Marie-Theres Tinnefeld, Benedikt Buchner, Thomas Petri, Hans-Joachim Hof
Einführung in das Datenschutzrecht

Marie-Theres Tinnefeld, Benedikt Buchner,
Thomas Petri, Hans-Joachim Hof

Einführung in das Datenschutzrecht

Datenschutz und Informationsfreiheit
in europäischer Sicht

7., überarbeitete und aktualisierte Auflage

DE GRUYTER
OLDENBOURG

ISBN 978-3-11-063031-2
e-ISBN (PDF) 978-3-11-063033-6
e-ISBN (EPUB) 978-3-11-063045-9

Library of Congress Control Number: 2019947130

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

© 2020 Walter de Gruyter GmbH, Berlin/Boston
Coverabbildung: alexskopje/iStock/Thinkstock
Satz: Integra Software Services Pvt. Ltd.
Druck und Bindung: CPI books GmbH, Leck

www.degruyter.com

Vorwort

Die siebte Auflage befasst sich schwerpunktmäßig wieder mit Fragen der Integration Europas und den Herausforderungen, die mit einer Harmonisierung des Datenschutzes und der Informationsfreiheit in der Europäischen Union sowie weltweit verbunden sind. Dass es heute ein Menschenrecht auf Privatheit **und** Datenschutz gibt, ist eine der größten Errungenschaften im digitalen Zeitalter und Gewähr dafür, dass keine Person in ihrer Privatheit und informationellen Selbstbestimmung existenziell beschädigt werden darf. Jedoch zeigt sich auch, dass die rechtliche und technische Gewährleistung von Privatheit und Datenschutz in der Union und ihren Mitgliedstaaten angesichts von Big Data und Künstlicher Intelligenz gefährdet ist. Technologien sind immer ambivalent. Sie können zum Guten und zum Schlechten eingesetzt werden. Ob sie zur Sicherung von individueller (solidarischer) Freiheit und sozialem Fortschritt beitragen oder zu staatlicher Überwachung privater Räume und vertraulicher (Tele-)Kommunikation eingesetzt werden, darüber können Bürger und Bürgerinnen in einer offenen Demokratie mitentscheiden. Ihre Fähigkeit, Entscheidungen zu treffen und Gründe gegeneinander abzuwägen, ist auf Datenschutz, Informationsfreiheit und Meinungsäußerungsfreiheit angewiesen.

Die zahlreichen Aspekte der Digitalisierung sind eine Herausforderung für Recht und Technik in der Union. Wesentlich im Prozess der Fortschreibung des Rechts auf Privatheit und Datenschutz sind die allgemeine Datenschutz-Grundverordnung (DS-GVO) und die spezielle Richtlinie für den Bereich der Strafjustiz (DSRLJ). Verordnung und Richtlinie haben den Mitgliedstaaten der Union die Herkulesaufgabe aufgegeben, das nationale Recht neu aufzustellen und mit dem Unionsrecht abzustimmen. Inzwischen ist der deutsche Bundesgesetzgeber dieser Aufgabe weitgehend nachgekommen. In der vorliegenden Einführung werden all diese neuen Regelungen auf europäischer und nationaler Ebene ausführlich erörtert – einschließlich eines Ausblicks auf die geplante ePrivacy-Verordnung für den Bereich der elektronischen Kommunikation.

Ein weiterer Schwerpunkt der Erörterungen ist auch in dieser Auflage auf Information und Meinungsbildung gelegt worden, die online wie offline eine originäre Aufgabe journalistischer Medien sind. Dazu gehören die Regeln der Sorgfaltspflicht und Wahrhaftigkeit sowie ein Austausch mittels open access über das Internet. Heute kursieren im Internet allerdings eine Fülle nicht journalistischer Angebote sowie Schlammfluten von Drohungen, Diskriminierungen, Schmähungen, Hassbotschaften und Halbwahrheiten, teilweise durch algorithmengenerierte Fake News, die betroffene Personen über alle Grenzen hinweg treffen. Es gibt auch Menschen, die dazu tendieren, sich mit suggestiv formulierten Meinungen in sozialen Medien abzuschotten. Die genannten Entwicklungen gefährden die freie Entfaltung der Persönlichkeit, die Teilhabe an Kommunikation und die Rechte auf Meinungs- und Informationsfreiheit.

Auch richtet sich der Fokus der folgenden Ausführungen auf die Abwehr der nur schwer greifbaren Bedrohungen der Menschen durch Terrorakte. Wie sind in

https://doi.org/10.1515/9783110630336-202

diesem Zusammenhang Regulierungen in den Mitgliedstaaten und in Staaten außerhalb der Union (sog. Drittstaaten) einzuordnen? Erfordert die Rolle des Internets in diesem Zusammenhang eine restriktivere Innen- und Sicherheitspolitik, etwa eine anlasslose Vorratsspeicherung von Telekommunikationsdaten zur Terrorbekämpfung? Ist die deutsche Regelung rechtmäßig und von Nutzen? Und schließlich widmet sich diese Einführung auch den Fragen der Datenschutz-Risikovorsorge, wozu Fragen der Rechtssicherheit durch Technik sowie der Transparenz der Datenverarbeitung hoheitlicher Entscheidungsträger, wie sie etwa in den Informationsfreiheitsgesetzen zum Ausdruck kommt, gehört.

Das Buch richtet sich in erster Linie an Studentinnen und Studenten, ebenso aber auch an Praktikerinnen und Praktiker, die sich mit dem reformierten Datenschutzrecht vertiefter befassen wollen. Vor diesem Hintergrund haben die Autorin und die Autoren auch bei dieser Auflage wieder besonderen Wert darauf gelegt, möglichst zahlreich konkrete Fälle aus der Praxis als Beispiele für die Erörterung von datenschutzrechtlichen Grundbegriffen darzustellen. Zugleich bringt es der Charakter des Buches als Einführung mit sich, dass die Darstellung auf wesentliche Grundfragen des Datenschutzes beschränkt bleibt und nicht alle Detailfragen geklärt werden können. Die Ausführungen in diesem Buch sind das Ergebnis der intensiven Zusammenarbeit zwischen der Autorin Marie-Theres Tinnefeld (Prolog und Kapitel 1) und den Autoren Benedikt Buchner (Kapitel 2 und 4), Thomas Petri (Kapitel 3) sowie Hans-Joachim Hof (Kapitel 5 und Glossar). In vielfältiger Weise unterstützt haben uns die Mitarbeiterinnen und Mitarbeiter am Institut für Informations-, Gesundheits- und Medizinrecht (IGMR) der Universität Bremen. Ihnen allen sei an dieser Stelle für ihren Einsatz gedankt, allen voran Merle Freye für ihren engagierten Einsatz als kompetente Probeleserin und Petra Wilkins für ihre auch bei dieser Auflage wieder souveräne Auf- und Übersicht, egal ob es um die Vielzahl an Dateiversionen oder den sprachlichen und formalen Feinschliff ging.

Gedankt sei des Weiteren auch Kai Brobeil, der als Informatikstudent alle Grafiken sorgfältig bearbeitet hat. Und last but not least gilt unser ganz besonderer Dank Kathleen Herfurth und Stefan Giesen vom Verlag De Gruyter. Beide haben die Herausgabe der Neuauflage mit viel Geduld, kompetentem Rat und großem Verständnis begleitet.

Juli 2019

Marie-Theres Tinnefeld
Benedikt Buchner
Thomas Petri
Hans-Joachim Hof

Inhaltsverzeichnis

Vorwort —— V

Abkürzungsverzeichnis —— XIII

Prolog —— XIX
Marie-Theres Tinnefeld

1 Grundfragen —— 1
Marie-Theres Tinnefeld
1.1 Technologische Entwicklung – Auswirkung auf menschliche Lebenswelten —— **1**
1.1.1 Informations-, Wissens- und Zivilgesellschaft —— **13**
1.1.2 Internetkommunikation und technischer Grundrechtsschutz —— **17**
1.1.3 Neue Räume und Zugriffsmöglichkeiten in der digitalen Netzwelt —— **22**
1.1.4 Entwicklung des Internets —— **24**
1.1.5 Explosion von Information —— **34**
1.1.6 Ganzheitliche Regelungsansätze —— **38**
1.2 Freiheit der Meinung, Presse und Information – Zeichen einer offenen Gesellschaft? —— **42**
1.2.1 Historische Eckpunkte und Definitionen —— **42**
1.2.2 Besondere Konflikte und Maßstäbe —— **52**
1.2.3 Vom Wert der Privatheit im sozialen und kulturellen Kontext —— **62**
1.2.4 Technologischer Wandel und das Prinzip Verantwortung —— **69**
1.3 Entwicklung von Datenschutz und Informationsfreiheit —— **72**
1.3.1 Kennzeichen und Grenzen einer transparenten Verwaltung —— **74**
1.3.2 Datenschutz und Informationszugang bei den Stasi-Akten —— **76**
1.4 Datenschutz in Europa —— **80**
1.4.1 Exkursion in die deutsche Entwicklung —— **81**
1.4.2 Datenschutz im Völkerrecht —— **84**
1.4.3 Schutznormen im supranationalem Recht (Unionsrecht) —— **94**
1.5 Dimensionen der Privatheit und des Datenschutzes in Deutschland —— **107**
1.5.1 Welche Grundrechte gewährleisten den Datenschutz? —— **108**
1.5.2 Abgrenzung der Grundrechte —— **127**
1.6 Bundes- und Landesrecht im Gefüge supra- und internationaler Rechtsquellen —— **131**
1.6.1 Kompetenzverteilung zwischen Bund und Ländern —— **133**
1.6.2 Rangordnung und Anwendbarkeit nationaler Parlamentsgesetze —— **135**

1.6.3 Rangverhältnis: Unionsrecht und nationales Recht — **135**
1.6.4 Völkerrecht, Unionsrecht und nationales Recht — **140**
1.6.5 Kooperation oder Konfrontation in der Union — **142**
1.7 Bereichsspezifische Regelungen in Auswahl — **151**
1.7.1 Beschäftigtendatenschutz in der Arbeitswelt 4.0 — **152**
1.7.2 Besondere Verarbeitungssituationen — **175**
1.7.3 Freiraum der Kunst, Wissenschaft und Forschung — **183**
1.7.4 Datenverarbeitung zu Archiv-, Forschungs- und statistischen Zwecken — **190**
1.7.5 Geheimhaltungspflichten als Gegenstand der DS-GVO — **197**
1.7.6 Sonderstatus der Kirchen, religiösen Vereinigungen oder Gemeinschaften — **206**
1.7.7 Schalter des Erbguts — **211**

2 Grundsätze des Datenschutzrechts — 220
Benedikt Buchner
2.1 Das datenschutzrechtliche Regelungsgefüge — **220**
2.1.1 Datenverarbeitung im öffentlichen und nicht-öffentlichen Bereich — **220**
2.1.2 Allgemeine und bereichsspezifische Datenschutzgesetzgebung — **223**
2.1.3 Anwendungsbereich des Datenschutzrechts — **224**
2.1.4 Umfassender versus punktueller Regelungsansatz — **239**
2.2 Datenschutzrechtliche Regelungsprinzipien — **243**
2.2.1 Allgemeine Grundsätze — **243**
2.2.2 Verarbeitung besonderer Kategorien personenbezogener Daten — **251**
2.2.3 Videoüberwachung — **253**
2.2.4 Automatisierte Entscheidungen — **265**
2.2.5 Profiling — **271**
2.2.6 Auftragsverarbeitung — **275**
2.2.7 Grenzüberschreitender Datenverkehr — **282**
2.2.8 Betroffenenrechte — **292**
2.2.9 Datenschutzkontrolle — **314**
2.2.10 Sanktionen — **327**

3 Datenverarbeitung im öffentlichen Interesse — 333
Thomas Petri
3.1 Überblick — **333**
3.2 Verarbeitung außerhalb des Anwendungsbereichs des EU-Datenschutzrechts — **335**
3.3 Verarbeitung zu Zwecken der Straftatenbekämpfung — **339**
3.3.1 Gegenstand und Ziele — **340**

3.3.2 Grundsätze für die Verarbeitung — **343**
3.3.3 Risikoträchtige Verarbeitungen, insbesondere besondere Kategorien personenbezogener Daten, automatisierte Entscheidungsfindung — **352**
3.3.4 Rechte der Betroffenen nach der Richtlinie — **357**
3.3.5 Übermittlung personenbezogener Daten an Drittstaaten oder internationale Organisationen nach der Richtlinie (EU) 2016/680 — **359**
3.3.6 Weitere Bestimmungen in der Richtlinie (EU) 2016/680 — **362**
3.4 Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe nach der DS-GVO — **363**
3.4.1 Folgen weitreichender Öffnungsklauseln am Beispiel der Verantwortlichkeit — **364**
3.4.2 Überblick zu bereichsspezifischem Recht — **365**
3.4.3 Anwendungsbereiche der allgemeinen Datenschutzgesetze — **389**
3.5 Datentransfers — **389**
3.5.1 Auftragsverarbeitung als Sonderfall der Datenweitergabe — **391**
3.5.2 Wesentliche Grundsätze der Datenübermittlung — **391**
3.5.3 Anforderungen an die Zulässigkeit der Datenübermittlung — **393**
3.5.4 Besonderheiten beim Datentransfer in Drittländer oder an internationale Organisationen — **400**

4 Datenverarbeitung im nicht-öffentlichen Bereich — 403
Benedikt Buchner
4.1 Öffentlicher und nicht-öffentlicher Bereich — **403**
4.1.1 Bislang: zweigeteilter Regelungsansatz — **403**
4.1.2 DS-GVO: Öffnungsklauseln für die Datenverarbeitung im öffentlichen Interesse — **404**
4.1.3 Rechtmäßigkeit der Datenverarbeitung im öffentlichen und nicht-öffentlichen Bereich — **404**
4.2 Der Erlaubnistatbestand der Einwilligung — **406**
4.2.1 Allgemeines — **406**
4.2.2 Wirksamkeit der Einwilligung — **417**
4.2.3 Einwilligung im Online- und Telekommunikationsbereich — **433**
4.2.4 Einwilligung und ärztliche Schweigepflicht — **436**
4.3 Gesetzliche Erlaubnistatbestände — **441**
4.3.1 Überblick — **442**
4.3.2 Durchführung eines (vor-)vertraglichen Schuldverhältnisses — **443**
4.3.3 Erfüllung einer rechtlichen Verpflichtung — **449**
4.3.4 Wahrung lebenswichtiger Interessen — **450**
4.3.5 Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt — **450**

4.3.6 Datenverarbeitung auf Grundlage einer Interessenabwägung — **451**
4.4 Datenverarbeitung im Bereich Telemedien und Telekommunikation — **461**
4.4.1 Überblick Telemediengesetz (TMG) — **461**
4.4.2 Bereichsspezifischer Datenschutz für Telemedien — **462**
4.4.3 TKG und ePrivacy-Verordnung — **467**

5 Datenschutz mittels IT-Sicherheit — 477
Hans-Joachim Hof
5.1 Aktuelle Entwicklung der IT-Sicherheit — **478**
5.1.1 Digitalisierung — **479**
5.1.2 Internet der Dinge, Wearables und Sprachagenten — **480**
5.1.3 Big Data — **483**
5.1.4 Selbstlernende Maschinen und Künstliche Intelligenz — **485**
5.1.5 Blockchain — **487**
5.1.6 Gleichbleibend schlechte Softwarequalität — **488**
5.1.7 Agile IT — **490**
5.1.8 Zunehmende Verwendung von Fremdkomponenten — **491**
5.1.9 Cloud Computing — **493**
5.1.10 Smart Grid, Smart Metering, Smart Home und Smart City — **495**
5.1.11 Apps und Web-Anwendungen ersetzen Desktop-Anwendungen — **496**
5.1.12 Allgegenwärtige Nutzung von Smartphones und Apps — **497**
5.1.13 Social Media als wichtige Kommunikationsplattform und Nachrichtenquelle — **499**
5.1.14 Geschäftsmodelle im Internet — **500**
5.1.15 Entwicklung von Angreifern und Angriffen — **501**
5.1.16 Zukünftige Trends — **505**
5.2 Informationstechnische Bedrohungen — **507**
5.2.1 Schadsoftware — **507**
5.2.2 Ausnutzen von Sicherheitslücken — **509**
5.2.3 Social Engineering und Phishing — **511**
5.2.4 Lauschangriff — **512**
5.2.5 Ausnutzen von schlechter Konfiguration — **513**
5.2.6 Fehler aufgrund von mangelhafter Benutzbarkeit — **514**
5.2.7 Fortgeschrittene Angriffe (Advanced Persistent Threats) — **515**
5.3 IT-Sicherheitskriterien und IT-Sicherheitsmanagement — **516**
5.3.1 Vorgehensweise bei einem IT-Sicherheitskonzept — **520**
5.3.2 Allgemeine Ziele der IT-Sicherheit — **521**

5.3.3 Intrusion Detection und Security Information and Event Management System — **525**
5.3.4 Verschlüsselung — **526**
5.3.5 Biometrie — **532**

Glossar — 537

Verzeichnis der häufig zitierten Literatur — 555

Stichwortverzeichnis — 557

Abkürzungsverzeichnis

A.	Auflage
a. M.	anderer Meinung
ABl.	Amtsblatt
ACTA	Anti-Counterfeiting Trade Agreement
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AfP	Archiv für Presserecht (Zeitschrift für Medien- und Kommunikationsrecht)
AGG	Allgemeines Gleichbehandlungsgesetz
AktG	Aktiengesetz
AO	Abgabenordnung
ArbG	Arbeitsgericht
ArbGG	Arbeitsgerichtsgesetz
ArbSichG	Arbeitssicherstellungsgesetz
ATDG	Antiterrordateigesetz
AufenthG	Aufenthaltsgesetz
AuR	Arbeit und Recht
AuslG	Ausländergesetz
BAFin	Bundesanstalt für Finanzdienstleistungen
BAG	Bundesarbeitsgericht
BAGE	Entscheidung des Bundesarbeitsgerichts
BÄK	Bundesärztekammer
BAnz.	Bundesanzeiger
BayHSchG	Bayerisches Hochschulgesetz
BayKrG	Bayerisches Krankenhausgesetz
BayLT	Bayerischer Landtag
BayPAG	Bayerisches Polizeiaufgabengesetz
BayVSG	Bayerisches Verfassungsschutzgesetz
BB	Betriebsberater
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BerlHG	Berliner Hochschulgesetz
BerufO	Berufsordnung
BetrVG	Betriebsverfassungsgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BFStrMG	Bundesfernstraßenmautgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BGHSt	Entscheidungssammlung des Bundesgerichtshofes in Strafsachen
BGHZ	Entscheidungen des Bundesgerichtshofes in Zivilsachen
BKA	Bundeskriminalamt
BKAG	Bundeskriminalamtgesetz
BlnDSG	Berliner Datenschutzgesetz
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BPersVG	Bundespersonalvertretungsgesetz
BPolG	Bundespolizeigesetz
BRAO	Bundesrechtsanwaltsordnung
BR-Drucks.	Drucksache des Deutschen Bundesrates

https://doi.org/10.1515/9783110630336-203

BRRG	Beamtenrechtsrahmengesetz
BSG	Bundessozialgericht
BSGE	Entscheidungen des Bundessozialgerichts
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
BT-Drucks.	Drucksache des Deutschen Bundestages
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichts
BYOD	Bring Your Own Device
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
CAD	Computer-aided design
CAM	Computer-aided manufacturing
CCC	Chaos Computer Club
CCTV	Closed Circuit Television
CGK	Corporate Governance Codex
CIS	Customs Information System
CR	Computer und Recht
CRM	Customer Relationship Management
CTG	Counter Terrorist Group
DDoS	Dedicated Denial of Service
DIN	Deutsches Institut für Normung
DMZ	demilitarisierte Zone
DNA	Desoxyribonukleinsäuren
DNS	Desoxyribonukleinsäuren
DSB	Datenschutzbeauftragter
DSG-EKD	Datenschutzgesetz der Evangelischen Kirche in Deutschland
DS-GVO	EU-Datenschutzgrundverordnung 2016/679
DSRL	EU-Datenschutzrichtlinie 95/46/EG
DSRLJ	EU-Datenschutzrichtlinie 2016/680 für den Bereich Justiz und Inneres
DSVO	Datenschutzverordnung 45/2001
DuD	Datenschutz und Datensicherheit
DvH	Declaration of Helsinki
DVO	Durchführungsverordnung
DWG	Deutsche-Welle-Gesetz
EAG	Europäische Atomgemeinschaft
ECJ	European Court of Justice
EEA	Einheitliche Europäische Akte
EFTA	Europäische Freihandelszone
EG	EG-Vertrag in der nach dem 1.5.1999 geltenden Fassung
EG	Europäische Gemeinschaft(en)
EG	Erwägungsgrund
EGKS	Europäische Gemeinschaft für Kohle und Stahl
EGMR	Europäischer Gerichtshof für Menschenrechte
EGRC	Europäische Grundrechte-Charta
EMRK	Europäische Menschenrechtskonvention

endg.	endgültig
EP	Europäisches Parlament
EU	Europäische Union
EU	EU-Vertrag in der nach dem 1.5.1999 geltenden Fassung
EuG	Europäisches Gericht 1. Instanz
EuGH	Europäischer Gerichtshof
EuGRZ	Europäische Grundrechte-Zeitschrift
Euratom	Europäische Atomgemeinschaft
Eurodac	Fingerabdruckdatenbank
EurRatS	Satzung des Europarates
EUV	EU-Vertrag
EWG	Europäische Wirtschaftsgemeinschaft
EZB	Europäische Zentralbank
FAR	False Acceptance Rate
FIDE	Customs File Identification Database
fMRT	funktionelle Magnetresonanztomografie, auch Kernspintomografie
FS	Festschrift
GASP	Gemeinsame Außen- und Sicherheitspolitik
GATS	Allgemeines Übereinkommen über den Handel und Dienstleistungen
GATT	Allgemeines Zoll- und Handelsabkommen
GBO	Grundbuchordnung
GenDG	Gendiagnostikgesetz
GewO	Gewerbeordnung
GPS	Global Positioning System
GRCh	EU-Grundrechte-Charta
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
HGB	Handelsgesetzbuch
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
IaaS	Infrastructure as a Service
ICMP	Internet Control Message Protocol
IFG	Informationsfreiheitsgesetz
IfSG	Infektionsschutzgesetz
ILO	Internationale Labour Organization (Internationale Arbeitsorganisation)
IP	Internet Protocol
ISO	International Organization for Standardization
ITK	Informations- und Telekommunikationstechnologie
JMStV	Jugendmedienschutz-Staatsvertrag
JR	Juristische Rundschau
JZ	Juristische Zeitung
KDO-DVO	Anordnung über den kirchlichen Datenschutz-Durchführungsverordnung
KIS	Krankenhausinformationssystem
KJM	Kommission für den Jugendmedienschutz
KMK	Kultusministerkonferenz
KUG	Kunsturhebergesetz
LBS	Location-based Services
LDSG	Landesdatenschutzgesetz
MAD	Militärischer Abschirmdienst
MADG	Gesetz über den militärischen Abschirmdienst
MAVO	Mitarbeitervertretungsordnung der katholischen Kirche

