

Inhaltsverzeichnis

Abkürzungsverzeichnis	25
1 Einführung	39
1.1 Videoüberwachung und Gesichtserkennung	40
1.2 Einsatz durch die Polizei zur Verhinderung und Verfolgung von Straftaten	44
1.2.1 Straftaten	44
1.2.2 Verhinderung und Verfolgung von Straftaten durch die Polizei	45
1.3 Überwachen und Überwachungsstaat: Visionen und Dystopien	51
1.3.1 Jeremy Bentham und das Panoptikum	52
1.3.2 George Orwell und der Große Bruder	57
1.3.3 Der Weg in die Überwachungsdemokratie?	62
1.4 Recht und Überwachung: Das Bundesverfassungsgericht und das Recht auf informationelle Selbstbestimmung	64
1.5 Recht und Technik	68
1.5.1 Grundsätzlicher Gegensatz zwischen Recht und Technik?	69
1.5.2 Geeignetheit der rechtlichen Steuerungsinstrumente?	73
1.5.3 Privater und staatlicher Technikeinsatz	76
1.5.3.1 Privater Technikeinsatz	76
1.5.3.2 Staatlicher Technikeinsatz	78
1.5.4 Mangelnder Sachverstand des Gesetzgebers?	79
1.5.5 Allianz von Recht und Technik	80
1.6 Ziele der Arbeit und weitere Vorgehensweise	81
2 Technisches Instrumentarium: Videoüberwachung und biometrische Gesichtserkennung	83
2.1 Videoüberwachung	83
2.1.1 Begriff	85
2.1.2 Technik	86
2.1.2.1 Technische Komponenten eines Videoüberwachungssystems	86
	11

2.1.2.2 Möglichkeiten der Bildbearbeitung und Bildverbesserung	89
2.1.3 Einsatz von Videoüberwachung	90
2.1.3.1 Zur Geschichte der polizeilichen Videoüberwachung in Deutschland	91
2.1.3.2 Verfolgte Zwecke polizeilicher Videoüberwachung	96
2.1.3.3 Typische Einsatzsituationen polizeilicher Videoüberwachung	99
2.1.3.4 Art und Weise der Videoüberwachung	100
2.1.3.5 Ausmaß der Videoüberwachung in Deutschland	102
2.1.4 Einstellung der Politik und Bevölkerung gegenüber Videoüberwachung	107
2.1.5 Wirkung und Wirksamkeit von Videoüberwachung	109
2.1.5.1 Verfolgung von Straftaten	110
2.1.5.2 Verhinderung von Straftaten	112
2.1.5.3 Sicherheitsgefühl	115
2.1.6 „Intelligente Videoüberwachung“	116
2.1.6.1 Das Problem der Bilderflut	116
2.1.6.2 „Intelligente Videoüberwachung“ als Lösungsansatz	117
2.2 Biometrische Gesichtserkennung	119
2.2.1 Das Gesicht und die menschliche Fähigkeit zur Gesichtserkennung	119
2.2.2 Biometrische Erkennung	122
2.2.2.1 Definition biometrischer Erkennung	122
2.2.2.2 Der Ablauf biometrischer Erkennung	125
2.2.3 Die Vielfalt biometrischer Verfahren	127
2.2.3.1 Aus der Geschichte der biometrischen Erkennung	127
2.2.3.1.1 Der Fall des Martin Guerre	128
2.2.3.1.2 Personenerkennung in der Bibel	129
2.2.3.1.3 Fingerabdrücke in alten Kulturen vor Christi Geburt	130
2.2.3.1.4 Ostasien und die Fingerabdrücke	131
2.2.3.1.5 Erforschung der Fingerabdrücke durch die Europäer	132
2.2.3.1.6 Alphonse Bertillon und die anthropometrischen Messungen	134
2.2.3.1.7 Triumph der Daktyloskopie über die anthropometrischen Messungen	136
2.2.3.1.8 Bertillons Verdienste	139

