Verfahren	46
II. Algorithmengestützte Verfahren	58
III. Fazit zu technologischem Hintergrund	73
F. Bestandsaufnahme: gegenwärtiger Einsatz	74
I. USA und Großbritannien	74
II. Deutschsprachiger Raum	83
G. Tatsächliche Grenzen	100
I. Keine Gesamtbetrachtung – Big Data heißt nicht All Data	101
II. Keine Kausalität	102
III. Keine Neutralität	105
H. Fazit zum Kapitel I. Grundlagen	115
Kapitel II. Rechtliche Grenzen des personenbezogenen Predictive Policing	116
A. Polizeirechtlicher Rahmen	118
I. Einordnung in die Gefahr-Dogmatik	118

Inhaltsübersicht

II. Fehler der Risikoscoreerstellung	135
III. Ermächtigungsgrundlage	137
B. Verfassungsrechtlicher Rahmen	154
I. Informationelle Selbstbestimmung	154
II. Diskriminierungsverbot	170
III. Transparenzgebot	194
IV. Unschuldsvermutung	242
C. Strafprozessuale Betrachtung: Umwidmung zum Tatermittlungswerkzeug	244
I. Vorüberlegungen	245
II. „Doppeltüren“ der Datenweiterverarbeitung	249
III. Fazit zur Umwidmung zum Tatermittlungswerkzeug	258
D. Fazit zum Kapitel II. Rechtliche Grenzen	258
 Kapitel III. Algorithmische Wende in der Kriminalitätskontrolle – kriminologische, soziologische und rechtstheoretische Analyse	 260
A. Risiko: eine Begriffsbestimmung	262
I. Doppeldeutigkeit	262
II. Negative Konnotation in der Risikogesellschaft	263
III. Ungleiche Verteilung von Risiken	265
IV. Gesellschaftliche Sinnzuweisung	265
V. Quantitative Risikoabschätzung	267
VI. Risikowahrnehmung	268
VII. Tolerierte Risiken	269
VIII. Begriffliche Abgrenzung von Risiko und Gefahr	270
IX. Fazit zu Risiko	272
B. Gegenwärtige Situation: Risikogestützte Kriminalitätskontrolle	273
I. Exemplarische Normen der Risikoorientierung	273
II. Kriminologische, soziologische und rechtstheoretische Interpretationsansätze	284
C. Entwicklung: Algorithmengestützte Kriminalitätskontrolle – Merkmale der algorithmischen Wende	295
I. Fortschreibung der risikogestützten Kriminalitätskontrolle	295
II. Neue Herausforderungen	300
D. Fazit zum Kapitel III. Algorithmische Wende	340

Kapitel IV. Empfehlungen für Mindestanforderungen an algorithmengestützte Straftatprognosen	343
A. Entwicklungsmodalitäten	344
I. Nachvollziehbarkeit und Transparenz	344
II. Unvoreingenommenheit	345
B. Einsatzmodalitäten	346
I. Rechtsgrundlage	346
II. Risikokommunikation	346
C. Kontrollmodalitäten	347
D. Fazit zum Kapitel IV. Empfehlungen für Mindestanforderungen	349
Kapitel V. Schlusswort: Tyrannenmord und Neuanfang	351
Kapitel VI. Thesen	353
Literaturverzeichnis	357