MDStV	Mediendienste-Staatsvertrag
MedR	Medizinrecht (Zeitschrift)
MfS	Ministerium für Staatssicherheit
MMR	MultiMedia und Recht
MPI	Max-Planck-Institut
MVG-EKD	Mitarbeitervertretungsgesetz der Evangelischen Kirche in Deutschland
NATO	North Atlantic Treaty Organization
NJW	Neue Juristische Wochenschrift
NZA	Neue Zeitschrift für Arbeitsrecht
OECD	Organization for Economic Co-operation and Development
OEEC	Organization for European Economic Cooperation
OWASP	Open Web Application Security Project
OWiG	Ordnungswidrigkeitengesetz
PaaS	Platform as a Service
PDA	Personal Digital Assistant
PET	Privacy-Enhancing Technologies
PID	Präimplantationsdiagnostik
PJZS	polizeiliche und justizielle Zusammenarbeit in Strafsachen
PND	pränatale Diagnostik
PNR	Passenger Name Records
PolG	Polizeigesetz
QuoS	Quality of Service
RDV	Recht der Datenverarbeitung
REFA	Verband für Arbeitsstudien und Betriebsorganisation e.V.
RFC	Request for Comment
RFID	Radio Frequency Identification
RL	Richtlinie
RNA	Ribonukleinsäuren
RStV	Rundfunkstaatsvertrag
SaaS	Software-as-a-Service oder Storage-as-a-Service
SächsPolG	Sächsisches Polizeigesetz
SchulG	Schulgesetz
SDÜ	Schengener Durchführungsbestimmungen
SGB	Sozialgesetzbuch
SIM	Subscriber Identity Module
SIS	Schengener Informationssystem
Slg.	Sammlung (der Rechtsprechung des EuGH)
SOX	Sarbanes-Oxley Act
SprAuG	Gesetz über Sprecherausschüsse der leitenden Angestellten
SSL	Secure Socket Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StUG	Stasi-Unterlagen-Gesetz
SÜG	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes
TCP	Transmission Control Protocol
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung

TMG	Telemediengesetz
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
TVG	Tarifvertragsgesetz
UDP	User Datagram Protocol
UKlaG	Unterlassungsklagengesetz
UN	United Nations
UNESCO	United Nations Educational, Scientific and Cultural Organization
URI	Uniform Resource Indicator
URL	Uniform Ressource Locators
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
VIS	Visa-Informationssystem
VO	Verordnung
VvA	Vertrag von Amsterdam
VvL	Vertrag von Lissabon
VvM	Vertrag von Maastricht
VvN	Vertrag von Nizza
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
VZG	Volkszählungsgesetz
WEU	Westeuropäische Union
WHO	World Health Organization
WMA	World Medical Association
WRV	Weimarer Reichsverfassung
WSA	Wirtschafts- und Sozialausschuss
WTO	World Trade Organization
WWW	World Wide Web
ZD	Zeitschrift für Datenschutz
ZPO	Zivilprozessordnung
ZSI	Zentralstelle für Sicherheit in der Informationstechnik

Prolog

Marie-Theres Tinnefeld

> Verabsolutierung eines immer partikulären Erkennens zum Ganzen einer Menschenerkenntnis führt zur Verwahrlosung des Menschenbildes. Die Verwahrlosung des Menschenbildes aber führt zur Verwahrlosung des Menschen selber. Denn das Bild eines Menschen, das wir für wahr halten, wird selbst ein Faktor unseres Lebens. (Karl Jaspers)[1]

1 Big Data und neue Bilder vom Menschen

Die Fragen „Wer und was der Mensch ist" gehören zu den Urthemen der Menschheit. Die Antworten werden von der jeweiligen Sicht mitbestimmt, aus der das Bild des Menschen betrachtet wird. Die Perspektiven sind kulturell, religiös, wissenschaftlich und technisch geprägt.[2] Sie wirken häufig in der jeweiligen Tradition des Menschen aufgrund eigener Erfahrungen, kommunikativer Einbindung und den gemeinsamen (Gruppen-)Überlieferungen auch außerhalb seines Herkunftslandes fort. Der Historiker Reinhart Kosellek spricht sogar vom Recht des Menschen auf „seine eigene Biographie", einschließlich „seiner eigenen Vergangenheit".[3]

Die Achtung vor individuellen Rechten entfaltete sich im Zeitalter der Renaissance. In dieser kulturellen Blütezeit (15. und 16. Jahrhundert) begann der Mensch, sich als eigenständiges Individuum zu betrachten. Der Blick auf den Menschen verlagerte sich im Gegensatz zum Mittelalter vom ideellen auf den physischen bzw. materiellen Raum: Er war körpergebunden.[4] Vor diesem Hintergrund entwickelte der französische Philosoph Maurice Merleau-Ponty im 20. Jahrhundert einflussreiche Theorien zum Menschen als Körper-Subjekt. Nach seinen Ausführungen begreife unser Körper für uns die Welt und sei unser „Mittel überhaupt, eine Welt zu haben".[5] Danach manifestiert sich die Welt nur durch eine Vielfalt von Blicken auf sie, und sie wahrzunehmen wird durch den Körper und dessen sensorisch-motorische Funktionen ermöglicht. Das visuelle Erfassen eines virtuellen Raumes würde demnach auch adäquate körperliche Erfahrungen bewirken.

Im 21. Jahrhundert gewinnt nicht nur der weltweit zugängliche, grenzenlose „virtuelle" Raum bzw. Cyberspace, sondern auch eine datenzentrische Sicht auf den Menschen an Bedeutung. Zugleich wächst das Risiko, dass sich Menschen

1 Jaspers, zit. nach Meinberg, Das Menschenbild der modernen Erziehungswissenschaft (1988), S. 318.
2 Weis (Hg.), Bilder von Menschen in Wissenschaft, Technik und Religion (1993).
3 Kosellek, zit. nach Assmann, Das neue Unbehagen an der Erinnerungskultur (2013), S. 18.
4 Belting, Eine westöstliche Geschichte des Blicks (2008), S. 17.
5 Merleau-Ponty, Phänomenologie der Wahrnehmung, aus dem Französischen v. R. Boehm (1966), s. vor allem S. 172–175.

https://doi.org/10.1515/9783110630336-204

stärker als in irgendeiner früheren Epoche aus dem Kontakt mit der Natur und von ihren Räumen, Texturen, Klängen, Gerüchen und Gesetzmäßigkeiten entfernen. Viele nehmen nicht mehr wahr, dass der bewohnbare Raum eine „Conditio sine qua non" für ihr Überleben ist.[6] Hinzu kommt, dass Menschen auch von Privaten wie etwa von Unternehmen oder vom Staat wie etwa von Geheimdiensten algorithmisch als „digitales Double" in Form von Daten aus vielfältigen Quellen erfasst werden und auf diese Weise die Bindung an ihren konkreten Körper verlieren.[7]

In der nahöstlichen Kultur hat der Bezug des Menschen zu seinem Körper eine andere Bedeutung. Dies umfasst bis in die Gegenwart hinein auch den Blick auf Bilder, Fotos oder Karikaturen, die sich auf Menschen beziehen. Dafür sprechen u. a. Bilderverbote in der arabischen Kultur, die in jüngerer Vergangenheit zu heftigen Kontroversen mit der westlichen Welt geführt haben. „Vom Verbot der Bilder ist ein Bildbegriff betroffen, bei dem es darum geht, körperliches Leben mit Stimme und Atem auf leblose Bilder zu übertragen." Solche Bilder werden als Verrat am Lebendigen gesehen. „Ein Kopf blickt oder scheint im Bild zu blicken. Deshalb lässt er sich auch mit dem Leben verwechseln."[8]

Beim Streit darüber, wie mit Bildern der islamischen Religion im Allgemeinen und mit satirischen Bildern des Propheten Mohammed im Besonderen umzugehen ist,[9] spielt die Meinungsfreiheit als elementares Menschenrecht eine zentrale Rolle. Menschen müssen im Ausdruck ihrer eigenen Auffassung geschützt werden und auch die funktionale Bedeutung der Meinungs-, Presse- und Medienfreiheit in einer offenen Demokratie kann nicht überschätzt werden. Andererseits bedingen der Gedanke und das Prinzip der Menschenrechte im Kontext von Toleranz, dass die Person des Anderen respektiert und seine Überzeugungen und Meinungen toleriert werden.[10] Das politische Eintreten für Ziele und Forderungen, die sich z. B. aus einem religiösen Bilderverbot herleiten, ist also keineswegs ausgeschlossen. Im Kern geht es um die Verteidigung von Freiheitsrechten im gesellschaftlichen Raum und die Vermeidung ethisch begründeter Diskriminierungen von Personen, für die bestimmte Werte eine besondere existenzielle Bedeutung haben. Daraus folgt jedoch nicht, dass der Staat religiösen oder weltanschaulichen Überzeugungen, welchen Rückhalt sie bei Menschen auch haben mögen, die Chance einräumen darf, seine freiheitliche Ordnung von innen aufzurollen und schließlich mit Gewalt abzubauen.

Zum Szenario von Toleranz gehört die Schärfung des Blicks für Konfliktkonstellationen und Bedeutungszusammenhänge. Die skizzierten Probleme erfordern einen wechselseitigen Blick zwischen Kulturen und Wissenschaften, aber auch

6 Tinnefeld, Überleben in Freiräumen (2018), s. vor allem S. 77 f. und S. 117 f.
7 Bauman/Lyon, Daten, Drohnen, Disziplin (2013), S. 19.
8 Belting, Eine westöstliche Geschichte des Blicks (2008), S. 77.
9 S. dazu etwa Schloemann, Mohammed-Karikaturen. Leider nicht lustig, SZ v. 30.09.2015, S. 4.
10 Forst, Toleranz im Konflikt (2003), S. 46.

zwischen zwei oder mehreren Menschen. Dabei können schwierige Wissens- und Kompetenzfragen entstehen, etwa zwischen Religionswissenschaftlern und Politikern, Hirnforschern, Medizinern und Philosophen, zwischen Sicherheitspolitikern und den Verteidigern der Freiheitsrechte eines jeden Menschen.

Im 21. Jahrhundert gewinnt das Bild des Menschen in Verbindung mit Big Data, mit Algorithmen und Künstlicher Intelligenz (KI) neue Konturen. Dahinter verbergen sich Fragen nach der Autonomie des Menschen und des freien Willens, Fragen der informationellen Selbstbestimmung und Fremdbestimmung etwa durch Daten, welche basierend auf Heuristiken aus einer Vielzahl von Datenquellen errechnet wurden. In diesem Zusammenhang ergeben sich zugleich aktuelle Fragen nach den Folgen der Überwachung von Menschen, die von Sensoren oder eingebetteten Systemen durch Kameradrohnen erfasst werden.

Wo sind die roten Linien bei der Schaffung von zunehmend einseitig bestimmten (partikulären) Bildern des Menschen im Kontext der Informatik, der Gentechnologie oder Gehirnforschung? In welche Richtung wandeln sich universale Menschenrechte unter dem Einfluss von technischen, wissenschaftlichen, religiösen und politischen Entwicklungen, die ihre eigenen Bilder prägen?

2 Big Data

Big Data beschreibt in Zeiten der Digitalisierung aktuelle technische Entwicklungen, welche die jederzeitige Erfassung, Speicherung und Analyse eines großen und beliebig erweiterbaren Volumens unterschiedlich strukturierter, komplexer Daten ermöglichen.[11] Der Begriff Big Data wird daher häufig durch „smart data“ ersetzt.

Daten werden durch eingebettete IT-Systeme in technischen Geräten oder der jeweiligen Lebensumgebung des Betroffenen erfasst. Es kann sich um Daten handeln, die der Benutzer selbst eingegeben hat (z. B. E-Mails oder Daten in sozialen Netzwerken). Es kann sich aber auch um Daten handeln, die erhoben werden, „ohne dass der Einzelne sie eingibt – nur durch das schlichte Verhalten in einer technikgeprägten Umgebung“.[12] Diese Datenmengen sind jederzeit für diejenigen verfügbar, die Zugang zu ihnen haben.[13]

Hinter der permanenten Zugänglichkeit bzw. Allgegenwart vernetzter Datenströme (smart environment) verbirgt sich das Risiko, dass periodische Zeiten, von denen das menschliche Leben in den meisten Kulturen der Welt seit Jahrtausenden geprägt wurde, verschwinden. Zwar bestehen die Unterscheidungen von Wochen- und

11 Deutscher Bundestag, Wissenschaftlicher Dienst, Aktueller Begriff Nr. 37/13: Big Data; s. a. Studie des DIVSI, Big Data, 2016 unter: https://www.divsi.de/publikationen/studien/big-data/# (letzter Abruf 01.07.2019).

12 Roßnagel/Nebel, DuD 2015, 455.

13 Rifkin, The Age of Access (2000).

Feiertagen, von Tag und Nacht fort. Aber dieser Takt wird in einer durchgängig eingeschalteten Welt zunehmend aufgelöst. Dadurch verändert sich der Blick auf das persönliche und soziale Leben.[14]

Der Einsatz digitaler Technologien ermöglicht es, durch Big-Data-Analysen bisher unbekannte Korrelationen im menschlichen Leben zu entdecken und Muster des Denkens und Handelns zu erkennen, die in Staat und Wirtschaft Grundlage für viele Entscheidungen sind. Hier besteht das Risiko, dass nicht nach der Ursache für eine Korrelation gesucht wird, sondern diese als vorhanden hingenommen und daraus eine Heuristik abgeleitet wird. Der Philosoph Bernard Stiegler befürchtet eine vereinheitlichte Wahrnehmung in der heutigen (Technik-)Kultur. Er ist der Auffassung, dass der Einzelne dadurch seine subjektive Identität und seine individuelle Fähigkeit verliert, am sozialen Leben teilzunehmen.[15]

Die sich anbahnende Externalisierung des Menschen zu einem überprüfbaren „Objekt" steht in engem Zusammenhang mit flächendeckenden staatlichen Antiterrormaßnahmen und dem viralen Marketing (Virusmarketing) von Großunternehmen. Beim Abhören und Tracking von Nutzern der Mobilkommunikation sind auch mächtige Geheimdienste beteiligt. Sie übermitteln ebenso wie transatlantische Unternehmen freizügig persönliche Daten. Big Data ermöglicht es Sicherheitsbehörden und Unternehmen, jeden Menschen über räumliche und zeitliche Distanzen hinweg zu tracken, zu überwachen und zu steuern. Viele Big-Data-Anwendungen bauen z. B. auf Tracking als zentraler Technologie im Bereich „Smart Mobility".

Die gegenwärtige Entwicklung versammelt Fragen nach den Bildern vom Menschen in unserer Gesellschaft: Welcher Wert kommt dem Menschen zu? Worin bestehen seine Aufgaben, seine Bedürfnisse und sein Nutzen? Der Mensch wird im Fortschritt der Technik betrachtet – prägt sie ihn oder prägt er sie? Darf er algorithmisch erfasst werden und wenn ja, in welcher Form? Wird er nur als Datensatz und damit als ein „hochgradig fluides und mobiles digitales Double" dargestellt?[16] Kann vorausgesagt werden, wie der Mensch „funktioniert"? Welche Bedeutung hat der Einsatz von unbemannten Drohnen, die Menschen bei Tag und bei Nacht beobachten und zu ihren Zielobjekten machen?[17]

Der Science-Fiction-Film „Minority Report" von Steven Spielberg (2002) zeigt, wie mit Mitteln der Überwachung und softwaregestützter Statistik der Versuch

14 Zu Erscheinungsformen von Big Data vgl. auch Schmale/Tinnefeld, Privatheit im digitalen Zeitalter (2014), S. 152–162.

15 Stiegler, De la misère symbolique, Bd. 1: L'époque hyperindustrielle (2004).

16 Bauman/Lyon, Daten, Drohnen, Disziplin (2013), S. 14 m. w. N.

17 Vgl. allgemein zum Thema Drohnen Biermann/Wiegold, Drohnen – Chancen und Gefahren einer neuen Technik (2015); zu den Drohnen der NSA über das GILGAMESH-System siehe Schneier, Everything We know About How the NSA Tracks People's Physical Location, The Atlantic, v. 11.02.2014 unter: https://www.theatlantic.com/technology/archive/2014/02/everything-we-know-about-how-the-nsa-tracks-peoples-physical-location/283745/ (letzter Abruf 01.07.2019).

unternommen wird, das Denken und zukünftige Agieren eines Menschen zu erfassen. Der Film spielt in Washington D. C. im Jahre 2054. Er zeigt den Verlust geschützter privater Sphären. Jede Person ist überall erkennbar. Allerorts sind Überwachungskameras angebracht, die die Individuen per Augenscan identifizieren. Sowohl die Abrechnung der eigenen Gebühren für die Benutzung des öffentlichen Verkehrssystems als auch die Übermittlung persönlicher Werbebotschaften erfolgt aufgrund von Big-Data-Analysen. Bei der präventiven Verbrechensbekämpfung werden mobile Überwachungsdrohnen eingesetzt. Sogenannte Precogs besitzen seherische Fähigkeiten und können mittels Gedankenlesetechnik vermeintliche Mörder vorher erkennen, sodass die Polizei sie verhaften kann, bevor sie ihre Tat begehen können. Dieses Vorgehen beruht nicht auf einer Tat, sondern auf einem Gesinnungsstrafrecht. Letztlich wird hier mit dem Mittel der Strafverfolgung im Vorfeld konkreter Gefahren Gefahrenabwehr in Form von Verhinderungsvorsorge betrieben. Der Film zeigt die Verwundbarkeit eines solchen vorausschauenden Systems. Denn im Film geht es auch darum, dass ein Mörder durch einen klug geplanten Mord unter Ausnutzung des Systems (fast) nicht ergriffen wird.

