

People Analytics in privatrechtlichen Arbeitsverhältnissen

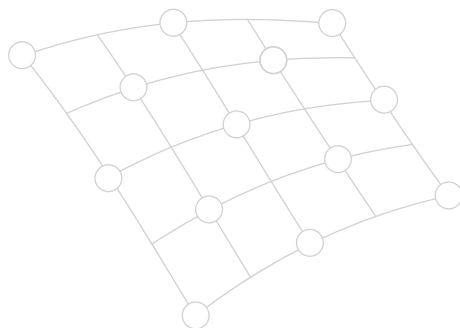
Vorschläge zur wirksameren Durchsetzung
des Datenschutzrechts

GABRIEL KASPER

Herausgegeben von
Malte-Christian Gruber
Valérie Junod
Isabelle Wildhaber

Gabriel Kasper

**People Analytics in privatrechtlichen
Arbeitsverhältnissen**



Herausgegeben von:

Prof. Dr. Malte-Christian Gruber

Ordinarius für Rechtsphilosophie und Wirtschaftsrecht mit Schwerpunkt Immaterialgüterrecht und Recht der neuen Technologien an der Universität Luzern

Prof. Dr. Valérie Junod, LL.M., J.S.M.

Professeure ordinaire à la Faculté des HEC de l'Université de Lausanne; professeure titulaire à la Faculté de droit de l'Université de Genève; co-directrice du Master en Droit et Economie

Prof. Dr. Isabelle Wildhaber, LL.M.

Ordinaria für Privat- und Wirtschaftsrecht unter besonderer Berücksichtigung des Arbeitsrechts an der Universität St. Gallen; Direktorin am Forschungsinstitut für Arbeit und Arbeitswelten (FAA-HSG)

People Analytics in privatrechtlichen Arbeitsverhältnissen

Vorschläge zur wirksameren Durchsetzung
des Datenschutzrechts

GABRIEL KASPER

DIKE 

 **Nomos**

ST. GALLER DISSERTATION 2021

Abdruck der an der Universität St. Gallen auf Antrag von
Frau Prof. Dr. Isabelle Wildhaber und Herrn Prof. Dr. Beat Rudin
genehmigten Dissertation Nr. 5051.

Publiziert gemäss dem Open-Access-Gold-Standard.
Die Druckvorstufe dieser Publikation wurde vom Schweizerischen Nationalfonds
zur Förderung der wissenschaftlichen Forschung unterstützt.

Publiziert von:

Dike Verlag
Weinbergstrasse 41
CH-8006 Zürich
www.dike.ch

Text © Gabriel Kasper 2021

ISBN (Hardback) 978-3-03891-273-6 (Dike Verlag AG, Zürich/St. Gallen)
ISBN (Hardback) 978-3-8487-8262-8 (Nomos Verlag, Baden-Baden)
ISBN (PDF): 978-3-03929-009-3

DOI: <https://doi.org/10.3256/978-3-03929-009-3>



Dieses Werk ist lizenziert unter
Creative Commons Lizenz CC BY-NC-ND.



Vorwort

Die vorliegende Arbeit wurde im Herbstsemester 2020 von der Law School der Universität St. Gallen als Dissertation angenommen. Sie ist im Zeitraum von April 2017 bis Mai 2020 entstanden, als ich für ein Forschungsprojekt zum Thema *«Big Data or Big Brother? – Big Data HR Control Practices and Employee Trust»* arbeitete. Es handelt sich um ein Projekt des Schweizerischen Nationalfonds im Rahmen des 75. Nationalen Forschungsprogramms zum Thema Big Data (NFP75). In dem interdisziplinären Projekt (im Folgenden: NFP75-Projekt) durften meine Doktormutter und ich als Rechtswissenschaftler mit Sozialwissenschaftlern aus den Bereichen Ethik und Personalmanagement zusammenwirken.

