

Inhaltsverzeichnis

Abkürzungsverzeichnis	19
Einleitung	23
A. Problemaufriss	23
B. Untersuchungsgegenstand und Methode	25
C. Gang der Untersuchung	26
Teil 1: Das menschliche Gesicht	28
A. Die Einzigartigkeit des menschlichen Gesichts	28
B. Das Gesicht als Schlüssel zur Persönlichkeit	29
I. Unmittelbare Erkenntnisse	32
II. Mittelbare Erkenntnisse	32
III. Das Gesicht als Zuordnungsmerkmal	32
C. Das menschliche Gesicht als technisches Erkennungsmerkmal	34
I. Identifikation	34
II. Verifikation	35
III. Klassifizierung	36
IV. Gesichtsdetektion	37
D. Das private Interesse am menschlichen Gesicht	37
I. Gesichtserkennung von Kunden	38
1. Identitätskontrolle	38
2. Individuelle Verhaltensbeobachtung	39
II. Gesichtserkennung von Mitarbeitern	42
III. Gesichtserkennung von Dritten	43
Teil 2: Die technische Funktionsweise der Gesichtserkennung	45
A. Maschinelles Lernen als Basistechnologie der Gesichtserkennung	45
I. Funktionsweise des maschinellen Lernens	47
II. Deep Learning	48
III. Convolutional Neural Networks	54
IV. Die Bedeutung der Daten	55
1. Datensammlung	56

2. Datenqualität	57
3. Aufbereitung der Daten	58
B. Funktionsweise des Gesichtserkennungsverfahrens	59
I. Gesichtsdetektion	59
II. Erkennung besonderer Merkmale und neutrale Ausrichtung	60
III. Vermessung des Gesichts	60
IV. Gesichtserkennung	61
C. Funktionsweise der unterschiedlichen Gesichtserkennungssysteme	62
I. Identifikation	62
1. Erstellen eines Referenzdatensatzes	62
2. Erstellen eines Templates des neuen Bildes	63
3. Abgleich des neuen Bildes mit dem Datensatz	63
4. Anzeige des Ergebnisses	64
II. Verifikation	64
III. Klassifikation	64
D. IT-Sicherheit des Gesichtserkennungssystems	65
I. Sicherheit während des Entwicklungsprozesses	66
II. Sicherheit der Softwareanwendung	67
E. Gefahren durch weitere Einsatzmöglichkeiten	69
Teil 3: Ethische Analyse des Rechts als Bewertungsmaßstab	71
A. Ethische Analyse als Untersuchungsmethode	71
B. Begriff der Autonomie	71
1. Grundlagen des Autonomiebegriffs	72
2. Der Autonomiebegriff nach Beate Rössler	74
a) Autonomie und die „richtige“ Wahl	75
b) Der Umgang mit dem Unterbewusstsein	77
c) Autonomie in gesellschaftlichen Strukturen	78
II. Bedeutung der Autonomie	79
C. Eignung des ethischen Bewertungsmaßstabs für die Untersuchung	81
Teil 4: Beeinträchtigung der Autonomie durch biometrische Gesichtserkennung	83
A. Autonomie und Privatsphäre	83

B. Maßgebliche Beurteilungskriterien für die Beeinträchtigung der Autonomie	85
I. Anlass, Streubreite und Chilling Effects	86
1. Anlass	86
2. Streubreite und Umfang der Datenverarbeitung	87
3. Einschüchterungseffekte	88
a) Potentieller Einsatz	88
b) Chilling Effects	89
II. Kenntnis vs. Heimlichkeit	91
III. Vertraulichkeitserwartung	93
IV. Persönlichkeitsrelevanz	94
V. Verknüpfung und Folgeeingriffe	95
VI. Zuverlässigkeit des Ergebnisses	99
VII. Ausweichmöglichkeiten und Rechtsschutz	99
C. Beurteilung des konkreten Einsatzszenarios	100
I. Beeinträchtigung der Autonomie im Identifikationsverfahren	100
1. Referenzdatenbank	101
2. Datenabgleich mit der Referenzdatenbank	102
II. Beeinträchtigung der Autonomie im Verifikationsverfahren	105
III. Beeinträchtigung der Autonomie im Klassifikationsverfahren	106
IV. Zwischenergebnis	106
Teil 5: Rechtliche Analyse und Bewertung der biometrischen Gesichtserkennung am Bewertungsmaßstab des ethischen Begriffs der Autonomie	108
A. Die einfachgesetzliche Dimension des biometrischen Identifikationsverfahrens	109
I. Erstellen des Referenzdatums und Speichern in der Referenzdatenbank	109
1. DSGVO	109
a) Verantwortlicher der Datenverarbeitung	110
aa) Verantwortlicher nach Art. 4 Nr. 7 DSGVO	110
bb) (Gemeinsam) Verantwortliche	111
cc) Auftragsverarbeiter nach Art. 4 Nr. 8 DSGVO	114
dd) Zwischenergebnis	115
b) Territorialer Anwendungsbereich	116
aa) Niederlassungsprinzip, Art. 3 Abs. 1 DSGVO	116