Bezieht sich das Menschenbild, von dem der Film ausgeht, auf einen Menschen, dessen Wille determiniert und im Voraus berechenbar ist? Der Protagonist des Films lässt Zweifel an dieser Betrachtungsweise aufkommen. Die Hirnforschung befasst sich aktuell mit dem Bild des determinierten Menschen. Die Forscher untersuchen die Frage, ob das menschliche Gehirn eine „neuronale Maschine“ ist, deren Systemzustände in ihrer endlosen Vielfalt für die Wissenschaft „berechenbar“ sind. Dann wären die Denkprozesse des Menschen tatsächlich ausrechenbar, instrumentalisier- und nutzbar. Dann wäre der Mensch in erster Linie bloß „Objekt“ und nicht ein Rechtssubjekt mit Würde, persönlicher Freiheit und dem Anspruch auf Persönlichkeitsschutz.

Davon zu unterscheiden ist die Frage nach dem Cyborg als einem Menschen, der aus biologischen und künstlichen Teilen besteht.[18] Hier ist der Bereich der subkutanen Chips und anderer Implantate wie Neuro-Implantate angesprochen, die im medizinischen Bereich eine wichtige Rolle haben können, etwa zur Verbesserung der Gehirnfunktion bei gelähmten Menschen. Der nicht medizinische Einsatz von technischen Elementen wie Neuro-Implantaten – etwa zu Überwachungszwecken nach Art der Gedankenpolizei im „Minority Report“ – muss dagegen über die Frage der Willensfreiheit des Menschen angesprochen und als potenzielle Bedrohung der Menschenwürde und darüber hinaus der demokratischen Gesellschaft betrachtet werden.[19]

18 Der Begriff Cyborg stammt aus der Raumfahrt und steht für cybernetic organism (kybernetischer Organismus).

19 Vgl. Stellungnahme der European Group on Ethics in Science and New Technologies der Europäischen Kommission zu ICT-Implantaten; abrufbar unter: https://ec.europa.eu/info/publications/ege-opinions_en (letzter Abruf 01.07.2019).

3 Hirnforschung

Die unaufhörliche und teils unbemerkte Erweiterung verfügbarer Daten aus allen denkbaren Lebensbereichen kann eine wichtige Quelle für die empirische Erforschung sozialer Zusammenhänge und für die Erforschung der Gene oder des Gehirns bieten. Es wird wissenschaftlich untersucht, ob der Mensch eine „Marionette seiner Gene“ ist. Zeitweise wurde angenommen, dass alle menschlichen Prägungen, Vorlieben und Handlungsweisen bereits im Erbgut festgelegt sind. Einige Wissenschaftler tendieren zu der Annahme, dass der Mensch von seinen Nervenzellen (Neuronen im Gehirn) und ihren Verbindungen (Synapsen) bestimmt ist.

Auch wenn die Gensequenz eines Menschen unveränderlich sein sollte, so wird doch die Aktivität der Gene durch von außen kommende Signale (mit-)gesteuert. Funktioniert nun das Denkorgan unabhängig von Umwelt, kultureller Prägung, mentalen Gegebenheiten, Traditionen und deren Erfahrung? Es ist unbestritten, dass das Gehirn ein Wissen darüber hat, was es im Laufe der Evolution gelernt hat. Dazu tritt aber auch das Wissen, was sich dem Menschen von früher Jugend an eingeprägt hat. Kann es sein, dass Verschaltungen des Wissens in der Gehirnarchitektur den Willen des Menschen festlegen?[20]

Die Hirnforschung geht in viele verschiedene Richtungen. Bekannt ist das sehr umstrittene Human-Brain-Projekt. Ziel des Projektes war es, das gesamte Wissen über das menschliche Hirn zusammenzufassen und mittels computerbasierter Modelle zu simulieren. Das interdisziplinäre Wissen für das Projekt reicht von der Molekularbiologie über die Zellbiologie bis zum Netzwerk des Gehirns. Das Projekt wurde inzwischen umfunktioniert. Die Kernprojekte befassen sich nun ausschließlich mit dem Aufbau einer „Informations- und Kommunikationsplattform“, während genuine Bereiche wie die kognitive Neurowissenschaft aus dem Kernbereich ausgeklammert worden sind.[21]

(Mechanisch verstandene) Hirnfunktionen sind zwar notwendig für geistige Akte wie Denken, Empfinden und Wahrnehmen, sie können diese aber nicht hinreichend erklären. Diese Einsicht findet sich bereits in dem Mühlengleichnis des Mathematikers und Philosophen Gottfried Wilhelm Leibniz (1646–1716), der in seiner Monadologie schrieb:

> Man muss übrigens notwendig zugestehen, dass die Perzeption und das, was von ihr abhängt, aus mechanischen Gründen [...] nicht erklärbar ist. Denkt man sich etwa eine Maschine, die so beschaffen wäre, dass sie denken, empfinden und perzipieren könnte, so könnte man sich diese derart proportional vergrößert denken, dass man in sie wie in eine Mühle eintreten könnte.

20 Singer, in: Geyer (Hg.), Hirnforschung und Willensfreiheit. Zur Deutung der neuesten Experimente (2004).

21 Stallmach, Flaggschiff auf Schlingerkurs, NZZ v. 16.06.2014, S. 50.

> Dies vorausgesetzt, wird man bei der Besichtigung des Inneren nichts weiter als einzelne Teile finden, die einander stoßen, niemals aber etwas, woraus eine Perzeption erklärbar wäre.[22]

Persönliche Erfahrung, insbesondere die Erfahrung von Freiheit ist nach dem Mediziner und Philosophen Günter Rager eine unmittelbare, „nicht hintergehbare“ und „nicht auf etwas anderes zurückführbare Gewissheit“.[23] Diese Einsicht findet sich in dem berühmten Satz des Königsberger Philosophen Immanuel Kant (1724–1804) wieder: „Das: Ich denke, muß alle meine Vorstellungen begleiten können [...].“[24] Zu ergänzen ist, dass Denken und Körper interagieren bzw. Verbindungen zueinander aufweisen, die die Rezeption der Welt erst ermöglichen. Diese Sicht betont in einer Zeit der Umweltzerstörung der Dichter und Umweltaktivist Gary Snyder.[25]

Die eigenen Vorstellungen beruhen auf der Geschichte und Kultur des Einzelnen, auf den Einflüssen von Kindheit an, auf den Medien, die Nachrichten, Unterhaltungen und andere Informationen in Wort und Bild liefern, auf Social Media, den privat oder beruflich genutzten Netzwerken und Multimedia-Plattformen. Das körpergebundene Ich und nicht das Gehirn fügt die vielfältigen Eindrücke und Einzelinformationen zusammen. Der Mensch entscheidet aufgrund dieser Informationen, seiner Gedanken, Empfindungen, Fantasien und Erinnerungen. Das bedeutet gleichzeitig, dass er niemals von diesen ursächlichen Teilen und seiner Umwelt frei ist. Die grundsätzliche Frage, die sich stellt, ist: Verfügt der Mensch über einen freien Willen?

Der Philosoph Peter Bieri stellt in seinem Buch „Das Handwerk der Freiheit“[26] fest, dass es einen unbedingt (absolut) freien Willen nicht gibt. Der freie Wille kommt nicht aus dem Nichts. Er ist immer der verstandene Wille, der anders als Automaten um seine Beschränkung weiß. Andernfalls würde sich ein Tor zu offener oder versteckter Fremdbestimmung öffnen; der Einzelne würde jeweils nach den Voraussetzungen der an ihn gerichteten persönlichen oder politischen Erwartungen funktionieren.

Freiheitsbezogene Staaten wissen, dass sich eine lebendige Selbstbestimmung des Bürgers und seine autonome Mitwirkung an öffentlichen Belangen vor allem über die Medien, über Information und über Teilhabe herstellen lässt. Information ist beides, die Voraussetzung von Selbstbestimmung ebenso wie die von Teilhabe. In Zeiten wachsender Datenfluten, von Big-Data-Analysen und Künstlicher Intelligenz wird es allerdings für den Menschen zunehmend schwieriger, sein eigenes Datenbild und dasjenige, das sich andere von ihm machen, zu verfolgen und zu steuern. Die europäische Rechtsordnung versucht den Einzelnen dabei zu

22 Leibniz, Monadologie (1714), § 17.
23 Rager/Brück, Grundzüge einer modernen Anthropologie (2012), S. 37.
24 Kant, Kritik der reinen Vernunft (1787), B 131.
25 Snyder, Lektionen der Wildnis (2011), S. 139.
26 Bieri, Das Handwerk der Freiheit. Über die Entdeckung des eigenen Willens (2001); s. aber Singer, Der Beobachter im Gehirn. Essays zur Gehirnforschung (2002).

unterstützen, indem sie ihm das Recht auf Privatheit und Datenschutz gegen den Staat und gegen Dritte an die Hand gibt. Sie staffelt rechtlich die Schutzbereiche, die gesetzlich einem Zugriff offen bzw. nicht offen stehen. Skizzieren lässt sich dies wie folgt:

Der intime und private Bereich und entsprechend sensible (besondere) Informationen entziehen sich ganz oder überwiegend der rechtlichen Gestaltung: Sie sind tabu. Dagegen sind Informationen über gemeinschaftsabhängige Lebensbedingungen (Beruf, Eigentum, Mitgliedschaft in Vereinen, Teilhabe am öffentlichen Leben) für eine digitale Datenerfassung und Verwendung grundsätzlich unter bestimmten Voraussetzungen zulässig. Dabei spielt das Gebot der Zweckbindung eine wichtige Rolle.

Das Gebot der Zweckbindung soll sicherstellen, dass personenbezogene Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie erhoben worden sind. Eine Weiterverarbeitung zu einem neuen Zweck muss ggf. kompatibel mit dem ursprünglichen Zweck sein, für den die Daten erhoben worden sind. Eine Datenspeicherung auf Halde (Vorratsdatenspeicherung zu unbestimmten Zwecken) ist grundsätzlich unzulässig. Sie ist auch kein angemessenes Instrument im Rahmen von Ermittlungsverfahren, die weit im Vorfeld konkreter Gefahren die repressive Nutzung von Daten ermöglichen, etwa die der auf Vorrat gespeicherten Telekommunikationsverkehrsdaten. Digitale Datenverarbeitung und Datennutzung jenseits des Grundsatzes der Zweckbindung wären wie eine Streubüchse. Niemand könnte wissen, wo seine Daten verbleiben und wer sie möglicherweise für fremde Zwecke verwendet, etwa für eine vorbeugende Verbrechensbekämpfung (Verhinderungsvorsorge). Seit Jahrzehnten verteidigen Mitglieder der Zivilgesellschaft Bürger- und Freiheitsrechte gegen eine solche Entwicklung.[27]

Je näher die reale Umgebung (die eigene Wohnung als räumliche Privatheit, Tagebuchaufzeichnungen, die vertrauliche Telekommunikation) und die Lebenssituation (Geburt, Tod, Scheidung) dem Einzelnen zugehören und von der Mitbetroffenheit anderer abgegrenzt werden können, desto strenger müssen die gesetzlichen Anforderungen an eine Datenerfassung, -verarbeitung und -nutzung sein. Falls sie nicht erfüllt sind, kommt alternativ eine Einwilligung des Betroffenen in den Umgang mit seinen Daten in Betracht. Eine Einwilligung kann jedoch nur dann Wirkkraft entfalten, wenn der Betroffene zuvor über den Zweck der Verarbeitung (durch Behörden, Forscher, Mediziner, Händler usw.) aufgeklärt worden ist. Jedoch darf eine solche kontextbezogene „sprechende" Information nicht ausarten in zu viel Information – *too much information*. Nur unter diesen Voraussetzungen kann von einer informierten Einwilligung (*informed consent*) gesprochen werden, die am ehesten als frei und verantwortlich bezeichnet werden kann.

27 Baum/Hirsch, Deutschland von seiner liberalen Seite (2016).

4 Algorithmen und Künstliche Intelligenz

Wer sich das handlungsleitende Bild eines selbstbestimmten Menschen vor Augen hält, fragt nach den Risiken für die reale Existenz und Selbstbestimmung eines Menschen, der durch Algorithmen auf ein „digitales Double" verengt werden kann. Der amerikanische Journalist Stephen Baker befasst sich in seinem Buch „Numerati"[28] mit der Frage, wie Menschen als Wähler, Käufer oder Blogger von leistungsfähigen Rechenprogrammen codiert und beeinflusst werden. Wirken Algorithmen als mächtige Verstärker etwa bei der Willensbildung von Wählern? Nach Studien der Verhaltensforscher Robert Epstein und Ronald E. Robertson können sie nachweisbar eine Mehrheitsumkehr in einer Demokratie herbeiführen.[29] Unbekannt ist allerdings, in welcher Hand die Einflussquellen liegen, wer für sie verantwortlich zeichnet.

Was genau ist ein Algorithmus? Der Algorithmus kann als rein mathematisches Konstrukt definiert werden, also eine Abbildung der Eingabe auf eine Ausgabe. Um einem Algorithmus ein „Gedächtnis" hinzuzufügen, kann als Eingabe auch ein interner Zustand des Algorithmus verwendet werden – über die mehrfache Anwendung des Algorithmus kann sich dieser Zustand dann weiterentwickeln. Den Entscheidungskriterien eines Algorithmus kann ein statistisches Modell oder eine Heuristik zugrunde liegen, welche fest im Algorithmus integriert ist. In diesem Fall ist das Urteil über einen Menschen im Algorithmus hinterlegt, ähnlich wie bei einem Credit Scoring. Der Algorithmus kann aber auch das statistische Modell selbst bilden. In einer Lernphase (oder kontinuierlich) wird er dann mit einer großen Menge an Daten gespeist, von denen einzelne markiert werden. Der Algorithmus sucht in der Folge nach Gemeinsamkeiten in den übergebenen Daten und erstellt darauf basierend das statistische Modell. Häufig kommen Mischformen der beiden Arten vor, etwa wenn Sicherheitsbehörden versuchen, Terroristen über statistisch aufgeladene Algorithmen rechtzeitig zu erkennen (*predictive policing*). Die auszuwertenden Datentypen wie „gewählte Mahlzeit im Flugzeug" und „Zahlungsart des Tickets" oder „Herkunft" und „Religionszugehörigkeit" können im Algorithmus vorgegeben werden, sodass der Algorithmus nur noch die Gewichtung lernt, mit der die Datentypen in den Terroristen-Score einfließen.

In diesem Prozess wird gleichsam ein transparentes „digitales Double" erzeugt. Die Daten, die damit an die Stelle des Betroffenen treten, sind dessen Kontrolle so gut wie entzogen. So können nicht nur Unbeteiligte in das Kontrollraster geraten. Es entstehen auch „soziale Klassifizierungen", für die niemand mehr verantwortlich zeichnet.[30] Ein Beispiel für die Logik der neuen Ermittlungsmethoden ist, dass

28 Baker, Die Numerati: Datenhaie und ihre geheimen Machenschaften (2008).

29 Siehe unter: http://www.faz.net/aktuell/wirtschaft/mayers-weltwirtschaft/mayers-weltwirtschaft-die-digitale-revolution-13841924.html (letzter Abruf 01.07.2019).

30 Bauman/Lyon, Daten, Drohnen, Disziplin (2013), S. 19.

„Araber“ und „Muslime“ häufiger als andere auf westlichen Flughäfen einer Überprüfung unterzogen werden. Anders formuliert: Nach den Suchkriterien ist ein Araber vorhanden, der die Eigenschaft hat, ein Muslim zu sein, und dem nun weitere Eigenschaften zugeschrieben (angeklebt) werden wie die, „gefährlich“ zu sein. Ein solches Vorgehen bezeichnet der Rechtsphilosoph Lothar Philipps als Ausdruck einer falschen Sichtweise.[31]

Zusammengefügte und „überklebte“ Merkmale sparen hinterfragbares Wissen über den Betroffenen aus. Der Ermittler weiß nicht, welche Daten nach welchem Algorithmus auf seinem Rechner angezeigt werden. Daraus resultierende Diskriminierungen aufgrund einer Religion oder einer ethnischen Zugehörigkeit (*racial profiling*) sind für ihn nicht erkennbar. Menschenbilder der Gesuchten erscheinen als Vorurteile, eben Vorab-Urteile. Sie steuern mit ihrer Eigendynamik die entsprechende Wahrnehmung der Ermittler. Zudem ist die Analysesoftware öffentlich nicht nachprüfbar.[32]

Ermittlungsbehörden zeichnen hier nicht für Entscheidungen im Sinne von „Konsequenzen-tragen-Müssen“, wie es Hans Jonas formuliert hat.[33] Sie können unbeteiligt wie Automaten Terroristen ausmachen. Die Überwachungssysteme bringen zwar aufgrund der softwaregestützten statistischen Erfassung viele konsistente Resultate hervor. Sie bewirken aber gleichzeitig soziale Klassifizierungen. Der Blick auf den Einzelnen erfasst nicht mehr den Menschen, wie er sich in seinen Eigenheiten und Lebenssituationen von anderen unterscheidet.

Nach dem Grundsatz von der Gleichheit aller Menschen kann nur eine Aussage über den Grad ihrer Ähnlichkeit oder Verschiedenheit getroffen werden. Ist die Wirklichkeit im Blickwinkel der zu beurteilenden Ermittlungsfrage „Terrorist oder Nicht-Terrorist“ realitätsgerecht abgebildet? Oder entwickelt sie Folgen, weil Vorurteile existieren? Die Problematik, die ein derlei verengter Blickwinkel mit sich bringt, hat der britische Astrophysiker Arthur Eddington (1882–1944) in seiner Parabel vom Ichthyologen („Fischkundiger“) anschaulich vor Augen geführt. Dieser Ichthyologe erforschte das Leben im Meer und stellte nach vielen Fangzügen mit dem immer gleichen Netz fest: Alle Fische sind größer als fünf Zentimeter. Er ignorierte den Einwurf, dass damit nur etwas über die Maschengröße seines Netzes ausgesagt würde, nicht aber die Natur der Fische. Er merkte an: „Was ich mit meinem Netz

31 Philipps zit. nach Tinnefeld, PinG 2015, 26.

32 Hoffmann-Riem, Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, AöR 142 (2017), 1, 6 f. Zur Diskriminierung von Afroamerikanern in den USA durch Algorithmen siehe Heise Online v. 24.05.2016; abrufbar unter: http://www.heise.de/newsticker/meldung/US-Justiz-Algorithmen-benachteiligen-systematisch-Schwarze-3216770.html (letzter Abruf 01.07.2019).

33 Jonas, Das Prinzip Verantwortung, Versuch einer Ethik für die technologische Zivilisation (1984).

nicht fangen kann, liegt prinzipiell außerhalb fachkundlichen Wissens [...]. Für mich als Ichthyologe gilt, was ich nicht fangen kann, ist kein Fisch."[34]

Wie vergleichbar ist die Feststellung des Fischforschers mit dem Vorgehen von vielen Terroristenfahndern? Vereinfacht formuliert könnte die Antwort lauten: Jede Person, die im Algorithmus der jeweiligen Spähsoftware hängenbleibt, ist ein Terrorist. Dieser verallgemeinerte Mensch ist jedoch nicht real. Die Folge ist, dass Menschenbilder von großer Ungleichheit geschaffen werden können. Besonders derjenige, der einer verdächtigen Bevölkerungs- oder Religionsgruppe angehört, muss sich verunsichert fühlen. Der Journalist Frank Schirrmacher sprach von dem wachsenden Wahn, „aus Angst vor Kontrollverlust die Welt in Formeln, Systematiken und Algorithmen [...] zu verwandeln".[35] Der amerikanische Publizist Jamie Holmes analysiert diese Entwicklung und ihre Folgen: „When our need for closure is high, we tend to revert to stereotypes, jump to conclusions, and deny contradictions."[36]

Die Frage nach den Möglichkeiten, Künstliche Intelligenz (KI) zu schaffen, beschäftigt Menschen nach der ersten computerähnlichen Maschine durch den Mathematiker Alan Turing und dem sog. Turing-Test, der als Maßstab zur Feststellung der Kommunikations-KI dienen soll. Der Test gilt als bestanden, wenn etwa bei einem Chatbot unsicher ist, ob die betroffene Person mit einem Menschen oder einer Maschine spricht. Es lässt sich vielleicht nicht immer sofort sagen, ob es sich bei einem Gegenüber um eine virtuelle Identität oder eine menschliche Person handelt. Nach wie vor weist aber das „Kommunikationsverhalten" einer KI im Verhältnis zu kommunikativen Akten einer Person erhebliche Defizite auf.[37]

Die rechtliche Bewältigung des Phänomens KI beginnt mit einer Begriffsbestimmung oder zumindest mit einer Arbeitsdefinition. Die moderne KI wird mit genuin menschlichen Eigenschaften und Fähigkeiten assoziiert. Hierzu gehört das namensgebende Wort „Intelligenz", außerdem „Lernen", „Wissen", „Bewusstsein", Handeln u. a.[38] Eine KI beruht auf selbstlernenden Algorithmen mittels tiefer neuronaler Netze, die der Struktur des menschlichen Gehirns nachgebildet sind. Solche Netze bestehen aus Eingangs- und Ausgangsneuronen sowie dazwischen liegenden Schichten, den sogenannten Hidden Layers.