Diese Arbeit bezieht vollumfänglich die zahlreichen Gesetzesänderungen mit ein, die bis zum 10.10.2020 stattgefunden haben: Genannt werden jeweils gleichzeitig die Fundstellen im geltenden Gesetz («DSG»), im bundesrätlichen Entwurf, über den das Parlament debattierte («E-DSG»), und im revidierten Gesetzestext, der vom Parlament verabschiedet wurde und voraussichtlich im Jahr 2022 in Kraft treten wird («rev-DSG»). Zudem berücksichtigt die vorliegende Arbeit die einschlägigen ausländischen Rechtsnormen, da die DSG-Revision in einem internationalen Kontext zu betrachten ist. Einerseits fliesst die europäische DSGVO ein, die seit dem 25.05.2018 anwendbar ist. Andererseits werden Vergleiche mit dem amerikanischen Recht gezogen, wobei berücksichtigt wird, dass in den USA sowohl unter dem Safe Harbor-Abkommen als auch unter dem nachfolgenden Swiss-US Privacy Shield Framework kein angemessener Datenschutz im Sinne des DSG bestand. Literatur und Rechtsprechung sind bis 31.05.2020 berücksichtigt. Internet-Adressen waren ebenfalls bis zu diesem Zeitpunkt unter der jeweiligen Adresse auffindbar.

Dankbar bin ich meiner akademischen Lehrerin und Doktormutter an der Universität St. Gallen, Prof. Dr. Isabelle Wildhaber, LL.M., für die umsichtige Betreuung der Dissertation und die abwechslungsreichen Aufgaben als wissenschaftlicher Mitarbeiter am Forschungsinstitut für Arbeit und Arbeitswelten der Universität St. Gallen (FAA-HSG), einschliesslich der gemeinsamen Organisation einer Konferenz zum vorliegenden Forschungsthema, der Unterrichtstätigkeit und eines Auslandsaufenthalts als Gastforscher in den USA. Mein grosser Dank gilt sodann meinem Korreferenten, Prof. Dr. Beat Rudin, Universität Basel, der mir eine Vielzahl äusserst wertvoller Hinweise gegeben hat. Es kam mir das Privileg zu, in der intellektuell stimulierenden Atmosphäre am Berkman Klein Center for Internet &

Society an der Harvard University in Cambridge (Massachusetts, USA) bedeutende Teile meines Werks zu entwerfen, wofür ich dem dortigen Direktor des Forschungszentrums, Prof. Dr. Urs Gasser, LL.M., und dem Schweizerischen Nationalfonds, der meinen Forschungsaufenthalt ermöglicht hat, gebührend danke.

Ganz bestimmt nicht zum Erfolg gekommen wäre diese Dissertationsschrift ohne die Unterstützung meiner Eltern Maja und Paul sowie meiner Freundin Celine, die mir alle auch in schwierigen Zeiten immer den Rücken gestärkt haben. Dank der Korrekturlesung meines Vaters, seines Zeichens Byzantinist, ist diese Arbeit auch für Nichtjuristen verständlich geworden. Nicht zuletzt geht mein herzlicher Dank an das Team der Literaturverwaltungs-Software Citavi, mit dessen Unterstützung selbst die formalen Aspekte des Abfassens einer Dissertation Freude bereiten.

Die vorliegende Arbeit wurde vom Komitee der Konvention 108 des Europarats mit dem Stefano Rodotà-Award 2021 ausgezeichnet. Sie hat zudem den Professor Walther Hug-Preis 2021 gewonnen.

St. Gallen, 10.10.2020

Gabriel Kasper

Inhaltsübersicht

Vorwort.....	V
Inhaltsverzeichnis	XI
Abkürzungsverzeichnis	XXI
Literaturverzeichnis	XXXIII
Materialienverzeichnis	LXIX
Abbildungsverzeichnis.....	LXXI
Zusammenfassung.....	LXXIII
Summary.....	LXXIV
Résumé	LXXV
1 Einführung	1
1.1 Problemaufriss: Chancen und Risiken	1
1.2 Forschungsstand und Forschungslücke	4
1.3 Zielsetzung und Forschungsfrage	11
1.4 Abgrenzung der Forschungsfrage.....	12
1.5 Methodik der begleitenden empirischen Datenerhebung.....	14
1.6 Aufbau.....	17
2 Phänomenbeschreibung	19
2.1 Übersicht	19
2.2 Technische Begriffserklärungen.....	19
2.3 Verwendungszwecke.....	42
2.4 Verbreitung und praktische Relevanz.....	60
2.5 Unterschiede zu älteren Überwachungsformen	69
2.6 Zwischenfazit: neuartiges, weit verbreitetes Phänomen	77
3 Rechtsprobleme	79
3.1 Übersicht	79
3.2 Machtverschiebung als Grundproblem.....	79
3.3 Persönlichkeitsverletzungen	82
3.4 Diskriminierungen.....	88