Inhaltsverzeichnis

Abbildungsverzeichnis	25
Tabellenverzeichnis	27
Danksagung	7
Kapitel I. Grundlagen des personenbezogenen Predictive Policing	29
A. Einführung	29
B. Gang der Untersuchung	32
C. Terminologie und Abgrenzung	34
I. Arten des Predictive Policing	36
1. Personenbezogen und ortsbezogen	36
2. Gefahrverdacht bestätigend und Gefahrverdacht erzeugend	39
II. Abgrenzung zum Einsatz von Algorithmen im Strafverfahren, Strafvollzug und Ermittlungsverfahren	40
D. Forschungszuschnitt	41
1. Aktualität	41
2. Transformatives Potenzial	43
3. Forschungslücke	44
E. Technologischer Hintergrund	45
I. Traditionelle statistische Verfahren	46
1. Zusammenstellen der Fallbasis	47
2. Festlegung der Zielvariablen	48
3. Festlegung der prädiktiven Inputvariablen	49
4. Ableitung eines prädiktiven Modells	50
5. Risikoübersetzung und -kommunikation	51
a) Prozentsatz	51
b) Kriminalitätswahrscheinlichkeit im Vergleich zur Durchschnittsbevölkerung	52
c) Basisrate	52
d) Fehlerrate	53
e) Cut-Off	54

Inhaltsverzeichnis

6. Anwendung auf den Einzelfall	54
a) Personenkreis der Beurteilten	55
b) Personenkreis der Beurteilenden	57
II. Algorithmengestützte Verfahren	58
1. Regelbasierte algorithmengestützte Entscheidungssysteme	59
2. Fallbasierte algorithmengestützte Entscheidungssysteme	62
a) Unterschiede: Zusammenstellen des Trainingsdatensatzes (Schritt 1)	63
b) Unterschiede: Festlegung der Zielvariablen (Schritt 2)	65
c) Unterschiede: Festlegung prädiktiver Inputvariablen (Schritt 3)	65
d) Unterschiede: Ableitung eines prädiktiven Modells (Schritt 4)	67
e) Unterschiede: Risikoübersetzung und -kommunikation (Schritt 5)	69
f) Unterschiede: Anwendung auf den Einzelfall (Schritt 6)	69
aa) Personenkreis der Beurteilten	70
bb) Personenkreis der Beurteilenden	71
(1) Von Prognose-Experten zu Prognose-Laien	71
(2) Automation Bias	71
III. Fazit zu technologischem Hintergrund	73
F. Bestandsaufnahme: gegenwärtiger Einsatz	74
I. USA und Großbritannien	74
1. Beware	76
2. HART (Harm Assessment Risk Tool)	78
3. Strategic Subject List	80
4. Zusammenfassung	83
II. Deutschsprachiger Raum	83
1. RADAR-iTE (Regelbasierte Analyse potenziell destruktiver Täter zur Einschätzung des akuten Risikos – islamistischer Terrorismus)	85
a) Entwicklung	85
b) Anwendung	86
aa) Personenkreis der Beurteilenden	88
bb) Personenkreis der Beurteilten	88
cc) Intransparenz	89
2. Palantir Gotham – hessenDATA	90

3. DyRiAS (Dynamisches Risiko-Analyse-System)	92
a) Entwicklung	93
b) Anwendung	94
aa) Personenkreis der Beurteilenden	95
bb) Personenkreis der Beurteilten	95
4. Fluggastdatenmusterabgleich	96
5. Zusammenfassung	99
G. Tatsächliche Grenzen	100
I. Keine Gesamtbetrachtung – Big Data heißt nicht All Data	101
II. Keine Kausalität	102
III. Keine Neutralität	105
1. Datenauswahlprozesse	106
a) Mangelnde Datenqualität	106
b) Dunkelfeld in den Statistiken	107
c) Keine Repräsentativität der Stichprobe	109
d) Perpetuierung gesellschaftlicher Diskriminierung	110
e) Zwischenfazit und Lösungsmöglichkeiten	111
2. Festlegung der Zielvariablen	112
3. Auswahl der Inputvariablen	112
4. Kalibrierung und Überwachung des Lernprozesses	113
a) Fehlerrate	113
b) Überanpassung – Zufällige Korrelationen	114
5. Zusammenfassung	115
H. Fazit zum Kapitel I. Grundlagen	115
Kapitel II. Rechtliche Grenzen des personenbezogenen Predictive Policing	116
A. Polizeirechtlicher Rahmen	118
I. Einordnung in die Gefahr-Dogmatik	118
1. Konkrete Gefahr	118
2. Gefahrverdacht	121
3. Risikoscore als konkrete Gefahr?	124
a) Gegenargumente	124
b) Quantifizierbarkeit von normativen Abwägungsentscheidungen	126
4. Risikoscore als Gefahrverdacht?	129
5. Risikoscore als ein tatsächlicher Anhaltspunkt	131
6. Zwischenergebnis	134
II. Fehler der Risikoscoreerstellung	135