Beim „Machine Learning" funktionieren Algorithmen nach dem traditionellen „Wenn-dann-Prinzip", die konkrete Reaktion im Algorithmus ist also vorgegeben (automatisches System). Eine KI basiert dagegen auf dem Konzept „Deep Learning". Lernend meint, dass eine KI Informationen aufnehmen und auswerten sowie eine Handlungsoption zur Erreichung bestimmter Ziele entwickeln kann. Zu betonen ist,

34 Dürr, in: ders. und Zimmerli (Hg.), Geist und Natur (3. A. 1990), S. 29 ff.

35 Schirrmacher, Payback (2. A. 2011), S. 32, 155 f.

36 Holmes, The Power of Not Knowing (2015), S. 13.

37 Turing, I. – Computing Machinery And Intelligence, Mind. Bd. LIX, Nr. 236 (1950), S. 433–460; kritisch Russel/Norvig, Artificial Intelligence, (3. A. 2016), S. 3.

38 Zum Konzept Deep Learning Schael, DuD 2018, 530.

dass KI häufig nicht Big-Data-basiert ist, sondern je nach Grad der Vernetzung auf möglichst wenig Daten etwa in Datenbanken zugreift, um ein Maximum an Wissen zu generieren. Die Zielsetzung einer KI kann darauf ausgerichtet sein, ein Muster etwa von Bildern oder Gesichtern sowie Bedeutungszusammenhänge zu erkennen. Die KI ist also dynamisch und entwickelt sich selbstständig bzw. „quasi-autonom" weiter. Das heißt: Konkrete Reaktionen sind nicht vorgegeben, der Programmierer kann die konkrete Reaktion des Programms auch nicht vorhersehen. Das macht KI zu einer Black Box für betroffene Personen.[39] Es muss daher zum Schutz des Betroffenen sichergestellt werden, dass Algorithmen für KI so programmiert werden, dass die betroffene Person nachvollziehen kann, welche ihrer Daten verwendet worden sind und warum ein bestimmtes Ergebnis bzw. eine Entscheidung erzeugt worden ist (Transparency by Design). Dieses Verfahren ist nicht nur bei der Verarbeitung von personenbezogenen Daten, sondern auch von Sachdaten (Planungen von Verkehrswegen und Stromtrassen, Wettervorhersagen, Prüfungen der Stabilität von Brücken usw.) wichtig. Andernfalls ist Verwaltungshandeln nicht hinreichend transparent, sodass eine autonome Mitwirkung von Bürgern an öffentlichen Belangen beeinträchtigt wäre.[40]

Bei näherem Hinsehen erweist sich eine kommunikative KI im Rahmen der Meinungs- und Pressefreiheit als besondere Herausforderung. Eine KI ist kein Subjekt. Sie kann keine eigene Meinung haben und generiert eine Meinung oder eine Tatsachenbehauptung algorithmisch auf der Grundlage vorhandener Eingaben und Datenbanken. Bei Äußerungen (z. B. Hassreden) einer KI, die in dieser Art im Algorithmus nicht vorgesehen waren, sondern die die KI erst gelernt und dann quasi autonom generiert hat, ist es möglich, dass es sich nicht um die eigene Meinung oder eine Tatsachenbehauptung des Anbieters oder Herstellers der KI handelt. Diese Frage ist im Verhältnis zum algorithmisch basierten Journalismus von spezieller rechtlicher Bedeutung. Hier gilt es zu klären, ob und ggf. inwieweit sich ein Nutzer der KI auf die grundrechtlich garantierte Pressefreiheit und die damit verbundenen Medienprivilegien berufen kann.[41]

Von besonderem Interesse ist die Frage nach der Bedeutung von Robotern etwa im Arbeits- oder Pflegeverhältnis.[42] Bei Robotern handelt es sich um eine „verkörperte KI". In der Debatte stehen u. a. Roboterassistenten für selbstbestimmtes personales

39 Hoeren/Niehoff, RW 1 (2018), 49 f.

40 Vgl. Positionspapier „Transparenz der Verwaltung beim Einsatz von Algorithmen für gelebten Grundrechtsschutz unabdingbar", unter: https://www.datenschutzzentrum.de/upload/informationsfreiheit/2018_Positionspapier-Transparenz-von-Algorithmen.pdf (letzter Abruf 01.07.2019).

41 Zum Problem Weberling, NJW 2018, 735, 739.

42 Die Bezeichnung von Maschinen als Roboter beruht auf einem Theaterstück des tschechischen Schriftstellers Karel Capek, der 1920 in dem Drama R.U.R. (Rossums Universal Roboter) den Mythos des Golem verarbeitete. Das Stück handelt von künstlichen Menschen, die als billige Arbeitskräfte eingesetzt werden, sich dagegen auflehnen und die Menschheit auslöschen; s. a. Stanislaw Lem, Also sprach Golem (1978), aus dem polnischen v. Friedrich Griese (11. A. 1986).

Leben im Alter. Roboter sind aber keine agierenden verantwortlichen Subjekte. Welche Informationen müssen daher von wem den betroffenen Personen zur Verfügung gestellt werden, bevor ein „smarter" Roboter in der Pflege eingesetzt werden darf? Damit keine Verantwortungslücken entstehen, ist vorab u. a. zu klären, welche Person, welches Unternehmen oder welche Institution beim Einsatz eines Roboters verantwortlich ist, sodass eine personenbezogene Datenverarbeitung für die betroffene Person transparent ist.[43]

Joseph Weizenbaum (1923–2008), ein Pionier im Bereich der Computerwissenschaft und der Erforschung von KI, gehörte zu den scharfen und phantasievollen Kritikern seines Fachs. Bekannt ist sein Computerprogramm Eliza, das er in den sechziger Jahren des 20. Jahrhunderts entwickelte. „Eliza" parodierte psychotherapeutische Gespräche, indem das Programm Sätze aufnahm und umformulierte (Tut mir leid zu hören, dass Sie heute depressiv sind). Weizenbaum war erschrocken darüber, dass Menschen „Eliza" als Gesprächspartner emotional ernst genommen haben. Denn das Motiv der Teilnahme setzt Empathie, nämlich die Fähigkeit, sich in andere Menschen hineinzuversetzen, voraus. Der Verhaltensforscher Michael Tomasello geht davon aus, dass es wohl diese Fähigkeit ist, die es möglich macht, dass Menschen in komplexer Weise miteinander kooperieren können.[44] Weizenbaum betonte, dass Computer allenfalls moralische Entscheidungen simulieren können. In seinem Werk taucht immer wieder die Utopie vom ganzen Menschen auf, der nicht durch „maschinelles Denken" erfasst werden kann, dem auch bestimmte Denkakte vorbehalten bleiben müssen.[45] Es ist zudem naheliegend, dass sich menschliche Kommunikation trotz großer Fortschritte einer KI immer noch am intensivsten in der persönlichen Begegnung entfalten kann. Dafür spricht auch, dass ein Gespräch mit physischen Signalen verbunden ist, die treffend als Körpersprache bezeichnet werden können.

43 Zum Projekt „Orient" der Universität Paderborn, das im Rahmen der EU Initiative „More years better Years" unter Leitung von Kirsten Thommes durchgeführt wird, unter: www.connectnrw.de/de/Projekt-Orient-der-Universitat-Paderborn-Mit-Robotik-die-Pflege-der-Zukunft-gestalten.php (letzter Abruf 01.07.2019).

44 Tomasello, Die Ursprünge der menschlichen Kommunikation, aus dem Amerikanischen v. Jürgen Schröder (2009).

45 Weizenbaum, Die Macht der Computer und die Ohnmacht der Vernunft (14. A. 1978); Tinnefeld, DuD 2018, 733. Stephen Hawking, Kurze Antworten auf große Fragen, aus dem Englischen v. S. Held u. H. Kober (7. A. 2018), 211f., warnt vor einem ungebremsten Einsatz der KI, die sich „mit ständig zunehmender Geschwindigkeit selbst überarbeitet" und „selbständig ihre Ziele auswählen und eliminieren kann", etwa im Feld autonomer Waffensysteme.

5 Drohnen

Die Revolution der Algorithmen und ihre Auswirkungen auf menschliches Leben werden durch den Einsatz von Drohnen noch einmal verstärkt. Die Entwicklung unbemannter, ferngesteuerter Drohnen, die auch „Predator“ (Raubtier) genannt werden, ist am weitesten in den USA fortgeschritten. Die Drohnen sind mit Kameras und anderen Sensoren versehen und können Gebiete stunden- und tagelang beobachten. Dazu benötigt jedes System einen eingebetteten Computer, auf dem die eingehenden Daten aller Sensoren gesammelt, zusammengeführt, aufbereitet, ausgewertet und zu Kommandostellen übertragen werden. Diese verfügen ebenfalls über ein Computersystem, mit dem weitere Auswertungen der Daten möglich sind. Durch den Bordcomputer werden alle Geräte gesteuert.

Mit Raketen bestückt können unbemannte Drohnen in Kampfeinsätzen Verwendung finden. Sie sind i. d. R. mit kritischen Programmen und als geheim klassifizierten Daten ausgestattet. Zunehmend werden autonome Waffensysteme eingesetzt. Diese sollen selbst signifikante Daten ausmachen und „eigenständig“ über weitere Aktionen entscheiden. Das autonome Waffensystem führt Algorithmen aus, die ggf. auch über Leben und Tod entscheiden. Fraglich ist, ob und wer in dieser Phase noch Verantwortung für Tötungen trägt, die auch zivile Personen treffen können. Die Drohnen revolutionieren die Kriegsführung und den Kampf gegen den Terror.[46]

Drohnen gibt es inzwischen in allen Preislagen, Formen und Größen. Die kleinsten Modelle kann das menschliche Auge nicht mehr von Vögeln oder Insekten unterscheiden. Sie weisen geringere Kosten auf, aber auch weniger Transparenz für diejenigen, deren Daten erfasst werden. Sie ersetzen gefährliche Einsätze von Soldaten vor Ort und dienen Journalisten für Recherchen, auch im Überflug umgrenzter privater Wohnbereiche.[47] Der veraltete Schlüssellochblick wird mittels in Drohnen eingebauter Sensoren abgelöst. Die neue Technik der amerikanischen Air Force nennt sich „Gorgon stare“.[48] Die Bezeichnung spielt auf die Gorgonen in der griechischen Mythologie an. Der Anblick der Gorgone Medusa ließ jeden Betrachter zu Stein erstarren.

Ein Mensch kann im Blickfeld der Drohne pausenlos „überprüft, beobachtet, getestet, bewertet und in Kategorien eingeteilt werden“.[49] Das System, da regelmäßig geheim gehalten, ist für den überwachten Menschen undurchsichtig. Dagegen wird der Einzelne für die Überwacher transparent, ohne Rücksicht auf private Räume und Zeiten für Ruhe und Intimität. Die neue Transparenz unter dem Blick

46 Braml, Der amerikanische Patient (2012), S. 82 ff; zur datenschutzrechtlichen Dimension der Überwachung durch Auflärungs- und sog. Killerdrohnen vgl. Tinnefeld, ZD 2016, 253, 254.
47 Hofmann/Hödl, DuD 2015, 167, 170.
48 Siehe unter: https://de.wikipedia.org/wiki/Gorgon_Stare (letzter Abruf 01.07.2019).
49 Bauman/Lyon, Daten, Drohnen, Disziplin (2013), S. 14.

der Medusa ist tyrannisch. Sie „schafft“ das Bild eines Menschen ohne Gemeinschaft und Zivilgesellschaft.

Die Chance des Menschen, seine Privatheit und Selbstbestimmung in Freiheit mit anderen zu leben, geht durch eine angestrebte totale Überwachung, die einäugig auf das Ziel „Sicherheit“ gerichtet ist, verloren, Diese Gefahr zeichnet sich auch durch die grenzenlose Tätigkeit von Geheimdiensten deutlich ab. Sie ist durch den Whistleblower Edward Snowden ins Scheinwerferlicht der Öffentlichkeit gelangt.[50] Franz Kafka hat in seiner Parabel „Der Bau“ die trostlose Existenz eines verwahrlosten kleinen „Ruinenbürgers“ dargestellt, der von jeglichem Miteinander abgeschnitten ist.[51]

Dieter Suhr spricht davon, dass Menschen sich erst durch andere Menschen entfalten.[52] Der Einzelne sei innerhalb der sozialen Gemeinschaft auf Kommunikation angewiesen. Die anderen seien das soziale Umfeld, in dessen Rahmen sich die Persönlichkeit des Einzelnen auch in vernetzten sozialen Lebensräumen entfalten kann. In der digitalen Zivilgesellschaft lebt die Idee der „Freiheitsausübung auf Gegenseitigkeit“[53] insbesondere vom Grundrecht auf Datenschutz als einem Dialogrecht, das auch in Zeiten von Big-Data-Anwendungen in der alltäglichen Rechtsverwirklichung nicht unterwandert werden darf. Der Einzelne soll grundsätzlich in der Lage sein, persönliche Daten steuern und über ihre Verwendung mitbestimmen zu können. Und das heißt auch, dass eine Entscheidung allein aufgrund der Gewichtung von Algorithmen und KI grundsätzlich nicht zulässig ist. Grund- und Menschenrechte bilden das Fundament für die gesetzgeberische Sicherung dieser und weiterer realen Freiheitsausübung der Menschen.

6 Grund- und Menschenrechte

Schon im Begriff „Grundrechte“ kommt zum Ausdruck, dass es sich um Rechte handelt, denen etwas Grundsätzliches und Dauerhaftes innewohnt.[54] Eine entsprechende Bedeutung kommt dem Begriff „Menschenrechte“ zu. Menschenrechte haben sich in der Zeit der Aufklärung näher herausgebildet. Die Niederlegung der Menschenrechte im 17./18. Jahrhundert gilt als Fanfarenstoß der Aufklärung, der

50 Rosenbach/Stark, Der NSA Komplex. Edward Snowden und der Weg in die totale Überwachung (2014); Bromwich, Snowden & Citizenfour, in: The New York Review of Books (2014), Vol. LXI, No. 19, S. 4–7.

51 Kafka, Nachgelassene Schriften und Fragmente, hg. von Schillemeit (1992), S. 590 f.; vgl. auch Tinnefeld/Schmale, DuD 2012, 401.

52 Suhr, Entfaltung der Menschen durch die Menschen (1976).

53 Hoffmann-Riem, Ganzheitliche Verfassungsrechtslehre und Grundrechtsdogmatik, AöR 1991, 501.

54 Hornung, Grundrechtsinnovationen (2015), S. 2 f.

auch in Zeiten wachsender Datenmonopole von Konzernriesen und mächtigen Geheimdiensten seine Wirkung nicht verlieren darf.[55] Thomas von Danwitz spricht in diesem Kontext von der extremen Gefährdung der Privatsphäre, die durch eine umfassende Speicherung von Verkehrsdaten auf Vorrat eintrete, weil sie sehr genaue Schlüsse auf das Privatleben der Betroffenen zulasse.[56]

In einer vernetzten Welt kann der Schutz von digitalen Grund- und Menschenrechten nur noch auf mehreren Ebenen verwirklicht werden: international, supranational und national. Nach zwei grausamen Weltkriegen haben die Vereinten Nationen (UN) 1948 in der Allgemeinen Erklärung der Menschenrechte (AEMR) zum ersten Mal grundlegende Prinzipien des menschlichen Zusammenlebens in freier Entscheidung mit der Mehrheit der auf Erden lebenden Menschen angenommen, vertreten durch ihre Regierungen.[57] Die ersten Worte der Menschenrechtsdeklaration lauten: „Alle Menschen werden frei geboren, mit gleicher Würde und mit gleichen Rechten." Hinter dieser Formulierung steht auch die Aufforderung zu einem toleranten Verhalten gegenüber Fremden. Die universalen Menschenrechte gestehen jeder Person Freiheitsrechte zu. Jeder hat das Recht, eine eigene Meinung zu haben. Toleranz ist so gesehen ein Gebot der Gleichheit.

Intoleranz wächst dann, wenn Menschen aufgrund ihrer Rasse, ihres Geschlechts, ihrer ethnischen Herkunft oder Religion als „unwerte" Personen adressiert, stigmatisiert und diskriminiert werden, wie dies im Nationalsozialismus, in faschistischen und neuerdings in radikal fundamentalistischen Staaten, aber auch in EU Staaten der Fall ist. Der Gewaltforscher Wilhelm Heitmeyer spricht davon, dass ein Teil der sog. Normalbevölkerung in Deutschland Einstellungsmuster zeige, die als „gruppenbezogene Menschenfeindlichkeit" bezeichnet werden könnten. Und ein kleinerer Teil sei in die Nähe extremistischer Gruppen, nämlich autoritär-nationalistischer sowie systematisch-feindlicher Milieus gerückt.[58] Auf diese Weise werden Menschen als sog. „Andere" aus der universalen Gemeinschaft derer, denen Menschenrechte zustehen, ausgeschlossen. Individuelle Personen werden zu Kollektiven verbunden, und Kollektive verbinden sich mit immer denselben Zuschreibungen. Eine solche Entwicklung führt zu Menschenbildern extremer Ungleichheit. Die Raster der Ungleichheit führen zu Diskriminierungen und produzieren Ausgrenzung, Ablehnung und Hate Speech, die millionenfach im Internet verbreitet zum Shitstorm in sozialen Medien wird. Solches online-erstarrte Gruppendenken ist das Gegenteil von der Vorstellung des Internets als einem freien virtuellen Raum, in dem

55 Von Danwitz, DuD 2015, 581.

56 Von Danwitz, DuD 2015, 581 unter Bezug auf die Rechtsprechung des EuGH v. 08.04.2014, DuD 2014, 488.

57 Bobbio, Das Zeitalter der Menschenrechte. Ist Toleranz durchsetzbar? (1998/1990).

58 Heitmeyer im Interview mit Sebastian Gierke unter: https://www.sueddeutsche.de/politik/wachsender-autoritarismus-kein-mensch-kann-auf-dauer-ohne-anerkennung-leben-1.4203226 (letzter Abruf 01.07.2019).

Argumente und Werte kritisch hinterfragt werden. Dem Anderen wird, sei es aufgrund seiner Rasse, seines Geschlechts, seiner ethnischen Herkunft oder Religion, online und offline ein geringerer oder fehlender Wert zugesprochen, sodass in Extremfällen seine Intimität und räumliche Privatheit zerstört wird.[59]

Angesichts der Zählebigkeit diskriminierender Menschenbilder ist es in der globalen digitalen Gesellschaft ein elementares Anliegen, den Blick auf Grund- und Menschenrechte zu richten. Sie sind die eigentliche und primäre Leistung in vielen Gemeinwesen nach dem Zweiten Weltkrieg. In ihrer Gesamtheit bilden sie die Grundlage von Rechtsstaat (*rule of law*) und Demokratie. Beide Prinzipien finden sich zusammen im Dienste der Freiheit, die zur großen Idee der Aufklärung im 17./18. Jahrhundert wurde.

Demokratie sichert die Selbstbestimmung eines Volkes, indem sie die Bildung, Legitimation und Kontrolle derjenigen Organe organisiert, die staatliche Herrschaftsgewalt gegenüber dem Bürger ausüben. Der Rechtsstaat beantwortet dagegen Fragen nach Inhalt, Umfang und Verfahrensweise staatlicher Tätigkeit. Rechtsstaat und Demokratie finden sich zusammen im Dienste unabdingbarer (mehrheitsfester) Freiheitsrechte. Diese Verbindung hat der Europäische Gerichtshof für Menschenrechte (EGMR) aus aktuellem Anlass betont. Der Gerichtshof hat die Türkei und Russland wegen der politischen Verfolgung Oppositioneller bzw. Regimekritiker verurteilt, weil sie damit den Pluralismus und die freie Debatte in einer Demokratie ersticken. Die Urteile zielen darauf ab, den offenen demokratischen Prozess zu erhalten. Das ausdrückliche Verbot einer Inhaftierung allein aus politischen Gründen soll Oppositionellen ein Mindestmaß an freier Meinungsäußerung erhalten.[60]

Schon die Präambel der Allgemeinen Erklärung der Menschenrechte der UN von 1948 stellt fest, „that human rights should be protected by the rule of law". Die Grund- und Menschenrechte sollen nicht nur entfaltet, sondern auch ins Detail des positiven Rechts umgesetzt werden. Angesichts des technischen Fortschritts von Big Data, KI, der Digitalisierung und flächendeckenden Vernetzung und Überwachung der Menschen ist für Gesetzgeber in allen Staaten der Welt das Recht auf Privatheit und Datenschutz in Verbindung bzw. als Voraussetzung kommunikativer Freiheitsrechte wie der Meinungs- und Informationsfreiheit von Bedeutung. Unverhältnismäßige Einschränkungen dieser individuellen Freiheitsrechte destabilisieren immer eine offene, pluralistische Staats- und Gesellschaftsordnung.

