

## Inhaltsverzeichnis

Abkürzungsverzeichnis	17
Einleitung	23
A. Themeneläuterung	23
B. Entwicklung des Predictive Policing	26
C. Gang der Untersuchung und Eingrenzung des Untersuchungsgegenstand	29
Teil 1: Der aktuelle Einsatz: Orts- bzw. Raumbezogenes Predictive Policing	33
A. Einführung	33
I. Kriminologischer Hintergrund	35
1. Rational Choice Theory	36
a) Inhalt	36
b) Kritik	39
c) Relevanz für Predictive Policing	41
2. Routine Activity Approach	41
a) Inhalt und Ausrichtung	42
b) Relevanz für Predictive Policing	45
3. Sozialkontrolltheorien: Broken Windows und Defensible Space	46
a) Broken Windows-Theorie	46
(1) Inhalt der Broken Windows-Theorie	47
(2) Stellungnahme	48
b) Defensible Space-Ansatz	49
c) Relevanz für Predictive Policing	50
4. Kriminalgeographische Ansätze	50
a) Hot Spot-Analyse	51
b) Near Repeat Victimization	54
5. Die raumbezogene Umsetzung der kriminologischen Ansätze für eine Vorhersage: Risk Terrain-Modeling	56
6. Abschließende Beurteilung	58

<b>II. Technische Umsetzung</b>	<b>59</b>
1. PRECOBS	59
a) Funktionsweise	60
b) Weiterentwicklung: PRECOBS Enterprise	63
2. SKALA	64
a) Verwendete Daten	64
b) Funktionsweise	66
c) Weiterentwicklung	69
3. KrimPro	69
4. PreMAP	70
5. KLB-operative	72
6. Zusammenfassung	73
<b>B. Rechtliche Bewertung</b>	<b>73</b>
I. Gesetzgebungskompetenz und Einordnung des Einsatzfeldes von Predictive Policing-Systemen	74
II. Das Erfordernis von Rechtsgrundlagen für den Einsatz von Predictive Policing	80
1. Gegenwärtige Praxis	80
2. Vorbehalt des Gesetzes	83
3. Grundrechtsrelevanz	85
a) Verdrängung der nationalen Grundrechte durch die Unionsgrundrechte?	85
(1) Anwendbarkeit auf rein nationale Sachverhalte	88
(2) Sachlicher Anwendungsbereich	93
(a) Das Vorbereitungssstadium	95
(b) Nutzung der georeferenzierten Daten	100
(3) Auswirkung auf die Anwendbarkeit der Grundrechte des Grundgesetzes	105
b) Die Grundrechte des Grundgesetzes	105
(1) Informationelle Selbstbestimmung	106
(a) Begriff der persönlichen Daten	107
(b) Einordnung der verwendeten Daten	111
(i) Das Vorbereitungssstadium	112
(ii) Die in den Algorithmen eingesetzten Daten	112
(iii) Besonderheit sozistrukturelle Daten	116
(iv) Die ausgegebenen Daten	116
(c) Fazit	117

(2) Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme	117
(3) Recht auf Datenschutz	120
(4) Eigentum und Unverletzlichkeit der Wohnung	121
(5) Allgemeine Handlungsfreiheit, Art. 2 Abs. 1 GG	125
(6) Allgemeiner Gleichheitssatz, Art. 3 Abs. 1 GG	128
c) Fazit	129
4. Wesentlichkeitstheorie, Art. 20 Abs. 3 GG	129
a) Polizeirecht als Ausdruck des Gewaltmonopols des Staates und Notwendigkeit der Sicherung des Vertrauens in die Sicherheitsbehörden	132
b) Staatliche Kontrollmöglichkeiten und Rechtsschutz des Bürgers	134
c) Spezifische Gefahren der automatischen Datenanalyse	138
d) Fazit	142
5. Stellungnahme	143
III. Analyse der Rechtsgrundlagen im Vorfeld des Einsatzes von Predictive Policing: Datenbeschaffung und -aufbereitung	144
1. Beschaffung der Daten für den Einsatz in der Software	144
a) Primärrechtliche Anforderungen an eine Rechtsgrundlage	145
b) Sekundärrechtliche Anforderungen an eine Rechtsgrundlage	149
c) Grundgesetzliche Anforderungen an eine Rechtsgrundlage	150
d) Länderspezifische Anforderungen an eine Rechtsgrundlage	150
e) Rechtsgrundlage	151
2. Aufbereitung der Daten für den Einsatz in der Software	152
a) Zweckänderung	152
(1) Primärrechtliche Anforderungen	152
(2) Sekundärrechtliche Anforderungen	152
(3) Anforderungen des Grundgesetzes	153
(4) Gemeinsame Anforderungen	154
(5) Rechtsgrundlagen	155
(a) Verwendung repressiv erhobener Daten zu präventiven Zwecken	156
(i) Bayern	157

(ii) NRW	159
(iii) Sachsen	160
(iv) Niedersachsen	162
(v) Hessen	162
(vi) Berlin	164
(b) Verwendung personenbezogener Daten zu statistischen und wissenschaftlichen Zwecken	164
(i) Repressiv erhobene Daten überhaupt erfasst?	165
(ii) Konkretisierung statistischer und wissenschaftlicher Zwecke	166
(iii) Entwicklungs- und Weiterentwicklungsphase	169
(c) Fazit	173
(6) Einwilligung als Alternative?	173
(a) Zulässigkeit nach dem Primärrecht	174
(b) Zulässigkeit nach dem Sekundärrecht	174
(c) Zulässigkeit nach dem Grundgesetz	175
(d) Fazit	176
b) Georeferenzierung	176
(1) Recht auf informationelle Selbstbestimmung	177
(2) Art. 8 EUGrCh	182
(3) JI-RiLi	184
(4) Rechtsgrundlagen	185
(5) Fazit	186
3. Gesamtwürdigung	186
IV. Präventiv-polizeiliche Folgemaßnahmen aufgrund von Prognosen	187
1. Grundsatz: keine konkrete Gefahr	187
2. Gefahrenverdacht oder Risiko- bzw. allgemeine Bedrohungslage?	191
a) Gefahrenverdacht	191
b) Risikolage bzw. allgemeine Bedrohungslage	193
c) Fazit	195
3. Generalklausel im Gefahrenvorfeld	196
a) Anwendbarkeit der Generalklausel bei Gefahrenverdacht	196
b) Generalklausel bei Gefahrerforschungsmaßnahmen	197

