

Inhaltsverzeichnis

A. Einführung	15
I. Eine technische Innovation mit überschießendem Potenzial	15
II. Begriffliche und technische Grundlagen	19
1. Schlüsselbegriffe	20
a) Videoüberwachung	20
b) Intelligente Videoüberwachung – <i>smart CCTV</i>	21
c) Video-Tracking	21
d) Mustererkennung	22
e) Automatisierung	24
2. Blick über den Stand der aktuellen technischen Entwicklung	24
a) Beispiele heutiger Praxis	24
b) Kleine Typologie der Systemarchitekturen	26
c) Technische Funktionsweise der Videoanalyse	27
III. Stand der Rechtswissenschaft	29
IV. Erkenntnisinteresse und Gang der Untersuchung	31
V. Rechtsmethodische Prämissen	34
B. Einfache Videoüberwachung im Spiegel von Rechtswissenschaft und -praxis	37
I. Gesetzgeberische Reaktionen	37
1. Der Weg zu Legalität und Bestimmtheit	37
2. Inhaltliche Analyse: Diversität nur im Detail	39
II. Skizze der Dogmatik	41
1. Gesetzgebungskompetenz	42
2. Würde des Menschen	43
3. Recht auf informationelle Selbstbestimmung	44
4. Recht am eigenen Bild	45
5. Versammlungsrecht	46
6. Weitere Grundrechte	46
III. Fazit: Dominanz der Verfassungsrechtsprechung	47

C. Smart CCTV als wesentlicher Entwicklungssprung	48
I. Algorithmische Analyse als automatisierte Datenverarbeitung personenbezogener Daten	50
1. Datenverarbeitung	51
a) Verarbeitung im engeren Sinne (§ 3 Abs. 4 BDSG)	51
b) Verarbeitung im weiteren Sinne (§ 3 Abs. 2 S. 1 BDSG)	52
2. Automatisierung	52
3. Personenbezogene Daten als Verarbeitungsobjekt	53
4. Zwischenergebnis	54
II. Von der Überwachungshilfe zur überwachenden Maschine	54
III. Normativität automatisierter Verhaltensanalyse?	55
1. Architektur, Funktion und Wirkung des Systems	56
a) Aufgabe des Analyse-Moduls	56
b) Alarm-Modul ein Reaktionsmechanismus	56
c) Die Reaktion des Operators	57
d) Bedeutung der subjektiven Seite	57
2. System und Sozialnorm	58
IV. Von der Symbol- zur Realpolitik	61
V. Fazit: nötige Neubewertung neuer Technik	62
D. Intelligente Überwachung und Menschenwürde	63
I. Stand der Würdediskussion	64
1. Unantastbarkeit der Menschenwürde	65
2. Positiv-abstrakte Erläuterungen	66
3. Positiv-konkrete Inhaltszuschreibungen	67
4. Negative Bestimmungen	68
5. Kritik der dargestellten Ansätze	69
6. Unterscheidung von Hierarchisierung und Operationalisierung	70
II. Bewertung anhand Art. 1 Abs. 1 GG	71
1. Biometrische Erfassung und Identifizierung	71
2. Verhaltensanalyse	73
3. Tracking	75
4. Einsatzintensitäten und -modalitäten	76
III. Fazit: intelligente Videoüberwachung nicht <i>per se</i> entwürdigend	76