bb) Marktortprinzip, Art. 3 Abs. 2 DSGVO	116
(1) Marktangebot, Art. 3 Abs. 2 lit. a DSGVO	117
(2) Verhaltensbeobachtung, Art. 3 Abs. 2 lit. b DSGVO	117
c) Sachlicher Anwendungsbereich	119
aa) Personenbezogenes Datum nach Art. 4 Nr. 1 DSGVO	120
(1) Bildaufnahme als Rohdatum	120
(a) Information	121
(b) Identifizierbarkeit	122
(c) Aufnahmen, die der Qualitätsprüfung nicht standhalten	124
(d) Zwischenergebnis	125
(2) Referenzdatum	125
bb) Biometrisches Datum nach Art. 4 Nr. 14 DSGVO	126
(1) Rohdatum	129
(2) Referenzdatum	129
cc) Datenschutzrechtliche Verarbeitung	130
dd) Ausnahmen nach Art. 2 Abs. 2 DSGVO	133
(1) Kein Anwendungsbereich des Unionsrechts, Art. 2 Abs. 2 lit. a DSGVO	133
(2) Gemeinsame Außen- und Sicherheitspolitik, Art. 2 Abs. 2 lit. b DSGVO	134
(3) Haushaltsausnahme, Art. 2 Abs. 2 lit. c DSGVO	134
(a) Zunehmende Datenverarbeitung durch Private	135
(b) Zugriffe Dritter auf die Daten	137
(c) Durchführung durch Auftragsverarbeiter	138
(d) Bedeutung für die Autonomie	138
(4) Strafverfolgung und Gefahrenabwehr, Art. 2 Abs. 2 lit. d DSGVO	139
d) Kein Verarbeitungsverbot nach Art. 9 Abs. 1 DSGVO	139
aa) Verhältnis von Art. 9 zu Art. 6 DSGVO	141
bb) Ausdrückliche Einwilligung der betroffenen Person	142
(1) Autonomie als Grundvoraussetzung der Einwilligung	142
(2) Einwilligung in der direkten Beziehung	144
(3) Einwilligung im Dreiecksverhältnis	149

cc) Arbeits- oder sozialrechtlicher Bezug	152
dd) Schutz lebenswichtiger Interessen	154
ee) Offenkundig öffentlich gemachte Daten	155
ff) Durchsetzung von Rechtsansprüchen	157
gg) Erhebliches öffentliches Interesse	159
(1) Anwendungsbereich des § 22 Abs. 1 Nr. 1 lit. d BDSG	159
(2) Erhebliches öffentliches Interesse	160
(3) Wahrung des Bestimmtheitsgrundsatzes	162
(4) Weitere Anforderungen an eine Umsetzungsnorm: insbesondere Wahrung des Verhältnismäßigkeitsgrundsatzes	163
(a) Erforderlichkeit	163
(i.) Identifikation vs. Verifikation	164
(ii.) Umfassende vs. individuelle Referenzdatenbank	165
(b) Bedeutung der Art. 8, 7 GRCh und Art. 8 EMRK	165
(i.) Art. 8 GRCh	166
(ii.) Art. 7 GRCh	167
(iii.) Art. 8 EMRK	168
(iv.) Bedeutung für das Generieren eines Templates und dessen Speicherung in einer Datenbank	169
(c) Wahrung des Wesensgehalts des Datenschutzes	172
(d) Maßnahmen zur Wahrung der Grundrechte und Interessen	173
(5) Zwischenergebnis	178
hh) Zwischenergebnis	178
e) Verarbeitungsgrund nach Art. 6 DSGVO	179
aa) Bedeutung im Hinblick auf Art. 9 DSGVO	180
bb) Überwiegendes Interesse nach Art. 6 Abs. 1 lit. f DSGVO	180
(1) Berechtigtes Interesse des für die Datenbank Verantwortlichen	181
(2) Erforderlichkeit	182
(3) Interessenabwägung	183
cc) Zweckänderung nach Art. 6 Abs. 4 DSGVO	184
(1) Zweckvereinbarkeit	185