Die wichtigsten grund- und menschenrechtlichen Regelungen zum Schutz der Privatheit und des Datenschutzes finden sich in folgenden Bestimmungen (siehe Abb. 1):

59 Vgl. den Text des Executive Directors von Human Rights Watch Kenneth Roth, Slavery: The ISIS Rules, in: The New York Review of Books (2015), Vol. LXII, No. 14, S. 69 f. m. w. N.

60 Vgl. EGMR v. 15.11.2018 – Nawalny (Russland) und v. 20.11.2018 – Demirtas (Türkei).

Abb. 1: Privatheit und Datenschutz.

In Art. 12 AEMR ist der Schutz der Privatheit (*right to privacy*) formuliert, der im Kontext von Datenschutz und Informationsfreiheit eine wichtige Rolle spielt. Die Erklärung der UN bezieht in Art. 19 AEMR die globale Freiheit der Meinungsäußerung ein. Im internationalem Pakt über bürgerliche und politische Rechte (IPbpR) von 1966, auch Zivilpakt der Vereinten Nationen genannt, werden auf der Basis der AEMR die Vertragsstaaten verpflichtet, die verbrieften Rechte zu respektieren und zu gewährleisten. Der Schutz des Privaten ist in Art. 17 IPbpR und der Schutz der Meinungsfreiheit in Art. 19 AEMR völkerrechtlich ausdrücklich geregelt. Im Zivilpakt heißt es weiter in Art. 20 Abs. 1, dass „jede Kriegspropaganda" per Gesetz verboten werden soll. Dasselbe betrifft nach Abs. 2 „jedes Eintreten für nationalen Hass, das zu Diskriminierung, Feindseligkeit oder Gewalt aufstachelt". Der Schutz der Privatheit wurde 2013 und 2016 durch UN-Resolutionen zum Recht auf Privatheit im digitalen Zeitalter ergänzt und bekräftigt. Die UN-Regelungen sind somit auch maßgebend für jede Art von digitaler Kommunikation.

In Europa finden sich entsprechende Gewährleistungen in der Europäischen Menschenrechtserklärung (EMRK) von 1948 und der EU-Grundrechte-Charta (GRCh), die 2009 zu verbindlichem Primärrecht in der EU erstarkte. Art. 8 EMRK schützt in teilweiser Orientierung an Art. 12 AEMR das Private in seinen vielen Facetten (räumliche Privatheit, Korrespondenz bzw. Telekommunikation u. a.). An dieser internationalen Regelung hat sich die EU ausgerichtet und den Schutz der Privatsphäre 2009 als Grundrecht in ihre supranationale Rechtsordnung aufgenommen. In die EU-Grundrechte-Charta sind explizit neue Entwicklungen der digitalen Datenverarbeitung eingeflossen. Art. 7 GRCh nimmt im Wesentlichen den Wortlaut von Art. 8 EMRK auf, der inhaltlich in Art. 8 GRCh als Schutz der personenbezogenen Daten einer jeden Person vertieft und mit ausdrücklichen prozeduralen Vorschriften zu Kontrollen und Auskunfts- und Korrekturrechten der betroffenen Personen verbunden ist.

Auch in den nationalen Verfassungen der EU-Mitgliedstaaten finden sich Datenschutzgrundrechte. Im deutschen Grundgesetz (GG) wird der Datenschutz durch die benannten Persönlichkeitsrechte z. B. aus Art. 10 Abs. 1 GG (Post- und

Fernsprechgeheimnis) und Art. 13 Abs. 1 GG (Die Wohnung ist unverletzlich.), vor allem aber durch das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistet.

Der UN-Zivilpakt und das europäische Recht sprechen jedem Menschen eine unantastbare Würde zu, allein weil er lebt und unabhängig von der Frage, wie er lebt. Demzufolge darf es keine Diskriminierung geben, die auf spezifischen Unterschieden zwischen den Menschen oder Gruppen von Menschen gründet (Art. 2 Abs. 1 AEMR).

Kein Mensch ist mit einem anderen identisch. Dies gibt allerdings Anlass für Differenzierungen. Hier beginnt die Kunst, gleichheitsgerechte Lösungen zu finden. Das heißt einerseits, dass der Mensch, sein Handeln und sein Umfeld in ihren Ähnlichkeiten und Verschiedenheiten gesehen und angemessen erfasst werden müssen. Da kein Mensch sich vom anderen in allen seinen Eigenheiten und Lebenssituationen unterscheidet, kann andererseits der Grundsatz von der Gleichheit aller Menschen nur eine Aussage über den Grad ihrer Ähnlichkeit oder Verschiedenheit treffen. Menschen, Reiche oder Arme, Junge oder Alte, Europäer oder Amerikaner, Afrikaner oder Araber, Muslime oder Christen sind daher jeweils nur mit Blick auf ein bestimmtes Vergleichsziel ähnlich oder verschieden. Die Anwendung des Gleichheitssatzes sagt über die Berechtigung der Befunde aber nur dann etwas aus, wenn er im Vergleichsmaßstab durch zusätzliche Informationen und Rechtswertungen auch in der digitalen Welt und ihren an Zielgruppen ausgerichteten Strategien vervollständigt wird.

Die Rechtsprechung der europäischen Gerichte

- des Europäischen Gerichtshofs für Menschenrechte (EGMR) mit Sitz in Straßburg
- des Europäischen Gerichtshofs (EuGH) mit Sitz in Luxemburg
- der nationalen Verfassungsgerichte wie des deutschen Bundesverfassungsgerichts (BVerfG) mit Sitz in Karlsruhe

steuert die Entwicklung des europäischen Grundrechtsschutzes. Der EuGH spielt eine zentrale Rolle als Originalinterpret der Verträge. Er war zunächst Hüter der wirtschaftlichen Freiheiten im europäischen Binnenmarkt (Raum ohne Binnengrenzen), in dem der freie Verkehr von Waren, Personen, Dienstleistungen und Kapital gewährleistet ist. Inzwischen ist das Gericht aber vor allem auch zu einer herausragenden Instanz in Fragen des Grundrechtsschutzes geworden. Hier ist ein zentrales Feld der Datenschutz, den er in einer Reihe von grundlegenden Entscheidungen zu einem wichtigen Projekt der EU gemacht hat.

Nach dem Urteil zur Vorratsdatenspeicherung[61] hat sich der EuGH im Fall „Google Spain“[62] mit dem Recht auf Vergessen befasst. Berichterstattungen auf Webseiten, die

61 EuGH v. 08.04.2014, DuD 2014, 488.

62 EuGH v. 13.05.2014, DuD 2014, 559; zur Bedeutung des Google-Urteils vgl. Leutheusser-Schnarrenberger, DuD 2015, 586.

persönlichkeitsverletzend sind, sollen zukünftig nicht mehr für immer im Internet auffindbar sein. Der EuGH widerlegte dabei auch die Argumente von Google, dass die Suchmaschine nicht „im Rahmen einer Tätigkeit" einer Niederlassung in Europa betrieben werde.[63] Er stellte fest, dass ohne die Werbevermarktung von Google Spain die Suche gar nicht zu finanzieren sei. Damit knüpft der EuGH bei der Anwendung der Datenschutzregeln an das Markortprinzip an, wie es auch die Datenschutz-Grundverordnung vorsieht. Zugleich bejahte der EuGH eine Verantwortlichkeit des Suchmaschinenbetreibers für die Suchergebnisse. Die Maschine funktioniere keineswegs „von allein" nur aufgrund des eingesetzten Algorithmus.[64]

Der EuGH hat sich auch mit dem umstrittenen Safe-Harbor-Übereinkommen der EU-Kommission auseinandergesetzt und dieses aufgehoben.[65] Das Gericht hat insbesondere hervorgehoben, die Kommission habe nicht hinreichend gewichtet, dass nach US-Recht die Belange der nationalen Sicherheit und der Strafverfolgung Vorrang vor den im Übereinkommen niedergelegten Grundsätzen des europäischen Datenschutzes haben.[66] Damit ist die bis dato zentrale Grundlage für Datenübermittlungen an Stellen mit Sitz in den USA entfallen. Die Forderung des Gerichtshofs nach Aussetzung des Datentransfers in die USA hätte zur Folge gehabt, dass geschützte Daten zukünftig in Europa verarbeitet werden müssen. Die Kommission und die USA haben sich daher auf ein neues Übereinkommen geeinigt (EU-US Privacy Shield), das an die Stelle von Safe Habor treten soll.[67] Der EuGH hat zudem festgestellt, dass die nationalen Datenschutzbehörden ein Klagerecht gegen Entscheidungen der EU-Kommission haben müssen. Diese Entscheidung hat sowohl im wirtschaftlichen Bereich als auch im nicht-öffentlichen Bereich enorme Auswirkungen.

Die Safe-Harbor-Entscheidung des EuGH ist durch den österreichischen Jurastudenten Max Schrems ausgelöst worden. Diesem war es gelungen, von Facebook eine endlose Liste seiner angeblich gelöschten, aber immer noch auf Servern in den USA gespeicherten Daten zu erhalten, die dem beliebigen Zugriff etwa von USA-Überwachungsprogrammen ausgeliefert sind. Die von Schrems erstrittene Entscheidung ist ein Meilenstein im Recht des Datenschutzes. Datenübermittlungen in Drittstaaten, also Staaten außerhalb der EU, sind nur dann zulässig, wenn diese Staaten ein gleichwertiges Datenschutzniveau gewährleisten. Künftige Vereinbarungen über den transatlantischen Datenverkehr unterliegen zudem der Kontrolle der Datenschutzbehörden und können vom EuGH verworfen werden.

---

63 EuGH v. 13.05.2014, DuD 2014, 559, 562 (Google I); s. a. EuGH v. 24.09.2019 (Google II), ein Urteil, in dem der Anspruch auf die globale Reichweite des Rechts auf Vergessenwerden in Frage steht.

64 EuGH v. 13.05.2014, DuD 2014, 559, 560; ausführlich zu Sachverhalt und Hintergrund von „Google Spain", zum Urteil des EuGH und den Kritikpunkten vgl. Holznagel/Hartmann, MMR 2016, 228.

65 EuGH v. 06.10.2015, DuD 2015, 823; siehe dazu die Anmerkung von Petri in DuD 2015, 801.

66 EuGH v. 06.10.2015, DuD 2015, 823, 828.

67 S. dazu Rn. 175 (Kap. 2.2.7.2.1).

Der EuGH hat mit seinen Entscheidungen das Versprechen der EU-Grundrechte-Charta eingelöst; der Gerichtshof schützt die bürgerliche Freiheit der Menschen in Europa. Er verändert mit seinem Urteil die globale zweckfreie Datenwirtschaft. Der Datenschutz ist damit zu einem zentralen Gemeinschaftsprojekt geworden.[68] Ein wesentlicher Ausgangspunkt sind die neuen EU-Normen: die allgemeine Datenschutzgrundverordnung (DS-GVO)[69] und die spezielle Richtlinie (RLDSJ)[70], die den Bereich der vorbeugenden Bekämpfung von Straftaten regelt. Es kommt nun auf die nationalen Gesetzgeber an, im Anwendungsbereich des Unionsrechts den reformierten Datenschutz in ihren Ländern umzusetzen. Die DS-GVO gilt in den EU-Mitgliedstaaten zwar ohne nationalen Umsetzungsakt unmittelbar und ist somit Teil ihrer jeweiligen Rechtsordnung. Als allgemeine Grundordnung ist sie aber ergänzungsbedürftig und regelt das Recht auf Privatheit und Datenschutz nur im Grundsatz abschließend.[71] Im Raum steht zudem die ePrivacy-Verordnung (ePV), die die DS-GVO insbesondere im Bereich elektronischer Kommunikation ergänzen und die Besonderheiten der Online-Datenverarbeitung regeln soll.[72]

68 Zum Stellenwert der EuGH-Entscheidungen im Vergleich zu nationalen Verfassungsgerichten vgl. von Danwitz, DuD 2015, 583.

69 Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DS-GVO), ABl. v. 04.05.2016 L 119, S. 1; zu Entstehungsprozess und Ausführung vgl. Albrecht/Jotzo, Das neue Datenschutzrecht der EU (2017).

70 Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. v. 04.05.2016 L 119, S. 89.

71 Ausführlich dazu Roßnagel, DuD, 2018, 741–745.

72 Näher zur ePrivacy-VO s. Rn. 84 und Rn. 180 (Kap 4.2.3.2 und Kap. 4.4.3).

1 Grundfragen

Marie-Theres Tinnefeld

1.1 Technologische Entwicklung – Auswirkung auf menschliche Lebenswelten

Der anhaltende Fortschritt in der **Informations- und Kommunikationstechnologie** (IKT) formt in immer stärkerem Maß menschliches Leben bis hin zum digitalisierten Alltag. Rund um die Uhr und überall entstehen erhebliche Mengen an Daten. Sie können fast lückenlos nachverfolgt, gespeichert und analysiert werden, um bisher unbekannte Korrelationen zu entdecken und menschliche Verhaltensmuster zu erkennen. Es ist die Frage, ob diese Entwicklung für digital vermittelte Entscheidungsprozesse in Staat und Wirtschaft eher förderlich als hinderlich ist. 1

Die IKT ermöglicht eine allgegenwärtige Verfügbarkeit von digitalisierten Informationen und Diensten zu jeder Zeit und an jedem Ort, eine „24/7-Welt", in der Menschen ohne Rücksicht auf einen Schlaf- und Nachtrhythmus 24 Stunden am Tag und sieben Tage die Woche kommunizieren.[1] Dieser Vorgang wird auch durch den Begriff des **„ubiquitous computing"**[2] gekennzeichnet. Dadurch sollen die Sinne des Menschen über körperabhängige Fähigkeiten hinaus technisch erweitert und geschärft und ganz allgemein Hilfeleistungen angeboten werden. Zu den Grundlagen gehören winzige, energiesparsame Sensoren, die vielfältige Informationen erfassen, sowie energieeffiziente und preiswerte Prozessoren mit integrierter drahtloser Kommunikationsfähigkeit. Auf diese Weise entstehen Sensornetze, die ihre Umgebung beobachten und Ereignisse melden können, ohne dass der Betroffene davon Kenntnis nimmt. 2

Chipkarten bieten als Datenspeicher Platz für sämtliche relevanten Informationen über Menschen in ihrer Rolle als Patient, Kunde, Arbeitnehmer, Autofahrer, Kontoinhaber und Strafgefangener. Personalisierte **Radio-Frequency-Identification(RFID)-Chips** (in Form von auslesbaren Funketiketten) werden von kommunizierenden RFID-Chips (aktive RFID-Tags) abgelöst und verändern private und öffentliche Lebenswelten. Viele Alltagsdinge werden „smart", indem sie mit Informationstechnologie zum Sammeln, Speichern, Verarbeiten und Kommunizieren von Daten ausgestattet werden. Beispiele für smarte Dinge sind Autoreifen, die den Fahrer rechtzeitig benachrichtigen, wenn der Luftdruck abnimmt, oder Medikamente, die sich bemerkbar machen, bevor das Haltbarkeitsdatum abläuft, Patientenarmbänder, die der Lokalisierung von demenzkranken oder desorientierten 3

1 Crary, 24/7. Schlaflos im Spätkapitalismus (2014).

2 Der Begriff „ubiquitous computing" wurde von Mark Weiser geprägt, s. Weiser, Scientific American, Special Issue: Communications, Computers and Networks: How to Work, Play and Thrive in Cyberspace (Sept. 1991), S 94 ff.

https://doi.org/10.1515/9783110630336-001

Menschen dienen oder die Erfassung von Vitalparametern (Blutdruck usw.) von Personen in Verbindung mit mobilen Endgeräten wie Smartphones. Weitere Beispiele sind Smart Watches und Fitness Tracker, die z. B. die Herzfrequenz und Geschwindigkeit eines Menschen erfassen und ggf. seine bisher zurückgelegte Strecke in sozialen Medien veröffentlichen. In diese Kategorie gehört auch das Smart Home, das z. B. mit einer intelligenten Glühbirnenbeleuchtung ausgestattet ist. So soll es künftig auch möglich sein, die Gemütsverfassung eines Menschen zu erkennen und dann für entsprechende Beleuchtung und Musik zu sorgen.

4 Die Vernetzung von intelligenten Dingen über das Internet wird als **„Internet der Dinge“** (IOT) bezeichnet. Die Lokalisierung von Dingen aus der Ferne wird immer einfacher und billiger. Die Dinge können ihre „erfahrenen“ Informationen protokollieren, sodass sie dem Nutzer, dem Hersteller oder einem Diensteanbieter zur Verfügung stehen. In diese Rubrik gehören auch WLAN-Verbindungen oder das satellitengestützte Global-Positioning-System (GPS), mit dem der Aufenthaltsort von Fahrzeugen und Personen festgestellt werden kann.

Beispiel
Bei hochwertigen Mietfahrzeugen wird von einigen Autoverleihern GPS eingesetzt, um vertraglich nicht erlaubte Fahrten (z. B. Grenzübertritte) mit technischen Mitteln zu verhindern. Nähert sich das Fahrzeug einem vertraglich nicht erlaubten Grenzübertritt, wird eine zentrale Leitstelle des Autoverleihers informiert, die dann über weitere Maßnahmen zu entscheiden hat.

5 Zunehmend verbreiten sich leistungsfähige digitale Endgeräte wie Smartphones, Tablet-PCs und Notebooks im Verbund mit einer breitbandigen drahtlosen Infrastruktur. Die mobilen Geräte laufen mit schlanken Betriebssystemen und Interaktionsmöglichkeiten z. B. durch berührungsempfindliche Bildschirme und Sprachsteuerungssysteme. Sie verfügen über erheblichen Speicherplatz und weitreichende Möglichkeiten im Zusammenhang mit der mobilen Internet- und E-Mail-Nutzung oder dem Abspielen von Audio- und Videodateien. Dafür wurden kleine **Softwareprogramme** („Apps“/Applications, Anwendungen) „erfunden“, die dem Nutzer bestimmte Funktionalitäten zur Verfügung stellen. Viele **Apps** nutzen die Ortung der aktuellen Position, gespeicherte Kontaktdaten oder die von den Geräten zur Verfügung gestellten Sensordaten, die den Nutzungskontext erfassen (z. B. Ort, Lage, Licht- und Bewegungsdaten, Bild und Ton). Vernetzte Smartphone-Dienste sind riskant, wenn die persönlichen Daten Dritten zugänglich sind und nicht mehr ausschließlich zu den vorgesehenen Zwecken genutzt werden. Es zeichnet sich auch ein Trend zu mobilen Geschäftsprozessen und zur Personalisierung von Produkten durch (Business) Apps ab.

6 Neue Technologien für die Identifizierung und/oder die Lokalisierung von Menschen bergen einiges an sozialem Sprengstoff, wenn sie zum Ausspionieren etwa von Mitarbeitern oder als Instrumente zur Kontrolle etwaiger Verdächtiger durch die Sicherheitsbehörden genutzt werden. In Deutschland ist die Einführung der mit RFID und **Biometrie** versehenen Pässe seit dem Jahre 2007 Pflicht. Dasselbe gilt

für den elektronischen Personalausweis, der seit dem Jahre 2010 biometrische Verfahren (Vermessung des Gesichts und auf freiwilliger Basis zwei Fingerabdrücke) vorschreibt. Er soll darüber hinaus auch das Internet sicherer machen und rechtssichere elektronische Anwendungen ermöglichen. Die auf dem Ausweis zu lesenden Daten sind in einem integrierten RFID-Chip gespeichert, der kontaktlos ausgelesen werden kann.

7 Grundsätzlich stellt sich die Frage nach den sozialen Auswirkungen biometrischer Verfahren, die unsichtbar zur Identifikationsfeststellung (maschinellen Ähnlichkeitsmessung) verwendet werden können, ohne dass der Betroffene dies durchschauen kann. Biometrische Merkmale auf elektronischen Dokumenten oder genetische Daten sollen auch dazu beitragen, Täter zu überführen. Problematisch werden biometrische Verfahren zudem, wenn sie als Anknüpfungspunkt für staatliche Leistungen fungieren: Ist ein Mensch, der wegen fehlender Gliedmaßen nicht die für einen Pass erforderliche Biometrie hat, kein Bürger mehr?[3] Werden Menschen angesichts dieser Entwicklung künftig noch über ihre Lebensführung selbst bestimmen können? Werden sie noch eine geschützte Privatsphäre haben? Wird die offene Kommunikation gefährdet?