E. Zentraler Maßstab: das Recht auf informationelle Selbstbestimmung	78
I. Normativer Gehalt des Rechts auf informationelle Selbstbestimmung	78
1. Subjektiv-rechtlicher Schutzbereich	78
a) Schutzgegenstand und Gewährleistungsgehalt in der Rechtsprechung des Bundesverfassungsgerichts	78
b) Den Schutzbereich begrenzende Vorschläge aus der Literatur	80
c) Daneben Schutz vor Einschüchterung?	82
aa) Genereller Schutz durch das informationelle Selbstbestimmungsrecht?	82
(1) Bejahende Interpreten des Volkszählungsurteils	82
(2) Analyse und Kritik	83
(3) Alternative Konzeption	85
bb) Exkurs: Einschüchterungsschutz durch spezielle Grundrechte am Beispiel Versammlungsfreiheit	87
cc) Zwischenergebnis	89
d) Relevanz intelligenter Videoüberwachung	90
2. Objektiv-rechtliche Dimension	90
a) Ausstrahlungswirkung, Schutzpflichten sowie Organisation und Verfahren	91
b) Grundrechtlicher Schutz des Gemeinwesens	91
aa) Zu interpretierende Rechtsprechung des Bundesverfassungsgerichts	91
bb) Literarische Rezeption	93
cc) Misslingende Systematisierung in objektiv-rechtliche Fallgruppen ..	94
dd) Demokratisch-funktionales Grundrechtsverständnis als Erbe Smends	96
c) Bedeutung für die Fragestellung	98
II. Eingriffe in die informationelle Selbstbestimmung	99
1. Dogmatik des Bundesverfassungsgerichts	100
a) Informationseingriff als Unterfall modernen Eingriffsverständnisses	100
b) Eingriff nur oberhalb einer Erheblichkeitsschwelle?	102
c) Jeder Umgang mit den Daten als eigener Eingriff	103
d) Folgerungen für die Fragestellung	104
2. Eingriffe durch herkömmliche Videoüberwachung	105
a) Übersichtsbeobachtung	105
b) Nahbeobachtung	106
c) Aufzeichnung und weiterer Umgang	108
d) Provokation psychischer Reaktionen	108
e) Resümee und Relevanz	109
3. Zusätzliche Eingriffe durch intelligente Videoüberwachung	109
a) Automatisierte Analyse	110

b) Detektion, Klassifizierung und Identifizierung	110
c) Automatisierte Alarmierung	111
d) Verstärkte psychische Reaktionen	112
e) Zwischenergebnis	113
4. Einwilligung in den Eingriff: kein gangbarer Weg	114
5. Trotz Eingriffsaddition kein „additiver“ Eingriff	114
6. Zusammenfassung	115
III. Rechtfertigung von Eingriffen in das Grundrecht	116
1. Anforderungen an Eingriffsgrundlagen	116
a) Normenklarheit und Normenbestimmtheit	117
b) Organisatorische und verfahrensrechtliche Vorkehrungen	118
aa) Spezielle Vorgaben für Organisation und Verfahren	118
bb) Folgerungen für intelligente Überwachungstechnik	119
cc) Weitere Möglichkeiten	120
2. Verhältnismäßigkeit als entscheidende Schranken-Schranke	121
a) Die wesentlichen legitimen Zwecke	123
aa) Herkömmliche Videoüberwachung	123
bb) Intelligente Videoüberwachung	124
b) Prüfung evidenter Ungeeignetheit	124
c) Abstrakte Erforderlichkeitsprüfung	126
d) Angemessenheit	128
aa) Verhältnis von gefährdetem Rechtsgut und Tiefe des Grundrechtseingriffs	128
bb) Gewicht der grundrechtlichen Beeinträchtigung	129
(1) Veranlassung als subjektive Rückkopplung der Maßnahme	129
(2) Streubreite als objektive Präzision einer Maßnahme	131
(3) Heimlichkeit als Autonomieverlust	133
(4) Das riskante Potenzial Automatisierung	136
(5) Qualität durch Quantität statt Quantität als Qualität	137
(6) Eine Systematik der Persönlichkeitsrelevanz	140
(7) Grundrechtlich geschützte Privatheit	144
(8) Verhältnis von Privatheit und Persönlichkeitsrelevanz	145
(9) Möglichkeiten der Verwendung und Verknüpfung	146
(10) Identifizierung	147
(11) Speicherung	148
(12) Ein Fazit oder das grundrechtsschonende Potenzial der neuen Technik	149