2.2.3.2 Biometrische Verfahren	140
2.2.3.2.1 Finger- und Handflächenabdruckerkennung	141
2.2.3.2.2 Handgeometriekerennung	142
2.2.3.2.3 Gesichtserkennung	143
2.2.3.2.4 Iris-, Retina- und Ohrerkennung	145
2.2.3.2.5 Stimm-, Unterschriften-, Tastenanschlag- und Geruchserkennung	147
2.2.3.2.6 Gangerkennung	148
2.2.3.2.7 DNS-Erkennung	148
2.2.3.2.8 Weitere Verfahren	150
2.2.3.3 Softbiometrie	150
2.2.4 Biometrische Gesichtserkennung: Technische Aspekte, Stärken und Schwächen	154
2.2.4.1 Ablauf biometrischer Gesichtserkennung	154
2.2.4.2 Vorteile und Herausforderungen biometrischer Gesichtserkennung	157
2.2.4.2.1 Vorteile biometrischer Gesichtserkennung	157
2.2.4.2.2 Herausforderungen biometrischer Gesichtserkennung und Lösungsansätze	160
2.2.4.2.2.1 Unterschiedliche Bildformate	160
2.2.4.2.2.2 Rechenleistung	160
2.2.4.2.2.3 Vermeintliche Einzigartigkeit und Veränderung durch Alterung	161
2.2.4.2.2.4 Beleuchtung, Aufnahmewinkel, Pose und eingesetzte Technik	163
2.2.4.2.2.5 Umgehung	165
2.2.4.2.2.6 Multibiometrie zur Stärkung der Robustheit der Erkennung	166
2.2.4.2.2.7 Menschliche Kontrolle	169
2.2.4.2.2.8 Angriffe auf das Erkennungssystem	169
2.2.4.2.2.9 Bewusstsein für Grenzen biometrischer Erkennung	170
2.2.4.3 Leistungsfähigkeit und Testreihen	171
2.2.4.3.1 Fehlerraten	171
2.2.4.3.2 Testreihen	174
2.2.5 Einsatzmöglichkeiten biometrischer (Gesichts-)Erkennung	177
2.2.5.1 Zugangssicherung	178
2.2.5.2 Private Anwendungsbereiche	181
2.2.5.2.1 Handels-, Dienstleistungs- und Bankgeschäfte	181

2.2.5.2.2 Zeiterfassung und Anwesenheitskontrolle in Unternehmen	183
2.2.5.2.3 Freizeit- und Unterhaltungsbereich	183
2.2.5.3 Staatliche Anwendungsbereiche	184
2.2.5.3.1 Grenzkontrolle	184
2.2.5.3.2 Doppelbezüge staatlicher Leistungen	186
2.2.5.3.3 Einsatz zur Bekämpfung von Straftaten	187
3 Konkrete Szenarien für den polizeilichen Einsatz von Gesichtserkennung mit Videoüberwachung	189
3.1 Szenario 1: Kontinuierliche Personenfahndung im öffentlichen Raum	190
3.1.1 Beschreibung	190
3.1.2 Pilotprojekte und Anwendungsbeispiele	193
3.1.2.1 Hauptbahnhof Mainz	193
3.1.2.2 Bahnhof Berlin Südkreuz	195
3.1.2.3 Super Bowl 2001	198
3.1.3 Parallele zur automatisierten Kfz-Kennzeichenerkennung	199
3.2 Szenario 2: Anlassbezogene Suche in Lichtbilddatenbanken	201
3.2.1 Beschreibung	202
3.2.2 Anwendung beim Bundeskriminalamt	205
3.2.3 Parallele zum AFIS	208
3.3 Szenario 3: Hilfsmittel zur Sichtung von Videoaufzeichnungen	209
3.3.1 Beschreibung	209
3.3.1.1 Personendetektion	210
3.3.1.2 Wiedererkennung einer Person in Videoaufzeichnungen	211
3.3.1.3 Suche mit Lichtbild in Videoaufzeichnungen	212
3.3.2 Anwendungsbeispiele	213
3.3.2.1 Anschlag auf den Boston Marathon	213
3.3.2.2 G20-Gipfel Soko „Schwarzer Block“	214
3.4 Szenario 4: Einsatz von Softbiometrie	216
4 Regelungsregime: Deutsches und europäisches Recht	219
4.1 Deutsches Recht	220
4.2 Europäische Menschenrechtskonvention	220
4.2.1 Entwicklung und Gewährleistungen	221