3.5	Verletzung von Mitwirkungsrechten	99
3.6	Zwischenfazit: Rechtsprobleme vom Kontext abhängig	106
4	Relevante Rechtsbestimmungen	107
4.1	Übersicht	107
4.2	Arbeitsrechtlicher Persönlichkeitsschutz	107
4.3	Datenschutzrechtlicher Persönlichkeitsschutz	108
4.4	Öffentlich-rechtlicher Arbeitnehmer-Gesundheitsschutz	114
4.5	Diskriminierungsschutz	115
4.6	Mitwirkungsrecht	126
4.7	Strafrecht	127
4.8	Europäische Menschenrechtskonvention und Verfassungsrecht	128
4.9	Weiteres Völkerrecht	129
4.10	Zwischenfazit: Querschnittsmaterie People Analytics	131
5	Datenschutzrechtliche Rahmenbedingungen	133
5.1	Übersicht	133
5.2	Aufbau des Datenschutzgesetzes	133
5.3	Zweck des Datenschutzgesetzes	135
5.4	Geltungsbereich des Datenschutzgesetzes	154
5.5	Zweckbindungsgebot	173
5.6	Erkennbarkeitsgebot	199
5.7	Richtigkeitsgebot	206
5.8	Datenminimierung und Speicherbegrenzung	206
5.9	Löschpflicht	209
5.10	Rechtfertigungsmöglichkeiten	212
5.11	Umsetzung der Datenschutznormen in der Praxis	242
5.12	Zwischenfazit: hoher Fachwissensbedarf bei gleichzeitigen Mängeln in der Datenschutzpraxis	247

6	Rechtsdurchsetzung	251
6.1	Übersicht: Individualrechtsschutz und weitere Rechtsbehelfe	251
6.2	Zivilrechtliche Individualklagen.....	253
6.3	Datenschutzrechtliche Aufsicht.....	275
6.4	Arbeitsgesetzliche Aufsicht.....	279
6.5	Strafverfolgung	281
6.6	Mitwirkungsrechtliche Behelfe	282
6.7	Gesellschaftsrechtliche Haftung der exekutiven Organe	288
6.8	Arbeitsverweigerung, Streik und Kündigung	290
6.9	Zwischenfazit: mühevollere Rechtsdurchsetzung.....	291
7	Neuausrichtung des Datenschutzrechts	295
7.1	Rekapitulation der gegenwärtigen Probleme	295
7.2	Neuausrichtung auf das Teilen von Information und die Stärkung des Vertrauens in das Datenschutzrecht	296
7.3	Professionalisierung und Demokratisierung als Mittel zur Umsetzung des neu ausgerichteten Datenschutzrechts.....	315
7.4	Zwischenfazit: effektiverer Datenschutz basierend auf Professionalisierung und Demokratisierung.....	364
8	Ergebnisse	369

Inhaltsverzeichnis

Vorwort.....	V
Inhaltsübersicht.....	VII
Abkürzungsverzeichnis.....	XXI
Literaturverzeichnis.....	XXXIII
Materialienverzeichnis.....	LXIX
Abbildungsverzeichnis.....	LXXI
Zusammenfassung.....	LXXIII
Summary.....	LXXIV
Résumé.....	LXXV
1 Einführung.....	1
1.1 Problemaufriss: Chancen und Risiken.....	1
1.2 Forschungsstand und Forschungslücke.....	4
1.2.1 Vorbemerkung: Berücksichtigung internationaler Quellen.....	4
1.2.2 Behördliche Verlautbarungen.....	5
1.2.3 Literatur.....	6
1.2.4 Forschungslücke.....	9
1.3 Zielsetzung und Forschungsfrage.....	11
1.4 Abgrenzung der Forschungsfrage.....	12
1.5 Methodik der begleitenden empirischen Datenerhebung.....	14
1.6 Aufbau.....	17
2 Phänomenbeschreibung.....	19
2.1 Übersicht.....	19
2.2 Technische Begriffserklärungen.....	19
2.2.1 Daten-Lebenszyklus.....	19
2.2.2 Daten.....	20
a) Daten und Information.....	20
b) Digitalisierung und Datafizierung.....	23

