

Stephan Schindler

# Biometrische Videoüberwachung

Zur Zulässigkeit biometrischer Gesichtserkennung in Verbindung  
mit Videoüberwachung zur Bekämpfung von Straftaten



**Nomos**

Der Elektronische Rechtsverkehr

Herausgegeben von  
Prof. Dr. Alexander Roßnagel und  
Prof. Dr. Gerrit Hornung, LL.M.  
in Zusammenarbeit mit  
dem TeleTrusT Deutschland e.V.

Band 47

Stephan Schindler

# Biometrische Videoüberwachung

Zur Zulässigkeit biometrischer Gesichtserkennung in Verbindung  
mit Videoüberwachung zur Bekämpfung von Straftaten



**Nomos**

Die Arbeit ist im Zusammenhang mit folgenden BMBF-geförderten Drittmittelprojekten entstanden: Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten (MisPel), Förderkennzeichen: 13N12064; Kooperative Systemplattform für Videoupload, Bewertung, teilautomatisierte Analyse und Archivierung (PERFORMANCE), Förderkennzeichen: 13N14030; Flexibles, teilautomatisiertes Analyse-system zur Auswertung von Videomassendaten (FLORIDA), Förderkennzeichen: 13N14252.

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

Zugl.: Kassel, Univ., Diss., 2020

Fachbereich 07, Tag der Disputation: 28.08.2020

ISBN 978-3-8487-7113-4 (Print)

ISBN 978-3-7489-1160-9 (ePDF)



Onlineversion  
Nomos eLibrary

1. Auflage 2021

© Nomos Verlagsgesellschaft, Baden-Baden 2021. Gesamtverantwortung für Druck und Herstellung bei der Nomos Verlagsgesellschaft mbH & Co. KG. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

## Vorwort der Herausgeber

Der Einsatz von Videoüberwachung zu Sicherheitszwecken gehört seit vielen Jahren zu den umstrittensten Fragen sowohl der deutschen Sicherheitspolitik als auch der rechtswissenschaftlichen Diskussion zur verfassungs- und datenschutzrechtlichen Zulässigkeit neuer Überwachungstechnologien. Die Erweiterung der Videoüberwachung durch biometrische Verfahren der Gesichtserkennung verstärkt aktuell sowohl die Hoffnungen als auch die Befürchtungen, die sich mit dem Einsatz dieser Technologie verbinden. Während die einen Chancen bei der Durchforstung von Videomassendaten erkennen, die beispielsweise im Jahre 2017 nach dem G20-Gipfel in Hamburg anfielen, befürchten andere die staatliche Macht, die mit einer KI-gestützten Auswertung intern-vernetzter Datenbanken der Sicherheitsbehörden einhergehen würde. Und während die einen mit der Echtzeitkontrolle an Bahnhöfen und anderen belebten Plätzen die Möglichkeit zur Vollstreckung von Haftbefehlen und zur Verfolgung von Gefährdern verbinden, weisen andere darauf hin, dass eine kontinuierliche Identifizierbarkeit im öffentlichen Raum den Einzelnen in seinen Beziehungen, Meinungsäußerungen und sozialen Handlungen zum Objekt staatlichen Interesses mache und damit Orwell'sche Dystopien real werden lasse.

Wie unter einem Brennglas zeigt die biometrische Videoüberwachung deshalb den klassischen Konflikt zwischen Sicherheit und Freiheit. Aus rechtswissenschaftlicher Sicht wirft dies zentrale grundrechtliche Fragestellungen auf, die sich in den letzten Jahren zunehmend auf die europäische Ebene verschieben und dadurch an Komplexität gewinnen. Während die Rechtsfragen der Videoüberwachung seit vielen Jahren diskutiert werden, fehlt es bislang an einer umfassenden, auch praktische Szenarien der Sicherheitsbehörden berücksichtigenden Untersuchung der Verbindung mit biometrischer Gesichtserkennung, die auch die neuen Vorgaben der JI-Richtlinie 2016/680 einbezieht. Eine solche umfassende Analyse bietet die vorliegende Arbeit von Herrn Schindler, die ausführlich Verwendungsmöglichkeiten betrachtet, grundrechtliche Anforderungen für gesetzliche Grundlagen und den praktischen Einsatz entwickelt und datenschutzrechtliche Vorgaben konkretisiert.

Herr Schindler kombiniert einen interdisziplinären, auch technikwissenschaftlich informierten Ansatz mit einem großen Verständnis für die

praxisorientierten Anwendungsszenarien der künftigen Tätigkeit der Sicherheitsbehörden und hat in mehreren interdisziplinären Forschungsprojekten unter Mitwirkung von Polizeipraktikern an der Entwicklung und rechtlichen Bewertung derartiger Szenarien mitgewirkt. Auf der Basis einer Vielzahl von Publikationen zu direkt auf das Dissertationsthema bezogenen Fragen, aber auch zu interdisziplinären Aspekten in angrenzenden Forschungsfeldern, gelingt es ihm, auf die drängenden Fragen der verfassungs- und datenschutzrechtlichen Zulässigkeit, aber auch auf die der rechtskonformen Gestaltung der technischen Innovationen in der Polizeipraxis der Zukunft innovative und praxisgerechte Antworten zu formulieren.

Besonders hervorzuheben ist die wissenschaftliche Tiefe, in der diese Ergebnisse bearbeitet werden. Um das Ziel der grundrechtlichen Bewertung der biometrischen Videoüberwachung zu erreichen, wählt Herr Schindler methodische Zugänge, die die Klärung wichtiger, rechtsdogmatisch komplexer und vielfach ungeklärter Rechtsfragen erfordern. Dies betrifft insbesondere komplexe Fragen des Verhältnisses der einzelnen Grundrechtsebenen im europäischen Mehrebenensystem und viele Fragen der deutschen Grundrechtsdogmatik. Die Arbeit ist außerdem von einer großen Breite der Darstellung geprägt und betrachtet z.B. die einzelnen relevanten Rechtsgrundlagen in den Gesetzen der Bundesländer. In der innovativen Konkretisierung der europa- und verfassungsrechtlichen Anforderungen auf die technischen Details der biometrischen Videoüberwachung werden aktuelle gesetzgeberische Aktivitäten, jüngste Rechtsprechung und detaillierte Vorschläge zur technischen Ausgestaltung im Sinne einer Reduzierung des Eingriffsgewichts berücksichtigt.

Herrn Schindler ist es gelungen, innerhalb des Spannungsverhältnisses zwischen Sicherheit und Freiheit zentrale Fragestellungen herauszuarbeiten, diese auf eine innovative und für die polizeiliche Arbeit der Zukunft sehr wichtige Technologie zu beziehen und durchgängig zu wohlbegründeten, wissenschaftlich tief ausgearbeiteten und überzeugenden Ergebnissen zu gelangen. Indem er die biometrische Gesichtserkennung auf ihre Zulässigkeit am Maßstab europäischer und nationaler Grundrechte befragt, trägt er zur Aktualisierung der Grundrechtsdogmatik im europäischen Mehrebenensystem bei und legt wichtige Elemente ihrer Fortentwicklung offen. Indem er konkrete Aussagen zu Anforderungen an eine gesetzliche Ermächtigungsgrundlage erarbeitet, gibt er wesentliche Hinweise für die künftige Praxis einer entsprechenden Gesetzgebung. Und indem er Vorgaben des Verhältnismäßigkeitsprinzips im Rahmen der verfassungskonformen Anwendung aktueller und denkbarer künfti-

ger Rechtsgrundlagen konkretisiert, entwickelt er praxisrelevante Anforderungen und Hinweise, beispielsweise zur Erforderlichkeit in konkreten Einsatzszenarien, zur Datensicherheit und zur (im Rahmen der Polizeiarbeit aufgrund des regelmäßig bestehenden Interesses an konkreten Personen begrenzten) Möglichkeit einer datenschutzfreundlichen Technikgestaltung.

Die biometrische Videoüberwachung wird nicht die letzte innovative Kontrolltechnologie bleiben, deren Herausforderungen und grundrechtliche Zulässigkeit zu einem Zeitpunkt bewertet werden muss, in dem die Einsatzszenarien noch in der Entwicklung begriffen sind und deren Eingriffsintensität demzufolge einerseits unter bestimmten Hypothesen betrachtet, andererseits aber auch durch rechtliche und technische Schutzmaßnahmen eingehegt werden kann. Auch aus diesem Grund leistet die Arbeit einen wichtigen Beitrag für die fortdauernde Kontroverse um die Möglichkeiten, aber auch die Grenzen der sicherheitsbehördlichen Kontrolle im demokratischen Rechtsstaat.

Kassel, im Mai 2021

*Prof. Dr. Gerrit Hornung, LL.M.*



## Vorwort des Autors

Die vorliegende Arbeit ist im Zusammenhang mit den vom Bundesministerium für Bildung und Forschung geförderten Verbundprojekten Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten (MisPel), Kooperative Systemplattform für Videoupload, Bewertung, teilautomatisierte Analyse und Archivierung (PERFORMANCE) sowie Flexibles, teilautomatisiertes Analysesystem zur Auswertung von Videomassendaten (FLORIDA) entstanden. Sie wurde im Sommer 2020 von der Universität Kassel als Dissertation angenommen.

Mein besonderer Dank gilt Prof. Dr. Gerrit Hornung, LL.M. für seine geduldige Betreuung. Herzlicher Dank richtet sich zudem an Prof. Dr. Alexander Roßnagel für die zügige Erstellung des Zweitgutachtens. Überdies danke ich den einschlägig bekannten Kolleginnen und Kollegen, insbesondere auch den Bürogenossen Kai Hofmann, Thilo Goeble und Florian Emanuel, für die anregenden Diskussionen und geselligen Abende. Schließlich danke ich meinen Eltern Ulrike und Andreas Schindler, meinem Bruder Christian Schindler sowie – ganz besonders – meiner Großmutter Gertrud Schindler für ihre Unterstützung. Ihnen ist diese Arbeit gewidmet.

Kassel, im Mai 2021

*Stephan Schindler*



# 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

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 Einschränkung des Rechts auf informationelle Selbstbestimmung	393
5.2.2.1.1.3 Einschränkung 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 Gesetzesesebene	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

## Abkürzungsverzeichnis

3D	dreidimensional
a.A.	andere Auffassung
ABG	automatisierte und biometriegestützte Grenzkontrolle
AbgH-Drs.	Abgeordnetenhaus-Drucksache
ABl.	Amtsblatt der Europäischen Union
Abs.	Absatz
Abschn.	Abschnitt
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a.F.	alte Fassung
AFIS	automatisiertes Fingerabdruck-Identifizierungssystem
AG	Aktiengesellschaft / Amtsgericht
AGPaßPAuswG	Gesetz zur Ausführung des Paßgesetzes und des Personalausweisgesetzes
allg.	allgemein
Alt.	Alternative
a.M.	am Main
Anh.	Anhang
AnwBl	Anwaltsblatt (Zeitschrift)
AO	Abgabenordnung
AöR	Archiv des öffentlichen Rechts (Zeitschrift)
Apr.	April
Art.	Artikel
ASOG Bln	Allgemeines Sicherheits- und Ordnungsgesetz Berlin
ATDG	Antiterrordateigesetz
AtG	Atomgesetz

## *Abkürzungsverzeichnis*

ATM	Automated Teller Machine
Aug.	August
AuR	Arbeit und Recht (Zeitschrift)
BayDSG	Bayerisches Datenschutzgesetz
BayLTGeschO	Geschäftsordnung für den Bayerischen Landtag
BayPAG	Bayerisches Polizeiaufgabengesetz
BayPAG-E	Bayerisches Polizeiaufgabengesetz Entwurf
BayVBl	Bayerische Verwaltungsblätter (Zeitschrift)
BayVersG	Bayerisches Versammlungsgesetz
BB	Brandenburg
BbgDSG	Brandenburgisches Datenschutzgesetz
BbgPolG	Brandenburgisches Polizeigesetz
BBI	Flughafen Berlin Brandenburg International (Kürzel inzwischen verworfen)
BDK	Bund Deutscher Kriminalbeamter
BDSG	Bundesdatenschutzgesetz
BE	Berlin
bearb.	bearbeitet
BeckRS	Beck-Rechtsprechung
Begr.	Begründer
Beschl.	Beschluss
BfDI	Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBI.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen
BGHZ	Entscheidungen des Bundesgerichtshofes in Zivilsachen
BImSchV	Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes
Biol. Lett.	Biology Letter (Zeitschrift)

BAKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BlnDSG	Berliner Datenschutzgesetz
BLS	Bund-Länder-System
BMBF	Bundesministerium für Bildung und Forschung
BMELV	Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz
BMI	Bundesministerium des Inneren
BNDG	Gesetz über den Bundesnachrichtendienst
BPol	Bundespolizei
BPolG	Bundespolizeigesetz
BR-Drs	Bundesrats-Drucksache
BremDSGVOAG	Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung
BremPolG	Bremisches Polizeigesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BT-Drs.	Bundestags-Drucksache
BtMG	Betäubungsmittelgesetz
Bürg.-Drs.	Bürgerschafts-Drucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
BW	Baden-Württemberg
BY	Freistaat Bayern
bzgl.	bezüglich
bzw.	beziehungsweise
ca.	circa

## *Abkürzungsverzeichnis*

CCTV	Closed Circuit Television
CDU	Christlich Demokratische Union Deutschlands
CR	Computer und Recht (Zeitschrift)
c't	Magazin für Computertechnik (Zeitschrift)
d.	der
DANA	Datenschutznachrichten (Zeitschrift)
DGRI	Deutsche Gesellschaft für Recht und Informatik
d.h.	das heißt
DI	Digital Intermediate
DIN	Deutsches Institut für Normung
DNA	Deoxyribonucleic Acid
DNS	Desoxyribonukleinsäure
DÖV	Die Öffentliche Verwaltung (Zeitschrift)
DRiZ	Deutsche Richterzeitung (Zeitschrift)
DSAnpUG-EU	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU
DSAG LSA	Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt
DSG M-V	Datenschutzgesetz Mecklenburg-Vorpommern
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DSGVO / DS-GVO	Datenschutz-Grundverordnung (Verordnung (EU) 2016/697)
DSRL	Datenschutzrichtlinie (Richtlinie 95/46/EG)
Dtl.	Deutschland
DuD	Datenschutz und Datensicherheit, bis 1995: Daten- schutz und Datensicherung (Zeitschrift)
DVBl	Deutsches Verwaltungsblatt (Zeitschrift)
DVD	Deutsche Vereinigung für Datenschutz e.V.
DVP	Deutsche Verwaltungspraxis (Zeitschrift)
EG	Europäische Gemeinschaft
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EGKS	Europäische Gemeinschaft für Kohle und Stahl
EGMR	Europäischer Gerichtshof für Menschenrechte

EGStGB	Einführungsgesetz zum Strafgesetzbuch
EGStPO	Einführungsgesetz zur Strafprozessordnung
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
eigtl.	eigentlich
Einf.	Einführung
Einl.	Einleitung
EKMR	Europäische Kommission für Menschenrechte
EMRK	Europäische Menschenrechtskonvention
endg.	endgültig
engl.	englisch
Ent.	Entscheidung
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union (hier verwendet für den Gerichtshof im Sinne von Art. 19 Abs. 1 Satz 1 EUV)
EuGRZ	Europäische Grundrechte-Zeitschrift (Zeitschrift)
EuR	Europarecht (Zeitschrift)
EURATOM	Europäische Atomgemeinschaft
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Zeitschrift)
e.V.	eingetragener Verein
evtl.	eventuell
EwG	Erwägungsgrund
EWG	Europäische Wirtschaftsgemeinschaft
EWK	Europäischer Wirtschaftsraum
f. / ff.	folgende
FAR	False Accept Rate
FBI	Federal Bureau of Investigation
Feb.	February
FERET	Face Recognition Technology

## *Abkürzungsverzeichnis*

FIDIS	Future of Identity in the Information Society
FIVE	Face in Video Evaluation
FMR	False Match Rate
Fn.	Fußnote
FNIR	False Negative Identification Rate
FNMR	False Non-Match Rate
FPIR	False Positive Identification Rate
FpVTE	Fingerprint Vendor Technology Evaluation
FRR	False Reject Rate
FRVT	Face Recognition Vendor Test
FTCR	Failure to Capture Rate
FTER	Failure to Enrol Rate
FVC	Fingerprint Verification Competition
G8	Gruppe der Acht
G10	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses
G20	Gruppe der Zwanzig
GASP	Gemeinsame Außen- und Sicherheitspolitik
GB	Gigabyte
gen.	genannt
GG	Grundgesetz
ggf.	gegebenenfalls
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GmbH	Gesellschaft mit beschränkter Haftung
GO-BT	Geschäftsordnung des Deutschen Bundestages
GPS	Global Positioning System
gr.	griechisch
GRCh / GRC	Charta der Grundrechte der Europäischen Union
GSZ	Zeitschrift für das Gesamte Sicherheitsrecht (Zeitschrift)
GVBl.	Gesetz- und Verordnungsblatt
GVG	Gerichtsverfassungsgesetz

HB	Freie Hansestadt Bremen
HbgPolDVG	Gesetz über die Datenverarbeitung der Polizei Hamburg
HD	High Definition
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
HE	Hessen
HH	Freie und Hansestadt Hamburg
h.M.	herrschende Meinung
HmbBfDI	Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
HmbDSG	Hamburgisches Datenschutzgesetz
Hrsg.	Herausgeber
hrsg.	herausgegeben
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
i.d.R.	in der Regel
INPOL	Informationssystem der Polizei
insb.	insbesondere
IPbpR / IPBPR	Internationaler Pakt über bürgerliche und politische Rechte
i.S.d.	im Sinne der / im Sinne des
ISDN	Integrated Services Digital Network
i.S.v.	im Sinne von
IT	Informationstechnik
ITRB	IT-Rechtsberater (Zeitschrift)
i.V.m.	in Verbindung mit
iX	Magazin für professionelle Informationstechnik (Zeitschrift)
Jan.	January
JGG	Jugendgerichtsgesetz
JI-RL / JI-Richtlinie	Richtlinie (EU) 2016/680
JR	Juristische Rundschau (Zeitschrift)