Inhaltsverzeichnis

III. Ermächtigungsgrundlage	137
1. Erforderlichkeit einer Ermächtigungsgrundlage	137
2. Vorliegen einer Ermächtigungsgrundlage	139
a) Standardbefugnisse	139
aa) Rasterfahndung	139
(1) Errichten eines PPP-Systems	140
(2) Erzeugen eines Risikoscores	140
(a) „Stehendes“ System	141
(b) „Muster“ statt Datenbestand	141
(c) Neues Datum	141
(d) Erhöhte Intransparenz	142
bb) Generalklauseln der Datenspeicherung und Weiterverarbeitung	143
(1) Datenspeicherung in automatisierten Dateisystemen	143
(2) Datenverarbeitung und Datenabgleich	144
(a) Datenverarbeitung	145
(b) Datenabgleich	147
cc) Automatisierte Anwendung zur Datenanalyse	147
b) Allgemeine polizeirechtliche Generalklausel	148
c) Datenschutzrecht	150
d) Fluggastdatengesetz	150
3. Neue Standardbefugnis	153
B. Verfassungsrechtlicher Rahmen	154
I. Informationelle Selbstbestimmung	154
1. Umfang	155
a) Entscheidung über die Preisgabe und Verwendung persönlicher Daten	156
b) Geschützte Daten	157
c) Verbot der Persönlichkeitsprofilbildung	157
d) Gemeinwohldimension und Einschüchterungseffekte	158
2. Grenzen und Verhältnismäßigkeit	159
3. Konkrete Anforderungen des Rechts auf informationelle Selbstbestimmung an PPP	161
a) Vorliegen einer hohen Eingriffsintensität	162
aa) Heimlichkeit und Mangel an Transparenz	162
bb) Streubreite	163
cc) Automatisierung	164
dd) Nähe zu Persönlichkeitsprofilen	165
ee) Stigmatisierung	166

b)	Folgen einer hohen Eingriffsintensität	166
aa)	Hinreichend gewichtige Straftaten	166
bb)	Konkrete Gefahr	167
(1)	Anforderung des BVerfG zur Rasterfahndung	167
(2)	Kein Absenken der Eingriffsschwelle unter eine konkrete Gefahr	167
c)	Organisations- und Verfahrensvorgaben	168
4.	Zusammenfassung	169
II.	Diskriminierungsverbot	170
1.	Einführung	170
2.	Quellen algorithmischer Diskriminierung	174
a)	Datenauswahlprozesse	174
b)	Festlegung der Zielvariablen	174
c)	Auswahl der Inputvariablen	175
d)	Kalibrierung und Überwachung des Lernprozesses	175
3.	Rechtliche Einordnung	176
a)	Gleichheitssätze	177
aa)	Besondere Gleichheitssätze	177
(1)	Ungleichbehandlung	177
(2)	Frage nach einer Rechtfertigung	178
bb)	Allgemeiner Gleichheitssatz	179
(1)	Ungleichbehandlung	179
(2)	Frage nach einer Rechtfertigung	180
b)	Besonderheiten im Rahmen von PPP	182
aa)	Erkennen einer Ungleichbehandlung	183
bb)	Ausdifferenzierte Fallgruppen der Ungleichbehandlung	183
cc)	Statistische Rechtfertigungen	189
(1)	Rechtfertigung einer Diskriminierung nach Art. 3 Abs. 3 S. 1 GG	190
(a)	Argument des „Rational Racism“	190
(b)	Argument des „kleineren Übels“	191
(2)	Rechtfertigung einer Diskriminierung nach Art. 3 Abs. 1 GG	192
4.	Fazit zum Diskriminierungsverbot	193
III.	Transparenzgebot	194
1.	Exkurs: Janusköpfigkeit des Blackbox-Narrativs	195