4.2.2 Stellung und Bedeutung in der deutschen Rechtsordnung	224
4.3 Recht der Europäischen Union	228
4.3.1 Die Europäische Union	229
4.3.1.1 Entstehung und Entwicklung	229
4.3.1.2 Verhältnis des Unionsrechts zum nationalen (deutschen) Recht	232
4.3.1.3 Verhältnis des Unionsrechts zur Europäischen Menschenrechtskonvention	234
4.3.2 Anwendbare Vorschriften des Unionsrechts	236
4.3.2.1 Der Raum der Freiheit, der Sicherheit und des Rechts	237
4.3.2.2 JI-Richtlinie	240
4.3.2.2.1 Anwendbarkeit auch auf die innerstaatliche polizeiliche Datenverarbeitung	241
4.3.2.2.2 Kompetenzmäßigkeit der JI-Richtlinie	242
4.3.2.2.2.1 Reichweite von Art. 16 Abs. 2 AEUV	243
4.3.2.2.2.2 JI-Richtlinie im Rahmen der Kompetenz des Art. 16 Abs. 2 AEUV	249
4.3.2.2.2.3 Subsidiarität und kompetenzrechtliche Verhältnismäßigkeit	250
4.3.2.2.3 Fazit: Anwendbarkeit und Kompetenzmäßigkeit der JI-Richtlinie	253
4.3.2.3 Grundrechtecharta	253
4.3.2.3.1 Grundrechte in der Europäischen Union	254
4.3.2.3.2 Anwendungsbereich der Grundrechtecharta	255
4.3.2.3.2.1 Bindung der Europäischen Union	255
4.3.2.3.2.2 Bindung der Mitgliedstaaten	256
4.3.2.3.2.2.1 Mitgliedstaaten	256
4.3.2.3.2.2.2 Recht der Union	256
4.3.2.3.2.2.3 Durchführung des Rechts der Union	257
4.3.2.3.3 Verhältnis der Grundrechte der Grundrechtecharta zu den nationalen Grundrechten	265
4.3.2.3.4 Überdies: Berücksichtigung der Grundrechtecharta bei der Auslegung	270
4.3.2.3.5 Fazit: Beachtung der deutschen Grundrechte und der Grundrechtecharta	271
4.4 Sonstiges Völkerrecht	271
4.5 Fazit: Anwendbarkeit des deutschen und des europäischen Rechts	274