## *Abkürzungsverzeichnis*

Jul.	July
Jura	Juristische Ausbildung (Zeitschrift)
JuS	Juristische Schulung (Zeitschrift)
JZ	Juristenzeitung (Zeitschrift)
K&R	Kommunikation und Recht (Zeitschrift)
Kap.	Kapitel
Kfz	Kraftfahrzeug
KG	Kammergericht
KK	Karlsruher Kommentar
Krim. Journal	Kriminologisches Journal (Zeitschrift)
KriPoZ	Kriminalpolitische Zeitschrift (Zeitschrift)
KUG	Kunsturhebergesetz
lat.	lateinisch
LDSG	Landesdatenschutzgesetz
LDSG BW	Landesdatenschutzgesetz Baden-Württemberg
LDSG RP	Landesdatenschutzgesetz Rheinland-Pfalz
LDSG SH	Landesdatenschutzgesetz Schleswig-Holstein
LDSG SH-E	Landesdatenschutzgesetz Schleswig-Holstein Entwurf
LfDI	Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
LG	Landgericht
lit.	Buchstabe
Lit.	Literatur
LKA	Landeskriminalamt
LKRZ	Zeitschrift für Landes- und Kommunalrecht Hessen - Rheinland-Pfalz - Saarland (Zeitschrift)
LKV	Landes- und Kommunalverwaltung (Zeitschrift)
LT-Drs.	Landtags-Drucksache
LVerf	Landesverfassung
LVwG SH	Landesverwaltungsgesetz Schleswig-Holstein
MADG	Gesetz über den Militärischen Abschirmdienst
Mar.	March

MHz	Megahertz
MiStra	Anordnung über Mitteilungen in Strafsachen
mm	Millimeter
MMR	Multimedia und Recht (Zeitschrift)
MschrKrim	Monatsschrift für Kriminologie und Strafrechtsreform (Zeitschrift)
MüKo-StGB	Münchener Kommentar zum Strafgesetzbuch
MüKo-StPO	Münchener Kommentar zur Strafprozessordnung
Multimed Tools Appl	Multimedia Tools and Applications (Zeitschrift)
MV	Mecklenburg-Vorpommern
m.w.N.	mit weiteren Nachweisen
n. Chr.	nach Christus
NDSG	Niedersächsisches Datenschutzgesetz
NdsVBl	Niedersächsische Verwaltungsblätter (Zeitschrift)
NI	Niedersachsen
NIST	National Institute of Standards and Technology
NJ	Neue Justiz (Zeitschrift)
NJOZ	Neue Juristische Online-Zeitschrift (Zeitschrift)
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NJW-RR	Neue Juristische Wochenschrift Rechtsprechungs-Report Zivilrecht (Zeitschrift)
NK	Neue Kriminalpolitik (Zeitschrift)
No.	number
NPOG	Niedersächsisches Polizei- und Ordnungsbehörden-gesetz
Nr.	Nummer
Nrn.	Nummern
NStZ	Neue Zeitschrift für Strafrecht (Zeitschrift)
NVersG	Niedersächsisches Versammlungsgesetz
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
NVwZ-RR	Neue Zeitschrift für Verwaltungsrecht Rechtsprechungs-Report (Zeitschrift)

## *Abkürzungsverzeichnis*

NVZ	Neue Zeitschrift für Verkehrsrecht (Zeitschrift)
NW	Nordrhein-Westfalen
NWVBl	Nordrhein-Westfälische Verwaltungsblätter (Zeitschrift)
NZA	Neue Zeitschrift für Arbeitsrecht (Zeitschrift)
o.Ä.	oder Ähnliche(s)
OECD	Organisation for Economic Co-operation and Development
ÖPNV	öffentlicher Personennahverkehr
o.g.	oben genannt
OLG	Oberlandesgericht
o.V.	ohne Verfasser
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
PAG TH	Polizeiaufgabengesetz Thüringen
PassG	Passgesetz
PassV	Passverordnung
PAuswG	Personalausweisgesetz
PIN	Persönliche Identifikationsnummer
PinG	Privacy in Germany (Zeitschrift)
PJZS	polizeiliche und justizielle Zusammenarbeit in Strafsachen
POG RP	Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz
PolG BW	Polizeigesetz Baden-Württemberg
PolG NRW	Polizeigesetz Nordrhein-Westfalen
PrOVG	Preußisches Oberverwaltungsgericht
PrOVGE	Entscheidungen des Preußischen Oberverwaltungsgerichts
PVS	Politische Vierteljahresschrift (Zeitschrift)
RABT 2006	Richtlinien für die Ausstattung und den Betrieb von Straßentunneln, Ausgabe 2006
RAF	Rote Armee Fraktion

RB	Rahmenbeschluss
RDV	Recht der Datenverarbeitung (Zeitschrift)
RG	Reichsgericht
RGSt	Entscheidungen des Reichsgerichts in Strafsachen
RGZ	Entscheidungen des Reichsgerichts in Zivilsachen
RiStBV	Richtlinien für das Strafverfahren und das Bußgeldverfahren
RL	Richtlinie
Rn.	Randnummer
RP	Rheinland-Pfalz
Rspr.	Rechtsprechung
S.	Seite
s.	siehe
s.a.	siehe auch
SächsDSDG	Sächsisches Datenschutzdurchführungsgesetz
SächsPBG	Sächsisches Polizeibehördengesetz
SächsPVDG	Sächsisches Polizeivollzugsdienstgesetz
SächsVersG	Sächsisches Versammlungsgesetz
SD	Secure Digital Memory Card
SDSG	Saarländisches Datenschutzgesetz
SEV	Sammlung der Europäischen Verträge
SGB	Sozialgesetzbuch
SH	Schleswig-Holstein
SIS	Schengener Informationssystem
SL	Saarland
SN	Freistaat Sachsen
SN-Kopf	Schwenk- und Neige-Kopf
s.o.	siehe oben
sog.	sogenannt
SOG LSA	Sicherheits- und Ordnungsgesetz Sachsen-Anhalt
SOG M-V	Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern
Soko	Sonderkommission

## *Abkürzungsverzeichnis*

SPD	Sozialdemokratische Partei Deutschlands
SPolDVG	Saarländisches Gesetz über die Verarbeitung personenbezogener Daten durch die Polizei
SPolG	Saarländisches Polizeigesetz
SRE	Speaker Recognition Evaluation
SSW	Südschleswigscher Wählerverband
ST	Sachsen-Anhalt
st.	ständig
StA	Staatsanwaltschaft
staatl.	staatlich
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StPO-E	Strafprozessordnung Entwurf
str.	strittig
StrEG	Gesetz über die Entschädigung für Strafverfolgungsmaßnahmen
StrRR	StrafRechtsReport (Zeitschrift)
StV	Der Strafverteidiger (Zeitschrift)
StVÄG	Strafverfahrensänderungsgesetz
StVO	Straßenverkehrsordnung
StVZO	Straßenverkehrs-Zulassungs-Ordnung
s.u.	siehe unten
TA Lärm	Technische Anleitung zum Schutz gegen Lärm
TA Luft	Technische Anleitung zur Reinhaltung der Luft
TB	Terabyte
TDDSG	Teledienstdatenschutzgesetz
TDM	Tausend Deutsche Mark
TeleTrusT	Bundesverband IT-Sicherheit e.V.
TH	Freistaat Thüringen
ThürDSG	Thüringer Datenschutzgesetz
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
u.	und

u.a.	unter anderem
UAbs.	Unterabsatz
UAV	Unmanned Aerial Vehicle
Urt.	Urteil
US	United States
USA	United States of America
USB	Universal Serial Bus
u.s.w.	und so weiter
u.U.	unter Umständen
v.	vom / von
v.a.	vor allem
VBIBW	Verwaltungsblätter für Baden-Württemberg (Zeitschrift)
v. Chr.	vor Christus
VerfGH	Verfassungsgerichtshof
VersammlG	Versammlungsgesetz (des Bundes)
VersammlG LSA	Versammlungsgesetz Sachsen-Anhalt
VersFG BE	Versammlungsfreiheitsgesetz Berlin
VersFG SH	Versammlungsfreiheitsgesetz Schleswig-Holstein
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
vgl.	vergleiche
VIS	Visa-Informationssystem
VO	Verordnung
Vorb.	Vorbemerkung
VR	Verwaltungsrundschau (Zeitschrift)
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
WP	Working Paper
WRV	Weimarer Reichsverfassung
ZAR	Zeitschrift für Ausländerrecht und Ausländerpolitik (Zeitschrift)
z.B.	zum Beispiel

## *Abkürzungsverzeichnis*

ZBJI	Zusammenarbeit im Bereich Justiz und Inneres
ZD	Zeitschrift für Datenschutz (Zeitschrift)
ZEuS	Zeitschrift für Europarechtliche Studien (Zeitschrift)
ZfWG	Zeitschrift für Wett- und Glücksspielrecht (Zeitschrift)
ZIS	Zeitschrift für Internationale Strafrechtsdogmatik (Zeitschrift) / Zollinformationssystem
ZJS	Zeitschrift für das Juristische Studium (Zeitschrift)
ZP	Zusatzprotokoll
ZRP	Zeitschrift für Rechtspolitik (Zeitschrift)
ZSHG	Zeugenschutz-Harmonisierungsgesetz
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft (Zeitschrift)
z.T.	zum Teil
ZWE	Zeitschrift für Wohnungseigentumsrecht (Zeitschrift)

# 1 Einführung<sup>1</sup>

„Es steht außer Frage, dass der Kampf gegen das Verbrechen und insbesondere gegen das organisierte Verbrechen und den Terrorismus, dem sich Europa heute stellen muss, weitgehend vom Einsatz moderner wissenschaftlicher Techniken der Ermittlung und Identifizierung abhängt.“<sup>2</sup> Diese Aussage stammt nicht etwa aus der Feder eines Law-and-Order-Politikers oder eines medienaffinen Polizeigewerkschafters, sondern aus einer Entscheidung des Europäischen Gerichtshofs für Menschenrechte. Doch auch von Seiten der Polizei praktiker heißt es lapidar, dass „Polizeiarbeit ohne Technikeinsatz [...] nicht mehr vorstellbar“ ist.<sup>3</sup> Da der Gesetzgeber ebenfalls erkannt hat, dass „der technische Fortschritt [...] der Polizei fortlaufend Möglichkeiten zur Optimierung ihrer Aufgabenerfüllung [eröffnet], indem er neue Technologien zur Verfügung stellt“,<sup>4</sup> fanden zahlreiche Befugnisse zum Einsatz technischer Verfahren Eingang in die Polizeigesetze von Bund und Ländern sowie die Strafprozessordnung. Dies betrifft beispielsweise die Telekommunikationsüberwachung (z.B. § 100a StPO), die Online-Durchsuchung (z.B. § 100b StPO), die akustischen Wohnraumüberwachung (z.B. § 100c StPO), die Rasterfahndung

---

1 Die vorliegende Arbeit ist im Zusammenhang mit folgenden Drittmittelprojekten entstanden: Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten (MisPel), Förderkennzeichen: 13N12064; Kooperative Systemplattform für Videoupload, Bewertung, teilautomatisierte Analyse und Archivierung (PERFORMANCE), Förderkennzeichen: 13N14030; Flexibles, teilautomatisiertes Analysesystem zur Auswertung von Videomassendaten (FLORIDA), Förderkennzeichen: 13N14252. Ergebnisse aus diesen Projekten sind in die vorliegende Arbeit eingeflossen (und umgekehrt). S. dazu die Projektberichte *Hornung/Schindler* 2015 zu MisPel u. *Hornung/Borell/Schindler/Schneider* 2019 zu FLORIDA (s.a. *Borell/Schindler*, ZD-Aktuell 2019, 06547); der Projektbericht zu PERFORMANCE stimmt hinsichtlich der hier relevanten Aspekte mit dem von FLORIDA überein und wird daher nicht gesondert aufgeführt. Einige zentrale Projektergebnisse finden sich (als Zwischenstand) zudem in *Hornung/Schindler*, ZD 2017, 203.

2 EGMR, NJOZ 2010, 696, 701 (in der engl. Fassung: „The Court finds it to be beyond dispute that the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today’s European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification.“).

3 *Bach*, Kriminallistik 1999, 657, 657.

4 LT-Drs. BY 15/2096, 12.

## 1 Einführung

(z.B. §§ 98a, 98b StPO) sowie molekulargenetische Untersuchungen (z.B. §§ 81e ff. StPO).

Auch der Umgang mit Bildaufnahmen wird als „unverzichtbar“ für die polizeiliche Arbeit angesehen.<sup>5</sup> Dementsprechend enthalten die maßgeblichen Gesetze zahlreiche Regelungen zur Anfertigung von Bild- und Videoaufnahmen. Dies gilt etwa für die erkennungsdienstliche Behandlung (z.B. § 81b StPO) sowie für verschiedene Formen der Videoüberwachung (z.B. § 100h StPO, § 14 HSOG, Art. 33 BayPAG). Aufgrund des technischen Fortschritts stehen inzwischen Verfahren zur automatisierten Auswertung der Bild- und Videoaufnahmen zur Verfügung. Zu denken ist beispielsweise an die automatisierte Kennzeichenerkennung, für deren Einsatz sowohl auf Bundes- als auch auf Landesebene Rechtsgrundlagen geschaffen wurden (z.B. § 27b BPolG, § 14a HSOG). In den letzten Jahren ist zudem der Einsatz biometrischer Gesichtserkennung in den Fokus sicherheitspolitischer und rechtswissenschaftlicher Diskussionen gerückt. Zahlreiche Polizei praktiker und Politiker erhoffen sich hiervon eine effektive Unterstützung bei der Kriminalitätsbekämpfung, wohingegen vor allem Juristen und Bürgerrechtler vor unverhältnismäßigen Grundrechtseingriffen warnen.

Vor diesem Hintergrund erläutert die vorliegende Arbeit die rechtlichen und technischen Anforderungen an den polizeilichen Einsatz von Gesichtserkennung in Verbindung mit Videoüberwachung zur Verhinderung und Verfolgung von Straftaten.

### 1.1 Videoüberwachung und Gesichtserkennung

Biometrische Gesichtserkennung benötigt Bildaufnahmen menschlicher Gesichter. Derartige Aufnahmen können in großer Zahl von bestehenden Videoüberwachungsanlagen zur Verfügung gestellt werden. Sowohl in der polizeilichen Praxis als auch in der rechtlichen Bewertung verbinden sich damit die spezifischen Herausforderungen der biometrischen Gesichtserkennung mit den bereits bestehenden Diskussionen um die Sinnhaftigkeit und die rechtliche Zulässigkeit der Videoüberwachung.

Der Einsatz von Videoüberwachung ist mit einem Sicherheitsversprechen verbunden: Videoüberwachung soll bei der Verhinderung und Verfolgung von Straftaten helfen und gleichzeitig das Sicherheitsgefühl der

---

<sup>5</sup> Bach, Kriminalistik 1999, 657, 658.

Menschen steigern.<sup>6</sup> Ob diese Ziele tatsächlich erreicht werden, ist allerdings umstritten.<sup>7</sup> Nicht zuletzt deshalb ist die Videoüberwachung aus politischer, sozialwissenschaftlicher und juristischer Sicht Gegenstand zahlreicher Auseinandersetzungen.

Dabei ist die Idee, zur Bekämpfung von Kriminalität Lichtbilder zu fertigen, nicht neu. Bereits im 19. Jahrhundert – im „Zeitalter der Erfindungen, des unaufhaltsamen Fortschritts und der elementaren Macht des Wissens“<sup>8</sup> – wurden für die aufkommende Fotografie Einsatzmöglichkeiten zur „Aufnahme der That selbst“, zur „Aufnahme von Personen zu polizeilichen Zwecken“ oder „zu Demonstrationen im Gerichtssaal“ erdacht.<sup>9</sup> Ab den 1950er Jahren kam in Deutschland Videoüberwachung zum Einsatz. Diese wurde zunächst zur Verkehrsüberwachung, später auch zur Kontrolle von Versammlungen und zur Überwachung öffentlicher Straßen und Plätze eingesetzt.<sup>10</sup>

Videoüberwachung gilt als das am häufigsten verwendete Symbol für Überwachung,<sup>11</sup> als „Ikone“<sup>12</sup> und „sichtbares Zeichen eines globalen Trends zum verstärkten Einsatz von Überwachungstechnologien“<sup>13</sup> sowie umstrittenes „Symbol einer Gesellschaft [...], in der das Erheben, Speichern und Verarbeiten von persönlichen Daten alltäglich geworden“<sup>14</sup> sei. Ihr Blick stelle sich als „entsubjektivierter Vorgang“<sup>15</sup> dar und habe „das Potenzial einer panoptischen Machtausübung, die sich dadurch auszeichnet, dass der Einzelne immer gesehen wird, während der Beobachtende ungesehen bleibt“<sup>16</sup>. In diesem Sinne entwarf der Bundesbeauftragte für den Datenschutz Ende der 1990er Jahre folgendes Szenario: „Ein völlig harmloser Zugreisender, der in einem Großstadtbahnhof nichts ahnend aus dem Zug steigt, wird durch die Kameras des bahneigenen Videosystems aufgenommen, was auch von den Beamten der nächsten Bahnpolizeiwache beobachtet werden kann. Beim Verlassen des Bahnhofs gerät der

---

6 Z.B. Simitis-Scholz, § 6b Rn. 10.

7 Zur Wirksamkeit der Videoüberwachung s. Kap. 2.1.5.

8 Paul, ZStW 1899, 1, 1.

9 Paul, ZStW 1899, 1, 9.

10 Zur Geschichte der Videoüberwachung s. Kap. 2.1.3.1.

11 *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* 2013, 49. Nach Briken 2011, 47 wurde zum „Inbegriff und Symbol der surveillance society [...] die Videokamera, nicht der Wachmann“.

12 Zurawski 2011, 10.

13 Hempel 2007a, 119.

14 Töpfer 2007, 33 f.

15 Benkel 2011, 113.

16 Schmitt Glaeser, BayVBl 2002, 584, 585.

Reisende in den Sichtbereich der Videokameras der Landespolizei, die ihn dann in der benachbarten Einkaufszone unbemerkt im Blick behält. Die Videokamera des Bankautomaten hält als nächstes sein Bild fest, und so ließe sich die Geschichte einer Beobachtung durch Videokameras fortsetzen.<sup>17</sup> Letztlich kennzeichne Videoüberwachung – so das Nachrichtenmagazin *Der Spiegel* bereits im Jahr 1983 – den Weg in den Überwachungsstaat: „Der im Bild erfaßte Mensch, sein Gesicht, seine Bewegungen und Handlungen amtlich abrufbar gespeichert – das sind Meilensteine auf dem Weg zum Überwachungsstaat.“<sup>18</sup>

Allerdings wird Videoüberwachung nicht immer derart kritisch gesehen. Nach anderer Ansicht ist Videoüberwachung nicht so sehr symbolischer Ausdruck allgegenwärtiger Überwachung, sondern vergleichbar mit der Situation, in der ein Polizeibeamter, „für jedermann an seiner Uniform erkennbar [...] Objekte und Personen wahrnimmt“.<sup>19</sup> Prinzipiell handele es sich um nichts anderes als den „Schutzmann an der Ecke“.<sup>20</sup> Kritik an der Videoüberwachung sei häufig „rein ideologisch“ geprägt.<sup>21</sup>

Insgesamt findet sich ein Meinungsspektrum, dass „von der Videoüberwachung als eine Art Allheilmittel im Kampf gegen die Kriminalität bis hin zu ihrer Verteufelung“ reicht.<sup>22</sup> In der Politik ist jedenfalls eine abwägend-zustimmende Ansicht weit verbreitet. Demnach kann „ein angemessener und zielgerichteter Einsatz von Videotechnik in Kombination mit anderen begleitenden Maßnahmen dazu beitragen [...], der staatlichen Verpflichtung zur Vermeidung und Verfolgung von Straftaten im konkreten Einzelfall nachzukommen“.<sup>23</sup> Daher überrascht es nicht, dass zahlreiche Erlaubnisnormen (z.B. Art. 33 BayPAG, § 14 HSOG, § 100h StPO, § 4 BDSG) den Einsatz von Videoüberwachung (bzw. die Anfertigung von Bildaufnahmen und -aufzeichnungen) gestatten. Von der Rechtsprechung wird der Einsatz von Videoüberwachung im Grundsatz nicht beanstan-

---

17 *Der Bundesbeauftragte für den Datenschutz* 1999, 13.