Inhaltsverzeichnis

2. Drei Schichten der Intransparenz	198
a) Begriffsklärung	198
aa) Unzugänglichkeit qua Geheimhaltung	200
bb) Unzugänglichkeit qua fehlendem Fachwissen	201
cc) Unzugänglichkeit qua systemimmanenter Komplexität	202
(1) Fallbasierte algorithmische Entscheidungssysteme	202
(2) Regelbasierte algorithmische Entscheidungssysteme	203
(3) Beispiele	203
(4) Lösungsansätze: „Explainable AI“	204
b) Fazit zu Transparenzschichten	205
3. Transparenzmechanismen	206
a) Erste Transparenzdimension: Zeitpunkt der Offenlegung	207
b) Zweite Transparenzdimension: Zur Einsichtnahme berechtigter Personenkreis	208
aa) Subjektiv Betroffene	208
(1) Einzelperson	208
(2) Kollaboratives Crowdsourcing	209
bb) Staatliche Kontrollinstitution	210
(1) Mögliche Ausgestaltungen	211
(2) Personelle Ausstattung	211
(3) Organisatorisch-strukturelle Überlegungen	212
(4) Fazit zu staatlichen Kontrollinstitutionen	213
cc) Breite Öffentlichkeit	214
dd) Fazit zum zur Einsichtnahme berechtigten Personenkreis	214
c) Dritte Transparenzdimension: Umfang der Offenlegung	215
aa) Abstrakte Informationen	216
(1) Existenz und Einsatz im Einzelfall	216
(2) Abstrakte Wirkungsprinzipien	216
(3) Quellcode	217
(4) Output-Testing	217
(5) Protokollierungspflichten der Designphase	218
bb) Begründung im Einzelfall	219
cc) Fazit zum Transparenzgebot	220

4. Argumente gegen Transparenz	221
a) Unmöglichkeit von Transparenz	222
b) Unnötigkeit von Transparenz	223
aa) „Human in the Loop“	223
bb) Vergleich mit bereits bestehender Intransparenz	224
c) Überwiegen konkurrierender Interessen	226
aa) Betriebsgeheimnis	226
bb) Ausspähung des Algorithmus	229
cc) Datenschutz Dritter	230
dd) Fazit zum Überwiegen konkurrierender Interessen	231
d) Fazit zu Argumenten gegen Transparenz	231
5. Rechtliche Verortung des Transparenzgebots	231
a) Einfachgesetzlich	232
aa) Datenschutzrecht	232
bb) Informationsfreiheitsgesetz	232
cc) Verwaltungsprozessrecht	233
b) Verfassungsrecht	234
aa) Menschenwürdekern des Rechts auf informationelle Selbstbestimmung	234
bb) Demokratieprinzip	236
(1) Legitimationskette	236
(2) Demokratische Willensbildung	237
(3) Demokratische Kontrolle	237
cc) Rechtsstaatsprinzip	238
6. Fazit zum Transparenzgebot	240
IV. Unschuldsvermutung	242
C. Strafprozessuale Betrachtung: Umwidmung zum Tatermittlungswerkzeug	244
I. Vorüberlegungen	245
1. Keine Beweisgeeignetheit	245
2. Zweifelhafte Aufklärungsgeeignetheit als Spurenansatz	246
3. Keine Ermittlungen „ins Blaue hinein“	247
4. Konkreter Ermittlungsansatz	248
II. „Doppeltüren“ der Datenweiterverarbeitung	249
1. Doppeltür: gefahrenabwehrrechtliche Seite	250
2. Doppeltür: strafprozessuale Seite	251
a) § 98 c S. 1 StPO: maschineller Abgleich von Daten	252
aa) Fehlen besonderer Eingriffsschwellen	252
bb) Keine Anwendbarkeit auf PPP	253