2.2.3	Ausgewählte physische Komponenten und Computerinfrastruktur	25
a)	Sensoren, Wearables und Roboter zur Datenbeschaffung	25
b)	Internet als Medium zur Datenübertragung	27
c)	Cloud-Computing	28
2.2.4	Algorithmen	29
a)	Zum Begriff «Algorithmus»	29
b)	Abgestufte Fähigkeiten von Algorithmen	29
c)	Künstliche Intelligenz	30
d)	Korrelationen und Kausalitäten	32
2.2.5	Big Data	36
a)	Fehlende Legaldefinition	36
b)	Die (mindestens) drei V-Eigenschaften	36
c)	Kritik am Begriff «Big Data»	40
d)	Verhältnis zu People Analytics	40
2.2.6	Zwischenfazit: zusammenhängende technische Konzepte	41
2.3	Verwendungszwecke	42
2.3.1	Arbeitnehmer-Lebenszyklus	42
2.3.2	Rekrutierung	43
2.3.3	Leistungssteuerung	45
2.3.4	Compliance-Management	50
2.3.5	Arbeits- und Arbeitsplatzgestaltung	52
2.3.6	Mitarbeiterbindung	55
2.3.7	Zwischenfazit und Vorbehalte zur Klassifizierung der Verwendungszwecke	58
2.4	Verbreitung und praktische Relevanz	60
2.4.1	NFP75-Daten zur Verbreitung in der Schweiz	60
2.4.2	Verbreitung in der Welt	64
2.4.3	Steigende künftige Verbreitung	66
2.4.4	Zwischenfazit	69
2.5	Unterschiede zu älteren Überwachungsformen	69
2.5.1	Vorbemerkungen	69
2.5.2	Geschichtliche Vorläufer der Mitarbeiterüberwachung	70

2.5.3	Drei Kernelemente von People Analytics	71
a)	Ubiquität.....	71
b)	Interoperabilität	74
c)	Steigende künstliche Intelligenz	75
2.5.4	Zwischenfazit zu den drei Kernelementen	76
2.6	Zwischenfazit: neuartiges, weit verbreitetes Phänomen	77
3	Rechtsprobleme	79
3.1	Übersicht	79
3.2	Machtverschiebung als Grundproblem.....	79
3.3	Persönlichkeitsverletzungen	82
3.3.1	Umfassender Persönlichkeitsschutz	82
3.3.2	Ausgewählte Aspekte der Persönlichkeit	83
a)	Privatsphäre	83
b)	Psychische Integrität.....	86
c)	Recht am eigenen Wort und Bild.....	87
3.4	Diskriminierungen.....	88
3.4.1	Problembeschreibung.....	88
3.4.2	Begriffserklärung.....	89
3.4.3	Ursachen der algorithmischen Diskriminierung.....	91
a)	Diskriminierungen während des gesamten Daten-Lebenszyklus.....	91
b)	Diskriminierungen in der Eingabephase	92
c)	Diskriminierendes Modell	94
d)	Diskriminierungen in der Ausgabephase	99
3.5	Verletzung von Mitwirkungsrechten	99
3.5.1	Zweck und zwingende Geltung der Mitwirkungsrechte	99
3.5.2	Informationsrecht.....	101
3.5.3	Mitspracherecht	103
3.5.4	Fehlendes Mitentscheidungsrecht	105
3.6	Zwischenfazit: Rechtsprobleme vom Kontext abhängig	106
4	Relevante Rechtsbestimmungen	107
4.1	Übersicht	107
4.2	Arbeitsrechtlicher Persönlichkeitsschutz.....	107