8 Spätestens seit den 1970er-Jahren ist es absehbar, dass im Zuge der technologischen Entwicklung immer mehr personenbezogene Informationen (in der EDV-geprägten Sprache: personenbezogene Daten) von Staat und Wirtschaft verarbeitet werden. Der weltweite Ausbau vernetzter privater Datenbestände wird gleichzeitig zum „potenziellen Datenreservoir" für staatliche Stellen. Dadurch wächst staatlichen Einrichtungen und wirtschaftlichen Unternehmen eine **Informationsmacht** zu, die zu neuen Informationsbedürfnissen und Begehrlichkeiten führt. Der Bürger selbst hat es nicht mehr nur mit einer Technologie der (Orwell'schen) Bedrohung,[4] sondern auch mit einer Technologie der Verführung zu tun, die ihn dazu verleitet, privaten Unternehmungen (Arbeitgebern, Banken, Versicherungen, Medienanstalten, Krankenhäusern) alle geforderten Informationen über sich preiszugeben, um im marktwirtschaftlichen Netz von Angebot und Nachfrage zu bestehen und sich tatsächliche oder vermeintliche Vorteile zu verschaffen.[5]

---

3 Lobe, Wer keine Biometrie hat, ist kein Bürger, SZ v. 25.10.2018, unter: https://www.sueddeutsche.de/digital/biometrie-gesichtserkennung-fingerabdruck-spracherkennung-1.4183394 (letzter Abruf 21.06.2019), Tinnefeld, MMR 2018, 777.

4 Orwell, Nineteen Eighty-Four (1949), S. 23; in seinem Roman beschreibt Orwell, wie „Big Brother" auf sogenannten Telescreens erscheint und die Menschen ununterbrochen mit Propaganda überschüttet. Sie ermöglichen der „Thought Police" die (unsichtbare) Observierung des Einzelnen: „There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork [. . .] You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard [. . .]."

5 Ström, Die Überwachungsmafia (2005).

9 Darüber hinaus haben Menschen im 21. Jahrhundert begonnen, in digitalen sozialen Netzwerken nicht nur vertrauensvoll neue Beziehungen und Freundschaften zu knüpfen, sondern wie Narziss[6] private und intime Informationen über sich selbst, gleichsam sich selbst und das eigene Tagebuch offenzulegen. Wie der Medienwissenschaftler Roberto Simanowski annimmt, verbirgt sich hinter der narzzistischen Selbstvergewisserung von Menschen über Selfies und andere Posts häufig eine Angst vor dem eigenen Erleben.[7] Wird narzisstisches Verhalten über soziale Medien wie Twitter oder Facebook gefördert? Unbestritten ist, dass das Phänomen **„Social Media“** in seinen ganz unterschiedlichen Ausprägungen Bestandteil des Alltags von vielen Menschen geworden ist und auch zur Entwicklung besonderer psychischer Auffälligkeiten führen kann.

10 Die heute üblichen sozialen Praktiken des Teilens, Empfehlens und Filterns umfassen „alle Darstellungsformate, alle Medienformate und alle multimedialen Formen wie Text, Bild, Bewegtbild und Audio“.[8] Es ist zwischen dem Potenzial des sozialen Mediums und seinem tatsächlichen Gebrauch zu unterscheiden. Die genutzten Kontakte nehmen eine wichtige Rolle bei der Entstehung von Öffentlichkeit im Sinne einer weltweit offenen Gesellschaft, aber auch einer Art Gesellschaft am Pranger ein. Die digitale Netzwelt verleitet Menschen als (aktive) Prosumenten dazu, Mitmenschen heimlich und anonym wegen körperlicher Gebrechen, aus Eifersucht und Rache an den digitalen Pranger zu stellen, mit Kindern über das Internet Verbindung zum Zwecke eines späteren sexuellen Kontakts oder zur Vorbereitung eines Missbrauchs aufzunehmen (Cyber Grooming) oder sich als Konsumenten den nicht tolerierbaren und europaweit verbotenen Zugang zu kinderpornografischen Inhalten zu verschaffen.

11 „Information“, wie sie in der Welt der sozialen Medien etwa auf Facebook zur Debatte steht, kann Persönlichkeitsrechte der Betroffenen dann schädigen, wenn sie zu Wahrnehmungsverzerrungen führt oder eine Quelle für Falschmeldungen (Fake News) durch **Softwareroboter** bzw. -agenten (Social Bots) wird und/oder die öffentliche Meinungsbildung durch Rufmord von politischen Gegnern beeinflusst.[9] Ein weiteres Problem entsteht, wenn sich (passive) Nutzer sozialer Medien mit Informationen begnügen, die ihnen etwa Google oder Facebook als „Informationsvermittler“ auf das Smartphone senden. Diese Informationen beruhen

---

6 Narziss, griechisch Narkissos, der (narkotisierte) Jüngling, der von seinem Spiegelbild besessen war und dieses in der Wasserspiegelung einer Quelle suchte, ist eine Gestalt aus der griechischen Mythologie.

7 Simanowski, Facebook-Gesellschaft (2006); s. a. Nida-Rümelin/Weidenfeld, Digitaler Humanismus (3. A. 2018), S. 145.

8 Hohlfeld/Godulla, in: Hornung/Müller-Terpitz (Hg.), Rechtshandbuch Social Media (2015), Kap. 2 Rn. 3–8.

9 Speziell zum Problem von sog. „bösartigen (malicious) Bots“ vgl. Volkmann, MMR 2018, 58 f. m. w. N.

im Wesentlichen auf der algorithmischen Steuerung von Selektionskriterien des Vermittlers (Intermediärs), die regelmäßig für den Nutzer intransparent sind und eine selbstständige Meinungsbildung behindern. Nutzer geraten so hinter digitale Einlassschranken, in denen Vielfalt und Ausgewogenheit von Informationen keine Rolle mehr spielen.

Information kann auf diese oder andere riskante Art zu einem „negativen Wert“ werden, der auch demokratisches Verhalten gefährdet. Anknüpfend an Orwells Albtraum einer perfekten Tyrannis mit technischen Mitteln schrieb Ernst Benda bereits 1983: **12**

> Die fortschreitende Erweiterung der technischen Möglichkeiten, die menschlichen Fähigkeiten zu einer sinnlichen Wahrnehmung um ein Vielfaches zu verstärken, stellt einen revolutionären Schritt dar, an dessen Ende die völlige Schutzlosigkeit der Privatsphäre stehen könnte [. . .]. George Orwell's 1984 mag eine unrealistische Vision sein. Die wirkliche Gefahr ist weniger die Unterwerfung der Menschen durch Menschen, also die subjektive Despotie mit Hilfe der Technik, als vielmehr die politische Herrschaft der Technik selbst, die freilich ihre Nutznießer finden wird.[10]

Die Entwicklung und Ausgestaltung der IKT bis hin zur Netzwerkstruktur digitaler Kommunikation verändert menschliches Wissen und Tun tiefgreifend. Beides, Wissen und Tun, hängt zusammen. Der Einzelne orientiert sich bei seinem Tun am Wissen. „Wo das (eigene) Wissen fehlt, wird der Mensch orientierungslos oder von fremdem Wissen abhängig. Er gehört in diesem Fall nicht sich selbst, weil ihm seine Orientierungen nicht gehören.“[11] **13**

Eine deutende und erklärende Aneignung von Wissen ist dem Einzelnen nur möglich, wenn ihm „seine“ Informationen nicht entfremdet werden. Menschen müssen die Möglichkeit haben „zu wissen, wer was wann wo und bei welcher Gelegenheit über sie weiß“.[12] Ohne dieses Wissen, so hat das Bundesverfassungsgericht (BVerfG) im „Volkszählungsurteil“ aus dem Jahre 1983[13] eindringlich festgestellt, kann der Einzelne nicht angstfrei am öffentlichen Leben teilnehmen. Jeder habe grundsätzlich das Recht, selbst zu bestimmen, welche Lebenssachverhalte er offenbaren will. Jeder hat, wie es Samuel Warren und Louis Brandeis (ein späterer Richter am Supreme Court der USA) schon im Jahre 1890 ausdrückten, den Anspruch auf das Recht „to be let alone“ (in Ruhe gelassen zu werden).[14] Der amerikanische Politikwissenschaftler Alan F. Westin erweitert den Begriff um den Aspekt der **14**

---

10 Benda, in: Benda/Maihofer/Vogel (Hg.), Handbuch des Verfassungsrechts der Bundesrepublik Deutschland (2. A. 1995), S. 122, 127.

11 Mittelstraß, Leonardo-Welt (2. A. 1992), S. 12 f.

12 Podlech, in: Hohmann (Hg.), Freiheitssicherung durch Datenschutz (1987), S. 21.

13 BVerfG v. 15.12.1983, BVerfGE 65, 1.

14 Warren/Brandeis, The Right to Privacy, in: Harv. L. Rev. (1890), Vol. 4, No. 5, S. 193.

Selbstdarstellung und definiert Privatheit (privacy) als „the right of the individual to decide for himself, with only extraordinary exceptions in the interest of society, when and on what terms his acts should be revealed to the general public".[15]

15 Ganz in diesem Sinn ergänzt das BVerfG mit Blick auf die Möglichkeiten der automatisierten Datenverarbeitung, der Einzelne habe auch das Recht zu wissen, wer welche Informationen bei welcher Gelegenheit über ihn erfasst, speichert, für oder gegen ihn verwendet. Nur derjenige werde sich am öffentlichen Leben beteiligen, der sich seines Persönlichkeitsrechts sicher sein könne. Unter dem Aspekt der stetig expandierenden Datenverarbeitung verknüpfte das BVerfG den Schutz personenbezogener Daten mit dem Konzept der Privatsphäre und dem **allgemeinen Persönlichkeitsrecht,** das grundrechtlich in Art. 2 Abs. 1 („Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt") und in Art. 1 Abs. 1 GG („Die Würde des Menschen ist unantastbar") verankert ist.[16] Damit hat das Gericht auf technikbedingte Freiheitsgefahren reagiert, die jünger sind als das Grundgesetz, das am 23. Mai 1949 in Kraft getreten ist. Die Rechtsprechung des BVerfG hat wesentlich dazu beigetragen, dass grundrechtliche Schutzbereiche fortgeschrieben wurden. So hat das Gericht im Volkszählungsurteil 1983 den rechtlichen und politischen Durchbruch für die Anerkennung des Grundrechts auf **informationelle Selbstbestimmung** bzw. des Datenschutzes bzw. des Rechts auf informationelle Privatheit und Intimität (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) eingeleitet. Es soll dem Einzelnen die Chance sichern, seine Individualität auch unter den Bedingungen subtiler Informationstechnologien zu entwickeln, sodass er sich in unterschiedlichen sozialen Kontexten darstellen und kommunizieren kann (personale Entfaltung durch Kommunikation).[17] Dabei gehe es dem Datenschutz auch um das Gemeinwohl im demokratischen Rechtsstaat und seine Voraussetzung: den mündigen, informierten Bürger, der sich politisch einmischen will.[18] Ihm hilft dabei ein Recht auf freie Information, um relevante Fakten zu finden sowie ein Recht auf freie Meinungäußerung, um widerstreitende Argumente aufnehmen und hinterfragen zu können. Der Datenschutz bildet zwar eine elementare Basis für die **Kommunikations- und Partizipationsfähigkeit der Individuen** und damit die **Demokratiefähigkeit der Gesellschaft.**[19] Er steht in diesem Sinn aber immer auch in enger Verbindung mit den kommunikativen Grundrechten (Meinungs- und Informationsfreiheit – Art. 5 Abs. 1 Satz 1 GG, Schutz der vertraulichen Kommunikation

15 Westin, Privacy and Freedom (1967), S. 36; vgl. auch Britz, Freie Entfaltung durch Selbstdarstellung (2007).

16 BVerfG v. 15.12.1983, BVerfGE 65, 1, 43.

17 BVerfG v. 05.06.1973, BVerfGE 35, 202, 220; ähnlich BVerfG v. 26.06.1990, BVerfGE 82, 236, 269; Freiheit des Einzelnen, selbst zu bestimmen, welches Persönlichkeitsbild er von sich vermitteln will.

18 Hirsch, Das Ende der Zuschauerdemokratie, SZ v. 30.10.2010, S. 2.

19 BVerfG v. 15.12.1983, BVerfGE 65, 1, 42.

durch das Fernmelde- bzw. Telekommunikationsgeheimnis – Art. 10 GG; Schutz der Wohnung – Art. 13 GG u. a.).[20] In allen diesen Fällen werden zugleich Sonderaspekte der Verarbeitung personenbezogener Daten angesprochen.[21]

16 Mit der Anerkennung der individuellen Freiheitsrechte erhält der Einzelne die Möglichkeit, autonom in sozialen Kontexten zu handeln. Er gewinnt damit gleichzeitig die Chance, persönliche Verantwortung zu übernehmen.[22] Dadurch kommen „gemeinschaftliche Bezüge" ins Spiel, von denen Zusammenhalt und **Solidarität** in einer Gesellschaft abhängig sind.[23] Dieses Verständnis legt es nahe, Einschränkungen im Grundrechtsschutz zu hinterfragen, die insbesondere durch die internationale Kriminalität und das Phänomen des **Terrorismus** entstanden sind.

17 Seit den brutalen Terroranschlägen in den USA vom 11. September 2001 und aufs Neue nach den Attentaten von Paris im Januar und November 2015/2016, in Deutschland 2016 und weiteren Gewaltakten etwa auf Weihnachtsmärkten tendieren die Strafverfolgungsbehörden und Geheimdienste verstärkt dazu, aktiv zu werden, bevor eine bestimmte, konkrete Gefahr aufgetreten ist oder sich realisiert hat. Das so verstandene Postulat „Freiheit durch Sicherheit" führt potenziell dazu, dass der Staat ohne Rücksicht auf Privat- und (Tele-)Kommunikationssphären tendenziell alles und jeden präventiv beobachten und die so gewonnenen Daten zu weiteren Sicherungszwecken auf Vorrat verarbeiten darf.[24]

18 Der Europäische Gerichtshof (EuGH) in Luxemburg hat sich mit der grundrechtlichen Problematik der verdachtsunabhängigen Speicherung von Kommunikationsdaten auf Vorrat eingehend befasst und für einen angemessenen Schutz der Kommunikationsfreiheit plädiert.[25] Andernfalls wäre Sicherheit in erster Linie nicht mehr „die Gewissheit der dem Individuum verbürgten Freiheit", sondern eine nie endende „staatliche Aktivität zum Schutz des Bürgers [. . .]".[26] Bei einer solchen Entwicklung könnte „der Einzelne den Staat durch legales Verhalten nicht mehr auf Distanz halten".[27] Daher ist es rechtsstaatlich geboten, grundrechtlich verankerte Freiheiten grundsätzlich über die Möglichkeiten einer umfassenden Straf- und

20 Simitis, KritV 2000, 368.

21 BVerfG v. 14.07.1999, BVerfGE 100, 313, 359.

22 Wilhelm von Humboldt schreibt bereits 1792 in seiner subtilen Schrift „Ideen zu einem Versuch, die Grenzen der Wirksamkeit des Staates zu bestimmen", dass die Entscheidung für die individuelle Freiheit auch eine Entscheidung zugunsten der persönlichen Verantwortung sei. Dazu Schmale/Tinnefeld, Privatheit im digitalen Zeitalter (2014), S. 25 f., 43.

23 Zur Solidarität mit den Schwächeren vgl. Herzog, in: Köbler/Heinze/Hromadka (Hg.), FS für Alfred Söllner (2000), S. 441; s. a. Denninger, Menschenrechte und Grundgesetz (1994), S. 46.

24 Leutheusser-Schnarrenberger, ZRP 2007, 9; s. a. Bäumler/Leutheusser-Schnarrenberger/Tinnefeld, DuD 2002, 562.

25 EuGH v. 08.04.2014, DuD 2014, 488 – Digital Rights/Ireland.

26 Bizer, in: Bizer/Koch (Hg.), Symposium zum 65. Geburtstag von Erhard Denninger (1998), S. 29; zur Staatslegitimation durch Sicherheit Hobbes, Das Grundrecht auf Sicherheit (1983), S. 1 f., 31 ff.

27 Grimm, Die Verfassung und die Politik (2001), S. 103.

Rechtsverfolgung zu stellen und zu diesem Zweck ein Minus an Sicherheit und Aufklärung bewusst in Kauf zu nehmen: „Zielgröße ist immer die Freiheit."[28] Erst daran, dass der Staat auch den Umgang mit seinen Gegnern den allgemein geltenden Grundsätzen unterwirft, zeigt sich die Kraft des Rechtsstaates. Angesichts von immer neuen Terrorwarnungen und den allgegenwärtigen Einsatzmöglichkeiten der IKT im polizeilichen und militärischen Bereich (Cyberwar) sehen sich nationale europäische Gesetzgeber veranlasst, die rechtlichen Schranken für den Zugriff auf Daten des Bürgers immer niedriger zu halten. Das höchste deutsche Gericht hat dazu kritisch angemerkt:

> Inzwischen scheint man sich an den Gedanken gewöhnt zu haben, dass mit den mittlerweile entwickelten technischen Möglichkeiten auch deren grenzenloser Einsatz hinzunehmen ist. Wenn aber selbst die persönliche Intimsphäre [. . .] kein Tabu mehr ist, vor dem das Sicherheitsbedürfnis Halt zu machen hat, stellt sich auch verfassungsrechtlich die Frage, ob das Menschenbild, das eine solche Vorgehensweise erzeugt, noch einer freiheitlich-rechtsstaatlichen Demokratie entspricht.[29]

19 In einer langen Kette von Entscheidungen hat das BVerfG das **Prinzip der Verhältnismäßigkeit** in den Dienst der Persönlichkeitsentfaltung gestellt.[30] Nicht von ungefähr hat dieses Prinzip etwas mit dem Gedanken des Maßhaltens zu tun. Spiros Simitis fordert angesichts der tendenziell schrankenlosen Verarbeitung persönlicher Daten einen Informationsverzicht als „freiheitssicherndes Prinzip".[31]

20 Der Schutz der Bürger vor Kriminalität, vor einem professionellen Diebstahl ihrer Daten, vor Verwertung und Verfälschung der eigenen Daten im Netz[32] sowie vor den Gräueln terroristischer Anschläge ist zwar ein wesentlicher Teil staatlicher Verantwortung. Je mehr aber im Interesse der inneren Sicherheit der vorbeugende Rechtsschutz Platz greift (Rasterfahndung, elektronische Abhörmaßnahmen, staatliche Trojaner usw.), desto deutlicher stellt sich die Frage nach dem Rangverhältnis zwischen der kollektiven Sicherheit und den individuellen Freiheitsrechten der Bürger. Auch angesichts neuer technikbestimmter Bedrohungen ändert sich nichts an der Aufgabe des Staates, eine Kombination beider Zielsetzungen so auszubalancieren, dass ein maximales Maß an Freiheit durch optimale technikunterstützte Sicherheitsmaßnahmen erhalten bleibt.[33] Auf diese Weise trägt das Verhältnismäßigkeitsprinzip mittlerweile die Hauptlast der Freiheitssicherung.

---

28 Baum, Rettet die Grundrechte (2009), S. 31.

29 Sondervoten in BVerfG v. 03.03.2004, BVerfGE 109, 279, 391.

30 So auch BVerfG v. 15.12.1983, BVerfGE 65, 1.

31 Simitis, in: Kroker/Dechamps (Hg.), Information – eine dritte Möglichkeit neben Materie und Geist (1995), S. 287 f.

32 Amann/Baumgärtner u. a., Plötzlich nackt, Der Spiegel v. 22.01.2019, S. 15.

33 Denninger, Recht in globaler Unordnung (2005), S. 207–220; zu neuen Sicherheitsinstrumenten Schneider, ZD 2011, 6, 12.