18 *Sternsdorff*, *Der Spiegel* 1983, Heft 2, 46, 48.

19 VG Halle, LKV 2000, 164, 165.

20 *Roggan*, NVwZ 2001, 134, 135, der diese Auffassung aber nicht teilt. Kritisch zu dieser Gleichsetzung auch *Kreutzträger/Osterloh* 2007, 90.

21 *Wendt* 2008, 127.

22 *Der Bundesbeauftragte für den Datenschutz* 2001, 22.

23 So z.B. die Bundesregierung im Jahr 2013, BT-Drs. 17/13071, 3. Positiv auch das bayerische Staatsministerium des Inneren, demnach Videoüberwachung „für Prävention, Fahndung und Tataufklärung ein unverzichtbares Hilfsmittel“ darstellt, welches die Sicherheitslage an kriminalitätsbelasteten Orten verbessern und das Sicherheitsgefühl der Bürger steigern kann, LT-Drs. BY 16/15571, 4; dazu s. Kap. 2.1.4.

det<sup>24</sup> und von den Bürgern (wohl) mehrheitlich<sup>25</sup> unterstützt. Und auch der Bundesbeauftragte für den Datenschutz ist der Auffassung, dass Videoüberwachung nicht „grundsätzlich von Übel“ ist, solange die rechtlichen Vorgaben und Eingrenzungen beachtet werden.<sup>26</sup>

Dementsprechend findet Videoüberwachung inzwischen eine weite Verbreitung im Alltag: Kaufhäuser, Supermärkte, Tankstellen, Parkhäuser, Geldinstitute, private Wohnanlagen, öffentliche Straßen und Plätze, Bahnhöfe und öffentliche Verkehrsmittel werden mittels Videotechnik überwacht, um Straftäter abzuschrecken, Beweise für Strafverfahren zu sichern und das Sicherheitsgefühl der Bürger zu stärken.<sup>27</sup>

Je mehr Videodaten auf diese Weise hervorgebracht werden, desto schwieriger ist es, der damit verbundenen „Bilderflut“<sup>28</sup> Herr zu werden. Die konventionelle Form der Videoüberwachung beschränkt sich darauf, Bilder – zum Beispiel die des „völlig harmlosen“ Zugreisenden<sup>29</sup> – auf einem Monitor wiederzugeben und/oder auf einem Datenträger aufzuzeichnen. Die Auswertung der Aufnahmen obliegt einem Menschen, was nicht nur Zeit, sondern auch (ununterbrochene) Aufmerksamkeit erfordert. Nicht erst seit einigen Jahren wird deshalb daran gearbeitet, Menschen bei der Auswertung durch computergestützte (teil-)automatisierte Verfahren zu unterstützen (sog. „intelligente Videoüberwachung“, „Smart Cameras“, „Thinking cameras“).<sup>30</sup> Dies betrifft beispielsweise die Verwendung automatisierter Verhaltenserkennung oder die – hier vor allem interessierende – biometrische Gesichtserkennung.

Unter biometrischer Erkennung im hier maßgeblichen Sinne ist die automatisierte Erkennung von Personen anhand von körperlichen oder verhaltensbezogenen Charakteristika zu verstehen.<sup>31</sup> Solche Charakteristika können beispielsweise die Haut- beziehungsweise Papillarleisten der Finger, die Iris oder Retina, die Stimme oder das menschliche Gesicht sein.<sup>32</sup> Biometrische Erkennung bedeutet dabei im Wesentlichen, dass zwei oder mehr Abbilder eines Charakteristikums (z.B. die Bildaufnahmen eines Ge-

---

24 Z.B. VGH Baden-Württemberg, NVwZ 2004, 498. Grundlegend aus verfassungsrechtlicher Sicht BVerfG, NVwZ 2007, 688.

25 Dazu s. Kap. 2.1.4.

26 *Der Bundesbeauftragte für den Datenschutz* 2001, 22.

27 Simitis-Scholz, § 6b Rn. 8 ff. m.w.N.

28 *Bäumler* 2000, 58.

29 S. Kap. 1.1.

30 Zur „intelligenten Videoüberwachung“ s. Kap. 2.1.6.

31 Zur Begriffsbestimmung s. Kap. 2.2.2.1.

32 Zu den verschiedenen biometrischen Verfahren s. Kap. 2.2.3.2.

sichts) automatisiert auf ihre Übereinstimmung hin überprüft werden. Automatisierte Erkennung schließt dabei ein gewisses Maß an menschlicher Mitwirkung nicht aus. Dies betrifft etwa die Überwachung des Erkennungsvorgangs sowie die Kontrolle und Interpretation der gefundenen Ergebnisse. Dabei ist immer auch die Fehleranfälligkeit der biometrischen Gesichtserkennung in Rechnung zu stellen. Ungenügende Beleuchtung, mangelhafte Kameratechnik oder ungeeignete Algorithmen können einen großen Einfluss auf die Erkennungsgenauigkeit der Gesichtserkennung haben.<sup>33</sup> Bereits aus diesem Grund sind menschliche Kontroll- und Interventionsmöglichkeiten regelmäßig unabdingbar.

Das technische Entwicklungspotential biometrischer Erkennung ist noch lange nicht ausgereizt. Einen Schub in der Entwicklung brachten die Anschläge vom 11. September 2001. Politische Forderungen nach stärkerem Einsatz biometrischer Erkennung wurden (und werden) insbesondere mit der Bekämpfung des internationalen Terrorismus begründet.<sup>34</sup> Hinzu tritt die steigende Rechenleistung moderner Computersysteme, die immer komplexere Verfahren ermöglicht. Daher ist davon auszugehen, dass die Leistungsfähigkeit und Genauigkeit der Gesichtserkennung in den nächsten Jahren und Jahrzehnten weiter steigen wird.

### 1.2 Einsatz durch die Polizei zur Verhinderung und Verfolgung von Straftaten

Gesichtserkennung und Videoüberwachung können zu unterschiedlichen Zwecken eingesetzt werden. Im Rahmen dieser Arbeit wird ihr Einsatz durch die deutsche Polizei zur Verhinderung und Verfolgung von Straftaten betrachtet.

#### 1.2.1 Straftaten

Eine Straftat „ist das vom Tatbestand des Strafgesetzes in seinen Merkmalen festgelegte, mit Strafe bedrohte rechtswidrige Verhalten, das der Täter schuldhaft verwirklicht hat“.<sup>35</sup> Derartige Straftatbestände finden sich vor

---

33 Zu den Fehlerquellen s. Kap. 2.2.4.2.2.

34 Kurz 2008, 102.

35 Jescheck/Weigend 1996, 13.

## 1.2 Einsatz durch die Polizei zur Verhinderung und Verfolgung von Straftaten

allem im Strafgesetzbuch, aber auch in zahlreichen Vorschriften des Nebenstrafrechts (z.B. §§ 29 ff. BtMG, §§ 369 ff. AO).<sup>36</sup>

Mit den Straftaten eng verwandt sind die Ordnungswidrigkeiten. Ordnungswidrigkeiten sind rechtswidrige und vorwerfbare Handlungen, die den Tatbestand eines Gesetzes verwirklichen, das die Ahndung mit einer Geldbuße zulässt (§ 1 Abs. 1 OWiG). Regelungen zu den Ordnungswidrigkeiten finden sich in dem Gesetz über Ordnungswidrigkeiten sowie in zahlreichen weiteren Normierungen, wobei insbesondere die Straßenverkehrsordnung von großer praktischer Bedeutung ist. Im Unterschied zur Straftat ist die Sanktionierung einer Ordnungswidrigkeit nicht mit einem „ethischen Schuldvorwurf“ verbunden.<sup>37</sup> Die verhängte Geldbuße kann als eine „nachdrückliche Pflichtenmahnung“ verstanden werden, die kein „ehrenrühriges, autoritatives Unwerturteil“ enthält.<sup>38</sup> Das „Fehlen jenen hohen Grades von Verwerflichkeit“ trennt die Ordnungswidrigkeit von der Straftat.<sup>39</sup>

Obwohl sich auch für den Bereich der Ordnungswidrigkeiten Anwendungsmöglichkeiten für den Einsatz von Gesichtserkennung in Verbindung mit Videoüberwachung finden lassen, zu denken ist beispielsweise an die Fahreridentifizierung bei Geschwindigkeitsüberschreitungen im Straßenverkehr, werden Ordnungswidrigkeiten im Folgenden nicht weiter betrachtet.

### 1.2.2 Verhinderung und Verfolgung von Straftaten durch die Polizei

Der Einsatz von Gesichtserkennung in Verbindung mit Videoüberwachung zur Verhinderung oder Verfolgung von Straftaten ist durch unterschiedliche Akteure denkbar. Beispielsweise können private Ladeninhaber Videoüberwachung zur Verhinderung von Diebstählen einsetzen. Jobcenter können mittels Videoüberwachung ihre Gebäude oder Bediensteten vor Übergriffen schützen. Denkbar ist auch ein Einsatz durch die Geheim-

---

36 Zum Nebenstrafrecht kurz MüKo-StGB-Joecks/Erb, Einl. Rn. 9 f. Ausführlich zu den Strafrechtsquellen außerhalb des StGB bei Jescheck/Weigend 1996, 109 ff.

37 BVerfGE 22, 49 (79).

38 BVerfGE 27, 18 (33).

39 Jescheck/Weigend 1996, 59. Kompetenzrechtlich zählt das Ordnungswidrigkeitenrecht allerdings zum Strafrecht i.S.d. Art. 74 Abs. 1 Nr. 1 GG, z.B. v. Mangoldt/Klein/Starck-Oeter, Art. 74 Rn. 16. Ausführlich zur Abgrenzung von Straftaten und Ordnungswidrigkeiten z.B. Graf-OWiG-Gerhold, Einl. OWiG Rn. 1 ff.

dienste. Geheimdienste<sup>40</sup> zählen aber genauso wenig zur Polizei wie private Ladeninhaber oder die Jobcenter. Sie werden daher im Folgenden nicht weiter betrachtet.

Vielmehr ist für diese Arbeit der Einsatz von Gesichtserkennung in Verbindung mit Videoüberwachung durch die Polizei von Interesse. Der Begriff der „Polizei“<sup>41</sup> bezeichnete zunächst (etwa ab dem 15. Jahrhundert) einen Zustand guter Ordnung des Gemeinwesens,<sup>42</sup> umspannte während des Absolutismus die innere Verwaltung des Staates in ihrer Gesamtheit<sup>43</sup> und wurde Ende des 19. Jahrhunderts von der Preußischen Justiz auf die gefahrenabwehrende Tätigkeit<sup>44</sup> zurückgeschnitten.<sup>45</sup> Hieran anknüpfend umfasst der sogenannte materielle Polizeibegriff die gesamte staatliche Tätigkeit, die der Abwehr von Gefahren dient.<sup>46</sup> Demnach existiert zum

---

40 Geheimdienste werden nicht als Polizei verstanden, z.B. *Kugelman* 2012, Kap. 4 Rn. 32 u. 41 u. *Thiel* 2020, § 3 Rn. 7 unter Verweis auf das Trennungsgesetz (BVerfGE 97, 198 (217)) und fehlende polizeiliche Befugnisse (§ 8 Abs. 3 BVerfSchG, § 2 Abs. 3 BNDG, § 4 Abs. 2 MADG); kritisch zustimmend *Schenke* 2021, Rn. 497.

41 „Polizei“ entstammt dem Griechischen und kann (wahrscheinlich) auf „politeia“ zurückgeführt werden, womit in der griechischen Antike die Angelegenheiten bezeichnet wurden, die die „polis“ (also den griechischen Stadtstaat) betrafen, *Möllers-Dams*, Eintrag zu Polizei.

42 Dies umfasste die Sicherung eines gottgefälligen Lebens, etwa durch das Verbot von Völlerei, Kuppelei und Ehebruch. Auch fanden sich Vorschriften gegen ungehörige Kleidung, Betrügereien beim Handel und Quacksalberei, *Lisken/Denninger-Stolleis*, Kap. A Rn. 4 f.

43 *Lisken/Denninger-Stolleis*, Kap. A Rn. 11. Die Polizeigewalt als Inbegriff der absolutistischen Herrschaft der Fürsten unterlag keinen rechtlichen Begrenzungen, so dass die absolutistischen Staaten auch als Polizeistaaten bezeichnet werden können, die aber immer auch Wohlfahrtsstaaten waren, *Kingreen/Poscher* 2020b, § 1 Rn. 4; *Schenke* 2021, Rn. 2.

44 Im Allgemeinen Landrecht für die Preußischen Staaten (1794) heißt es in § 10 II 17, dass die „nöthigen Anstalten zur Erhaltung der öffentlichen Ruhe, Sicherheit, und Ordnung, und zur Abwendung der dem Publico, oder einzelnen Mitgliedern desselben, bevorstehenden Gefahr zu treffen, [...] das Amt der Polizey [ist]“. Darauf Bezug nehmend urteilte das PrOVG im sog. Kreuzbergurteil (1882), dass die Aufgabe der Polizei in der Gefahrenabwehr zu sehen ist. Das Urteil ist abgedruckt in DVBl 1985, 219; kurze Besprechung bei *Rott*, NVwZ 1982, 363; zu der Entwicklung hin zum Kreuzbergurteil *Lisken/Denninger-Stolleis*, Kap. A Rn. 20 ff.; *Kingreen/Poscher* 2020b, § 1 Rn. 5 ff.; *Schenke* 2021, Rn. 3 ff.

45 Zur geschichtlichen Entwicklung der Polizei in Deutschland *Lisken/Denninger-Stolleis*, Kap. A Rn. 1 ff.; kürzer *Kingreen/Poscher* 2020b, § 1 Rn. 2 ff.; *Kugelman* 2012, Kap. 2 Rn. 1 ff.; *Schenke* 2021, Rn. 2 ff.

46 *Kugelman* 2012, Kap. 2 Rn. 28 u. *Thiel* 2020, § 2 Rn. 9.

Beispiel eine Bau-, Feuer-, Fremden-, Jugend-, Markt- oder Sittenpolizei,<sup>47</sup> obwohl der „Normalmensch“ viele dieser Tätigkeiten heute nicht mehr mit der Polizei in Verbindung bringen wird.<sup>48</sup> Dem Einsatz von Videotechnik tun sich in diesem Zusammenhang zahlreiche Anwendungsfelder auf. So ist es beispielsweise denkbar, Videokameras bei der Brandbekämpfung<sup>49</sup> oder mit bauordnungsrechtlicher Zielsetzung zu nutzen.

Ein derart weiter Polizeibegriff, der gleichzeitig die Strafverfolgung nicht erfasst, liegt dieser Arbeit allerdings nicht zugrunde. In einem institutionell<sup>50</sup>-formellen<sup>51</sup> Sinne meint Polizei dann auch die als Polizei bezeichneten Behörden und die ihnen übertragenen Aufgaben.<sup>52</sup> Der Polizei kommt insoweit eine „Doppelfunktion“<sup>53</sup> zu: Ihr Aufgabenbereich umfasst sowohl die Gefahrenabwehr (z.B. Art. 2 Abs. 1 BayPAG, § 1 Abs. 1

---

47 *Kingreen/Poscher* 2020b, § 1 Rn. 19.

48 *Kramer* 2021, Rn. 12.

49 Im Zusammenhang mit der Brandbekämpfung in Tunneln OVG Niedersachsen, DVBl 2010, 262.

50 Polizei im institutionellen Sinne umfasst alle Stellen, die dem Organisationsbereich der Polizei zugerechnet werden, *Schenke* 2021, Rn. 15. Gemeint sind als „Polizei“ firmierende Behörden, *Lisken/Denninger-Stolleis*, Kap. A Rn. 39. Auf Bundesebene zählen hierzu die BPol und das BKA. Auf Landesebene bestehen verschiedene Behördenstrukturen, auf die hier nicht weiter eingegangen wird. Im Grundsatz haben sich das Trennungssystem und das Einheitssystem herausgebildet. Im Trennungssystem (Bayern, Berlin, Brandenburg, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt, Schleswig-Holstein, Thüringen) wird die Gefahrenabwehr überwiegend von allgemeinen Verwaltungsbehörden wahrgenommen, die als Ordnungs-, Sicherheits- oder auch Gefahrenabwehrbehörden firmieren. Die als „Polizei“ bezeichneten Behörden werden nur in Eilfällen, zur Vollzugshilfe und bei sonstigen aufgetragenen Aufgaben tätig, z.B. *Schenke* 2021, Rn. 15; *Kugelmann* 2012, Kap. 4 Rn. 52 f.; *Thiel* 2020, § 3 Rn. 14. Im Einheitssystem (Baden-Württemberg, Bremen, Saarland, Sachsen) umfasst die Polizei im institutionellen Sinne alle Behörden, die Aufgaben im Sinne des materiellen Polizeibegriffs wahrnehmen. Unterteilt wird dann in Polizei(verwaltungs)behörden und Polizeivollzugsbehörden, z.B. *Schenke* 2021, Rn. 16; *Kugelmann* 2012, Kap. 4 Rn. 50; *Thiel* 2020, § 3 Rn. 13. In der Praxis unterscheiden sich beide Systeme nicht sonderlich, *Kugelmann* 2012, Kap. 4 Rn. 55 u. *Kingreen/Poscher* 2020b, § 2 Rn. 24 f.

51 Der formelle Polizeibegriff umschreibt die Aufgaben, die ausdrücklich der Polizei im institutionellen Sinne, also allen als „Polizei“ bezeichneten Behörden, zugewiesen sind, *Schenke* 2021, Rn. 17.

52 Die verschiedenen Polizeibegriffe sind nicht als sich ausschließende Theorien zu verstehen, sondern umschreiben das Phänomen „Polizei“ aus unterschiedlichen Blickwinkeln, *Thiel* 2020, § 2 Rn. 7.

53 *Beulke/Swoboda* 2020, Rn. 162 u. *Hartmann/Schmidt* 2018, Rn. 171.

HSOG) als auch die Strafverfolgung (z.B. Art. 2 Abs. 4 BayPAG, § 1 Abs. 1 HSOG i.V.m. §§ 161 Abs. 1, 163 Abs. 1 StPO).