5	Rechtliche Bewertung des Einsatzes von Gesichtserkennung mit Videoüberwachung	275
5.1	Polizeiliche Tätigkeit im Spannungsverhältnis zwischen Aufgabenerfüllung und Grundrechtsschutz	275
5.1.1	Bedeutung der Verhinderung und Verfolgung von Straftaten	276
5.1.2	Bedeutung der Grundrechte	278
5.1.2.1	Grundrechte als Abwehrrechte	279
5.1.2.2	Schutzpflichten	280
5.1.2.3	Grundrecht auf Sicherheit?	281
5.1.2.4	Freiheits- und Gleichheitsrechte	282
5.2	Vereinbarkeit mit den Freiheitsrechten	283
5.2.1	Grundrechtseingriffe	284
5.2.1.1	Deutsche Grundrechte	285
5.2.1.1.1	Grundrecht auf informationelle Selbstbestimmung	285
5.2.1.1.1.1	Herleitung und Begründung	286
5.2.1.1.1.2	Schutzbereich	291
5.2.1.1.1.2.1	Personenbezug von Bild- und Videodaten	292
5.2.1.1.1.2.2	Schutzbereichseröffnung durch Einschüchterung und Überwachungsdruck?	300
5.2.1.1.1.2.3	Personenbezug biometrischer Daten	302
5.2.1.1.1.3	Eingriff	305
5.2.1.1.1.3.1	Eingriff durch Videoüberwachung	306
5.2.1.1.1.3.1.1	Kamera-Monitor-Verfahren	307
5.2.1.1.1.3.1.2	Aufzeichnung	310
5.2.1.1.1.3.2	Eingriff durch Gesichtserkennung	312
5.2.1.1.1.3.2.1	Bereitstellung der Referenzdaten	312
5.2.1.1.1.3.2.2	Abgleich der Gesichtsaufnahmen	313
5.2.1.1.1.3.2.3	Templateerstellung	314
5.2.1.1.1.3.3	Eingriff durch Softbiometrie	315
5.2.1.1.1.3.4	Entfallen des Eingriffs	316
5.2.1.1.1.3.4.1	Einwilligung	316
5.2.1.1.1.3.4.2	Ungezielte Erfassung und sofortige Löschung	320
5.2.1.1.2	Menschenwürde und ihre Ausprägungen	325
5.2.1.1.2.1	Vom Wesen der Menschenwürde	325
5.2.1.1.2.2	Beobachtung und Zugriff auf den menschlichen Körper	328
5.2.1.1.2.3	Registrierung und Katalogisierung	332

5.2.1.1.2.4 Kernbereich privater Lebensgestaltung	335
5.2.1.1.2.5 Nemo-tenetur-Prinzip	339
5.2.1.1.3 Weitere Grundrechte	344
5.2.1.1.3.1 Weitere Ausprägungen des allgemeinen Persönlichkeitsrechts	344
5.2.1.1.3.2 Versammlungsfreiheit	347
5.2.1.1.3.3 Unverletzlichkeit der Wohnung	350
5.2.1.1.3.4 Freizügigkeit und Fortbewegungsfreiheit	352
5.2.1.2 Europäische Menschenrechtskonvention	355
5.2.1.2.1 Achtung des Privatlebens und der Wohnung	355
5.2.1.2.1.1 Schutzbereich	356
5.2.1.2.1.1.1 Privatleben	357
5.2.1.2.1.1.2 Wohnung	358
5.2.1.2.1.2 Eingriff	359
5.2.1.2.1.2.1 Privatleben	359
5.2.1.2.1.2.1.1 Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte	359
5.2.1.2.1.2.1.2 Eingriff durch Videoüberwachung	362
5.2.1.2.1.2.1.3 Eingriff durch Gesichtserkennung	363
5.2.1.2.1.2.2 Wohnung	365
5.2.1.2.2 Menschenwürde	366
5.2.1.2.3 Weitere Grundrechte	368
5.2.1.2.3.1 Versammlungsfreiheit	368
5.2.1.2.3.2 Freizügigkeit und Freiheit der Person	369
5.2.1.2.3.3 Nemo-tenetur-Prinzip	370
5.2.1.3 Europäische Grundrechtecharta	371
5.2.1.3.1 Grundrecht auf Schutz personenbezogener Daten	371
5.2.1.3.1.1 Wesen sowie Verhältnis zu Art. 16 AEUV und Art. 8 EMRK	372
5.2.1.3.1.2 Schutzbereich	374
5.2.1.3.1.3 Eingriff	377
5.2.1.3.2 Menschenwürde	378
5.2.1.3.3 Weitere Grundrechte	380
5.2.1.3.3.1 Achtung des Privatlebens und der Wohnung	380
5.2.1.3.3.2 Versammlungsfreiheit	384
5.2.1.3.3.3 Freizügigkeit und Freiheit der Person	385
5.2.1.3.3.4 Nemo-tenetur-Prinzip	386
5.2.1.4 Fazit: Eingriff in deutsche und europäische Grundrechte	386