Teil der verfassungsmäßigen Verhältnismäßigkeit ist das Prinzip der Erforderlichkeit, das auf Strukturen und Zusammenhänge verweist, welche regelmäßig empirischer Natur sind und der rechtlichen Regelung vorausgehen. Mit anderen Worten: Die Erforderlichkeit bringt die rechtsrelevanten Tatsachen (z. B. Korruption oder Betrug) und ihre rechtliche Beurteilung (datenschutzrechtlich, strafrechtlich usw.) in einen nachvollziehbaren Zusammenhang. In Anwendung dieser Grundsätze ist bei den grundrechtseinschränkenden Maßnahmen jeweils zu fragen, **21**

- ob sie überhaupt geeignet (tauglich) sind, das erstrebte Ziel zu erreichen (z. B. den Terrorismus erfolgreich zu bekämpfen),
- ob sie den geringsten Eingriff unter den möglichen Varianten darstellen (der klassische Fall der Erforderlichkeit),
- ob die damit verbundene Einbuße an Freiheit in einem angemessenen Verhältnis zur Schwere des Eingriffs steht (verhältnismäßig im engeren Sinn) und schließlich
- ob „die beabsichtigten Maßnahmen nicht mit gravierenden Nebenfolgen verbunden sind, sodass sie in ihrer Summe die Freiheit verkümmern lassen".[34]

Bei einem Ausgleich zwischen den rivalisierenden Forderungen ist immer zu prüfen, ob etwa eine verdachtslose Vorratsdatenspeicherung über die näheren Umstände einer Telekommunikation (Verkehrs- und Standortdaten, einschließlich erfolgloser Anruf- und Verbindungsversuche) zu Zwecken einer umfassenden Sicherheitsüberwachung noch den Anforderungen der Verhältnismäßigkeit genügen kann.[35] Von ihrer Wirkungsweise her kann auch eine verdachtslose Rasterfahndung nicht nur durch den massiven Ausbau der inzwischen gescheiterten Speicherpflichten für TK-Unternehmen[36] unerwünschte Nebenfolgen haben. Es ist nicht auszuschließen, dass sie „einen demütigenden Effekt hat und eher Feinde schafft als dass sie Schläfer aufdeckt".[37] Das Bundesverfassungsgericht hat sich bereits 2010 im Urteil zur Vorratsdatenspeicherung mit den mentalen Auswirkungen anlassloser Kontrollen befasst und geht darauf ein, wie ein „diffus bedrohliches Gefühl des Beobachtenseins" bzw. des Überwachtwerdens den Einzelnen an der unbefangenen Wahrnehmung seiner Grundrechte hindern könne.[38] In seinem Beschluss von 2019 zu KfZ-Kennzeichenkontrollen, mit denen vor allem unversicherte Autos automatisiert erfasst werden sollen, betont das höchste deutsche Gericht, dass durch die große Streubreite dieser Kontrollen ein **Gefühl des Überwachtwerdens** entstehen und die **individuelle Freiheit** und zugleich die **Freiheitlichkeit der Gesellschaft** gefährden könne: „Die Durchführung von Kontrollen zu beliebiger Zeit und an **22**

34 Dazu Grimm, Die Verfassung und die Politik (2001), S. 103.

35 Vgl. Petri, RDV 2010, 197, 201 f.

36 Vgl. Kühling, VerfBlog v. 29.06.2017 unter: http://verfassungsbblog.de/todesstoß-fuer-die-vorratsdatenspeicherung-der-beschluss-des-ovg-nrw-und-seine-folgen/ (letzter Abruf 21.06.2019).

37 Limbach, Festvortrag anlässlich des 53. Deutschen Anwaltstages (2000).

38 BVerfGE v. 02.03.2010, NJW 2010, 833, 839.

beliebigem Ort ins Blaue hinein ist mit dem Rechtsstaatsprinzip grundsätzlich unvereinbar“[39] und widerspricht dem Gebot des Maßhaltens, das einen hohen verfassungsrechtlichen Rang hat. Der EuGH trifft in einem Urteil 2016 eine entsprechende Kernaussage, nach der eine Vorratsdatenspeicherung auch zum Zwecke der Strafverfolgung nicht zu rechtfertigen sei, wenn der damit verbundene Grundrechtseingriff „nicht auf das absolut Notwendige“ beschränkt wird.[40]

23 Im Anschluss an technisch bedingte Persönlichkeitsgefährdungen durch die Vernetzung von informationstechnischen Systemen hat das Bundesverfassungsgericht im Jahre 2008 aus dem allgemeinen Persönlichkeitsrecht ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht) abgeleitet.[41] Im Ausgangsfall ermächtigte das Verfassungsschutzgesetz eines Bundeslandes die eigene Verfassungsschutzbehörde, Computer von verdächtigen Personen zu infiltrieren und Spionageprogramme einzusetzen, um die Kommunikation und abgelegte Daten auf internetfähigen Rechnern verdächtiger Personen heimlich zu erforschen. Der „Zugriff“ auf die gesamten Datenbestände eines privat genutzten PC gehe „in seinem Gewicht für die Persönlichkeit des Betroffenen über einzelne Datenerhebungen, vor denen das Recht auf informationelle Selbstbestimmung schützen soll, weit hinaus“.[42] Das IT-Grundrecht soll dem Umstand Rechnung tragen, dass eigene „informationstechnische Systeme einen besonders großen Funktionsumfang und besonders weitreichende Entfaltungschancen bieten, zugleich für den Nutzer aber wenig beherrschbar sind“.[43] Da der Einzelne wesentlich von der Nutzung informationstechnischer Systeme abhängig ist, betont das Gericht den grundrechtlichen Schutz der Integrität dieser physischen Systeme. Bestehende softwaretechnische Schutzmechanismen werden damit durch verfassungsrechtliche Schranken abgesichert, ein wirkungsvoller technischer Selbstschutz für Nutzer (z. B. bei PDAs und Mobiltelefonen) bleibt zwar schwierig, wird aber durch diese normativen Vorgaben gestärkt.

24 Das BVerfG fordert daher verfahrensrechtliche Vorkehrungen zum Schutz des Betroffenen. Sie sollen insbesondere ein Eindringen in den „absolut geschützten Kernbereich privater Lebensgestaltung“ verhindern.

25 Zur Entfaltung der Persönlichkeit im **Kernbereich privater Lebensgestaltung** gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen.[44]

---

39 Zur anlasslosen Kfz-Kennzeichenkontrolle BVerfG v. 18.12.2018, NJW 2019, 827, 834.

40 EuGH v. 21.12.2016, NJW 2017, 7171, 721; zum verfassungsrechtlich problematischen Themenkomplex „Vorratsdatenspeicherung“ Petri in: Bayerischer LfD, 28. TB (2018), 6.3.1.

41 BVerfG v. 27.02.2008, BVerfGE 120, 274; s. a. Hoffmann-Riem, JZ 2008, 1009, 1015 f.

42 BVerfG v. 27.02.2008, BVerfGE 120, 274, 313.

43 Bäcker, in: Uerpmann-Wittzack (Hg.), Das neue Computergrundrecht (2009), S. 11.

44 BVerfG v. 27.02.2008, BVerfGE 120, 274, 335 unter Berufung auf BVerfG v. 03.03.2004, BVerfGE 109, 279, 313; zur Bedeutung des Kernbereichs vgl. Hornung, Grundrechtsinnovationen (2015), S. 321.

In einem früheren Urteil, in dem sich das Gericht mit dem Abhören von Gesprä- **26**
chen innerhalb der Wohnung (Wanze) zu Zwecken der Strafverfolgung durch die Polizei befasste, hieß es weiter: „Die Privatwohnung ist als ‚letztes Refugium' ein Mittel zur Wahrung der Menschenwürde."[45] Totalitäre Regime haben den Schutz der Wohnung (Art. 7 und 8 GRCh; Art. 8 EMRK; Art. 13 Abs. 1 GG) immer missachtet und hemmungslos observiert. Der Schutz **räumlicher Privatheit** war seit jeher Teil einer zivilen Rechtskultur und trägt in tatsächlicher Hinsicht zur Wahrung und Erweiterung innerer Freiräume bei.[46] Vor diesem Hintergrund ist der Einsatz von Polizeivollzugsbeamten mit am Körper getragenen kleinen Videokameras in Wohnungen – sog. **Bodycams –**, ein besonders **schwerwiegender Eingriff** und eine technische Überwachung (Art. 13 Abs. 4 GG), die nicht nur die räumlichen Gegebenheiten einer Wohnung aufzeichnet, sondern auch die intensive Verletzung der Privatheit und Intimität betroffener Personen durch die Bildaufnahme riskiert.[47] Nach deutschem Recht unterliegt in solchen Fällen das polizeiliche Zugriffsregime einer externen richterlichen Anordnung (Richtervorbehalt).[48]

Zu den Möglichkeiten höchstpersönlicher (intimer) Selbstdarstellung gehören **27**
etwa Tagebücher oder persönliche Film- und Tonaufzeichnungen, unabhängig davon, ob sie an geografisch bestimmbaren Orten oder im virtuellen Raum stattfinden.[49] Gleichwohl spielt der geografische Raum als „organisierendes Prinzip und als ein Konstituens sozialer Beziehungen" weiterhin eine besondere Rolle.[50] Der virtuelle Raum ist zunehmend durch die IKT mit der physikalischen Welt verknüpft (Cyber Physical Systems). In beiden stellen sich neue Herausforderungen an den Datenschutz und die Informationsfreiheit.

Im europäischen Datenschutz ist der Schutz der Privatheit mit der Forderung **28**
nach Transparenz verbunden. Der Betroffene muss klar und deutlich darüber informiert werden, welche Daten (Gesundheits- und Sozialdaten, Konto-, Kredit-, und Steuerdaten usw.) über ihn gesammelt werden und zu welchem Zweck, an wen sie weitergeleitet werden und für wen sie transparent sind.

Viele grundrechtlich hoch entwickelte Staaten der Welt haben das datenschutz- **29**
rechtliche Transparenzprinzip mit dem Recht auf Informationsfreiheit verbunden. In erster Linie handelt es sich um das Recht auf Zugang zu den Informationen der

45 BVerfG v. 03.03.2004, BVerfGE 109, 279, 314; dazu Hohmann-Dennhardt, in: Duttge/Tinnefeld (Hg.), Gärten, Parkanlagen und Kommunikation (2006), S. 85–95.

46 S. a. Britz, Freie Entfaltung durch Selbstdarstellung (2007), S. 36 f.

47 Petri, ZD 2018, 453, 458.

48 Zum verfassungsrechtlich vorgegebenen Richtervorbehalt (Art. 13 Abs. 2 GG) im Zusammenhang mit Grundrechtseingriffen bei Wohnungsdurchsuchungen vgl. BVerfG v. 28.09.2004, NJW 2005, 275, 276.

49 BVerfG v. 27.02.2008, BVerfGE 120, 274, 335 f.

50 Schlögel, Im Raume lesen wir die Zeit (3. A. 2003), S. 36 f.

öffentlichen Verwaltung (freedom of information).[51] Die Informationsfreiheit ist ein Kennzeichen moderner Verwaltung und soll dem Einzelnen einen möglichst unbeschränkten Zugang zu Informationen und Dokumenten des Staates einräumen. In einer Demokratie bilden öffentlich zugängliche Informationen die Voraussetzung für die politische Auseinandersetzung und die Einflussnahme der Bürger auf Staatsgeschäfte. Dies gilt entsprechend für den Prozess der Willensbildung von EU-Bürgern. Eine reale Mitbestimmung ist nur möglich, wenn sie Zugang zu relevanten und zutreffenden Informationen erhalten, etwa bei Wahlen zum Europaparlament oder Referenden wie der Brexit-Abstimmung im Vereinigten Königreich.

30 Social-Media-Angebote, die eine digitale Öffentlichkeit schaffen, sind i. d. R. allgemein zugängliche Informationsquellen, die international einen „free flow of information" ermöglichen. Sie haben ggf. Auswirkungen für die Rechtspositionen des Datenschutzes. Das bedeutet, beide Rechte in eine jeweils optimale Konkordanz zu bringen. Denn: Datenschutz und Informationsfreiheit sind beide Bedingung für eine freie Entfaltung des Einzelnen und eine freiheitliche, demokratische Ordnung.[52]

31 Seit dem 1. Dezember 2009 ist der (supranationale) Vertrag von Lissabon in Kraft. Damit ist auch die Charta der Grundrechte der Europäischen Union (GRCh) rechtswirksam geworden. Der deutsche Staat ist wie alle Mitgliedstaaten der Europäischen Union als Unterzeichnerstaat an die Europäische Menschenrechtskonvention (EMRK) und im Geltungsbereich des Lissaboner Vertrags an die Grundrechte der Union gebunden. Die Erhaltung und Entfaltung der Grundrechte richten sich wesentlich nach den Vorgaben der Konvention, die 1953 als völkerrechtlicher Vertrag wirksam geworden ist. Die Konvention enthält zwar keine Bestimmungen über die Art ihrer Geltung in den einzelnen Mitgliedstaaten. Einigkeit besteht aber darüber, dass mangels besonderer Regelungen für die Bestimmungen des Beitrittsabkommens sowie für die EMRK selbst die allgemeinen Regeln über den Rang völkerrechtlicher Verträge der Union zum Tragen kommen.[53] Als Teil der Unionsrechtsordnung hat die EMRK in den Mitgliedstaaten Geltung. Unabhängig davon ist für jede Norm der EMRK zu bestimmen, ob sie eine eindeutige Verpflichtung für die Unterzeichnerstaaten enthält. Mit der Erklärung von Menschenrechtsverträgen erklären sich die Staaten dazu bereit, ihre Souveränitätsrechte einzuschränken, sodass sich betroffene Bürger im Einzelfall auf Menschenrechtsverletzungen vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) berufen können.[54] Der Gerichtshof in Straßburg bezieht in

---

51 Zur Entstehungsgeschichte vgl. Masing, Transparente Verwaltung: Konturen eines Informationsverwaltungsrechts, VVDStRL 63 (2004), S. 377; grundlegend Vismann, Akten: Medientechnik und Recht (2. A. 2001).

52 Simitis, KritV 2000, 368.

53 Vgl. Gragl, ZeuS 2011, 414; Leutheusser-Schnarrenberger, DuD 2010, 519.

54 Schiedermair, Der Schutz des Privaten als internationales Grundrecht (2012), S. 172 f.

seinen Entscheidungen die Rechtsordnungen der Mitgliedstaaten im Wege einer wertenden Rechtsvergleichung mit Blick auf die Zielsetzung der EMRK für seine eigenständige Interpretation heran und kann als einflussreiches Gericht Entscheidungen der nationalen Verfassungsgerichte infrage stellen.[55] Schon bisher hat insbesondere der EGMR den unantastbaren Menschenrechtsgehalt der Freiheitsrechte unmissverständlich verteidigt.

Nach der Rechtsprechung des EuGH fallen supranational gestaltete Regelungen **32**
wie das Datenschutzrecht unter die Jurisdiktion des Unionsrechts.[56] Infrage steht jedoch die Jurisdiktion der nationalen Verfassungsgerichte, wenn es sich um die Durchführung von Unionsrecht in Bereichen handelt, in denen den Mitgliedstaaten vom Gesetzgeber der EU ein Gestaltungsspielraum eingeräumt wurde wie etwa in einigen Artikeln der DS-GVO, die Öffnungs- bzw. Spezifierungsklauseln enthalten (z. B. im Bereich der Medien oder des Beschäftigtendatenschutzes). Nach dem EuGH handelt es sich auch in solchen Fällen um die Durchführung von Unionsrecht (Art. 51 Abs. 1 GRCh).[57] Das Bundesverfassungsgericht betont hingegen die Zuständigkeit der mitgliedstaatlichen Verfassungsgerichte im Bereich nationaler Gestaltungsspielräume.[58] Unbestritten ist jedoch, dass der **EuGH** auf **europäischer Ebene** zunehmend eine **zentrale Rolle** bei der datenschutzrechtlichen Rechtsprechung einnimmt.[59]

1.1.1 Informations-, Wissens- und Zivilgesellschaft

Die vernetzte, digitale Welt-Gesellschaft versteht sich als Informations- und Wis- **33**
sensgesellschaft. Was aber bedeuten Information und Wissen in Verbindung mit den Informations- und Kommunikationstechnologien (IKT)? Welcher Zusammenhang besteht zwischen menschlichem Tun, Kulturen und Zivilisationen?

Information zeichnet sich durch ihren immateriellen Charakter aus. Sie **34**
bestimmt als dritte Grundgröße neben der Materie und der Energie alle Lebensbereiche. Information ist Grundlage der interaktiven Freiheit aller Menschen und zugleich unentbehrlich für die Funktionserfüllung des Staates.[60] Information leistet Dienste und erzeugt Wirkungen (pragmatische Dimension). Sie ist zu einer dynamischen Produktivkraft im Wirtschaftsleben geworden und gewinnt

55 EuGH v. 09.11.2010, DuD 2011, 137.
56 EuGH v. 26.02.2013, NJW 2013, 1415 Rn. 17 f.
57 EuGH v. 26.02.2013, NJW 2013, 1415 Rn. 19 ff.
58 BVerfG v. 11.03.2008, BVerfGE 121, 1, 15; BVerfG v. 24.4.2013, BVerfGE 133, 277, 316.
59 Spieker gen. Döhmann/Eisenbarth, JZ 2011, 169, 173 ff.
60 Hoffmann-Riem, in: Der Landesbeauftragte für Datenschutz und für das Recht auf Akteneinsicht Brandenburg (Hg.), Dokumentation internationales Symposium Informationsfreiheit und Datenschutz in der erweiterten Europäischen Union (2001), S. 28 f.

als **Wirtschaftsgut** und damit auch als wichtiger **Wettbewerbsfaktor** zunehmend an Bedeutung.[61] Es ist daher nur folgerichtig, dass das Bundeskartellamt als deutsche Wettbewerbsbehörde Facebook das Sammeln von Nutzerdaten aus unterschiedlichen externen Quellen ohne Einwilligung untersagt, mit denen das Netzwerk Profile generiert, die etwa für die Werbewirtschaft interessant sind.[62] Eine marktbeherrschende Firma wie Facebook, die mit 23 Millionen Nutzern einen Marktanteil von 95 Prozent auf dem deutschen Markt besitzt, beutet nicht nur Nutzerdaten der Marktgegenseite aus.[63] Der Umfang, in dem Facebook Daten ohne Einwilligung der Nutzer sammelt, dem Nutzerkonto zuführt und zweckentfremdet verwertet, verstößt auch gegen die DS-GVO.

35 **Wissen** und Information stehen zueinander in einer Verbindung bzw. Wechselbeziehung. Informationsinhalte beeinflussen menschliches Bewusstsein und das Wissen über die Bedeutung der Privatheit in unterschiedlichen situationsspezifischen **Kontexten.** Insofern ist es konsequent, wenn der Datenschutz hervorhebt, dass die persönliche Information nur im Rahmen einer konkreten sozialen Relation rechtlich zugeordnet werden kann. Das datenschutzrechtliche **Gebot der Zweckbindung**, wonach Informationen nur zu bestimmten, legitimen Zwecken verwendet werden dürfen,[64] folgt auch auf europäischer Ebene dieser Einsicht. Andernfalls kann gerade unter dem Aspekt von Big Data und mithilfe von Algorithmen „ein Bild des Betroffenen entstehen, das ihn einerseits in Schablonen presst oder ihn andererseits missrepräsentiert".[65]

Beispiel

Die Berufsbezeichnung „Staatsanwalt" oder „Organist einer Kirche" usw. kann in Verbindung mit einer Namensliste von Patienten, die sich vorübergehend in psychiatrischer Behandlung befunden haben, eine berufliche Gefährdung einleiten. Die Verknüpfung der Patientennamen mit dem jeweiligen Beruf auf der Namensliste ist für die Zwecke der Behandlung nicht erforderlich. Das Wissen des Dienstherrn oder des Arbeitgebers über die Tatsache der Behandlung kann dazu führen, dass der Betroffene als „psychisch Kranker" diskriminiert sowie als untauglich für das Arbeitsleben eingestuft und entlassen wird. Das Recht auf informationelle Selbstbestimmung und Diskriminierungsverbote garantieren, dass die betroffene Person „sich selbst" darstellen kann und nicht automatisch als Mitglied einer bestimmten Gruppe mit bestimmten (vermeintlichen) Eigenschaften wahrgenommen wird.[66]

61 Zur marktwirtschaftlichen Orientierung des Datenschutzes Roßnagel/Pfitzmann/Garstka, Gutachten Modernisierung des Datenschutzrechts (2001), S. 72ff.

62 BKartA v. 06.02.2019, WuW 2019, 277. Zur wegweisenden Entscheidung des Bundeskartellamtes vgl. BfDI, Pressemitteilung v. 07.02.2019 unter: https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/06_BundeskartellamtzuFacebook.html (letzter Abruf 21.06.2019).