4.3	Datenschutzrechtlicher Persönlichkeitsschutz	108
4.3.1	Schweizerisches Datenschutzrecht.....	108
4.3.2	Europäisches Datenschutzrecht.....	109
	a) Datenschutz-Grundverordnung der Europäischen Union	109
	b) Nationale Bestimmungen der Mitgliedstaaten der Europäischen Union betreffend Beschäftigtendaten	112
4.4	Öffentlich-rechtlicher Arbeitnehmer-Gesundheitsschutz	114
4.5	Diskriminierungsschutz.....	115
4.5.1	Beschränkter Geltungsbereich der Diskriminierungsverbote	115
4.5.2	Arbeitsrechtlicher Diskriminierungsschutz.....	121
4.5.3	Datenschutzinstrumente gegen Diskriminierungen.....	122
4.5.4	Zwischenfazit zum Geltungsbereich des Diskriminierungsschutzrechts....	126
4.6	Mitwirkungsrecht	126
4.7	Strafrecht	127
4.8	Europäische Menschenrechtskonvention und Verfassungsrecht	128
4.9	Weiteres Völkerrecht.....	129
4.10	Zwischenfazit: Querschnittsmaterie People Analytics	131
5	Datenschutzrechtliche Rahmenbedingungen	133
5.1	Übersicht	133
5.2	Aufbau des Datenschutzgesetzes.....	133
5.3	Zweck des Datenschutzgesetzes	135
5.3.1	Zwei Aspekte des Zweckartikels des Datenschutzgesetzes	135
	a) Schutz vor Persönlichkeitsrisiken.....	135
	b) Regelung der Datenbearbeitungsprozesse	136
5.3.2	Risikoorientierte Auslegung der prozessorientierten Regeln	140
	a) Allgemeines	140
	b) Parameter für die risikoorientierte Auslegung	141
	aa) Unterscheidung von Wissensgewinnung und -anwendung.....	141
	bb) Intensität der Wissens- und Machtasymmetrie.....	145
	cc) Datenherkunft, Nutzung von Interoperabilität	145
	dd) Umfang der Datenbearbeitung	147
	ee) Gezielter Personenbezug.....	148

5.3.3	Risikoorientierung am praktischen Beispiel der Verhaltensüberwachung.....	149
a)	Verordnung und frühere Rechtsprechung.....	149
b)	Aktuelle Rechtsprechung.....	150
5.3.4	Zwischenfazit zum Zweck des Datenschutzgesetzes	154
5.4	Geltungsbereich des Datenschutzgesetzes.....	154
5.4.1	Überblick	154
5.4.2	Unterscheidung zwischen Personendaten und Sachdaten	155
5.4.3	Re-identifizierbare Daten.....	157
5.4.4	Typisierungen	160
a)	Zum Begriff der Typisierung.....	160
b)	Argumentation gegen den Datenschutz bei Typisierungen.....	161
c)	Argumentation für den Datenschutz bei Typisierungen	162
aa)	Hinterfragung der Rechtsprechung und Lehre	162
bb)	Begriff der Identität.....	163
cc)	Generelle rechtliche Erfassung von Typisierungen	165
dd)	Einzelfallweise rechtliche Erfassung von Typisierungen in Abhängigkeit von ihrem Risikopotenzial.....	167
i.	Übersicht	167
ii.	Verschwimmende Grenzen zwischen den Daten- kategorien.....	167
iii.	Typisierungen mit hohem Persönlichkeitsschutz- rechtlichem Risiko.....	170
5.4.5	Zwischenfazit: risikoorientierte Auslegung des Geltungsbereichs des Datenschutzgesetzes	173
5.5	Zweckbindungsgebot	173
5.5.1	Doppelte Zweckbindung bei People Analytics	173
5.5.2	Datenschutzrechtliche Zweckbindung	174
a)	Normzweck und Gesetzessystematik.....	174
b)	Anforderungen an die Zweckfestsetzung.....	175
c)	Konflikt zwischen People Analytics und Zweckbindung	176
d)	Vereinbare Zwecke.....	177
e)	Veränderte Zwecke.....	180
5.5.3	Arbeitsrechtliche Zweckbeschränkung	181
a)	Übersicht	181
b)	Normzweck und Gesetzessystematik.....	181
c)	Geltungsbereich	182