5.2.2 Rechtfertigung der Grundrechtseingriffe	387
5.2.2.1 Der Gesetzesvorbehalt und das Erfordernis einer gesetzlichen Grundlage	387
5.2.2.1.1 Deutschland	387
5.2.2.1.1.1 Vorbehalt des Gesetzes und grundrechtlicher Gesetzesvorbehalt	387
5.2.2.1.1.2 Einschränkungbarkeit des Rechts auf informationelle Selbstbestimmung	393
5.2.2.1.1.3 Einschränkungbarkeit Versammlungsfreiheit und Unverletzlichkeit der Wohnung	395
5.2.2.1.2 Europäische Menschenrechtskonvention	396
5.2.2.1.3 Europäische Grundrechtecharta	398
5.2.2.1.3.1 Verhältnis von Art. 52 Abs. 1 GRCh zu Art. 8 Abs. 2 GRCh	399
5.2.2.1.3.2 Bedeutung von Art. 52 Abs. 2 GRCh mit Blick auf Art. 16 AEUV	401
5.2.2.1.3.3 Bedeutung von Art. 52 Abs. 3 GRCh	403
5.2.2.2 Mögliche gesetzliche Rechtsgrundlagen	404
5.2.2.2.1 Einsatz von Videoüberwachung	405
5.2.2.2.1.1 Datenschutzgesetze des Bundes und der Länder	406
5.2.2.2.1.2 Regelungen des Bundes in den Polizeigesetzen, dem Versammlungsgesetz und der Strafprozessordnung	407
5.2.2.2.1.3 Regelungen der Länder in den Polizei- und Versammlungsgesetzen	409
5.2.2.2.2 Einsatz von Gesichtserkennung und Softbiometrie	410
5.2.2.2.2.1 Ausdrückliche Regelungen	410
5.2.2.2.2.1.1 Baden-Württemberg	411
5.2.2.2.2.1.2 Bayern	411
5.2.2.2.2.1.3 Hessen	414
5.2.2.2.2.1.4 Sachsen	414
5.2.2.2.2.1.5 Schleswig-Holstein	415
5.2.2.2.2.2 Analoge Anwendung der Vorschriften zur Kennzeichenerkennung	416
5.2.2.2.2.3 Heranziehung anderer Vorschriften	416
5.2.2.2.2.3.1 Vorschriften zur Videoüberwachung	417
5.2.2.2.2.3.2 Vorschriften zur Rasterfahndung und zum Datenabgleich	422
5.2.2.2.2.3.2.1 Strafprozessuale Vorschriften	422
5.2.2.2.2.3.2.1.1 Rasterfahndung, §§ 98a, 98b StPO	422

5.2.2.2.3.2.1.2 Datenabgleich, § 98c StPO	425
5.2.2.2.3.2.2 Polizeigesetzliche Vorschriften	428
5.2.2.2.3.2.2.1 Rasterfahndung	428
5.2.2.2.3.2.2.2 Datenabgleich	429
5.2.2.2.3.3 Vorschriften zur erkennungsdienstlichen Behandlung	430
5.2.2.2.3.3.1 Strafprozessuale Vorschriften	430
5.2.2.2.3.3.2 Polizeigesetzliche Vorschriften	432
5.2.2.2.3.4 Vorschriften zur Identitätsfeststellung	432
5.2.2.2.3.4.1 Strafprozessuale Vorschriften	433
5.2.2.2.3.4.2 Polizeigesetzliche Vorschriften	435
5.2.2.2.3.5 Generalklauseln	436
5.2.2.2.3.5.1 Strafprozessuale Generalklauseln	436
5.2.2.2.3.5.1.1 Ermittlungsgeneralklauseln, §§ 161, 163 StPO	436
5.2.2.2.3.5.1.2 Datenverarbeitung für Zwecke des Strafverfahrens, § 483 StPO	438
5.2.2.2.3.5.2 Polizeigesetzliche Generalklauseln	442
5.2.2.2.3.5.3 Generalklauseln zur Verarbeitung besonderer Kategorien personenbezogener Daten	443
5.2.2.2.3 Datenspeicherung und Bereitstellung der Referenzdaten	446
5.2.2.2.4 Fazit: Kaum explizite Vorschriften zum Einsatz biometrischer Erkennung	448
5.2.2.3 Vereinbarkeit der Rechtsgrundlagen mit den grund- und verfassungsrechtlichen Anforderungen	448
5.2.2.3.1 Kompetenz- und verfahrensgemäß zustande gekommenes Gesetz	450
5.2.2.3.2 Verbot von Einzelfallgesetzen und Zitiergebot	456
5.2.2.3.2.1 Verbot des Einzelfallgesetzes	456
5.2.2.3.2.2 Zitiergebot	457
5.2.2.3.3 Wesensgehaltsgarantie	460
5.2.2.3.3.1 Deutschland	460
5.2.2.3.3.2 Europäische Menschenrechtskonvention und Grundrechtecharta	467