(2) Einwilligung in die Zweckänderung	187
(3) Rechtsvorschrift der Union oder eines Mitgliedsstaats	188
dd) Zwischenergebnis	190
f) Wahrung der Autonomie durch Ausübung der Betroffenenrechte	190
aa) Kenntnis der betroffenen Person	191
(1) Informationspflicht des Verantwortlichen	192
(2) Auskunftsrecht des Betroffenen	194
bb) Abwehr der Datenverarbeitung	195
(1) Widerspruchsrecht	195
(2) Recht auf Löschung	196
cc) Zwischenergebnis	199
g) Pflichten des Verantwortlichen	200
aa) Autonomie durch Technikgestaltung und Voreinstellung	200
bb) Datensicherheit	201
cc) Weitere Pflichten	204
dd) Zwischenergebnis	205
h) Schutz der Autonomie durch die Aufsichtsbehörden	205
i) Zwischenergebnis	207
2. BDSG	208
3. KUG	209
a) Das Verhältnis zwischen KUG und BDSG a.F.	210
b) Das Verhältnis zwischen KUG und DSGVO	211
aa) Konformität von KUG und DSGVO	213
bb) Anwendungsvorrang der §§ 22, 23 KUG	213
cc) Anwendungsvorrang der DSGVO	213
(1) Anpassungsauftrag nach Art. 85 Abs. 1 DSGVO	214
(2) Art. 85 Abs. 2 DSGVO als taugliche Öffnungsklausel	215
dd) Orientierung am verfolgten Schutzzweck	217
c) Zwischenergebnis	219
4. § 1004 Abs. 1 BGB analog i. V. m. dem allgemeinen Persönlichkeitsrecht	219
a) Anspruch auf Beseitigung	220
aa) Recht auf informationelle Selbstbestimmung	220

bb) Recht auf Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen	222
cc) Recht am eigenen Bild	222
dd) Allgemeines Persönlichkeitsrecht	224
b) Anspruch auf Unterlassung	224
c) Zwischenergebnis	227
5. Nutzungsbedingungen sozialer Netzwerke	227
a) Unmittelbarer Schutz	228
b) Mittelbarer Schutz	230
c) Zwischenergebnis	231
6. Zwischenergebnis	231
II. Einsatz des Identifikationssystems	231
1. Nichtstaatliche Videoüberwachung	232
a) Anwendbarkeit des BDSG	232
b) Anwendbarkeit der DSGVO	233
2. Erstellen des Templates und Abgleich mit der Referenzdatenbank nach der DSGVO	234
a) Verantwortlicher der Datenverarbeitung	234
aa) Verantwortlicher nach Art. 4 Nr. 7 DSGVO	234
bb) (Gemeinsam) Verantwortliche	235
cc) Auftragsverarbeiter nach Art. 4 Nr. 8 DSGVO	236
b) Territorialer Anwendungsbereich	236
c) Sachlicher Anwendungsbereich	236
aa) Personenbezogene Daten nach Art. 4 Nr. 1 DSGVO	237
bb) Template als biometrisches Datum nach Art. 4 Nr. 14 DSGVO	237
cc) Datenschutzrechtlich relevante Handlung	237
dd) Haushaltsausnahme, Art. 2 Abs. 2 lit. c DSGVO	238
d) Kein Verarbeitungsverbot nach Art. 9 Abs. 1 DSGVO	239
aa) Ausdrückliche Einwilligung	239
bb) Arbeits- oder sozialrechtlicher Bezug	240
cc) Schutz lebenswichtiger Interessen	241
dd) Offenkundig öffentlich gemachte Daten	242
ee) Durchsetzung von Rechtsansprüchen	242
ff) Erhebliches öffentliches Interesse	243
(1) Erforderlichkeit	244