Inhaltsverzeichnis

b) § 161 Abs. 2 StPO: katalogabhängige Maßnahmen der Datenerhebung	254
c) §§ 161 Abs. 1, 163 Abs. 1 StPO: Ermittlungsgeneralklausel	255
aa) Vergleich mit der Onlinedurchsuchung vor 2017	256
(1) e. A. Zulassen der Verwendung als Spurenansatz	256
(2) a. A. Ablehnung jeglicher Verwertung	257
bb) Übertragung auf PPP	257
III. Fazit zur Umwidmung zum Tatermittlungswerkzeug	258
D. Fazit zum Kapitel II. Rechtliche Grenzen	258
Kapitel III. Algorithmische Wende in der Kriminalitätskontrolle – kriminologische, soziologische und rechtstheoretische Analyse	260
A. Risiko: eine Begriffsbestimmung	262
I. Doppeldeutigkeit	262
II. Negative Konnotation in der Risikogesellschaft	263
III. Ungleiche Verteilung von Risiken	265
IV. Gesellschaftliche Sinnzuweisung	265
V. Quantitative Risikoabschätzung	267
VI. Risikowahrnehmung	268
VII. Tolerierte Risiken	269
VIII. Begriffliche Abgrenzung von Risiko und Gefahr	270
IX. Fazit zu Risiko	272
B. Gegenwärtige Situation: Risikogestützte Kriminalitätskontrolle	273
I. Exemplarische Normen der Risikoorientierung	273
1. Materielles Strafrecht – Versuchsvorfeld	275
a) § 89 a StGB – Vorbereitung einer schweren staatsgefährdenden Gewalttat	277
b) § 129 a StGB – Bildung terroristischer Vereinigungen	278
c) Gruppenrisiko einer zukünftigen ungewissen Rechtsgutsverletzung	279
2. Strafprozessrecht	279
3. Sanktionenrecht	281
4. Polizeirecht	282
5. Zusammenfassung	283

II. Kriminologische, soziologische und rechtstheoretische Interpretationsansätze	284
1. Risikostrafrecht – Strafrecht als Großsteuerungsmittel	284
2. Kriminalpräventionsrecht und symbolisches Strafrecht	285
3. Risikokriminologie	286
4. Feindstrafrecht – Die „riskante“ Person als Feind?	287
5. Sicherheitsgesellschaft	289
6. Actuarial Turn	291
7. Zusammenfassung	293
C. Entwicklung: Algorithmengestützte Kriminalitätskontrolle – Merkmale der algorithmischen Wende	295
I. Fortschreibung der risikogestützten Kriminalitätskontrolle	295
1. Vorfeldfokussierung	295
2. Individualisierte Risikozuschreibung anhand überindividueller Gruppenmerkmale	296
3. „Feind“-Perspektive	297
4. Verschleierung politischer Wertentscheidungen	298
5. Sonderopfer	299
6. Zusammenfassung	300
II. Neue Herausforderungen	300
1. Rückkehr der Lebensführungsschuld	301
a) Strafrecht	303
b) Polizeirecht	304
2. Legitimitätsverlust durch mangelnde Verfahrensgerechtigkeit	305
a) Legitimität und Rechtsbefolgung	306
b) Kernelemente der Verfahrensgerechtigkeit	307
c) Stand der Forschung in Deutschland	308
d) Verfahrensgerechtigkeit algorithmengestützter Entscheidungssysteme	309
aa) Beteiligung	310
bb) Neutralität	311
cc) Respektvoller Umgang	312
dd) Vertrauen in die Motive	313
e) Transparenz als Antwort auf mangelnde Verfahrensgerechtigkeit	314
f) Zusammenfassung	317