5.2.2.3.4 Grundsatz der Verhältnismäßigkeit und Bestimmtheitsgebot	471
5.2.2.3.4.1 Bedeutung des Eingriffsgewichts	471
5.2.2.3.4.1.1 Kriterien für das Eingriffsgewicht	472
5.2.2.3.4.1.1.1 Anlasslosigkeit, Streubreite und Einschüchterungseffekte	474
5.2.2.3.4.1.1.2 Heimlichkeit	479
5.2.2.3.4.1.1.3 Persönlichkeitsrelevanz und Vertraulichkeitserwartungen	481
5.2.2.3.4.1.1.4 Auswertung, Verknüpfung und Austausch von Informationen sowie Profilbildung	485
5.2.2.3.4.1.1.5 Folgeeingriffe und drohende Nachteile	489
5.2.2.3.4.1.1.6 Ausweichmöglichkeit	492
5.2.2.3.4.1.1.7 Verstärkung durch den zunehmenden Einsatz leistungsfähigerer Technik	493
5.2.2.3.4.1.1.8 Additive Eingriffe	496
5.2.2.3.4.1.2 Eingriffsgewicht von Gesichtserkennung in Verbindung mit Videoüberwachung	497
5.2.2.3.4.1.2.1 Konventionelle Videoüberwachung	497
5.2.2.3.4.1.2.1.1 Videoüberwachung öffentlicher Orte und Objekte	498
5.2.2.3.4.1.2.1.2 Videoüberwachung mit Fokus auf einzelne Personen	500
5.2.2.3.4.1.2.2 Gesichtserkennung und Softbiometrie	503
5.2.2.3.4.1.2.2.1 Szenario 1: Kontinuierliche Personenfahndung im öffentlichen Raum	505
5.2.2.3.4.1.2.2.2 Szenario 2: Anlassbezogene Suche in Lichtbilddatenbanken	509
5.2.2.3.4.1.2.2.3 Szenario 3: Hilfsmittel zur Sichtung von Videoaufzeichnungen	511
5.2.2.3.4.1.2.2.3.1 Personendetektion	511
5.2.2.3.4.1.2.2.3.2 Wiedererkennung einer Person in Videoaufzeichnungen	512
5.2.2.3.4.1.2.2.3.3 Suche mit Lichtbild in Videoaufzeichnungen	514
5.2.2.3.4.1.2.2.4 Szenario 4: Softbiometrie	515
5.2.2.3.4.2 Bestimmtheitsgebot	517
5.2.2.3.4.2.1 Bestimmtheitsgebot in Deutschland	517