Im Folgenden interessiert die Gefahrenabwehr nur insoweit, als sie auf die Verhinderungen von Straftaten gerichtet ist. Unter einer Gefahr ist eine Sachlage zu verstehen, die bei ungehindertem Fortgang mit hinreichender Wahrscheinlichkeit in der Schädigung eines polizeilich geschützten Rechtsguts münden wird.<sup>54</sup> Von ihrem Charakter her ist die Gefahrenabwehr dementsprechend in die Zukunft gerichtet. Sie soll drohende Schäden abwehren und wirkt in erster Linie präventiv. Ob eine Gefahr besteht, unterliegt einer Prognoseentscheidung. Gefahrenabwehrendes polizeiliches Handeln ist somit prognostisches Handeln.<sup>55</sup>

Dabei existieren verschiedene Ausprägungen des Gefahrbegriffs. Dies betrifft etwa die konkrete und die abstrakte Gefahr sowie unterschiedliche Qualifikationen der konkreten Gefahr.<sup>56</sup> Gemeinsam ist ihnen, dass sie sich auf die polizeilichen Schutzgüter der öffentlichen Sicherheit und Ordnung<sup>57</sup> beziehen. Unter der öffentlichen Sicherheit wird die Unverletzlichkeit der Rechtsordnung, die Unverletzlichkeit subjektiver Rechte und Rechtsgüter des Einzelnen sowie der Bestand des Staates und seiner Einrichtungen verstanden.<sup>58</sup> Öffentliche Ordnung meint hingegen die „ungeschriebenen Regeln [...], deren Befolgung nach den jeweils herrschenden sozialen und ethischen Anschauungen als unerläßliche Voraussetzung eines geordneten menschlichen Zusammenlebens innerhalb eines bestimmten Gebiets angesehen wird“.<sup>59</sup> Das Konzept der öffentlichen Ordnung wird aufgrund der Durchnormierung weiter Lebensbereiche teilweise als

---

54 In der Lit. z.B. *Kingreen/Poscher* 2020b, § 8 Rn. 2; in der Rspr. z.B. BVerwGE 45, 51 (57).

55 *Kugelmann* 2012, Kap. 5 Rn. 108.

56 *Kingreen/Poscher* 2020b, § 8 Rn. 2. Verschiedene Ausprägungen werden z.B. in § 3 Nr. 3 SOG LSA definiert.

57 Die öffentliche Ordnung wird nicht von allen Polizeigesetzen genannt, z.B. § 1 Abs. 1 BremPolG.

58 Z.B. *Kingreen/Poscher* 2020b, § 7 Rn. 2; ebenfalls BVerfGE 69, 315 (352). In § 3 Nr. 1 SOG LSA definiert als die „Unverletzlichkeit der Rechtsordnung, der subjektiven Rechte und Rechtsgüter des Einzelnen sowie des Bestandes, der Einrichtungen und Veranstaltungen des Staates oder sonstiger Träger der Hoheitsgewalt“.

59 BVerfGE 69, 315 (352); ebenfalls *Kingreen/Poscher* 2020b, § 7 Rn. 42. In § 3 Nr. 2 SOG LSA definiert als „die Gesamtheit der im Rahmen der verfassungsmäßigen Ordnung liegenden ungeschriebenen Regeln für das Verhalten des Einzelnen in der Öffentlichkeit, deren Beachtung nach den jeweils herrschenden Anschauungen als unerlässliche Voraussetzung eines geordneten staatsbürgerlichen Zusammenlebens betrachtet wird“.

überflüssig angesehen und unterliegt wegen der Berufung auf außerrechtliche Normen verfassungsrechtlichen Bedenken.<sup>60</sup>

Droht die Verwirklichung gesetzlicher Straftatbestände, liegt jedenfalls eine Gefahr für die öffentliche Sicherheit vor, da hierdurch die Rechtsordnung sowie subjektive Rechte gefährdet werden. Die polizeiliche Aufgabe der Gefahrenabwehr umfasst daher auch die Verhinderung von Straftaten<sup>61</sup> einschließlich der Verhütung zu erwartender Straftaten (sog. vorbeugende Bekämpfung von Straftaten).<sup>62</sup>

Überdies hat die Polizei die Aufgabe, begangene Straftaten zu verfolgen. Gemäß §§ 161 Abs. 1, 163 Abs. 1 StPO hat die Polizei auf Ersuchen oder Auftrag<sup>63</sup> der Staatsanwaltschaft sowie im Rahmen des ersten Zugriffs Ermittlungen jeder Art durchzuführen. Diese Aufgabenzuweisung wird in den Polizeigesetzen aufgegriffen (z.B. Art. 2 Abs. 4 BayPAG, § 1 Abs. 2 HSOG).

Strafverfolgung grenzt sich von der Gefahrenabwehr – grundsätzlich – durch das zeitliche Moment ab: Während die Gefahrenabwehr präventiv in die Zukunft gerichtet ist, knüpft die Strafverfolgung an eine bereits begangene Straftat an und ist auf deren Aufklärung und Aburteilung gerichtet. Strafverfolgung wirkt somit zuvorderst<sup>64</sup> repressiv.<sup>65</sup> Auch wenn der Unterschied zwischen Strafverfolgung und Gefahrenabwehr auf den ersten Blick eindeutig zu sein scheint, bestehen doch zahlreiche Abgrenzungsprobleme. Gefahrenabwehr und Strafverfolgung gehen „Hand in Hand und sind in ihren Wirkungen miteinander eng verwoben“.<sup>66</sup> Dies zeigt sich unter anderem bei der Strafverfolgungsvorsorge, die als Unterfall

---

60 *Kingreen/Poscher* 2020b, § 7 Rn. 44 ff.

61 Nach BVerfGE 69, 315 (352) wird „in der Regel eine Gefährdung der öffentlichen Sicherheit angenommen [...], wenn eine strafbare Verletzung dieser Schutzgüter droht.“

62 Vorbeugende Bekämpfung von Straftaten als Aufgabe der Polizei z.B. in § 1 Abs. 4 HSOG; in der Lit. z.B. *Kingreen/Poscher* 2020b, § 3 Rn. 4 f. BVerwGE 141, 329 (335) spricht von der Gefahrenvorsorge, die „die Verhütung von noch nicht konkret drohenden Straftaten“ umfasst; dazu auch *Schenke* 2021, Rn. 11.

63 Der Auftrag der Staatsanwaltschaft richtet sich an die Ermittlungspersonen der Staatsanwaltschaft (§ 152 GVG), das Ersuchen an die übrigen Behörden und Beamten des Polizeidienstes, KK-StPO-*Griesbaum*, § 161 StPO Rn. 28.

64 Je nach Sichtweise verfolgt das Strafrecht auf der Ebene der Strafe aber auch eine präventive Zielsetzung. Zu den verschiedenen Straftheorien MüKo-StGB-*Joecks/ Erb*, Einl. Rn. 50 ff. u. BVerfGE 45, 187 (253 ff.).

65 Zur Strafverfolgung als Aufgabe der Polizei in Abgrenzung zur Gefahrenabwehr z.B. *Kugelman* 2012, Kap. 1 Rn. 40 ff.; *Schenke* 2021, Rn. 465 ff.; *Thiel* 2020, § 4 Rn. 11 u. 17 ff.

66 BVerfGE 150, 244 (275).

der vorbeugenden Bekämpfung von Straftaten (z.B. § 1 Abs. 4 HSOG) zwar präventiv ausgerichtet ist, kompetenzrechtlich aber dem Strafverfahren zuzurechnen ist.<sup>67</sup>

Gesichtserkennung in Verbindung mit Videoüberwachung kann ein polizeiliches Instrument zur Verhinderung und Verfolgung von Straftaten sein. Videoüberwachung wird eingesetzt, um potentielle Straftäter abzuschrecken, der Polizei eine zeitnahe Reaktion zur Unterbindung sich anbahnender Straftaten zu ermöglichen und für die Aufklärung begangener Straftaten Ermittlungsansätze sowie Beweismittel zu gewinnen.<sup>68</sup> Gesichtserkennung kann diese Ziele durch die (automatisierte) Erkennung tatverdächtiger oder gefährlicher Personen sowie die zeitnahe Auswertung großer Mengen an Videomaterial unterstützen.<sup>69</sup>

Das Potential der Gesichtserkennung erkennend formulierte *Thilo Weichert*, ehemaliger Datenschutzbeauftragter des Landes Schleswig-Holstein, bereits vor 15 Jahren, es wäre für die Polizei „sicher eine faszinierende Ermittlungsgrundlage, Gesichtsprofile aller erwachsenen Männer und Frauen in einer elektronischen Datenbank abgespeichert zu haben. Im Fall einer per Videoüberwachung dokumentierten Straftat wäre es dann ein Leichtes, von den 60 Millionen potenziellen Tätern bzw. Täterinnen vielleicht 99% per automatisiertem Datenabgleich auszuschließen.“<sup>70</sup> Entpuppt sich also der bereits erwähnte Zugreisende<sup>71</sup> als gar nicht so harmlos, sondern als ein zur Fahndung ausgeschriebener Schwerverbrecher, kann der Abgleich der Videoaufnahmen seines Gesichts mit einer polizeilich Lichtbilddatenbank seine Identifizierung ermöglichen und so dazu beitragen, ihn für seine Verbrechen zur Rechenschaft zu ziehen. Allerdings hieße es Herrn *Weichert* Unrecht tun, würde an dieser Stelle verschwiegen, dass er ein solches Szenario aus rechtlicher Sicht als „keineswegs harmlos und banal“ eingeordnet hat.<sup>72</sup> Überdies können derartige Szenarien die Befürchtung hervorrufen, die deutsche Gesellschaft befinde sich auf dem Weg in den Überwachungsstaat.

---

67 Dazu s. Kap. 5.2.2.3.1.

68 Zum Einsatz von Videoüberwachung s. Kap. 2.1.3.

69 Zu den hier betrachteten Szenarien s. Kap. 3.

70 *Weichert* 2004, 36 f.

71 S. Kap. 1.1.

72 *Weichert* 2004, 37.

### 1.3 Überwachen und Überwachungsstaat: Visionen und Dystopien

Videoüberwachung und biometrische Gesichtserkennung sind Teil des sich ständig erweiternden Kreises verfügbarer Überwachungstechnologien. Das mit diesen Technologien verbundene Phänomen der Überwachung kann aus verschiedenen Blickwinkeln betrachtet werden. Neben der rechtlichen Perspektive bestehen unter anderem technische, soziale und politische Dimensionen der Überwachung.<sup>73</sup>

Überwachung stellt sich als eine Mischung aus „Maßnahmen, Zielen, Technologien sowie gesellschaftlichen Bedingungen und Konstellationen“ dar.<sup>74</sup> Dementsprechend vielfältig und interdisziplinär sind die Diskurse über und die Betrachtungen von Überwachung. Bereits der Begriff der Überwachung entzieht sich einer allgemeingültigen Definition. Das Deutsche Wörterbuch von *Jacob und Wilhelm Grimm* nennt als Bedeutung von überwachen einerseits „die nacht durchwachen“, andererseits „bewachen, beaufsichtigen, im auge behalten“.<sup>75</sup> Im Duden wird überwachen unter anderem verstanden als „genau verfolgen, was jemand (der verdächtig ist) tut“, sowie „beobachtend, kontrollierend für den richtigen Ablauf einer Sache sorgen“.<sup>76</sup> Aus soziologischer Sicht wird vorgeschlagen, Überwachung als „Phänomen der Schaffung, Steuerung und Erhaltung gesellschaftlicher Ordnung“ zu betrachten.<sup>77</sup> Überwachung sei ein zielgerichtetes, „routinemäßiges und systematisches Überprüfen und Beobachten persönlicher Daten durch Datenspeicherungen aller Art, um zu kontrollieren, Zugänge zu regeln oder Prozesse zu beeinflussen“, und bedeute das Vorhandensein einer übergeordneten Kontrolle durch verschiedene „Instanzen der Macht“, die ein Interesse an der Erhaltung der jeweiligen gesellschaftlichen und wirtschaftlichen Ordnung haben. Dies können neben staatlichen Stellen auch private Akteure (z.B. Sicherheitsdienste) sein.<sup>78</sup>

---

73 Zurawski 2011, 7.

74 Zurawski 2007b, 8.

75 Der Eintrag ist über die Online-Ausgabe der Universität Trier abrufbar: [http://woerterbuchnetz.de/cgi-bin/WBNetz/wbgui\\_py?sigle=DWB&lemid=GU02285&mode=Vernetzung&hitlist=&patternlist=&mainmode](http://woerterbuchnetz.de/cgi-bin/WBNetz/wbgui_py?sigle=DWB&lemid=GU02285&mode=Vernetzung&hitlist=&patternlist=&mainmode) (Stand: 11.05.2021).

76 Duden online, Eintrag zu überwachen.

77 Zurawski 2007b, 9 unter Berufung auf Lyon 2001.

78 Zurawski 2007b, 9 f. S.a. Zurawski 2007c, 85 f. zu einem Verständnis von Überwachung als „Kartierungsprozess gesellschaftlichen Lebens“, um soziale, geografische und politische Räume zu erfassen und darzustellen und so eine Kontrolle von Mensch und Raum zu erzielen.

Überwachung weist jedenfalls ein kontrollierendes Element auf. Abstrakt gesprochen lässt sie sich „als eine zeitlich und logisch miteinander verbundene Abfolge einzelner Kontrollakte“<sup>79</sup> verstehen, wobei diese Kontrollakte auf einen „Vergleich zwischen einem Sollwert und einem Istwert“<sup>80</sup> gerichtet sind. Eine Videokamera mag hierfür das Symbol sein, stellt für sich gesehen aber noch keine Überwachung dar. Vielmehr handelt es sich bei Überwachung um eine Tätigkeit, die von Menschen erdacht, initiiert und durchgeführt wird.<sup>81</sup> Diese Tätigkeit ist nicht immer spannend, sondern kann sich darin erschöpfen, dass „Sicherheitskräfte [...] des nachts um leere Grundstücke herumlaufen“.<sup>82</sup> Sie kann aber auch bedeuten, dass die überwachende Stelle unbemerkt in das Privat- und Intimleben einer Person eintaucht – sei es aus bloßer Neugier, sei es aus finanziellem Interesse, sei es, um die überwachte Person eines Verbrechens zu überführen. Gerade der Einsatz moderner Überwachungstechnologien ist dabei untrennbar mit der Besorgnis der (schleichenden) Errichtung eines Überwachungsstaates verbunden, „der seine Bürger bis ins Kleinste überwacht“<sup>83</sup>. In diesem Zusammenhang werden regelmäßig zwei Namen genannt: *Jeremy Bentham* und *George Orwell*.

### 1.3.1 Jeremy Bentham und das Panoptikum

Auf *Jeremy Bentham* (1748 bis 1832) wird Bezug genommen, wenn der Videüberwachung das Potential „panoptischer Machtausübung“<sup>84</sup> zugesprochen wird. Der als „Prophet der totalen Überwachung“<sup>85</sup> bezeichnete Philosoph und Jurist entwickelte Ende des 18. Jahrhunderts das Panoptikum als ein Konstruktionsprinzip, welches anwendbar sein soll „auf jedwede Einrichtung, in der Personen jeder Art unterzubringen oder zu kontrollieren sind“. Gedacht hat er dabei an „Gefängnisse, Armenhäuser,

---

79 *Nogala*, Telepolis v. 25.10.2000.

80 *Purgathofer* 2008, 195.

81 *Zurwaski* 2011, 9 f.

82 *Zurwaski* 2011, 10 f.

83 *Duden online*, Eintrag zu Überwachungsstaat.

84 *Schmitt Glaeser*, BayVBl 2002, 584. Auch andere zur Überwachung taugliche Technologien werden mit dem Panoptikum in Verbindung gebracht, wie etwa die Gesundheitskarte, z.B. *Decker* 2007, 159 („Panoptismus und die Gesundheitskarte“).

85 *Welzbacher* 2013, 196. *Welzbacher* sieht darin ein Missverständnis, das er auf *Foucault* zurückführt.

Lazarette, Fabriken, Manufakturen, Hospitäler, Arbeitshäuser, Irrenhäuser und Schulen“.<sup>86</sup>

Immer dann, wenn in einem Gebäude oder innerhalb eines überschaubaren Raums eine Anzahl von Personen beaufsichtigt werden soll, um „die Unverbesserlichen zu bestrafen, die Verrückten zu beaufsichtigen, die Gemeingefährlichen zu bessern, die Verdächtigen unter Aufsicht zu stellen, die Müßigen zu beschäftigen, die Hilflosen zu betreuen, die Kranken zu behandeln [...] oder die zukünftige Generation auf den Pfad der Bildung zu führen“, liegt es nach *Bentham* „auf der Hand“, dass diese Ziele am besten erreicht werden können, wenn jede der betroffenen Personen zu jedem Zeitpunkt von einem Aufseher überwacht wird. Da dies nicht immer möglich ist, ist es hiernach das Nächstbeste, wenn die Personen zumindest davon ausgehen müssen, dass eine Überwachung stattfindet.<sup>87</sup>

Das daraus abgeleitete Konstruktionsprinzip des Panoptikums wird von *Bentham* am Beispiel eines Gefängnisses erläutert: Das Gebäude ist kreisförmig angelegt. Die Zellen der Gefangenen liegen im Kreisumfang. Im Zentrum befindet sich die Loge des Aufsehers. Durch bauliche Maßnahmen wird sichergestellt, dass der Aufseher jede Zelle überblicken kann, während die Gefangenen nicht erkennen können, ob die Aufseherloge besetzt ist und was der Aufseher gerade tut.<sup>88</sup> So ist es dem Aufseher möglich, „zu sehen, ohne selbst gesehen zu werden“. Den Gefangenen soll auf diese Weise der Eindruck vermittelt werden, dass sie – zumindest mit großer Wahrscheinlichkeit – kontrolliert werden.<sup>89</sup> Dabei soll die Konstruktion aber nicht nur den Eindruck der Überwachung vermitteln, sondern eine solche über einen größtmöglichen Zeitraum auch tatsächlich ermöglichen, denn je größer die Wahrscheinlichkeit ist, dass eine Person überwacht wird, desto „intensiver wird ihr Gefühl sein, [...] dass dem wirklich so sei“.<sup>90</sup> Jede Zelle ist also ein „kleines Theater“, in dem die Gefangenen jederzeit sichtbar sein sollen.<sup>91</sup>

*Benthams* Panoptikum ist ausdrücklich nicht auf Heimlichkeit ausgelegt. Es sollen nicht heimlich Gespräche belauscht, Gedanken ausgeforscht oder „die geheimen Winkel des Herzens“ ergründet werden. Vielmehr sollen sich die Betroffenen der Überwachung bewusst sein.<sup>92</sup> Gerade davon ver-

---

86 *Bentham* 2013b, 7.