d) Norminhalt.....	183
e) Variante 1: Eignungsabklärung	184
aa) Objektivität der Eignungsabklärung.....	184
bb) Persönlichkeitsdurchleuchtung	187
f) Variante 2: Erforderliche Daten zur Durchführung des Arbeitsvertrags	191
g) Einwilligung zu Abweichungen von Artikel 328b Satz 1 Obligationenrecht	193
h) Frageverbot.....	197
5.6 Erkennbarkeitsgebot.....	199
5.6.1 Normzweck und Norminhalt.....	199
5.6.2 Ungenügende Umsetzung der Erkennbarkeit.....	201
5.6.3 Restriktive Auslegung der Erkennbarkeit	202
5.7 Richtigkeitsgebot.....	206
5.8 Datenminimierung und Speicherbegrenzung.....	206
5.9 Löschpflicht.....	209
5.9.1 Norminhalt.....	209
5.9.2 Umsetzung der Löschung	211
5.10 Rechtfertigungsmöglichkeiten.....	212
5.10.1 Übersicht zu den relevanten Bestimmungen	212
5.10.2 Rechtfertigungsmöglichkeit für Grundsatzverstöße.....	213
5.10.3 Bearbeitbarkeit allgemein zugänglich gemachter Daten	214
a) Tatbestandsmerkmale und Rechtsfolge	214
b) Zugänglichkeit von Internetdaten	216
5.10.4 Einwilligung im Arbeitskontext.....	219
a) Rückblick auf die arbeitsrechtlichen Bedingungen der Einwilligung..	219
b) Datenschutzrechtliche Voraussetzungen der Einwilligung.....	220
aa) Übersicht.....	220
bb) Freiwilligkeit.....	221
cc) Informiertheit	225
dd) Ausdrücklichkeit	229
c) Jederzeitiges Widerrufsrecht.....	230
d) Zwischenfazit zur Einwilligung.....	231

5.10.5	Überwiegendes Interesse	234
a)	Gesetzessystematik	234
b)	Privates Interesse	234
c)	Öffentliches Interesse	235
d)	Forschung, Planung und Statistik	237
e)	Arbeitnehmerinteressen	239
f)	Fehlende Methode zur Interessenabwägung	239
5.10.6	Gesetzliche Rechtfertigung	240
5.11	Umsetzung der Datenschutznormen in der Praxis	242
5.11.1	NFP75-Daten zur Umsetzung	242
5.11.2	Öffentlich bekannt gewordene Datenskandale	246
5.12	Zwischenfazit: hoher Fachwissensbedarf bei gleichzeitigen Mängeln in der Datenschutzpraxis	247
6	Rechtsdurchsetzung	251
6.1	Übersicht: Individualrechtsschutz und weitere Rechtsbehelfe	251
6.2	Zivilrechtliche Individualklagen	253
6.2.1	Zivilrechtliche Ansprüche der Arbeitnehmer	253
6.2.2	Persönlichkeitsschutz als Abwehrrecht (<i>privacy-as-secrecy</i>)	254
a)	Abwehrrecht im Zivilgesetzbuch	254
b)	Geheimsphäreschutz im Common Law	255
c)	Sphärentheorie in der bundesgerichtlichen Rechtsprechung	256
d)	Ungenügen der Sphärentheorie	256
6.2.3	Persönlichkeitsschutz durch informationelle Selbstbestimmung (<i>privacy-as-control</i>)	258
a)	Deutsches Konzept der informationellen Selbstbestimmung	258
b)	Schweizerische Rezeption der informationellen Selbstbestimmung	260
c)	Zwei Stossrichtungen der Kritik am Recht auf informationelle Selbstbestimmung	263
aa)	Übersicht	263
bb)	Informationsverbot infolge ausufernder Kontrollrechte	263
cc)	Überforderung durch informationelle Selbstbestimmung	267
i.	Last der informationellen Selbstbestimmung	267
ii.	Materiell-rechtliche Beweisschwierigkeiten von Persönlichkeitsschutzklagen	268