5.2.2.3.4.2.2 Bestimmtheitsgebot in der Europäischen Menschenrechtskonvention und der Grundrechtecharta	521
5.2.2.3.4.2.3 Zusammenhang zwischen dem Bestimmtheitsgebot und dem Grundsatz der Verhältnismäßigkeit	524
5.2.2.3.4.2.4 Konventionelle Videoüberwachung	525
5.2.2.3.4.2.4.1 Videoüberwachung öffentlicher Orte und Objekte	526
5.2.2.3.4.2.4.2 Videoüberwachung mit Fokus auf einzelne Personen	530
5.2.2.3.4.2.5 Gesichtserkennung und Softbiometrie	533
5.2.2.3.4.2.5.1 Szenario 1: Kontinuierliche Personenfahndung im öffentlichen Raum	534
5.2.2.3.4.2.5.2 Szenario 2: Anlassbezogene Suche in Lichtbilddatenbanken	544
5.2.2.3.4.2.5.3 Szenario 3: Hilfsmittel zur Sichtung von Videoaufzeichnungen	548
5.2.2.3.4.2.5.4 Szenario 4: Softbiometrie	550
5.2.2.3.4.3 Grundsatz der Verhältnismäßigkeit	552
5.2.2.3.4.3.1 Verhältnismäßigkeit in Deutschland und Europa	552
5.2.2.3.4.3.2 Konvergenz der Prüfungsschritte auf deutscher und europäischer Ebene	555
5.2.2.3.4.3.3 Beurteilungsspielräume und Kontrolldichte	557
5.2.2.3.4.3.4 Verhältnismäßigkeit der Gesichtserkennung in Verbindung mit Videoüberwachung	561
5.2.2.3.4.3.4.1 Legitimer Zweck	561
5.2.2.3.4.3.4.2 Geeignetheit	563
5.2.2.3.4.3.4.2.1 Videoüberwachung	563
5.2.2.3.4.3.4.2.2 Gesichtserkennung und Softbiometrie	564
5.2.2.3.4.3.4.3 Erforderlichkeit	567
5.2.2.3.4.3.4.3.1 Videoüberwachung	568
5.2.2.3.4.3.4.3.2 Gesichtserkennung und Softbiometrie	570
5.2.2.3.4.3.4.3.3 Sicherstellung durch Subsidiaritätsklauseln	572
5.2.2.3.4.3.4.4 Angemessenheit	573

5.2.2.3.4.3.4.4.1	Vom Wesen der Angemessenheit und ihrer Prüfung	573
5.2.2.3.4.3.4.4.2	Instrumente zur Herstellung von Angemessenheit	577
5.2.2.3.4.3.4.4.2.1	Rang des Rechtsguts: Anforderungen an Rechtsgut, Verdacht und Gefahr	578
5.2.2.3.4.3.4.4.2.2	Betroffener Personenkreis	584
5.2.2.3.4.3.4.4.2.3	Steuerung des Eingriffsgewichts	586
5.2.2.3.4.3.4.4.2.4	Verfahrens- und organisationsrechtliche Vorkehrungen	587
5.2.2.3.4.3.4.4.3	Konventionelle Videoüberwachung	594
5.2.2.3.4.3.4.4.3.1	Videoüberwachung öffentlicher Orte und Objekte	594
5.2.2.3.4.3.4.4.3.2	Videoüberwachung mit Fokus auf einzelne Personen	598
5.2.2.3.4.3.4.4.3.3	(Weitere) verfahrens- und organisationsrechtliche Vorkehrungen	602
5.2.2.3.4.3.4.4.4	Gesichtserkennung und Softbiometrie	608
5.2.2.3.4.3.4.4.4.1	Szenario 1: Kontinuierliche Personenfahndung im öffentlichen Raum	608
5.2.2.3.4.3.4.4.4.2	Szenario 2: Anlassbezogene Suche in Lichtbilddatenbanken	613
5.2.2.3.4.3.4.4.4.3	Szenario 3: Hilfsmittel zur Sichtung von Videoaufzeichnungen	615
5.2.2.3.4.3.4.4.4.4	Szenario 4: Softbiometrie	617
5.2.2.3.4.3.5	Überwachungsgesamtrechnung	618
5.2.2.3.5	Fazit: Unterschiedliche Anforderungen an die Rechtfertigung	624
5.2.2.4	Verfassungskonforme Anwendung	624
5.2.2.4.1	Kernbereich privater Lebensgestaltung	626
5.2.2.4.2	Verhältnismäßigkeit	626
5.2.2.4.2.1	Legitimer Zweck	627
5.2.2.4.2.2	Geeignetheit	628
5.2.2.4.2.3	Erforderlichkeit	629