87 *Bentham* 2013b, 12.

88 *Bentham* 2013b, 13 ff.

89 *Bentham* 2013b, 29 f.

90 *Bentham* 2013b, 30.

91 *Foucault* 1994, 257.

92 *Bentham* 2013b, 107.

spricht sich *Bentham* einen Einfluss auf ihr Verhalten, da sie jederzeit damit rechnen müssen, dass Regelverstöße registriert werden und eine (repressive) Reaktion hervorrufen. *Bentham* geht mithin davon aus, dass bereits die (ernstzunehmende) Möglichkeit der Beobachtung regelkonformes Verhalten des (vermeintlich) Beobachteten herbeiführen kann. Der Gedanke, durch permanente Überwachung das Verhalten von Menschen zu beeinflussen, ist freilich älter als *Bentham* und kann bereits in der Figur des allwissenden Gottes ausgemacht werden, der alles sieht und (spätestens) nach dem Tod eines Menschen entsprechende Sanktionen ausspricht.<sup>93</sup>

Gerne wird das panoptische Prinzip auf moderne Überwachungstechnologien übertragen. Vor allem der Videoüberwachung wird das „Potenzial einer panoptischen Machtausübung“ zugesprochen.<sup>94</sup> Der durch die Kamera vermittelte Blick zeichne sich dadurch aus, dass der Einzelne gesehen wird, während der Überwacher ungesehen bleibt. Dies könne zu einer „neuen Form der Macht über den Geist“ führen.<sup>95</sup> Profaner gesprochen: Videoüberwachung soll dem Einzelnen den Eindruck vermitteln, jederzeit gesehen zu werden. Damit verbunden ist die Drohung, dass die Überwacher regelwidriges Verhalten erkennen und sanktionieren können. Hierdurch sollen insbesondere potentielle Straftäter von der Tatbegehung abgeschreckt werden. Ob tatsächlich zu jedem Zeitpunkt eine Überwachung stattfindet, mithin die Videoaufnahmen beständig betrachtet und ausgewertet werden, ist für die Betroffenen nicht erkennbar. So wenig, wie die Insassen in *Benthams* Gefängnis in die Aufseherloge blicken können, so wenig kann der Einzelne erkennen, ob ihn die Betreiber der Kamera gerade im Blick haben. Ausreichen soll bereits das bloße Gefühl, dass es so sein könnte. Ob dies in der Praxis tatsächlich funktioniert, ist eine andere Frage.<sup>96</sup>

*Michel Foucault* hat die Gedanken *Benthams* fortentwickelt und das Panoptikum als beispielhaft für die Herrschaftstechniken in der liberalen bürgerlichen Gesellschaft angesehen. Dabei handele es sich um ein Prinzip zur Kontrolle und Disziplinierung der Gesellschaft, das bei ihm als Panoptismus bezeichnet wird.<sup>97</sup> Maßgeblich sei die beständige Sichtbarkeit des

---

93 *Glatzner* 2006, 27 f. zur Selbstdisziplinierung und Kontrolltheorien.

94 *Schmitt Glaeser*, BayVBl 2002, 584, 585.

95 *Schmitt Glaeser*, BayVBl 2002, 584, 585.

96 Zu Wirkung und Wirksamkeit von Videoüberwachung s. Kap. 2.1.5.

97 *Foucault* 1994, 251 ff.; dazu auch *Decker* 2007, 168 f. u. *Bung*, ZStW 2013, 536, 538 f. („Machttechnik“).

Individuums, das hierdurch „zu jedem Zeitpunkt in seinem individuellen Handeln und seinen individuellen Motiven ausgemacht werden und seine Handlung auf Stimmigkeit mit der herrschenden Rationalität überprüft werden kann“.<sup>98</sup> Denn derjenige, „welcher der Sichtbarkeit unterworfen ist und dies weiß, übernimmt die Zwangsmittel der Macht und spielt sie gegen sich selber aus; er internalisiert das Machtverhältnis, in welchem er gleichzeitig beide Rollen spielt; er wird zum Prinzip seiner eigenen Unterwerfung“.<sup>99</sup>

Allerdings darf *Benthams* Panoptikum nicht als Blaupause für ein tyrannisches System der Unterdrückung verstanden werden. Betroffen ist nicht nur der Überwachte, sondern auch der Überwacher selbst. Dieser soll zusammen mit seiner Familie in der Aufseherloge seine „Wohnstatt“ finden und so vollständig in der Überwachung aufgehen. Wenn seine Familienmitglieder „ihre alltäglichen Verrichtungen für einen Augenblick unterbrechen“, werden auch sie „ihre Blicke in den Dienst dieser Aufgabe stellen“.<sup>100</sup> Vor allem aber soll es das Panoptikum ermöglichen, den Überwacher einer „unnachgiebigen Kontrolle“ durch seine Vorgesetzten zu unterwerfen, was nicht zuletzt dem Schutz der Häftlinge vor Machtmissbrauch dienen soll.<sup>101</sup> Höherrangige Inspektoren sollen sich auf einfache Weise einen Überblick über die Situation in der Anlage verschaffen können.<sup>102</sup> Und auch die interessierte Öffentlichkeit soll die ordnungsgemäße Pflichterfüllung der Aufseher kontrollieren können, was vor dem Hintergrund zu verstehen ist, dass zu *Benthams* Zeiten dem Publikum gegen Entgelt der Zugang zu Haftanstalten sowie Kranken- und Irrenhäusern möglich war.<sup>103</sup> *Bentham* machte sich also durchaus Gedanken über die Frage „quis custodiet ipsos custodes?“<sup>104</sup> Folglich sind Mechanismen vorgesehen, die verhindern sollen, „dass die der panoptischen Maschine zu verdankende Machtsteigerung in Tyrannei entarten könnte“.<sup>105</sup>

Für die Einordnung des Panoptikums ist außerdem von Bedeutung, dass *Bentham* (zusammen mit *John Stuart Mill*) als Begründer des Utilitarismus

---

98 Decker 2007, 168.

99 Foucault 1994, 260.

100 Bentham 2013b, 31.

101 Bentham 2013b, 32 f.

102 Bentham 2013b, 33.

103 Bentham 2013b, 35.

104 Bentham 2013b, 33. Die Sentenz „quis custodiet ipsos custodes?“ („Wer bewacht die Wächter?“) stammt aus den Satiren des römischen Dichters *Juvenal*.

105 Foucault 1994, 266.

gilt.<sup>106</sup> Grundlage dieses ethischen Systems ist das Prinzip der Nützlichkeit. Als *Maxime* formuliert bedeutet dies: „Handle so, daß die Folgen deiner Handlung bzw. Handlungsregel für das Wohlergehen aller Betroffenen optimal sind.“<sup>107</sup> Anstatt vom Prinzip der Nützlichkeit sprach *Bentham* in diesem Zusammenhang auch vom Prinzip des größten Glücks.<sup>108</sup> Nach seinem Verständnis war demnach die beste Regierungsform jene, die „das größte Glück der größten Zahl“ hervorbringt.<sup>109</sup> Mit dem Panoptikum wählte *Bentham* verschiedene Ziele auf diesem Weg erreicht: „Die Sitten reformiert – der Gesundheit einen Dienst erwiesen – das Gewerbe gestärkt – die Methoden der Unterweisung verbessert – die öffentlichen Ausgaben gesenkt – die Wirtschaft gleichsam auf ein festes Fundament gestellt – der Gordische Knoten der Armengesetze nicht durchschlagen, sondern gelöst – all das durch eine einfache architektonische Idee!“<sup>110</sup> Überwachung war für ihn mithin kein Selbstzweck, sondern „Motor des sozialreformatischen, wirtschaftlichen und humanistischen Fortschritts“.<sup>111</sup> Seine Überlegungen sind als Instrumente der Glücksförderung anzusehen und wurden von *Bentham* nur in diesem Sinne betrachtet.<sup>112</sup>

Dass Überwachung gesellschaftlich sinnvollen Zielen dienen kann, ist nicht ernsthaft zu bestreiten. Zu denken ist nur an die Verhinderung und Verfolgung von Straftaten. Allerdings kann Überwachung auch schützenswerte Interessen der überwachten Personen beeinträchtigen, was bei *Bentham* nicht thematisiert wird, für die heutige (rechtliche) Einordnung von Überwachung aber von zentraler Bedeutung ist. Zudem werden in der Literatur Unterschiede zur Wirkweise des Panoptikums im Vergleich zur Videoüberwachung herausgestellt. Ein wenig kryptisch heißt es etwa, jede Überwachungskamera sei eine „Antithese“ zum Panoptikum, da sie „die ermittelten Informationen nicht mehr an einem visuell erfahrbaren Punkt [bündelt], der dem ‚Delinquenten‘ (uns allen) real (und im allegorischen Spiel) entgegentritt, um die Bewusstwerdung des (tatsächlichen oder virtuellen) Beobachtetseins zum Bestandteil eines wechselseitigen Prozesses zu machen“. Das Kameraauge blicke leer und offenbare „selbstgenügsam und asozial“ die Intentionlosigkeit der Überwacher.<sup>113</sup> Die „weit verbreitete

---

106 Höffe 2013, 13 ff. zum sog. klassischen Utilitarismus.

107 Höffe 2013, 11.

108 *Bentham* 2013a, 55 Fn. 1.

109 *Bentham* 2013b, 120.

110 *Bentham* 2013b, 8.

111 *Welzbacher* 2013, 198.

112 *Sidgwick* 2013, 145.

113 *Welzbacher* 2013, 211 f.

Annahme“, dass die Videoüberwachung als Visualisierungstechnik entsprechend den Denkmodellen von *Bentham* und *Foucault* eine disziplinierende Wirkung entfalte, verkenne ihre „Formen- und Funktionsvielfalt“. Die einzelnen Systeme seien zu isoliert und häufig schlicht wirkungslos.<sup>114</sup> Jedenfalls fehle eine Zentralstelle der Überwachung. Diese sei vielmehr auf unterschiedliche (staatliche und private) Akteure verteilt.<sup>115</sup>

### 1.3.2 George Orwell und der Große Bruder

Sollte *Benthams* Panoptikum der Glücksförderung dienen, ist dies für die in *George Orwells* Roman „Nineteen Eighty-Four“ (im Folgenden: 1984) beschriebenen Überwachungspraktiken und -ziele erkennbar nicht der Fall. Gerade deshalb gehört ein Hinweis auf *George Orwell*, seinen Roman oder den darin auftretenden Großen Bruder (Big Brother) gewissermaßen zum guten Ton überwachungskritischer Überlegungen.<sup>116</sup>

Der 1949 erschienene Roman<sup>117</sup> ist in die ideologischen Auseinandersetzungen nach dem Ende des 2. Weltkrieges eingebettet<sup>118</sup> und handelt von einer Welt im Jahr 1984, die von den drei Großmächten Ozeanien, Eurasi-

---

114 Töpfer 2007, 38.

115 Rammert 2008, 189 f.

116 Erwähnung finden *George Orwell* (bzw. *Eric Blair*), 1984, der Große Bruder oder Big Brother im Zusammenhang mit der rechtlichen Auseinandersetzung mit Videoüberwachung z.B. bei *Bull*, JZ 2017, 797, 797 (der die Heranziehung von *Orwell* allerdings als übertriebene „Projektion von Ängsten“ kritisiert); *Schenke* 2013, 1077; *Vahle*, DVP 2012, 486, 486; *Maximini* 2010, 2 f.; *Vable*, DVP 2008, 444, 444; *Zilkens*, DuD 2007, 279, 279; *Gras* 2003, 5; *Roggan*, NVwZ 2001, 134, 134; *Woblfarth*, RDV 2000, 101, 101. Den „Orwellschen Überwachungsstaat“ erwähnt das OLG Stuttgart, NJW 2016, 2280, 2282. Mit Blick auf die biometrische Erkennung findet sich die Sorge vor einem Big Brother Szenario etwa in *Woodward* 1999, 395 („Biometric-Based Big Brother Szenario“). *Saeltzer*, DuD 2004, 218, 218 möchte „quantitativ abschätzen, unter welchen technischen Voraussetzungen eine Gesichts- und Personenerkennung jedes Bürgers mit intelligenten biometrischen Videoüberwachungssystemen, also *George Orwells* totale Überwachungsvision, in Deutschland (und anderswo) Alltag werden kann“. Auch im Zusammenhang mit dem Volkszählungsurteil (weiter unten) wird *George Orwell* bemüht, z.B. *Benda*, DuD 1984, 86, 87 u. *Krause*, JuS 1984, 268, 270.

117 Mit juristischem Blick auf das Buch *Uwer*, NJW 2009, 723 u. *Heussen*, AnwBl 2014, 458.

118 *Uwer*, NJW 2009, 723, 723 m.w.N.

en und Ostasien beherrscht wird.<sup>119</sup> Diese Mächte befinden sich in wechselnden Koalitionen in einem immerwährenden Krieg miteinander. Die Handlung des Romans spielt in Ozeanien, welches die Gebiete von Nord- und Südamerika, Großbritannien, Südafrika und Australien umfasst, und dessen Gesellschaft – hierin unterscheiden sich die drei Staaten nur unwesentlich voneinander – pyramidal aufgebaut ist. An der Spitze steht der Große Bruder, den zwar noch nie jemand in persona gesehen hat, der aber als unfehlbar, allgegenwärtig und ewig anzusehen ist.<sup>120</sup> Sein Gesicht findet sich auf Münzen, Briefmarken, Buchumschlägen, Zigarettenverpackungen und Transparenten. Tatsächlich geführt wird der Staat von der Partei, die sich in eine innere und eine äußere Partei unterteilt. Während die innere Partei etwa zwei Prozent der Bevölkerung ausmacht und die Oberschicht stellt, sind die Mitglieder der äußeren Partei mit mehr oder weniger anspruchsvollen Verwaltungsaufgaben beschäftigt. Den mit 85 Prozent größten Teil der Bevölkerung stellen die sogenannten Proles.

Oberstes Ziel der Partei ist der Machterhalt.<sup>121</sup> Der Krieg dient nicht der Vernichtung des Gegners, sondern der Zerstörung der Produkte menschlicher Arbeit, die ansonsten zur Steigerung des Lebensstandards der Bevölkerung eingesetzt werden könnten.<sup>122</sup> Er soll daher auch nicht gewonnen werden, er soll ewig andauern. Auf diese Weise wird die Bevölkerung in einem Zustand fortwährender Armut gehalten, so dass der alltägliche Kampf um banale Dinge wie Rasierklingen oder Kochgeschirr sie davon abhält, sich Gedanken über den Zustand der Gesellschaft zu machen. Hinzu tritt der durch die allgegenwärtige Propaganda geschürte Hass auf innere und äußere Feinde. Dieser Hass richtet sich nicht nur gegen den jeweiligen Kriegsgegner, sondern vor allem auch gegen eine Person namens Emmanuel Goldstein, der als „Urverräter“<sup>123</sup> an den Idealen der Partei dargestellt wird.

---

119 Die folgenden Angaben sind dem Roman entnommen, *Orwell* 2011.

120 Der Große Bruder (Big Brother) ist allwissend, allmächtig und allgegenwärtig, aber doch nur eine Fiktion, „eine Propagandamaschine der Macht“, *Uwer*, NJW 2009, 723, 725.

121 „Das Wohl anderer interessiert uns nicht; uns interessiert einzig die Macht.“, *Orwell* 2011, 315 f.

122 „Das Hauptziel der modernen Kriegsführung [...] besteht darin, die maschinellen Produkte zu verbrauchen, ohne den allgemeinen Lebensstandard zu heben.“, *Orwell* 2011, 227.

123 „Er war der Urverräter, der erste, der die Reinheit der Partei besudelt hatte.“, *Orwell* 2011, 19.

Um ihren absoluten Wahrheitsanspruch durchzusetzen, betreibt die Partei ein komplexes System zur Verfälschung der Geschichte. Mit großem Aufwand werden Zeitungen, Bücher und Fotografien beständig verändert, um sie der jeweiligen Parteilinie anzupassen, nicht eingetretene Vorhersagen zu korrigieren oder in Ungnade gefallene Personen zu tilgen. Die überholten Exemplare werden eingezogen und durch die geänderten Versionen ersetzt, so dass im Nachhinein niemand eine Fälschung nachweisen kann.<sup>124</sup> Von zentraler Bedeutung für den Wahrheitsanspruch der Partei ist aber das gedankliche Prinzip des Doppeldenk, dessen konsequente Anwendung von allen Parteimitgliedern erwartet wird. Doppeldenk ermöglicht es, bewusst Lügen zu erzählen und doch ehrlich daran zu glauben, die eigene Unfehlbarkeit zu propagieren und doch aus Fehlern zu lernen, mithin verschiedene widersprüchliche Überzeugungen aufrechtzuerhalten und den Widerspruch bewusst-unbewusst nicht zu sehen.<sup>125</sup> Je nach Bedarf kann demnach zwei und zwei vier, aber auch drei oder fünf oder alles gemeinsam ergeben. Mithin ist „bei jeder gedanklichen Operation [...] zugleich das Gegenteil mitzudenken, wobei das Bewusstsein der Gegensätzlichkeit gelöscht, gerade wie das Gegenteil gewusst, aber per angestrebter Denkoperation als nichtexistent angesehen wird“.<sup>126</sup>

Ein Synonym geworden ist *Orwells* 1984 aber vor allem für die dargestellten Überwachungstechniken. Die Überwachung betrifft dabei keineswegs die gesamte Einwohnerschaft Ozeaniens, sondern richtet sich in erster Linie gegen die (äußeren) Parteimitglieder. Die Proles werden weitestgehend sich selbst überlassen, da von ihnen aufgrund ihres geringen Bildungsstandes und ihrer beständigen Sorge um das eigene Überleben keine Bedrohung für die Herrschaft der Partei ausgeht.<sup>127</sup> Zur Überwachung der Parteimitglieder werden verschiedene Techniken und Methoden eingesetzt. Dies betrifft den Einsatz von Hubschraubern, um an den Fenstern der Menschen zu schnüffeln, das routinemäßige Öffnen von Briefen, den Einsatz versteckter Mikrofone sowie die Denunziation durch Arbeitskolle-

---

124 Folge ist ein Verlust historischer Faktizität, die von der Partei durch ihre Version der Geschichte ersetzt wird, *Uwer*, NJW 2009, 723, 725.

125 „Doppeldenk bedeutet die Fähigkeit, gleichzeitig zwei einander widersprechende Überzeugungen zu hegen und beide gelten zu lassen.“, *Orwell* 2011, 258.

126 *Uwer*, NJW 2009, 723, 726.