cc) Rechtsgutgeföhrung	150
dd) Abwägung exemplifizierter Konstellationen	151
(1) Reine intelligente Videoüberwachung: grundrechtsschonende Architektur	152
(2) Reine intelligente Überwachung mit Identifizierung	152
(3) Kombination mit herkömmlicher Technik als tieferer Eingriff ..	153
(4) Fazit: nur hybride Architekturen als schwierige Gemengelage ..	153
ee) Vorschlag eines „Drei-Stufen-Modells“	154
(1) Darstellung	154
(2) Kritik	155
IV. Zusammenfassung: von der Ideengeschichte zum differenzierten Ergebnis	155
F. Gleichheitsgrundrechte und algorithmische Differenzierung	157
I. Systemimmanente Differenzierungen	157
II. Intelligente Videoüberwachung und die Dogmatik des Art. 3 GG	159
1. Strukturelle Verortung der Ungleichbehandlung und Anwendung von Art. 3 GG	161
2. Inhaltlicher Maßstab des Art. 3 GG	162
III. Ungleichbehandlung von Männern?	164
1. Aggressive Körpersprache als Ziele der Verhaltensanalyse	164
2. Biometrische Detektion von Männern	167
a) Striktes Anknüpfungsverbot	167
b) Geschlecht als verbotene Begründung	168
c) Gleichstellungsgebot	169
IV. Benachteiligte Menschen mit Behinderung?	169
1. Mittelbare Diskriminierung nach der Verfassungsrechtsprechung	170
2. Mittelbare Diskriminierung jenseits von Statistik?	171
3. Ungleichbehandlung von besonderem Gewicht?	172
4. Dogmatische Folgerungen	173
V. Detektion von dunkelhäutigen Zielpersonen	173
VI. Fazit: zwischen Relevanz und Relativität	175
G. Zulässigkeit und Legitimation des neuen Instruments	176
I. Zulässigkeit <i>de lege lata</i>	176
1. Verfassungsrechtliche Anforderungen an Rechtsgrundlagen	177
a) Vorbehalt des Gesetzes als Ausgangspunkt	177

aa) Allgemeiner Gesetzesvorbehalt	178
bb) Grundrechtliche Gesetzesvorbehalte	179
cc) Parlamentsvorbehalt	179
dd) Verhältnis von allgemeinem Vorbehalt des Gesetzes und grundrechtlichen Gesetzesvorbehalten	180
b) Bestimmtheitsgebot als verwandter Maßstab	182
c) Automatisierte Auswertung als das Wesentliche	183
2. Auslegung der Rechtsgrundlagen	184
a) Zur Auswertung der Bilder schweigender Wortlaut	185
b) Folgerung aus der Systematik	185
c) Genese: zwischen technischer Entwicklungsoffenheit und instrumenteller Begrenzung	186
d) Teleologie: Maßnahmzweck und Normzweck	187
e) Zwischenergebnis: automatisierte Auswertung nicht normgedeckt	188
II. Demokratische Legitimation der Algorithmen	188
1. Algorithmenkonfiguration als Legitimationsobjekt	188
2. Dogmatik der demokratischen Legitimation	190
a) Drei klassische Modelle	190
b) Niveau- statt Modellentscheidung	192
c) Demokratische Legitimation von Referenzmaßnahmen	194
aa) Verwaltungsvorschriften als formale Referenz	194
bb) Rasterfahndung als materiale Orientierungshilfe	195
(1) Präventive Rasterfahndung nach den Polizeigesetzen der Länder	195
(2) Repressive Rasterfahndung gemäß der Strafprozessordnung	197
(3) Vergleichende Auswertung	198
3. Folgerungen für das Legitimationsniveau	199
III. Zulässigkeit <i>de lege ferenda</i>	201
1. Vorschlag zu Art. 32 PAG	202
a) Gesetzestext	202
b) Erläuterungen	203
aa) Abs. 1	203
bb) Abs. 2	203
cc) Abs. 3	204
dd) Abs. 4	204
2. Vorschlag zu Art. 36 PAG	204
a) Gesetzestext	204
b) Erläuterungen	205

H. Konsistenz der Ergebnisse vor der EMRK	207
I. Relevanz der EMRK und deren Art. 8	207
II. Die Entscheidung Köpke gegen Deutschland	209
III. Die Entscheidung Peck gegen Vereinigtes Königreich	211
IV. Die Entscheidungen zum Art. 10-Gesetz	212
V. Fazit: EMRK veranlasst keine anderen Auslegungsergebnisse	214
I. Wesentliche Ergebnisse dieser Arbeit in Thesen	216
I. Einführung	216
II. Einfache Videoüberwachung im Spiegel von Rechtswissenschaft und -praxis	216
III. <i>Smart CCTV</i> als wesentlicher Entwicklungssprung	216
IV. Intelligente Überwachung und Menschenwürde	217
V. Zentraler Maßstab: das Recht auf informationelle Selbstbestimmung	217
VI. Gleichheitsgrundrechte und algorithmische Differenzierung	218
VII. Zulässigkeit und Legitimation des neuen Instruments	219
VIII. Konsistenz der Ergebnisse vor der EMRK	219
Literaturverzeichnis	220
Sach- und Personenverzeichnis	246