(2) Angemessenheit	244
(a) Datenverarbeitung und positives Ergebnis	245
(b) Datenerfassung und negatives Ergebnis	245
(3) Zwischenergebnis	249
gg) Zwischenergebnis	249
e) Automatisierte Entscheidungsfindung	250
aa) Entscheidungsfindung	251
bb) Einsatz des Identifikationssystems als automatisierte Entscheidung	252
cc) Zwischenergebnis	254
f) Verarbeitungsgrund nach Art. 6 Abs. 1 DSGVO	254
g) Wahrung der Autonomie durch Ausübung der Betroffenenrechte	254
aa) Kenntnis der betroffenen Person	255
(1) Informationspflicht des Verantwortlichen	255
(2) Auskunftsrecht des Betroffenen	256
bb) Abwehr der Datenverarbeitung	257
(1) Widerspruchsrecht	257
(2) Recht auf Löschung	258
cc) Zwischenergebnis	259
h) Pflichten des Verantwortlichen	259
aa) Autonomie durch Technikgestaltung und Voreinstellung	259
bb) Datensicherheit	261
cc) Weitere Pflichten	261
dd) Zwischenergebnis	262
i) Schutz der Autonomie durch die Aufsichtsbehörden	262
j) Zwischenergebnis	263
III. Ergebnis	263
B. Die einfachgesetzliche Dimension des biometrischen Klassifikationsverfahrens	263
I. Sachlicher Anwendungsbereich der DSGVO	264
1. Verarbeitung personenbezogener Daten nach Art. 4 Nr. 1 DSGVO	264
2. Anonymisierung personenbezogener Daten	266
a) Anonyme Daten nach der DSGVO	266
b) Umsetzung der Anonymisierung	267
c) Anonymisierungsvorgang als datenschutzrechtlich relevante Verarbeitung	268

3. Ausschließliche Verarbeitung anonymer Daten	268
II. Ergebnis	270
Teil 6: Verordnungsentwurf der Europäischen Kommission zur Regulierung der Künstlichen Intelligenz	271
A. Hintergrund	271
B. Ziel des Vorschlags	272
C. Verbot bestimmter Anwendungen der Künstlichen Intelligenz	273
I. Biometrische Echtzeit-Fernidentifikationssysteme zur Straf- verfolgung	274
1. Beschränkter Anwendungsbereich	274
2. Ausnahme vom Verbot oder Erlaubnis zum Einsatz	276
3. Bedeutung für den Schutz der Autonomie	277
4. Ausweitung des Anwendungsbereichs auf nichtstaatliche Maßnahmen	278
5. Zwischenergebnis	279
II. Unterschwellige Verhaltensbeeinflussung durch KI-Systeme	279
D. Identifikationssystem als Hochrisiko-KI-System	280
I. Anforderungen an Hochrisiko-KI-Systeme	280
1. Konformitätsbewertungsverfahren	280
2. Risikomanagementsystem und Beobachtung nach dem Inverkehrbringen	281
3. Registrierung	282
4. Datenanforderungen	282
5. Technische Dokumentation und Protokollierung	282
6. Transparenz	283
7. Menschliche Aufsicht	284
8. Genauigkeit, Robustheit und Cybersicherheit	284
II. Bedeutung für den Schutz der Autonomie	285
E. Transparenzpflicht für ausgewählte KI-Systeme	286
I. Anwendungsbereich	286
II. Bedeutung für den Schutz der Autonomie	286
F. Kompromissvorschlag Slowenien vom 29. November 2021	287
G. Kompromissvorschlag Frankreich vom 13. Januar 2022	289
H. Ergebnis	289

Gesamtergebnis und Ausblick	291
A. Zusammenfassung der Ergebnisse	291
B. Gefahr für die Autonomie (?)	292
C. Rechtspolitischer Ausblick	294
Literaturverzeichnis	297