127 „Körperliche Schwerarbeit, die Sorge um Heim und Kinder, kleinliche Streitereien mit den Nachbarn, Kino, Fußball, Bier und vor allem Glücksspiel stecken ihren Denkhorizont ab.“ Da von ihnen keine Gefahr für die Partei ausgeht, werden sie kaum behelligt. Daher heißt es: „Proles und Tiere sind frei“, *Orwell* 2011, 89 f.

gen oder die eigene Familie. Gerade Kinder werden angeleitet, ihre Eltern zu bespitzeln und bei Verdacht anzuzeigen.<sup>128</sup> Auch kommen sogenannte Teleschirme zum Einsatz. Dabei handelt es sich um Fernsehgeräte, die sowohl empfangen als auch senden können. Auf öffentlichen Straßen und Plätzen sowie in den Wohnungen der Parteimitglieder installiert, ermöglichen sie nicht nur die Ausstrahlung von Propaganda, sondern auch die beständige (akustische und visuelle) Überwachung ihrer Umgebung. Jedes Geräusch, jede Bewegung kann registriert werden. Ob und wie häufig eine Überwachung tatsächlich stattfindet, ist allerdings nicht erkennbar. Da mit beständiger Überwachung zu rechnen ist, verhalten sich die Betroffenen aber so, als ob sie tatsächlich überwacht werden. Abschaltbar sind die Geräte nicht. So kann jeder „Bürger, oder zumindest jeder, der wichtig genug war, um beobachtet zu werden, [...] vierundzwanzig Stunden am Tag den Augen der Polizei und den offiziellen Propagandasendungen ausgeliefert werden“.<sup>129</sup>

Die Partei verlangt absoluten Gehorsam. Schwerstes denkbares Verbrechen ist das Gedankendelikt, mithin die gedankliche Abweichung von der Parteidoktrin. Verraten kann sich der Einzelne durch eine unbedachte Äußerung, einen falschen Gesichtsausdruck oder das Sprechen im Schlaf. Das Gedankendelikt schließt alle anderen Verbrechen in sich ein, es ist gewissermaßen ihre Grundlage, auch wenn formale Verbote nicht existieren, wie auch sonst keine Gesetze bestehen. Nichts ist ausdrücklich verboten, auch nicht Handlungen oder Gedanken, die bei Entdeckung mit Sicherheit den Tod zur Folge haben.<sup>130</sup> Dieser erschöpft sich nicht in der Tötung des Opfers, sondern bedeutet seine vollständige Auslöschung. Der Betroffene wird aus der Geschichte getilgt, so als habe er nie existiert. Er wird „varporisiert“ und zur Unperson. Dabei tötet die Partei den Abweichler nie, solange er noch verstockt ist. Sie will keine Märtyrer. Mittels Folter und Gehirnwäsche werden der Wille und die Persönlichkeit des Betroffe-

---

128 Ein Kind, das seine Eltern denunziert, wird in der Presse als „Kinderheld“ bezeichnet, *Orwell* 2011, 33.

129 *Orwell* 2011, 248.

130 „Jetzt wollte er ein Tagebuch beginnen. Das war nicht illegal (nichts war illegal, denn es gab ja keine Gesetze mehr), aber wenn es herauskam, durfte man ziemlich sicher mit der Todesstrafe oder zumindest mit fünfundzwanzig Jahren Zwangsarbeitslager rechnen.“, *Orwell* 2011, 13. Dieser Zustand hat dann auch zur Folge, dass Juristen nicht mehr gebraucht werden, *Uwer*, NJW 2009, 723, 724. Eine unangenehme Vorstellung.

nen gebrochen, um ihm echte Liebe zum Großen Bruder einzugeben. Erst dann wird er getötet.<sup>131</sup>

*Orwells 1984* ist bei alledem kein technisches Buch. Weder in Ozeanien noch in den beiden anderen Großmächten findet echter technologischer Fortschritt statt. Das wissenschaftlich-technische Niveau befindet sich auf dem Stand der 1950er Jahre. Geforscht wird nur noch auf dem Gebiet der Kriegsführung, aber auch hier werden keine wirklichen Ergebnisse erzielt. Insoweit ist es auch nicht vorstellbar, dass in *Orwells Ozeanien* Überwachungsmittel wie die biometrische Gesichtserkennung, die Vorratsdatenspeicherung, die Online-Durchsuchung oder der genetische Fingerabdruck hervorgebracht werden. Als technische Blaupause für den modernen Überwachungsstaat taugt *Orwells 1984* mithin nicht.

So sehr die Beschäftigung mit *Orwells 1984* die Fantasie anzuregen und Assoziationen zu wecken vermag, so sehr unterscheiden sich aber auch die politischen, gesellschaftlichen und rechtlichen Gegebenheiten der Bundesrepublik Deutschland – und anderer westlicher Staaten – von denen in Ozeanien. Während in Deutschland die Würde des Menschen „tragendes Konstitutionsprinzip und oberster Verfassungswert“ ist,<sup>132</sup> ist die Sichtweise in Ozeanien eine andere: „Wenn Sie ein Bild von der Zukunft haben wollen, dann stellen Sie sich einen Stiefel vor, der auf ein Gesicht tritt – unaufhörlich.“<sup>133</sup> Selbst wenn also die technischen Überwachungsszenarien aus *Orwells 1984* in Deutschland realisierbar sind – oder vor dem Hintergrund der technischen Entwicklung sogar noch übertroffen werden können –, so weichen doch die politischen und gesellschaftlichen Rahmenbedingungen deutlich voneinander ab.

Dystopien wie *Orwells 1984* spiegeln die Ängste ihrer Zeit wieder.<sup>134</sup> Bei *George Orwell* betrifft dies vor allem die Erfahrungen mit den totalitären und menschenverachtenden kommunistischen und nationalsozialistischen Regimen in der ersten Hälfte des 20. Jahrhunderts. Dass sich in absehbarer Zeit eine mit Ozeanien vergleichbare Staats- und Regierungsform auf

---

131 „Wir vernichten den Ketzler nicht, weil er uns Widerstand leistet: solange er uns Widerstand leistet, vernichten wir ihn nie. Wir bekehren ihn [...] bevor wir ihn töten. [...] Sogar im Angesicht des Todes dürfen wir keine Abweichung dulden.“, *Orwell 2011*, 306.

132 BVerfGE 109, 279 (311).

133 *Orwell 2011*, 321.

134 *Strasser 2006*, 12. Ähnlich *Bull*, JZ 2017, 797, 797, der in einer Berufung auf *Orwell* eine „Projektion von Ängsten [sieht], die ohne Rücksicht auf die rechtlichen und die tatsächlichen sozialen und politischen Verhältnisse nur aus technischen Möglichkeiten abgeleitet sind“.

deutschem Boden etabliert, ist sehr unwahrscheinlich. Auch unterscheidet sich die Struktur der in Deutschland bestehenden Überwachung deutlich von der in *Orwells* Ozeanien. Die Videoüberwachung am Bahnhof, im Supermarkt oder in der Bankfiliale ist nicht von einem böswilligen Staat im Sinne totaler Kontrolle erdacht,<sup>135</sup> sondern das Ergebnis verschiedener Einzelentscheidungen der Bundespolizei, des Supermarktbetreibers oder der Filialleiterin. Diese Maßnahmen zielen nicht darauf ab, dem Ideal des Großen Bruders nachzueifern.<sup>136</sup>

### 1.3.3 Der Weg in die Überwachungsdemokratie?

Schon eher realistisch ist die Befürchtung, dass sich die liberalen westlichen Demokratien auf dem Weg zur „Überwachungsdemokratie“ befinden.<sup>137</sup> Überwachung verfolgt, wie sich schon bei *Bentham* gezeigt hat, nicht zwangsläufig schlechte Ziele und muss nicht zwingend dem Machterhalt einer pervertierten politischen Klasse dienen. Moderne Überwachungstechnologien können einen Beitrag zur Bekämpfung von Kriminalität leisten und die Sicherheit der Bevölkerung fördern. Dies ist grundsätzlich zu begrüßen. Sie können aber auch mit den Rechten der Bürger in Konflikt geraten.<sup>138</sup> Das verfassungsrechtliche Freiheitsverständnis in Deutschland ist geprägt von den Grundrechten, die als Abwehrrechte<sup>139</sup> gegen staatliches Handeln fungieren. Bestimmte Maßnahmen sind daher von vornherein untersagt (z.B. Beeinträchtigungen der Menschenwürde<sup>140</sup>), andere nur eingeschränkt zulässig. Das bedeutet auch, dass sich der Staat bewusst verschiedener Möglichkeiten „beraubt“, zu wissen oder wissen zu können. Dies kann als „Selbstblendung“ des Staates bezeichnet werden.<sup>141</sup>

---

135 Und sie ist auch nicht auf einen böartigen Großen Bruder zurückzuführen, *Henatsch* 2007, 23.

136 *Zurawski* 2011, 11. *Der Bundesbeauftragte für den Datenschutz* 1999, 12 verweist darauf, dass es „keinen allmächtigen Big Brother“ gibt, sondern „viele kleinere Brüder“; ähnlich sprechen *Singelstein/Stolle* 2012, 158 von „einer Vielzahl von kleineren und größeren Geschwistern“.

137 *Strasser* 2006, 12.

138 Zu diesem Spannungsverhältnis s. Kap. 5.1.

139 Dazu s. Kap. 5.1.2.1.

140 Zur Beeinträchtigung der Menschenwürde nach deutschem Verständnis s. Kap. 5.2.1.1.2.

141 *Strasser* 2006, 17.

Die Idee der „Überwachungsdemokratie“ besteht nun darin, dass der Staat derartige Beschränkungen zurückdrängt und alle verfügbaren Technologien einsetzt, um die Sicherheit der Bürger zu gewährleisten.<sup>142</sup> Entgegenstehende Individualrechte werden dann vor allem als Behinderung der staatlichen Sicherheitsorgane wahrgenommen: Wer nichts zu verbergen hat, der hat ja auch nichts zu befürchten! Politiker, die mit markig-ironischen Worten an die Vernunft appellieren, sinnvolle Überwachungsmaßnahmen doch nicht durch kleingeistige rechtliche Bedenken zu verhindern, können sich nicht selten der Zustimmung der Zuhörer sicher sein.<sup>143</sup> So ist der Vorwurf, Datenschutz sei „Täterschutz“, wahrscheinlich so alt wie der Gedanke des Datenschutzes an sich.<sup>144</sup> Mithin besteht die Gefahr, dass die Rechte des Einzelnen in immer stärkerem Maße hinter das Erfordernis einer effektiven Bekämpfung von Kriminalität und Terrorismus zurückzutreten haben. Auf diese Weise könnte ein „sanfter Überwachungsstaat“<sup>145</sup> entstehen, der für jede einzelne Maßnahme gute Gründe anführen kann, sich aber in der Gesamtheit in einer immer weiter ausufernden Überwachung verliert.

Hinzu tritt die Gefahr, dass die bestehenden Überwachungstechnologien und Informationssammlungen im Falle eines grundlegenden gesellschaftlichen und politischen Wandels in die Hände eines „Law-&-Order-Staates“<sup>146</sup> geraten, der sich bei ihrem Gebrauch keinerlei Beschränkungen unterworfen sieht. Datenschützer sollten daher beim Ausmalen zukünftiger Szenarien nicht zu zimperlich sein.<sup>147</sup> Vor allem aber sollten sie den Vorwurf nicht scheuen, sie seien „über ein vernünftiges Maß hinaus aktivierte Hypochonder“. <sup>148</sup> In diesem Zusammenhang ist *Orwells* 1984 nicht als eine bisher nicht eingetretene „zukunftsgehemte Prophezeiung“, sondern als eine Mahnung vor den Gefahren totalitärer Verhältnisse zu verstehen,<sup>149</sup> als eine Warnung vor einem Willkür- und Überwachungsstaat als

---

142 *Strasser* 2006, 19.

143 Z.B. bei *Dix* 2008, 151 f. zu der Aussage von *Otto Schily*, die Würde des Fingerabdrucks sei nicht unantastbar.

144 Z.B. *Der Landesbeauftragte für den Datenschutz Bremen* 1983, 5 f. zur Diffamierung, Behinderung, Einschüchterung und Entmachtung der Datenschützer; bei *Schneider* 1983, 95 zu dem Vorwurf, „Datenschutz gleich Täterschutz“. Zum Datenschutz als „leichte Beute“ sowie als „Täterschutz“ bei *Dix* 2008, 149 ff.

145 *Strasser* 2006, 23.

146 *Strasser* 2006, 20.

147 *Strasser* 2006, 20.

148 *Gaycken* 2008, 27. Sie haben der „Rotz am Ärmel“ der Mächtigen zu sein, *Brink*, *PinG* 2014, 15, 17.

149 *Erzgräber* 1983, 31.

dem Ergebnis menschlicher Entscheidungen.<sup>150</sup> Seine Fiktion ist geeignet, starke Assoziationen zu wecken und „ein Gefühl des Ausgeliefert-Seins“<sup>151</sup> gegenüber einer übermächtigen Überwachungsmaschinerie zum Ausdruck zu bringen. In den Worten des ehemaligen Präsidenten des Bundeskriminalamts *Horst Herold*: „Die Gefahren des ‚großen Bruders‘ sind nicht mehr bloß Literatur. Sie sind nach dem heutigen Stand der Technik real.“<sup>152</sup> Das bedeutet aber nicht, dass sie sich auch tatsächlich realisieren.<sup>153</sup> Nicht hinter jeder Überwachungskamera ist ein Großer Bruder verborgen.

#### 1.4 *Recht und Überwachung: Das Bundesverfassungsgericht und das Recht auf informationelle Selbstbestimmung*

Zumindest in einem Rechtsstaat, wie die Bundesrepublik Deutschland einer ist (Art. 20 Abs. 3 GG und Art. 28 Abs. 1 Satz 1 GG), haben beim Einsatz von Überwachungstechnologien nicht die Schriftsteller, Ingenieure, Soziologen oder Philosophen, sondern die Juristen – genauer gesagt die Gerichte – das letzte Wort. Nahezu jede (staatliche) Überwachungstechnologie wird früher oder später Gegenstand eines Gerichtsverfahrens, wobei zu guter Letzt das Bundesverfassungsgericht<sup>154</sup> dazu berufen ist, grundlegende Anforderungen an ihren Einsatz zu formulieren.<sup>155</sup> Entscheidungen des Bundesverfassungsgerichts finden sich daher unter anderem zur Überwachung der Telekommunikation, zur akustischen Wohnraumüberwachung, zur Überwachung der Bewegungen eines Fahrzeugs mittels eines GPS-Empfängers, zum Einsatz elektronischer Rasterfahndung, zur Videoüberwachung des öffentlichen Raums, zur Durchführung von Online-Durchsuchungen, zur automatisierten Kennzeichenerkennung, zur Vorratsdatenspeicherung sowie zur Errichtung einer Antiterrordatei.<sup>156</sup>

---

150 *Uwer*, NJW 2009, 723, 726.

151 *Klein* 2011, 94.

152 *Horst Herold*, zitiert nach: *Sternsdorff*, Der Spiegel 1983, Heft 2, 46, 46.

153 Als „Farce“ wurde *Orwells Big Brother* bereits im Fernsehen aufgeführt, *Heussen*, AnwBl 2014, 458, 461.

154 Ggf. auch der EuGH.

155 Dies betont *Hornung* 2008, 251.

156 BVerfGE 100, 313 (Telekommunikationsüberwachung); BVerfGE 109, 279 (akustische Wohnraumüberwachung); BVerfGE 112, 304 (GPS-Empfänger); BVerfGE 115, 320 (Rasterfahndung); BVerfG, NVwZ 2007, 688 (Videoüberwachung öffentlicher Räume); BVerfGE 120, 274 (Online-Durchsuchungen); BVerfGE 120, 378 (automatisierte Kennzeichenerkennung); BVerfGE 125, 260

Der Einsatz moderner Überwachungstechnologien durch die Polizei ist regelmäßig mit der Erhebung und Verarbeitung von Informationen verbunden. Die erfolgreiche Bekämpfung von Straftaten bedarf – zur rechten Zeit an der rechten Stelle – ausreichender Informationen über Tatumstände, Täter, Zeugen und Opfer.<sup>157</sup> Dementsprechend besteht polizeiliches Handeln zu großen Teilen aus dem Sammeln und Verarbeiten von Informationen. Der Umgang mit Informationen ist mithin zentral für die polizeiliche Aufgabenerfüllung.<sup>158</sup>

Bei diesen Informationen wird es sich regelmäßig um personenbezogene Daten, also um Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 3 Nr. 1 JI-RL, § 46 Nr. 1 BDSG), handeln. Dazu zählen auch Videoaufnahmen, wenn sie Personen identifizierbar erfassen.<sup>159</sup> Die Erkenntnis, dass der Umgang mit derartigen Daten von erheblicher rechtlicher Relevanz ist und in die Grundrechte betroffener Personen eingreifen kann, geht maßgeblich auf das Volkszählungsurteil<sup>160</sup> des Bundesverfassungsgerichts aus dem Jahr 1983 – mithin kurz vor dem Zeitpunkt der Handlung in *Orwells* 1984 – zurück. In diesem Urteil hat das Bundesverfassungsgericht aus dem grundrechtlich verbürgten Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein Recht auf informationelle Selbstbestimmung abgeleitet, das die „die Befugnis des Einzelnen [schützt], grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.<sup>161</sup> Ein solcher Schutz findet sich inzwischen zwar auch im Unionsrecht (z.B. Art. 8 GRCh) und in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zu Art. 8 EMRK.<sup>162</sup> Dennoch ist das Bundesverfassungsgericht hier als Vorreiter anzusehen.

Das Volkszählungsurteil baut dabei auf Gedanken auf, die sich auch bei *George Orwell* finden. Mit Blick auf die Teleschirme heißt es bei *Or-*

---

(Vorratsdatenspeicherung); BVerfGE 133, 277 (Errichtung einer Antiterrordatei).

157 Zöller 2002, 135 u. 139.

158 Letztlich ist jede Verwaltungstätigkeit zu großen Teilen Informationsverarbeitung, Gusy 2012, Rn. 1 u. Holznel 2012, Rn. 1. Dies gilt auch für die polizeiliche Tätigkeit, s. bei Lisken/Denninger-Schwabenbauer, Kap. G Rn. 1 ff. zur Gefahrenabwehr und Strafverfolgung als Daten- und Informationsverarbeitung.