Inhaltsverzeichnis

3. Kriminalitätskontrolle ohne Kriminologie	317
a) Algorithmenkundige Kriminologie	321
aa) Nutzen algorithmengestützter Methoden für die Kriminologie	322
bb) Kritische Begleitung algorithmengestützter Kriminalitätskontrolle	323
b) Zusammenfassung	324
4. Selbst auferlegte Gedankenlosigkeit	325
a) Anwendung auf algorithmengestützte Entscheidungssysteme	328
aa) Entmenschlichung – „Moral Buffer“	328
bb) Verantwortungsentledigung – Vom Werkzeug zur Autoritätsfigur	329
cc) Zwischenergebnis	331
b) Steigerung: Selbst verschuldete Unmündigkeit – Bewusstes Begeben in eine Situation des „Nicht-Verstehen-Könnens“	331
aa) Deskillung	332
bb) Systemimmanent intransparente Entscheidungsverfahren	333
cc) „Übermenschlich“ medierte Wissensvermittlung	333
c) Zwischenergebnis	335
5. Zwang des Rechts unter die Maschinenlogik	335
6. Zwischenfazit zu Neuen Herausforderungen	340
D. Fazit zum Kapitel III. Algorithmische Wende	340
Kapitel IV. Empfehlungen für Mindestanforderungen an algorithmengestützte Straftatprognosen	343
A. Entwicklungsmodalitäten	344
I. Nachvollziehbarkeit und Transparenz	344
II. Unvoreingenommenheit	345
B. Einsatzmodalitäten	346
I. Rechtsgrundlage	346
II. Risikokommunikation	346
C. Kontrollmodalitäten	347
D. Fazit zum Kapitel IV. Empfehlungen für Mindestanforderungen	349

Inhaltsverzeichnis

Kapitel V. Schlusswort: Tyrannenmord und Neuanfang	351
Kapitel VI. Thesen	353
Literaturverzeichnis	357

Abbildungsverzeichnis

Abb. 1.	Übersicht über mögliche Verwendungskontexte prädiktiver Algorithmen zur Kriminalitätsprognose	35
Abb. 2.	Streubreite verschiedener Predictive-Policing-Ansätze zwischen den Polen „Gefahrverdacht bestätigend“ und „Gefahrverdacht erzeugend“	38
Abb. 3.	Kernelemente des polizeilichen Gefahrenbegriffs: Tatsächliche Anhaltspunkte und Prognose	121
Abb. 4.	Einordnung des algorithmischen Risikoscores in den polizeirechtlichen Gefahrenbegriff: Variante Nr. 1 (Risikoscore = tatsächliche Anhaltspunkte + Prognose) ist unzutreffend; Variante Nr. 2 (Risikoscore = ein tatsächlicher Anhaltspunkt) ist zutreffend	132
Abb. 5.	Übersicht über neue Fallgruppen algorithmischer Diskriminierungen und die gegen sie vorgebrachten statistischen Rechtfertigungen	186
Abb. 6.	Drei Schichten algorithmischer Intransparenz	200
Abb. 7.	Drei Transparenzdimensionen	206
Abb. 8.	Dreieck algorithmischer Transparenz für PPP-Systeme	241
Abb. 9.	Risikoorientierte Kriminalitätskontrolle	275
Abb. 10.	Dreieck algorithmischer Transparenz für PPP-Systeme	348

Tabellenverzeichnis

Tbl. 1. Vergleich traditionell statistische und algorithmengestützte Kriminalprognosen (Hervorhebung der Unterschiede durch Umrandung)	59
Tbl. 2. Übersicht ausgewählter, in den USA und Großbritannien eingesetzter algorithmengestützter Entscheidungssysteme zur Straftatprognose	76
Tbl. 3. Übersicht über im deutschsprachigen Raum zum Einsatz kommende algorithmengestützte Entscheidungssysteme und ihre Vorstufen zur Straftatprognose	84
Tbl. 4. Transparenz: Zeitpunkt der Offenlegung	207
Tbl. 5. Transparenz: Zur Einsichtnahme berechtigter Personenkreis	208
Tbl. 6. Transparenz: Umfang der Offenlegung	215
Tbl. 7. Übersicht über Transparenzmechanismen der drei Transparenzdimensionen	221