c) Vorreiter Bayern: eigene Generalklausel für das Gefahrenvorfeld	199
4. Gefahrerforschungsmaßnahmen	205
5. Bestimmte Standardmaßnahmen	205
a) Identitätsfeststellung	208
(1) Die unterschiedliche tatbestandliche Ausgestaltung	209
(a) NRW	209
(b) Niedersachsen	216
(c) Bayern	219
(d) Hessen	229
(e) Berlin	232
(f) Sachsen	236
(2) Rechtsfolge und Adressatenauswahl	242
(3) Fazit	246
b) Strategische Fahndung	248
6. Fazit	253
V. Repressiv-polizeiliche Folgemaßnahmen	254
VI. Spezifische Gefahren und Probleme des Einsatzes von Predictive Policing und Lösungsansätze	257
1. Gefahr von Verdrängungseffekten	257
2. Gefahr der Schaffung immer neuer Befugnisse, die die Eingriffsschwelle kontinuierlich weiter ins Vorfeld einer konkreten Gefahr verlagern	259
3. Gefahr der Aufweichung des Trennungsgebots	264
4. Gefahr einer Technikhörigkeit	267
5. Gefahr der Versteinerung bereits bekannter Probleme	269
6. Problem der nicht bestimmmbaren Kosten-Nutzen-Relation	271
7. Fazit	274
VII. Einfachrechtliche Vorgaben und Überlegungen für den Einsatz von Predictive Policing-Software	275
1. Datenschutzrechtliche Vorgaben	275
2. Datenqualität und -quantität	276
3. Algorithmenkontrolle	276
4. Fazit	278

C. Sonderfall PRECOBS: Rechtliche Anforderungen an den Einsatz privater Software auf staatlicher (Sicherheits-)Ebene	278
I. Einordnung des Beteiligungsgrades Privater bei der Wahrnehmung der öffentlichen Aufgabe der Gefahrenabwehr durch Predictive Policing-Software	280
1. Fiskalisches Hilfsgeschäft	280
2. Privatisierungsformen	282
a) Verwaltungshelfer	284
b) PPP	284
c) Einordnung	286
3. Fazit	286
II. Grenzen der Beteiligung	286
1. Gewaltmonopol des Staates	288
2. Der Funktionsvorbehalt, Art. 33 Abs. 4 GG	291
a) Meinungsstand zu Art. 33 Abs. 4 GG als Privatisierungsschranke	291
b) Stellungnahme	298
c) Fazit	300
3. Demokratie- und Rechtsstaatsprinzip	301
a) Entwicklungen in der Rechtsprechung	305
(1) Einsatz von Wahlcomputern, BVerfGE 123, 39-88	306
(2) Das BVerfG zur elektronischen Aufenthaltsüberwachung	309
(3) Die oberlandesgerichtliche Rechtsprechung zur Verkehrsüberwachung durch Private	312
(a) Die Rechtsprechungsentwicklung bis einschließlich 2015	314
(b) Die jüngere Rechtsprechung des OLG Frankfurt am Main	317
(c) Die jüngere Rechtsprechung des Bayerischen Obersten Landesgerichts	321
(4) Zusammenfassung der Erkenntnisse aus der Rechtsprechung im Hinblick auf den Einsatz privater Software	324
b) Übertragung der Erkenntnisse auf den Einsatz privater Software zur Erfüllung hoheitlicher Aufgaben insbesondere im Bereich der Gefahrenabwehr	326
4. Einordnung von PRECOBS	330

III. Vergaberecht	331
IV. Datenbeschaffung und -verwaltung	336
V. Fazit	338
D. Abschließende Würdigung	339
 Teil 2: Weiterentwicklungsmöglichkeiten des raumbezogenen Predictive Policing und seine rechtlichen Grenzen	341
A. Ausdehnung auf andere Delikte	342
B. Verwendung von bzw. Verknüpfung mit personenbezogenen Daten	343
I. Erforderlichkeit einer Rechtsgrundlage	343
II. Datenschutzrechtliche Implikationen	344
III. Herkunft der Daten	347
1. Die Nutzung von Daten, die durch besonders tiefe Grundrechtseingriffe erhoben wurden	348
2. Die Nutzung von Daten, die durch Nachrichtendienste erhoben wurden	350
IV. Kategorien von personenbezogenen Daten	351
V. Fazit	352
C. Big Data Policing/ Einsatz von (fortgeschrittener) KI	352
I. Nachvollziehbarkeit der Entscheidungen	354
II. Chancen	356
III. Konflikt mit dem Grundsatz der Zweckbindung von Daten und Datenminimierung	356
1. Grundsatz der Zweckbindung	357
2. Grundsatz der Datenminimierung	358
3. BVerfG zu § 6a ATDG a.F.	359
IV. Fazit	361
V. Exkurs: Das Digitalisierungsgesetz von Schleswig-Holstein	362
D. Verknüpfung der polizeilichen Datenbanken, Polizei 2020	364
E. Fazit	368
 Teil 3 Zusammenfassung in Thesen	369
Literaturverzeichnis	373