159 Zum Personenbezug von Bild- u. Videoaufnahmen s. Kap. 5.2.1.1.2.1 (für das deutsche Recht).

160 BVerfGE 65, 1.

161 BVerfGE 65, 1 (43).

162 Dazu s. Kap. 5.2.1.2.1 (EMRK) u. Kap. 5.2.1.3.1 (GRCh).

*well*: „Man konnte natürlich nie wissen, ob man im Augenblick gerade beobachtet wurde oder nicht. Wie oft oder nach welchem System sich die Gedankenpolizei in jede Privatleitung einschaltete, darüber ließ sich bloß spekulieren. Es war sogar denkbar, daß sie ständig alle beobachtete. Sie konnte sich jedenfalls jederzeit in jede Leitung einschalten. Man mußte folglich in der Annahme leben – und tat dies auch aus Gewohnheit, die einem zum Instinkt wurde –, daß jedes Geräusch, das man verursachte, gehört und, außer bei Dunkelheit, jede Bewegung beäugt wurde.“<sup>163</sup> Das Bundesverfassungsgericht formulierte im Jahr 1983 ähnlich: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“<sup>164</sup>

Sowohl das Bundesverfassungsgericht als auch *George Orwell* – und *Jeremy Bentham* – gehen also davon aus, dass bereits die als möglich erachtete Überwachung Auswirkungen auf das Verhalten betroffener Personen haben kann. Um dem Betroffenen zumindest ein Stück weit die Kontrolle über die Erhebung, Verarbeitung und Nutzung der ihn betreffenden Informationen zu ermöglichen, gewährleistet das Recht auf informationelle Selbstbestimmung „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.<sup>165</sup> Gewiss hat sich das Bundesverfassungsgericht bei der Konzeption des Rechts auf informationelle Selbstbestimmung nicht (primär) an *Orwells* Dystopie, sondern an den Entwicklungslinien seiner eigenen Rechtsprechung<sup>166</sup> sowie an verschiedenen Vorarbeiten (v.a. denen von

---

163 *Orwell* 2011, 9.

164 BVerfGE 65, 1 (43).

165 BVerfGE 65, 1 (43).

166 Dazu BVerfGE 65, 1 (41 f.).

Steinmüller<sup>167</sup>) orientiert.<sup>168</sup> Trotzdem ist anzunehmen, dass die dystopischen Überlegungen *Orwells* das Urteil zumindest mittelbar beeinflussen haben. Das dem Urteil zugrundeliegende Volkszählungsgesetz rief massive Proteste in der Bevölkerung hervor, die zum Teil unmittelbar an *Orwells* 1984 anknüpften<sup>169</sup> und die, obwohl sie auf so manchen (ausländischen) Beobachter einen überzogenen Eindruck machten,<sup>170</sup> wahrscheinlich auch Einfluss auf die Entscheidung des Gerichts hatten.<sup>171</sup>

Das Recht auf informationelle Selbstbestimmung ist als Antwort auf die Gefahren der modernen Datenverarbeitung zu verstehen. Diese zeigen sich nach Auffassung des Bundesverfassungsgerichts darin, dass Informationen „technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind“. Überdies können sie „mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden“. Auf diese Weise entstehen neue Möglichkeiten der Einsichtnahme und Einflussnahme, die der Einzelne nur noch schwer kontrollieren oder auch nur überblicken kann.<sup>172</sup> Das Recht auf informationelle Selbstbestimmung soll unter diesen Bedingungen nicht nur die selbstbestimmte Entwicklung des Einzelnen schützen, sondern ist auch Grundlage einer freien und demokratischen Kommunikationsordnung.<sup>173</sup>

Dies bedeutet aber nicht, dass dem Einzelnen eine absolute, uneingeschränkte Herrschaft über „seine“ Daten zukommt. Das Grundrecht auf informationelle Selbstbestimmung wird nicht schrankenlos gewährleistet. Überwiegende Interessen der Allgemeinheit können die Erhebung, Verarbeitung und Nutzung personenbezogener Daten auch gegen den Willen des Betroffenen rechtfertigen.<sup>174</sup> Zu diesen überwiegenden Interessen

---

167 Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider 1971 (veröffentlicht in BT-Drs. VI/3826).

168 Zur Herleitung des Rechts auf informationelle Selbstbestimmung s. Kap. 5.2.1.1.1.1.

169 So z.B. in einem Leserbrief an die Wochenzeitung *Die Zeit*: „Erschreckende Parallelen deuten sich bei der geplanten Volkszählung zu George Orwells Visionen von 1984 an. Wer die Möglichkeit der Eskalation der totalen Erfassung kennt, sollte ihren Anfängen wehren, zur Erhaltung der Individualität und gegen mehr Staat.“, zitiert nach *Erzgräber* 1983, 12.

170 Lewy 1983, 62.

171 Hornung 2008, 252.

172 BVerfGE 65, 1 (42).

173 *Roßnagel*, Informatik Spektrum 2005, 462, 463 f.

174 BVerfGE 65, 1 (43 f.).

kann auch die Verhinderung und Verfolgung von Straftaten gehören.<sup>175</sup> So betont das Bundesverfassungsgericht die „unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung und Verbrechensbekämpfung“<sup>176</sup> und stellt fest, dass „die Sicherung des Rechtsfriedens durch Strafrecht [...] seit jeher eine wichtige Aufgabe staatlicher Gewalt“ ist.<sup>177</sup>

Wird also der (vermeintlich) harmlose Zugreisende<sup>178</sup> zur Verhinderung oder Verfolgung von Straftaten von der Polizei videoteknisch erfasst, beeinträchtigt dies sein Grundrecht auf informationelle Selbstbestimmung. Es stellt sich sodann die Frage, ob der verfolgte Zweck dies zu rechtfertigen vermag. Dabei ist zu berücksichtigen, dass grundrechtseingreifende Maßnahmen nur aufgrund einer gesetzlichen Grundlage, die wiederum dem Bestimmtheitsgebot und dem Grundsatz der Verhältnismäßigkeit genügt, erfolgen dürfen.<sup>179</sup> Überdies sind bestimmte letzte Grenzen (z.B. die Menschenwürde) einzuhalten. Dass die „Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“, ist Ausdruck der „verfassungsrechtlichen Identität der Bundesrepublik Deutschland“.<sup>180</sup> Hier einen angemessenen Ausgleich herzustellen, ist in erster Linie Aufgabe des demokratisch legitimierten Gesetzgebers, wobei das Bundesverfassungsgericht eine Reihe von Vorgaben entwickelt hat, die dabei zu berücksichtigen sind.

### 1.5 Recht und Technik

Dass das Bundesverfassungsgericht mit dem Volkszählungsurteil auf den technologischen Fortschritt und die damit einhergehenden Gefahren reagiert hat, wirft ein Schlaglicht auf das Verhältnis von Recht und Technik.<sup>181</sup>

---

175 Zur Bedeutung der Verhinderung und Verfolgung von Straftaten s. Kap. 5.1.1.

176 BVerfGE 100, 313 (389).

177 BVerfGE 107, 104 (118).

178 S. Kap. 1.1.

179 Z.B. BVerfGE 65, 1 (44) u. BVerfGE 120, 378 (401).

180 BVerfGE 125, 260 (324).

181 Zum Recht im technischen Zeitalter *Huber* 1971, 57 ff. Zum Verhältnis von Recht und Technik vor dem Hintergrund der Kernenergie-debatte *Roßnagel* 1984, 13 ff. u. *Lukes*, NJW 1978, 241; mit Blick auf die Verfassungsverträglichkeit der Informations- u. Kommunikationstechnik *Roßnagel/Wedde/Hammer/Pordesch* 1990; bezogen auf die Informationsgesellschaft und das Internet *Roßnagel* 2003, 423 ff.; zu den Problemen des Gesetzgebers *Ossenbühl* 2000; zur Technik-

Technische Neuerungen können neue rechtliche Regelungen erforderlich machen, da sie zu vorher nicht möglichen Verhaltensweisen befähigen. Sie können aber auch auf den Bedeutungsgehalt bestehender Regelungen einwirken. Konkret kann dies etwa bedeuten, dass die technische Vereinfachung polizeilicher Ermittlungsmaßnahmen Einfluss auf die Verhältnismäßigkeit der einzelnen Maßnahmen nimmt. Abstrakter gesprochen können technische Neuerungen „die faktischen Verwirklichungsbedingungen des Rechts“ verändern, indem sie die sozialen oder gesellschaftlichen Verhältnisse beeinflussen.<sup>182</sup> Rechtliche Vorgaben, Anreize oder Grenzziehungen wiederum können die Entwicklung oder den Einsatz neuer Techniken begünstigen oder verhindern. Recht und Technik sind also auf vielfältige Weise miteinander verbunden.<sup>183</sup>

### 1.5.1 Grundsätzlicher Gegensatz zwischen Recht und Technik?

In der Literatur wird es als „fast schon trivial [bezeichnet], dem rechtlichen Regelungssystem sein Zurückbleiben hinter der Dynamik des technischen Prozesses vorzuhalten“.<sup>184</sup> Die technische Entwicklung schreitet voran und zwingt das Recht (bzw. die das Recht setzenden Instanzen) zu einer Reaktion. Dies zeigt sich beispielhaft an der Entwicklung des Internets, die den Gesetzgeber mit der Frage konfrontiert hat, ob und wie dieses „Neuland“ zu regulieren ist.<sup>185</sup> Das „Hinterherhinken“ des Gesetzgebers hinter der technischen Entwicklung weist dem Juristen dabei nicht selten die Rolle des „stauenden Zuschauers“ zu.<sup>186</sup> Gerade im Bereich des Datenschutzes ist zu beobachten, dass die rechtliche Regulierung nicht mit der technischen Entwicklung Schritt hält und auf Neuerungen nur unzureichend zu reagieren vermag.<sup>187</sup>

---

folgenforschung *Roßnagel* 1997, 139 ff. u. *Roßnagel* 1993; zur „Allianz“ von Recht und Technik *Roßnagel* 2001, 17 ff. u. *Roßnagel*, DuD 1999, 253, 255.

182 *Hornung* 2005, 87. *Roßnagel* 1997, 139 f. verweist auf ISDN-Telekommunikationsanlagen, bei denen der Angerufene aus technischen Gründen nicht entscheiden konnte, ob er Name und Nummer mitsendet, so dass sein Persönlichkeitsrecht von den technischen Einstellungen der ISDN-Anlagen abhängig war.

183 *Hornung* 2005, 87.

184 *Neumann* 1984, 88.

185 Zu den Anfängen der Regulierung in Deutschland *Roßnagel*, DuD 1999, 253 bezogen auf das TDDSG.

186 *Berg*, JZ 1985, 401, 401.

187 Z.B. *Roßnagel/Pfitzmann/Garstka* 2001, 22 ff. zum alten BDSG. Dieser Gedanke kommt auch in EwG 6 DSGVO zum Ausdruck: „Rasche technologische Ent-

Prägend für das Verhältnis von Recht und Technik ist zunächst der Umstand, dass es sich sowohl beim Recht als auch bei der Technik um vielschichtige Gebilde handelt.<sup>188</sup> Ein allgemein hin akzeptierter Begriff des Rechts ist schwierig zu finden.<sup>189</sup> Einigkeit besteht aber darin, dass unter dem Recht eine Ordnung zu verstehen ist, die das Zusammenleben der Menschen regelt.<sup>190</sup> Mithin bedarf erst die menschliche Gesellschaft, also das Zusammensein mehrerer Personen, einer solchen Ordnung.<sup>191</sup> Dabei kommt dem Recht die Aufgabe zu, ordnend auf die gesellschaftliche Entwicklung einzuwirken, Rechte und Freiheiten der Bürger zu schützen und Allgemeininteressen zu verwirklichen.<sup>192</sup> Im Kern sind die dafür erforderlichen Regelungen – zumindest in einem demokratischen Staatswesen – Festlegungen des demokratischen Souveräns<sup>193</sup> und damit Ausdruck des Versuchs der Gesellschaft, ihre Entwicklung selbst zu gestalten. Unzumutbare Freiheitseingriffe sollen abgewehrt, (legitime) Interessen geschützt und Regeln zur Lösung von Konflikten angeboten werden.<sup>194</sup>

Technik hingegen ist vom Grundsatz her auf die Naturgesetze bezogen.<sup>195</sup> Allerdings greift es zu kurz, Technik lediglich als den Einsatz von Naturkräften zu verstehen. Technik ist ein vielschichtiger und komplizierter Bereich menschlichen Handelns, der mit anderen Sozialphänomenen verzahnt ist.<sup>196</sup> In diesem Zusammenhang kann von soziotechnischen Systemen<sup>197</sup> gesprochen werden, worin der Gedanke zum Ausdruck

---

wicklungen und die Globalisierung haben den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. [...] Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert [...].“ Der europäische Gesetzgeber hat darauf mit dem Erlass der DSGVO reagiert.

188 So zum Recht *Zippelius* 2011, 1; zur Technik *Roßnagel* 1984, 13.

189 Zum Begriff des Rechts und den verschiedenen Ansätzen ausführlich *Zippelius* 2011, 3 ff.

190 *Zippelius* 2011, 3.

191 *Berg*, JZ 1985, 401, 403 u. 404.

192 *Roßnagel* 2001, 18. *Roßnagel* 1984, 14 spricht von der „Aufgabe, Tatbestände des Soziallebens unter den Zielen der Rechtssicherheit, der Freiheitssicherung und des Gemeinwohls dauerhaft zu ordnen“. Zu den Funktionen des Rechts auch bei *Horn* 2016, Rn. 33 ff.

193 In Dtl. ist dies das Volk, das von gewählten Abgeordneten repräsentiert wird, Art. 20 Abs. 2, 38 Abs. 1 GG.

194 *Roßnagel* 2001, 18.

195 *Berg*, JZ 1985, 401, 403.

196 *Roßnagel* 1984, 13.

197 Der Begriff geht auf Arbeiten des Tavistock Institute of Human Relations in den 1950er Jahren zurück. Ein Überblick über die Entwicklung und Verbreitung

kommt, dass Technik nie für sich allein steht, sondern in menschliches Handeln und menschliche Interaktionen eingebunden ist. Eine genaue Bestimmung des Begriffs der Technik ist daher ähnlich schwierig wie eine Begriffsfindung im Bereich des Rechts. Jedenfalls ist moderne Technik „ihrem Wesen nach auf Ursache und Wirkung, auf Entdeckung und Erfindung bezogen“. Richtig ist, was machbar ist und funktioniert.<sup>198</sup> Sie ist durch ein hohes Maß an Dynamik gekennzeichnet und befindet sich gewissermaßen in einem Zustand der „permanenten Revolution“.<sup>199</sup>

Hierin ist einer der zentralen Gründe für die (teilweise) „wesensmäßige Unvereinbarkeit“<sup>200</sup> von Recht und Technik zu verorten. Technik ist auf beständigen Fortschritt, das Recht auf Beständigkeit angelegt,<sup>201</sup> denn „erfüllt von Vergangenheit will das Recht [bzw. der hinter dem Recht stehende Gesetzgeber<sup>202</sup>] aus der Gegenwart heraus schon dem künftigen menschlichen Verhalten Richtung weisen. Soll soziale Ordnung erzielt werden, so dürfen die Rechtsnormen nicht allzu flüchtig sein. Menschliches Tun und Lassen muss für eine längere Dauer denselben Regeln unterworfen sein. Neuem Recht müssen die Menschen sich angewöhnen, sie müssen es in ihr Bewußtsein aufnehmen können, es muss unter ihnen glaubhaft werden. Sodann will<sup>203</sup> das Recht immer auch stabilisieren und erhalten. Ununterbrochener Revisionismus und ungehemmter Voluntarismus – die permanente Revolution – sind ihm zuwider.“<sup>204</sup>

Diese Fokussierung auf die Beständigkeit des Rechts mag zwar in mancher Hinsicht als zu kurz gegriffen erscheinen, da rechtliche Regulierung auch eine explizit innovationsfördernde- oder steuernde, also auf Veränderung ausgerichtete Zielsetzung aufweisen kann (etwa durch monetäre Anreize in Form von Steuern oder Subventionen; zu denken ist z.B. an die Kohlenstoffdioxid-Steuer, die unter anderem Anreize für die Entwicklung

---

findet sich bei *Mumford*, *Information Systems Journal* 2006, 317 u. *Mumford* 2000, 33 ff.

198 *Roßnagel* 1984, 13 f.

199 *Ossenbühl* 2000, 12.

200 *Ossenbühl* 2000, 12.

201 *Ossenbühl* 2000, 12; ebenfalls *Roßnagel* 1984, 13 f.

202 Das Recht selber „will“ gar nichts. Ihm kommen bestimmte Funktionen zu und es wird von bestimmten Personen bzw. Institutionen, z.B. den Abgeordneten des Bundestages, zur Erreichung bestimmter Ziele gesetzt. „Wollen“ tun also diejenigen, die das Recht setzen.

203 Auch hier gilt, dass nicht das Recht etwas „will“, sondern der dahinterstehende Gesetzgeber.

204 *Huber* 1971, 69. Darauf verweist auch *Roßnagel* 1984, 14.

emissionsarmer technischer Verfahren setzen soll).<sup>205</sup> Hierdurch sollen sinnvolle Innovationen ermöglicht, schädliche Innovationen vermieden und Innovationen allgemein so gesteuert werden, dass das Kosten-Nutzen-Verhältnis optimiert wird. Doch sind auch derartige Regelungen das Ergebnis eines oft mühevollen und langwierigen Aushandlungsprozesses. Sie sollen regelmäßig nicht sofort wieder geändert werden, da gesellschaftliche Akteure (z.B. Unternehmen oder Forschungseinrichtungen) ansonsten keinerlei Planungssicherheit hätten, was wiederum das Erreichen der mit der Regulierung verfolgten Ziele in Frage stellen würde. Auch das innovationsfördernde Recht ist daher auf Beständigkeit angewiesen.<sup>206</sup>

Die dynamische Technik auf der einen und das auf Beständigkeit ausgerichtete Recht auf der anderen Seite stehen also in einem Widerspruch zueinander. Das Recht hält „nicht Schritt“ mit der technischen Entwicklung,<sup>207</sup> es hat eine „notorische Verspätung“<sup>208</sup> und befindet sich selten auf „Ballhöhe“<sup>209</sup> mit dem technischen Fortschritt. Die Technik steigert beständig die menschlichen Handlungsmöglichkeiten.<sup>210</sup> Die Dampfmaschine erlaubte die Bewegung von Lasten, die die menschlichen Kräfte weit übersteigen, während Kraftfahrzeuge Reisezeiten drastisch verkürzten. Die sich mit „explosionsartiger Wucht“<sup>211</sup> entwickelnde Informations- und Kommunikationstechnologie schafft neue Möglichkeiten, Informationen zu erheben, zu übermitteln und auszuwerten. Informationen können inzwischen nahezu unbegrenzt gespeichert, in Sekundenschnelle abgerufen und zu (Persönlichkeits-)Profilen zusammengefügt werden.<sup>212</sup> Hierdurch werden auch neue Möglichkeiten staatlicher Überwachung geschaffen.

---

205 Zur innovationsfördernden Regulierung *Eifert/Hoffmann-Riem* 2009. Das Recht kann einen Rahmen schaffen, technische Innovationen zu unterstützen und „Innovationskorridore“ zu ebnet, *Roßnagel* 2001, 25 ff.

206 Dies entspricht auch der Funktion des Rechts, Rechtssicherheit zu gewährleisten, die bei sich ständig ändernden Rechtsregeln in Frage steht. Zur Rechtssicherheit als Funktion des Rechts *Horn* 2016, Rn. 35 (dort unter dem Oberpunkt der Freiheitsordnung).