5.2.2.4.2.4 Angemessenheit	636
5.2.2.4.3 Additive beziehungsweise kumulative Eingriffe	638
5.2.2.5 Fazit: Möglichkeit der Rechtfertigung	640
5.3 Vereinbarkeit mit den Gleichheitsrechten	641
5.3.1 Gleichbehandlungsgebote im deutschen und europäischen Recht	642
5.3.1.1 Allgemeiner Gleichheitssatz	646
5.3.1.1.1 Ungleichbehandlung	646
5.3.1.1.2 Rechtfertigung	647
5.3.1.2 Besondere Gleichheitssätze	648
5.3.1.2.1 Diskriminierungsverbote	648
5.3.1.2.2 Benachteiligung „wegen“	652
5.3.1.2.3 Rechtfertigung	654
5.3.2 Ungleichbehandlung durch Videoüberwachung und biometrische Erkennung	655
5.3.2.1 Relevante Merkmale (Geschlecht, Rasse und Alter)	656
5.3.2.2 Ungleichbehandlung auf Gesetzesebene	658
5.3.2.3 Ungleichbehandlung durch die Polizei	659
5.3.2.3.1 Ungleichbehandlung	659
5.3.2.3.2 Rechtfertigung	662
5.3.2.3.3 Sonderproblem: Technische Diskriminierung	665
5.3.3 Fazit: Mögliche Ungleichbehandlung wegen Rasse, Geschlecht und Alter	666
5.4 Anforderungen der JI-Richtlinie	667
5.4.1 Umsetzungspflicht gemäß Art. 288 Abs. 3 AEUV	667
5.4.2 Anwendungsbereich der JI-Richtlinie	670
5.4.3 Vorgaben der JI-Richtlinie	674
5.4.3.1 Rechtmäßigkeit der Verarbeitung	674
5.4.3.1.1 Vorgaben des Art. 8 JI-RL	675
5.4.3.1.2 Vorgaben des Art. 10 JI-RL	675
5.4.3.1.2.1 Videoüberwachung als Verarbeitung besonderer Kategorien personenbezogener Daten	678
5.4.3.1.2.2 Gesichtserkennung als Verarbeitung besonderer Kategorien personenbezogener Daten	680
5.4.3.1.3 Umsetzung der Vorgaben in das deutsche Recht	683

5.4.3.2 Automatisierte Entscheidungsfindung im Einzelfall	690
5.4.3.2.1 Vorgaben des Art. 11 JI-RL	690
5.4.3.2.1.1 Auf automatisierter Verarbeitung beruhende Entscheidung	691
5.4.3.2.1.2 Anforderungen an Rechtsgrundlage und geeignete Garantien	694
5.4.3.2.2 Gesichtserkennung und Softbiometrie als automatisierte Entscheidungsfindung	697
5.4.3.2.3 Diskriminierendes Profiling	701
5.4.3.3 Betroffenenrechte und Pflichten des Verantwortlichen	704
5.4.3.3.1 Betroffenenrechte	706
5.4.3.3.1.1 Die verschiedenen Betroffenenrechte	706
5.4.3.3.1.2 Insbesondere Informations- und Benachrichtigungspflichten	707
5.4.3.3.2 Pflichten des Verantwortlichen	718
5.4.3.3.2.1 Datenschutz durch Technik und Voreinstellungen	719
5.4.3.3.2.2 Datensicherheit	721
5.4.3.3.2.3 Weitere Pflichten	722
5.4.3.4 Aufsicht	724
6 Zusammenfassung und Ausblick	725
Literaturverzeichnis	733