63 Eisenring, Deutschland will Facebook zähmen, NZZ International v. 09.02.2019, S. 7.

64 BVerfG v. 15.12.1983, BVerfGE 65, 1, 43.

65 Simitis/Hornung/Spiecker gen. Döhmann, in: dies. (Hg.), DSchR (2019), Einl. Rn. 11.

66 Britz, Freie Entfaltung durch Selbstdarstellung (2007), S. 55.

Wo die kontextgebundene Einbettung der Information durch eine zweckfreie Verarbeitung verloren geht, verliert sich Wissen und mithin auch die Transparenz über bedeutungstragende Zusammenhänge. Wenn aber die an einem Informationsprozess Beteiligten nicht mehr durchschauen können, was ihnen in Form von Informationen zur Verfügung steht, wachsen „die Abhängigkeiten gegenüber Informationen und das selbst erworbene und selbst beherrschte Wissen nimmt ab“.[67] 36

Francis Bacon (1561–1626) hat sich bereits vor dem eigentlichen Zeitalter der Aufklärung nach der Maxime **„Wissen ist Macht“** mit den Informationsbedingungen befasst, unter denen der wissenschaftliche und technische Fortschritt wirkungsvoll organisiert werden kann.[68] Danach ist es nicht mehr die Wissenschaft selbst (ipsa scientia), sondern „die gezielt erhobene, sicher gespeicherte, vernetzbare und abrufbare Information über ein spezifisches Faktum“, welche Macht schaffen kann.[69] Die Einsicht von Bacon kann angesichts der digitalen Datenverarbeitung auch so formuliert werden: Macht, die nur auf unzureichender Information basiert, ist **Macht ohne Wissen,** die Unsicherheit, Angst und Unterlegenheit bei vielen Menschen erzeugt. Der Philosoph Hans Jonas verdeutlicht diese Situation, wenn er auf die „enorme Entmündigung des Einzelnen durch den faktischen und psychologischen Massenzwang der technologischen Ordnung“ hinweist.[70] 37

Kultur ist die Art, wie Menschen miteinander und mit der Umwelt umgehen. Kulturen müssen mit Mehrdeutigkeiten leben: Sprache, Gesten und Zeichen sind häufig nicht eindeutig, Handlungen müssen interpretiert und Werte müssen miteinander versöhnt oder unversöhnt nebeneinander toleriert werden. Die Konsequenzen für die jeweiligen Gesellschaften sind einschneidend. Politik, Recht und Religion, der Umgang mit sexuellem Verhalten, mit Freunden, Fremden und mit Minderheiten sind wesentlich davon geprägt. Die menschenrechtlichen Probleme, die im Umgang mit „kultureller Differenz“ auftreten, sind vielgestaltig und im vereinten Europa jeweils aus der konkreten verfassungsrechtlichen Perspektive der EU und ihren Mitgliedstaaten auch für Flüchtlinge, für ein Miteinander zu erschließen.[71] Denn mit einem verengten Blick schwindet die Möglichkeit eines Menschen zur Einfühlung in ein konkretes Gegenüber. In solchen Fällen nehmen sie nicht wahr, dass sich ihre Überzeugungen oder bestimmte digitalisierte personenbezogene Datenauswertungen auch als falsch herausstellen können. An dieser 38

67 Mittelstraß, Leonardo-Welt (2. A. 1992), S. 232 ff.

68 Bacon, Neues Organ der Wissenschaften (1974).

69 Hassemer, Datenschutz und Datenverarbeitung heute (1995), S. 28.

70 Jonas, Das Prinzip Verantwortung (1985), S. 219; Beck, Risikogesellschaft (1986), S. 24, charakterisiert die heutige Gesellschaft als Risikogesellschaft, die zur „Einschätzung und Abwendung des Schlimmsten an das Urteil der Techniker (aus)geliefert ist“.

71 S. a. Britz, Kulturelle Rechte und Verfassung (2000), S. 2 f.

Stelle gewinnt das Datenschutzrecht als Lotse im menschlichen Miteinander an Relevanz, in dem es Dialogrechte bereithält, damit falsche Ergebnisse korrigiert oder diskriminierende Mechanismen etwa bei algorithmenbasierten Ergebnissen bzw. Beurteilungen im Arbeitsleben oder im Flüchtlingswesen durchbrochen werden.[72]

39 Eine umweltbezogene Modifikation des Begriffs „Kultur" findet sich bei Andrea Raschèr und Christoph Reichenau. Beide verbinden Kultur mit den drei Dimensionen des Begriffs „Nachhaltigkeit" im Sinne des Brundtlandberichts von 1987, der von der Untrennbarkeit der ökologisch-ökonomisch-sozialen Lebensgrundlagen ausgeht.[73] Die so verstandene Kultur ist Ausdruck einer ganzheitlichen Sicht menschlichen Lebens, die den **„zivilisatorischen Kulturbegriff"** ausmacht.[74] Auch der EGMR in Straßburg hat die umweltbezogenen Einwirkungen auf die Entfaltung des Privatlebens (Art. 8 Abs. 1 EMRK) betont und ausgeführt, dass sie als äußerer Teil zur Lebenswirklichkeit der Privatsphäre des Einzelnen gehören, in der er die Entwicklung und Erfüllung seiner Persönlichkeit anstreben kann.[75]

40 Zu der als **Zivilisation** verstandenen Kultur gehört die Anerkennung der Allgemeinen Menschenrechte (1948), „die als der bisher größte Beweis [...] hinsichtlich eines bestimmten Wertesystems angesehen werden kann".[76] Seither betonen europäische Grundrechtskataloge die **Achtung der Menschenwürde** (Art. 1 GRCh, Art. 1 Abs. 1 GG), die jedem Menschen zusteht, die unantastbar und unveräußerlich ist. Es gehört zu den maßgeblichen Prinzipien einer Verfassung, die in der Menschenwürde wurzelnde Gleichheit aller zu respektieren: Die Anerkennung der **Gleichheit jedes Menschen** vor dem Gesetz (vgl. etwa Art. 20 GRCh; Art. 3 Abs. 1 GG) verbietet das Entwürdigen und die Verächtlichmachung Anderer, begründet ein rechtliches Unterscheidungsverbot bei der Verarbeitung personenbezogener Daten nach Abstammung, Geschlecht, Stand, Herkunft und Religion (vgl. etwa Art. 14 EMRK; Art. 21 GRCh; Art. 3 Abs. 3 GG). Die DS-GVO befasst sich vor dem Hintergrund neuer Entwicklungen mit der Frage besonders **risikoträchtiger Daten** (besondere Kategorien von personenbezogenen Daten), aus denen die „rassische, und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen

72 Zum Datenschutz als Lotse in der Informationsgesellschaft Tinnefeld, DuD 2005, 328; Schmale/Tinnefeld, Privatheit im digitalen Zeitalter (2014), S. 77–94.

73 S. unter: https://www.nachhaltigkeit.info/artikel/brundtland_report_563.htm?sid=4m2abjth0dtld997ka2pk51432 (letzter Abruf 21.06.2019); s. a. Klein, Die Entscheidung Kapitalismus vs. Klima, (2015).

74 Zum Begriff Kulturen – Zivilisationen vgl. Raschèr/Reichenau, in: Mosimann/Renold/Raschèr (Hg.), Kultur, Kunst und Recht (2009), Kap. 1 § 1 Rn. 1 ff. m. w. N.; Tinnefeld, DuD 2011, 598 m. w. N.

75 Vgl. EGMR v. 19.02.1998, NVwZ 1999, 57. In dem Urteil ging es um Staatenpflichten im Zusammenhang mit Umweltverschmutzungen aufgrund industrieller Emissionen.

76 Bobbio, Das Zeitalter der Menschenrechte (1999), S. 9.

Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“ (Art. 9 Abs. 2 DS-GVO). Sie sind als Selektionskriterien in gesetzlichen Regelungen bzw. als Grundlage für Entscheidungen grundsätzlich nicht zulässig.

41 Seit den zwei brutalen Weltkriegen im 20. Jahrhundert leben Menschen- und Grundrechtserklärungen von der Bindung an die Menschenwürde und den daraus folgenden Grundsätzen individueller Selbstbestimmung und gleicher Freiheit.[77] Sie schützen die Autonomie der verschiedenen Subsysteme: politische und wirtschaftliche Instanzen, Gewerkschaften oder andere Einrichtungen und mithin eine pluralistische (tolerante) Demokratie.[78]

42 Der moderne (liberale) Staat ist verpflichtet, die universalen Menschenrechte mit den rechtsstaatlichen Grundsätzen der Verfassung (Gesetzmäßigkeit der Verwaltung und Unabhängigkeit der Gerichte) zu verbinden und einzuhalten.[79] Dieser zivilisatorische Zugewinn macht die freie Rede sowie eine kritische öffentliche Auseinandersetzung möglich, in der Menschen argumentieren und auch auf ihr Gegenüber eingehen können. Insbesondere die potenziell befreienden Möglichkeiten des Internets haben totalitäre Regime zum Aufbau massiver Kontroll-Systeme für die Eindämmung der Meinungs- und Informationsfreiheit veranlasst.[80]

1.1.2 Internetkommunikation und technischer Grundrechtsschutz

43 Im Zusammenhang mit den neuen **Technologien** zeichnet sich zunehmend eine **kulturelle Wende** in Verbindung mit einer globalen Kommunikationsstruktur ab.[81] Das Denken und Tun des Menschen ist zwar nach wie vor durch seine Kultur (in Stamm, Volk, Nation, Religion, Klasse usw.) geprägt. Meinungsbildung und -macht wird aber mehr und mehr durch die Internetkommunikation verändert.

> Wir sind sprachliche Wesen. Wir verstehen uns nur im Gespräch mit anderen. Erzählend entwickeln wir unsere Vorstellung von uns selbst. Von unserer Herkunft erfahren wir durch die Geschichten, die erinnerten, die erfundenen unserer Vorfahren, von uns selbst erfahren wir durch die Reaktionen der anderen. Als solche sprachlichen Wesen, die sich dialogisch, mit und durch andere begreifen, sind wir abhängig davon, dass wir unsere Erfahrungen in eine Geschichte betten können. Wie mäandernd sich unsere Leben auch ihren Weg bahnen, suchen

77 Dazu Joas, Die Sakralität der Person (2011), S. 108 ff.

78 Zur Respekt-Toleranz vgl. Forst, Toleranz im Konflikt (2003), S. 45.

79 Grundlegend Häberle, Europäische Rechtskultur (1997).

80 Zu Zensurmaßnahmen Chinas im Internet vgl. Ash, Redefreiheit, aus dem Englischen v. Dierlamm (2016), S. 67.

81 Raschèr/Reichenau, in: Mosimann/Renold/Raschèr (Hg.), Kultur, Kunst und Recht (2009), Kap. 1 § 1 Rn. 10.

> wir doch danach, den Verlauf in ein Narrativ bringen zu können. [...]. Durch Anerkennung oder Abweisung der Gegenüber zeichnen sich unsere Eigenarten und Andersartigkeiten, Ähnlichkeiten und Verschiedenheiten, unsere Individualität also, erst ab und aus.[82]

44 Oder anders ausgedrückt: Andere Menschen bilden online und offline das soziale Umfeld, in dessen Rahmen sich der Einzelne kulturell bewegt.[83]

45 Im Internet konnte bisher niemand sicher wissen, wer der Kommunikationspartner war. Jedem war es möglich, prinzipiell jedwede „Identität" anzunehmen, die nichts oder wenig mit ihm als „Persönlichkeit" zu tun hat. Die Zeit, in der das Internet ein anonymes Medium war, wo jeder in der Maske eines Anderen auftreten konnte, wo, so die Worte auf der berühmten New Yorker Karikatur von Peter Steiner (1993), „nobody knows you're a dog", wandelt sich. Das Internet wird zunehmend zu einem Medium der personalisierten Suche und Analyse, wo die Ergebnisse für neue Zwecke (z. B. durch Auslesen von Profildaten für das Beschäftigtenverhältnis, für speziell ausgesuchte Werbung oder für „Friendfinder" in sozialen Netzwerken) verwandt werden.[84] Die umstrittene anlasslose Speicherung von Daten über die näheren Umstände einer Telekommunikation (Verkehrsdaten) für Zwecke der Strafverfolgung ist ein besonders aussagekräftiges Beispiel für die Tendenz, unbeobachtete menschliche Kommunikation zu eliminieren. Vor dem Hintergrund dieser Entwicklung ist es fraglich, ob und wie Kommunikationspartner noch anonym an vertrauliche Nachrichten gelangen können.

46 Zahlreiche Menschen, insbesondere Jugendliche, erproben neue kommunikative Rollen im World Wide Web (WWW). In welcher Gestalt und in welcher Rolle (identifizierbar, anonym oder pseudonym) wollen und können sie ihre Privatheit und Selbstbestimmung leben? Im Zusammenhang mit den technischen Möglichkeiten und Maßnahmen zum Schutz der Privatheit sind die dafür wesentlichen Begriffe der Anonymität, Pseudonymität und Vertraulichkeit näher zu betrachten.

47 Die Sprache gibt erste Hinweise auf die Bedeutung von **Anonymität**. Das Wort ist griechischen Ursprungs. „Anonymus" ist der Namenlose, aber auch der Un-Bekannte, den man nicht kennt oder der nicht identifiziert werden kann. Menschen identifizieren sich gegenseitig vornehmlich über ihren Namen. Damit wird bereits deutlich, dass Anonymität sich auf zwei oder mehrere Parteien beziehen kann.

Beispiel

Der Sender einer Nachricht will gegenüber seinem Kommunikationspartner unerkannt, also anonym bleiben. Der Patient möchte nicht, dass seine Kommunikation mit einem Arzt gegenüber Dritten offenbar wird. Sie soll „geheim" und vertraulich bleiben. In der Verbindung Arzt – Patient wird

---

82 Emcke, Stumme Gewalt, Zeit Online v. 06.09.2007 unter: http://www.zeit.de/2007/37/Herrhausen-Emckehttp://www.zeit.de/2007/37/Herrhausen-Emcke (letzter Abruf 21.06.2019).

83 Dazu Suhr, Entfaltung der Menschen durch die Menschen (1976), S. 78 f.

84 Übersicht bei Pariser, The Filter Bubble: What the Internet is Hiding from You (2012), S. 6 ff.

der Inhalt der Kommunikationsbeziehung als solche durch das Patientengeheimnis und ggf. durch das Telekommunikationsgeheimnis geschützt.

Rechtlich handelt es sich um „Senderanonymität“, wenn der Empfänger einer Nachricht nicht weiß, wer sie verschickt hat. Dagegen spricht man von „Empfängeranonymität“, wenn der Sender eine Nachricht abschicken kann, ohne dass er weiß, wer der Empfänger ist. Technisch gesehen wäre bei einer Web-Anfrage Senderanonymität gegeben, wenn der Rechner nicht einem bestimmten Webserver zugeordnet werden kann.[85] **48**

Beispiel
Ein Aidsverdächtiger möchte, dass sein HIV-Test anonym durchgeführt wird. Der Getestete kann zu diesem Zweck ein Codewort mit der testenden Stelle vereinbaren und darüber das Ergebnis der Blutuntersuchung erfahren. Das Verfahren ist aufgrund des Selbstbestimmungsrechts der betroffenen Person geboten und auch möglich, da die testende Einrichtung bei einem positiven Ergebnis keine namentliche Meldepflicht an das Robert-Koch-Institut in Berlin hat, das für seine Zwecke nur die Anzahl der infizierten Personen, nicht aber die persönliche Zuordnung der besonderen (sensiblen) Information benötigt.[86]

Anonymität hat pragmatisch betrachtet immer auch etwas mit den konkreten Gefährdungslagen zu tun, aus denen heraus sich der wesentliche Inhalt, das Ausmaß und die Wirkungen des grundrechtlichen Schutzes bestimmen lassen. **49**

Beispiel
Bankräuber maskieren sich, um eine Bank auszurauben. Sie wollen anonym bleiben, damit ihnen die Tat nicht zugerechnet werden kann. Whistleblower, die erhebliche Missstände in ihrer Firma öffentlich machen, wollen anonym bleiben, um vor einer Kündigung durch den betroffenen Arbeitgeber geschützt zu sein. Wenn ihnen die Meldung nicht zugerechnet werden kann, ist es aber für einen anderen angeschuldigten Mitarbeiter wesentlich schwerer, sich zu rechtfertigen. Datenschutzrechtlich ist ein Verfahren zu suchen, dass auch den Angegriffenen schützt.[87] Strafverfolgungsbehörden nutzen deanonymisierende Elemente wie biometrische Merkmale, DNA-Material, Daten aus einer Videoüberwachung, um verdächtige Personen zu identifizieren oder anlasslos gespeicherte Telekommunikationsdaten, um mögliche Täter zu finden.[88]

Beispiel
Informanten von Journalisten wollen anonym bleiben. In Fällen schwerer Kriminalität und Menschenrechtsverletzungen (z. B. Folter) hängt häufig der Schutz ihres Lebens davon ab, dass sie unbekannt

85 Ausführlich Brunst, Anonymität im Internet (2009), S. 7–31.
86 Vgl. § 7 Abs. 3 Nr. 2 i. V. m. Abs. 2 IFSG. Damit identische Fälle nicht mehrfach erfasst werden, muss eine fallbezogene Verschlüsselung übermittelt werden.
87 Tinnefeld/Rauhofer, DuD 2008, 717 m. w. N.
88 Zur Verfassungswidrigkeit und zur Datenschutzfrage in Europa vgl. Petri, DuD 2011, 607.

bleiben. Der EGMR hat den Schutz journalistischer Quellen als eine der Grundbedingungen der Pressefreiheit und als wichtigen Beitrag zur Meinungsfreiheit anerkannt.[89] Anonymität steht daher häufig nicht nur im Zusammenhang mit dem Schutz der Privatheit, sondern auch mit den Möglichkeiten der freien Meinungsäußerung und der Informationsfreiheit.

50 In der Realität liegt Anonymität immer nur relativ vor. Die Frage ist, welche zusätzlichen Informationen mit welchem Aufwand für eine De-Anonymisierung notwendig sind. Roger Dingledine formuliert treffend: „[...] the question shifts from, is it anonymous? to is it anonymous enough?“[90] Es gibt verschiedene Auffassungen darüber, wie Anonymität zu definieren ist.

51 Die Informatik orientiert sich an internationalen Standards (z. B. an ISO 15408) und spricht von einem Zustand, in dem jemand oder etwas innerhalb der ihn umgebenden Subjekte nicht identifizierbar ist (Anonymitätsset).[91] Das Risiko personenbezogener Datenspuren in einer vernetzten Welt lässt sich durch Maßnahmen der Nutzer oder durch die Inanspruchnahme von Anonymisierungsdiensten (z. B. von JAP) oder anderen datenschutzfördernden Techniken (z. B. attributbasierter Zertifikate statt Identitätszertifikate) selbst minimieren. Sie sind Teil begrenzter Möglichkeiten des **Selbstdatenschutzes**[92] und der digitalen Selbstverteidigung im Internet.[93] Werden mehr als nur die erforderlichen Informationen offenbart, dann erhöht sich die Gefahr des Identitätsmissbrauches, etwa im Rahmen mobiler sozialer Netzwerke. Ein gewisses Dilemma ergibt sich allerdings für die Sicherheitsbehörden: Der kriminelle Nutzer soll enttarnt, der unbescholtene Nutzer aber nicht identifiziert werden.

52 In vielen Fällen, in denen von Anonymität die Rede ist, handelt es sich allerdings um pseudonyme Konstruktionen. Unter dem aus dem Griechischen kommenden Begriff **Pseudonym** wird ein Deckname verstanden. Die Handlungen eines pseudonymen Nutzers sind mit einer alternativen Identität, etwa einem frei gewählten Nutzernamen oder auch einer Nummer verbunden.

Beispiel

Ein weltberühmtes Pseudonym war „Deep Throat“. Unter diesem Decknamen gab der wichtigste Informant in der Watergate-Affäre (1972–1974) Journalisten der Washington Post Einblicke in korruptes Regierungsverhalten, die zum Rücktritt des US-Präsidenten Nixon führten.[94] Die Zuordnung des Pseudonyms zum „realen“ Namen des Agenten William Mark Felt wurde 30 Jahre lang geheim

89 EGMR v. 27.03.1996, MR 1996, 123; zum Schutz des Vertrauensverhältnisses von Informanten vgl. BVerfG v. 27.02.2007, BVerfGE 117, 244.

90 Dingledine, The Free Haven Project (2000), S. 11.

91 Pfitzmann/Hansen, Anonymity, Unlikability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A consolidated proposal for Terminology (2008).

92 Albrecht, Finger weg von unseren Daten! (2014), S. 70–94.

93 S. unter: https://digitalcourage.de/https://digitalcourage.de (letzter Abruf 21.06.2019).

94 Detaillierter Überblick bei Bernstein/Woodward, All The President’s Men (1974).