207 *Lukes*, NJW 1978, 241, 241 bezogen auf das technische Sicherheitsrecht.

208 *Ossenbühl* 2000, 12 f.

209 *Roßnagel* 2001, 19.

210 *Ossenbühl* 2000, 10.

211 *Berg*, JZ 1985, 401, 401. Diese Aussage aus dem Jahr 1985 ist auch heute noch zutreffend. Zur Entwicklung der computergestützten Informationsverarbeitung, v.a. mit Blick auf Speicherkapazität und Rechenleistung, vom Jahr 1990 zum Jahr 2000 sowie mit einer aus damaliger Sicht in die Zukunft gerichteten Erwartung für das Jahr 2010 bei *Roßnagel/Pfitzmann/Garstka* 2001, 223 ff.

212 So bereits BVerfGE 65, 1 (42).

Nicht nur die Rasterfahndung oder die Online-Durchsuchung, sondern auch die Videoüberwachung ist ein Ergebnis dieser Entwicklung. Biometrische Gesichtserkennung soll die Auswertung umfangreicher Bild- und Videoaufnahmen unterstützen. Eine solche Auswertung ist zwar auch ohne Gesichtserkennung möglich, kann sich aber als sehr zeit- und personalintensiv erweisen. Das Recht (bzw. der Gesetzgeber) steht damit vor der Aufgabe, sich mit diesen Entwicklungen auseinanderzusetzen und angemessen darauf zu reagieren.

Die wesensmäßige Verschiedenheit von Recht und Technik mag auch der Grund dafür sein, dass sich die Vertreter von Recht und Technik mit einem gewissen Misstrauen begegnen. Während die Juristen befürchten, dass die technische Entwicklung die Grundprinzipien des Rechts untergräbt und rechtliche Ziele und Schutzaufträge gefährdet,<sup>213</sup> sehen (zumindest einige) Techniker (Ingenieure, Informatiker etc.) in dem Recht vor allem eine Behinderung ihrer Arbeit aufgrund rechtlicher Eingrenzungsversuche.<sup>214</sup> Ähnlich denken vermutlich auch viele Polizeibeamte, die – aus ihrer Sicht – durch mannigfaltige rechtliche Vorgaben in ihrer Aufgabenerfüllung behindert werden. Wegen dieser Differenzen die Technik „wie eine Person auf die Anklagebank zu setzen“,<sup>215</sup> die das mühsam erarbeitete Regelungsgefüge bedroht, ist allerdings nicht hilfreich. Dies gilt umgekehrt aber auch für das Verfallen in eine technische „Goldgräbermentalität“, die jegliche rechtliche Begrenzung und Regulierung sogleich als Technik- und Fortschrittsfeindlichkeit auffasst.<sup>216</sup>

### 1.5.2 Geeignetheit der rechtlichen Steuerungsinstrumente?

Dass auf eine rechtliche Regulierung nicht einfach verzichtet werden kann, zeigen die Risiken und Gefahren, die technische Neuerungen mit sich bringen können. Dampfmaschinen können durch Brände oder Explosionen Schäden an Leib, Leben oder Eigentum verursachen. Ein weit größeres Schadenspotential weisen Großtechniken auf.<sup>217</sup> Zu denken ist beispielsweise an den Einsatz von Kernenergie und das damit einhergehende Risiko einer atomaren Katastrophe. Von der Informationstechnologie

---

213 *Roßnagel* 2001, 17.

214 *Berg*, JZ 1985, 401, 403 u. *Roßnagel* 2001, 17.

215 *Huber* 1971, 61.

216 *Berg*, JZ 1985, 401, 405.

217 *Roßnagel* 1984, 14.

gehen zunächst keine derartigen Gefahren für Leib oder Leben aus. Vielmehr wird das Persönlichkeitsrecht des Einzelnen, seine Befugnis, über die Preisgabe und Verwendung ihn betreffender Informationen selbst zu bestimmen, beeinträchtigt, was gleichzeitig negative gesellschaftliche Folgen haben kann.<sup>218</sup> Angriffe auf informationsverarbeitende Systeme können allerdings auch massive physische Auswirkungen haben, wenn hierdurch etwa kritische Infrastrukturen<sup>219</sup> getroffen werden. Da es Aufgabe des Rechts ist, Rechte und Freiheiten der Bürger zu schützen und Interessenkonflikte aufzulösen, kann der Gesetzgeber hierbei nicht untätig zuschauen.

Mit Blick auf das schnelle Fortschreiten, die Komplexität und die Unwägbarkeit der Folgen moderner Technik stellt sich die Frage, ob die bestehenden Regelungsmechanismen überhaupt noch zur Regulierung in der Lage sind. Das klassische rechtliche Regelungsinstrument in Deutschland ist die parlamentarische Willensäußerung in Form eines Gesetzes.<sup>220</sup> Allerdings könnte sich das Gesetz als Ergebnis eines komplexen Gesetzgebungsverfahrens (z.B. Art. 70 ff. GG sowie §§ 75 ff. GO-BT auf Bundesebene) auf Dauer als zu schwerfällig erweisen. Verwiesen wird daher auf Maßnahme- oder Moratoriumsgesetze sowie experimentelle und befristete Gesetze. Während es Maßnahmegesetze<sup>221</sup> erlauben, auf Einzelfälle zu reagieren, können durch die anderen genannten Typen gesetzgeberische Entscheidungen auf eine vorläufige, unter dem Vorbehalt der weiteren Entwicklung stehende Grundlage gestellt werden, ohne dass damit der Anspruch verbunden ist, eine Regelung für die „Ewigkeit“ zu treffen.<sup>222</sup> Nach Erlass eines Gesetzes sind zudem die vom Bundesverfassungsgericht eingeforderten Überwachungs-, Beobachtungs- und Korrekturpflichten<sup>223</sup> des Gesetzgebers zu beachten. Demnach ist der Gesetzgeber gehalten, seine Regelungen und deren Auswirkungen zu beobachten und gegebenenfalls zu korrigieren. Aber auch diese Instrumente sind nicht geeignet, die notorischen Verspätungen des Gesetzgebers gegenüber der technischen Entwicklung zu verhindern.<sup>224</sup>

---

218 S. hierzu die Ausführungen in BVerfGE 65, 1 (42 f.).

219 S. § 2 Abs. 10 BSIG.

220 *Ossenbühl* 2000, 20 m.w.N.

221 Maßnahmegesetze sind mit Blick auf das Einzelfallgesetzverbot in Art. 19 Abs. 1 Satz 1 GG nicht unzulässig, *Sachs-Sachs*, Art. 19 Rn. 22 m.w.N.

222 *Ossenbühl* 2000, 22 f. m.w.N.

223 Zu solchen Pflichten z.B. BVerfGE 111, 10 (42) zur Beobachtung des Ladenschlussgesetzes; BVerfGE 112, 304 (320) zur Beobachtung verfahrensrechtlicher Vorkehrungen im Strafprozessrecht.

224 *Ossenbühl* 2000, 23.

Als weitere Steuerungsinstrumente kommen in Deutschland Rechtsverordnungen und Verwaltungsvorschriften in Betracht.<sup>225</sup> Rechtsverordnungen sind „rechtsetzende Akte der Exekutive“,<sup>226</sup> die auf Grundlage einer gesetzlichen Ermächtigung (s. Art. 80 GG) erlassen werden. Ihnen kommt ein Entlastungs- und Flexibilitätsfunktion zu, indem sie unter Verzicht auf ein aufwändiges Gesetzgebungsverfahren den parlamentarischen Gesetzgeber von Detailarbeit entlasten.<sup>227</sup> Rechtsverordnungen finden in vielen Bereichen Einsatz, nicht zuletzt auch im technischen Bereich, wie etwa zahlreiche Bundesimmissionsschutzverordnungen (BImSchV) belegen.<sup>228</sup> Hingegen handelt es sich bei Verwaltungsvorschriften um Innenrecht der Verwaltungsbehörden, also verwaltungsinterne Regelungen ohne (unmittelbare) Außenwirkung.<sup>229</sup> Im technischen Bereich zählen hierzu zum Beispiel die Technische Anleitung zur Reinhaltung der Luft (TA Luft) und die Technische Anleitung zum Schutz gegen Lärm (TA Lärm). Allerdings haben Rechtsverordnungen und (erst recht) Verwaltungsvorschriften nicht das gleiche Maß an demokratischer Legitimation wie die Parlamentsgesetze. Wesentliche Entscheidungen, das heißt Entscheidungen „in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung“,<sup>230</sup> hat der parlamentarische Gesetzgeber selbst zu treffen (sog. Wesentlichkeitstheorie). Eine Delegation an die Exekutive ist nicht zulässig.<sup>231</sup> Ein Ausweichen auf Regulierungsformen, die flexibler als parlamentarische Gesetze sind, ist daher unter Geltung des Grundgesetzes von vornherein nur begrenzt möglich.

Nun ließe sich einwenden, dass inzwischen viele Materien von der Europäischen Union reguliert werden. Jedoch ist das Gesetzgebungsverfahren auf Ebene der Union (s. Art. 288 ff. AEUV) auch nicht schneller als auf Ebene der Nationalstaaten, wie beispielhaft das jahrelange Ringen um die europäische Datenschutzreform belegt.

---

225 Dazu *Ossenbühl* 2000, 24.

226 BVerfGE 1, 184 (196). Zum Begriff der Rechtsverordnung *Maunz/Dürig-Remmert*, Art. 80 Rn. 24 ff.

227 *Maunz/Dürig-Remmert*, Art. 80 Rn. 7.

228 *Maunz/Dürig-Remmert*, Art. 80 Rn. 2.

229 Zum Begriff der Verwaltungsvorschrift z.B. *Mann/Sennekamp/Uechtritz-Sennekamp*, § 9 Rn. 15.

230 BVerfGE 49, 89 (126).

231 Zur Wesentlichkeitstheorie z.B. *Maunz/Dürig-Grzeszick*, Art. 20, VI Rn. 105 f. sowie Kap. 5.2.2.1.1.1.

### 1.5.3 Privater und staatlicher Technikeinsatz

Das Problem der Verspätung des Gesetzgebers würde aber entscheidend an Bedeutung verlieren, wenn eine gesetzliche Regulierung Voraussetzung dafür ist, dass bestimmte Techniken überhaupt eingesetzt werden dürfen. Dabei ist zwischen dem privaten und dem staatlichen Einsatz von Technik zu unterscheiden.

#### 1.5.3.1 Privater Technikeinsatz

Privater Technikeinsatz ist als Ausdruck (mindestens) der Handlungsfreiheit gemäß Art. 2 Abs. 1 GG<sup>232</sup> grundsätzlich zulässig. Möchte der staatliche Gesetzgeber hier regulierend – vor allem auch verbietend – eingreifen, benötigt er dafür gute Gründe. Solche Gründe können unter anderem vorliegen, wenn die Rechte anderer Personen beeinträchtigt werden. In derartigen Situationen ist ferner zu berücksichtigen, dass die Rechte der beeinträchtigten Personen dem Technikeinsatz auch ohne spezielle Regulierung Grenzen ziehen können. Dies gilt etwa bei der Verarbeitung personenbezogener Daten, die das Persönlichkeitsrecht beeinträchtigen und Unterlassungsansprüche der betroffenen Personen (§§ 1004, 823 BGB) auslösen können.<sup>233</sup>

Überdies zeigt ein exemplarischer Blick in die Geschichte, dass eine rechtliche Steuerung, und sei es mit Verzögerung, möglich ist:

Als sich das traditionelle Handwerk im 17. und 18. Jahrhundert durch technische Neuerungen wie Textilmaschinen oder Webstühle bedroht sah, wurden diese verschiedentlich schlicht verboten.<sup>234</sup> Dies verhinderte im Ergebnis freilich nicht, dass sich die genannten Neuerungen durchsetzen konnten.

Nachdem in der ersten Hälfte des 19. Jahrhunderts die Dampfmaschine immer größere Verbreitung fand, wurden in Preußen durch eine „Allerhöchste Kabinettsorder vom 1sten Januar 1831., die Anlagen und

---

232 Nach heute ganz h.M. schützt Art. 2 Abs. 1 GG die Handlungsfreiheit in einem umfassenden Sinn, z.B. Maunz/Dürig-Di Fabio, Art. 2 Abs. 1 Rn. 12 m.w.N. In der Rspr. z.B. BVerfGE 80, 137 (152 ff.).

233 S. Simitis/Hornung/Spiecker-Roßnagel, Art. 5 Rn. 37, der darauf hinweist, dass die Datenverarbeitung auch im privaten Bereich nicht eigentlich frei ist, da sie jedenfalls in das Recht auf informationelle Selbstbestimmung der betroffenen Person eingreift, wofür der Verantwortliche einer Erlaubnis bedarf.

234 Roßnagel 1984, 18. Hintergründig zum sog. Maschinensturm Steferle 1983, 203.

den Gebrauch der Dampfmaschinen betreffend“, Regelungen erlassen, „um den Gefahren, welche von dem in neuerer Zeit immer allgemeiner werdenden Gebrauche der Dampfmaschinen zu besorgen sind, möglichst vorzubeugen“. Mit der „Instruktion zur Vollziehung der Allerhöchsten Kabinettsorder vom 1. Januar 1831., die Anlagen und den Gebrauch der Dampfmaschinen betreffend“, wurde „zur Wahrnehmung des technisch-polizeilichen Interesses“ ein Regulativ geschaffen, das verschiedene Sicherheitsvorkehrungen vorsah, um den von Dampfmaschinen ausgehenden Gefahren zu begegnen. Dies betraf beispielsweise die Nutzung von „gläsernen Wasserstandsrohren“ sowie „zweckmäßige Sicherheitsventile“. <sup>235</sup> Ziel dieser Maßnahmen war die Verhinderung von Schäden durch Explosionen oder Brände.

Ende des 19. Jahrhunderts musste das Reichsgericht entscheiden, ob es strafbar ist, wenn Privatpersonen ohne Erlaubnis des Elektrizitätswerkes elektrischen Strom abzweigen. Maßgeblich war die Frage, ob elektrischer Strom eine Sache im Sinne von § 242 StGB ist. <sup>236</sup> Nachdem dies vom Reichsgericht verneint worden war, schuf der Gesetzgeber einen neuen Straftatbestand, mit dem die Entziehung elektrischer Energie unter Strafe gestellt wurde (§ 248c StGB).

Diese Beispiele zeigen, dass das Recht auch in vergangenen Jahrhunderten vor der Aufgabe stand, auf neue technische Entwicklungen zu reagieren – und auch reagiert hat. Ob die gefundenen Antworten immer gut oder richtig waren, ist eine andere Frage.

Dass das Recht auch in der heutigen Zeit zur Steuerung technischer Entwicklungen in der Lage ist, zeigt sich bei der Nutzung der Kernenergie zur gewerblichen Erzeugung von Elektrizität. Hat sich die Bundesrepublik Deutschland, und damit auch der Gesetzgeber, über mehrere Jahrzehnte mit dieser Technik identifiziert, <sup>237</sup> ist es inzwischen beschlossene Sache, die Nutzung der Kernenergie zur gewerblichen Erzeugung von Elektrizität geordnet zu beenden (§ 1 Nr. 1 AtG). Insofern sind es „drei berichtigende Worte des Gesetzgebers“, die nicht nur „ganze Bibliotheken [...] zu Makulatur“ werden lassen, <sup>238</sup> sondern auch den Einsatz einer weit verbreiteten Großtechnik unterbinden können.

---

235 Die „Kabinettsorder“ sowie die „Instruktion zur Vollziehung“ finden sich in der „Gesetz-Sammlung für die Königlichen Preußischen Staaten 1831“.

236 RGSt 29, 111 u. RGSt 32, 165.

237 *Ossenbühl* 2000, 14.

238 *V. Kirchmann* 1848, 17.

### 1.5.3.2 Staatlicher Technikeinsatz

Beim staatlichen Technikeinsatz ist eine rechtliche Steuerung regelmäßig bedeutend einfacher. Greift das staatliche Handeln in die Grundrechte ein, bedarf es einer gesetzlichen Ermächtigung (Vorbehalt des Gesetzes).<sup>239</sup> Fehlt eine solche, ist der Einsatz der in Frage stehenden Technik von vornherein unzulässig und hat zu unterbleiben. Dementsprechend kann die Technik das Recht an dieser Stelle nicht überholen.

Dies gilt auch für den polizeilichen Einsatz von Gesichtserkennung in Verbindung mit Videoüberwachung, der erhebliche Grundrechtseingriffe<sup>240</sup> hervorrufen kann und daher auf eine entsprechende Ermächtigungsgrundlage gestützt werden muss. Dabei lässt sich die Frage nach dem richtigen Regelungsinstrument vergleichsweise einfach beantworten. Zwar mögen Rechtsverordnungen und Verwaltungsvorschriften gegenüber Parlamentsgesetzen den Vorteil der Schnelligkeit und Flexibilität haben. Aufgrund der erheblichen Grundrechtseingriffe bedarf es aber einer gesetzlichen Regelung durch den parlamentarischen Bundes- oder Landesgesetzgeber. Eine Delegation an die Verwaltung ist nicht zulässig.<sup>241</sup> Die damit gegebenenfalls verbundene Schwerfälligkeit bei der Reaktion auf technische Neuerungen ist hinzunehmen. Wird dies als nicht tragbar angesehen, muss die Verfassung geändert werden.

Der Behauptung, „was technisch möglich ist, wird auch gemacht“,<sup>242</sup> kann vor diesem Hintergrund nicht beigetreten werden. Ob die erforderlichen gesetzlichen Ermächtigungen für den Einsatz von Überwachungstechnik geschaffen werden, ist zuvorderst eine Entscheidung der demokratisch legitimierten Abgeordneten (Art. 20 Abs. 2, 38 Abs. 1 GG). Erlassen sie entsprechende Regelungen, sind sie darin nicht frei, sondern müssen übergeordnete grund- und verfassungsrechtliche Vorgaben beachten. Die Einhaltung dieser Vorgaben unterliegt gerichtlicher Kontrolle. Insbesondere das Bundesverfassungsgericht hat dem staatlichen Technikeinsatz

---

239 Zum Erfordernis einer gesetzlichen Grundlage s. Kap. 5.2.2.1.

240 Zum Eingriffsgewicht s. Kap. 5.2.2.3.4.1.2.

241 Zwar ist nicht von vornherein ausgeschlossen, dass der parlamentarische Gesetzgeber die Grundlinien einer eingreifenden Maßnahme selbst regelt, während er die konkrete Ausgestaltung der Exekutive als Befugnis zum Erlass einer Rechtsverordnung (Art. 80 GG) überlässt. Im Bereich eingriffsintensiver staatlicher Überwachungsmaßnahmen besteht aber auch hierfür regelmäßig kein Raum; dazu s. Kap. 5.2.2.1.

242 *Gaycken/Kurz* 2008, 13.