iii.	Verfahrensrechtliche Hürden von Persönlichkeits-	
	schutzklagen	271
iv.	Diskriminierungsklagen	273
6.2.4	Zwischenfazit zu den Individualklagen.....	274
6.3	Datenschutzrechtliche Aufsicht	275
6.3.1	Abklärungen und Empfehlungen des Eidgenössischen Datenschutz-	
	und Öffentlichkeitsbeauftragten	275
6.3.2	Aufsichtskompetenzen nach der Datenschutz-Grundverordnung	278
6.4	Arbeitsgesetzliche Aufsicht.....	279
6.5	Strafverfolgung	281
6.6	Mitwirkungsrechtliche Behelfe	282
6.6.1	Grosses Potenzial für die Durchsetzung des Datenschutzrechts	282
6.6.2	Öffentlich-rechtliches Anzeigeverfahren	284
6.6.3	Privatrechtliche Klage.....	285
a)	Zuständigkeit und Verfahren	285
b)	Aktivlegitimation.....	285
c)	Rechtsbegehren.....	287
6.6.4	NFP75-Daten zur Mitwirkung	288
6.7	Gesellschaftsrechtliche Haftung der exekutiven Organe	288
6.8	Arbeitsverweigerung, Streik und Kündigung	290
6.9	Zwischenfazit: mühevolle Rechtsdurchsetzung.....	291
7	Neuausrichtung des Datenschutzrechts	295
7.1	Rekapitulation der gegenwärtigen Probleme	295
7.2	Neuausrichtung auf das Teilen von Information und die Stärkung	
	des Vertrauens in das Datenschutzrecht	296
7.2.1	Überblick	296
7.2.2	Förderung des Teilens von Information	296
a)	Bedeutung des Teilens für die Informationsgesellschaft	296
b)	Schranken des Teilens	298
aa)	Richtiges Mass an Teilen	298
bb)	Untermass an Teilen	298
cc)	Übermass an Teilen.....	299
c)	Regulierungsgefäss für die am Teilen ausgerichtete Neuordnung	300

7.2.3	Stärkung des Vertrauens in das Datenschutzrecht.....	301
a)	Datenschutz mit Vertrauenskomponente (<i>privacy-as-trust</i>)	301
b)	Begriff des Vertrauens.....	304
c)	Hohes bestehendes Vertrauen.....	306
d)	NFP75-Daten zum Vertrauen	308
7.2.4	Kritik zur Ausrichtung auf das Teilen und zum Datenschutz mit Vertrauenskomponente	313
7.3	Professionalisierung und Demokratisierung als Mittel zur Umsetzung des neu ausgerichteten Datenschutzrechts	315
7.3.1	Vorbemerkungen	315
a)	Herleitung der Begriffe «Professionalisierung» und «Demokratisierung»	315
b)	Regulierungsumfang, Bewahrung der Flexibilität im System	317
c)	Gesundheitssystem als Inspirationsquelle.....	318
7.3.2	Professionalisierungsvorschläge	319
a)	Professionalisierungstendenzen im Entwurf zum revidierten Datenschutzgesetz.....	319
aa)	Vorbemerkungen zum Datenschutz durch Technik und zur Datenschutz-Folgenabschätzung.....	319
bb)	Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen	321
i.	Rechtsgrundlage	321
ii.	Entstehungsgeschichte.....	322
iii.	Normzweck und Norminhalt	323
iv.	Norminhalt und Umsetzungsmassnahmen.....	324
v.	Grenzen des Datenschutzes durch Technik	326
cc)	Datenschutz-Folgenabschätzung.....	327
i.	Rechtsgrundlage und Normzweck.....	327
ii.	Voraussetzungen	328
iii.	Umsetzung.....	329
iv.	Konsultationen des EDÖB und der Arbeitnehmer.....	331
v.	Fehlende Publizität des Berichts zur Datenschutz- Folgenabschätzung	332
dd)	Datenschutzberater.....	333
ee)	Förderung der regulierten Selbstregulierung.....	335
ff)	Verzeichnis-, Informations- und Meldepflicht.....	338
b)	Weitere Professionalisierungsvorschläge	339
aa)	Rechenschaftspflicht.....	339
bb)	Lösungen gegen algorithmische Diskriminierungen.....	342
cc)	Schulungen	343

7.3.3	Demokratisierungsvorschläge	344
a)	Befähigung der einzelnen Arbeitnehmer	344
aa)	Technologische «Werkzeuge»	344
bb)	Rechtliche Verbesserungen für Individuen	345
b)	Stärkung der Arbeitnehmervertretungen und -verbände	346
aa)	Stärkung der Mitwirkung	346
bb)	Finanzielle Mitarbeiterbeteiligung	347
c)	Stärkung des Staats	348
aa)	Stärkung der Datenschutzaufsicht	348
bb)	Stärkung der Strafbehörden	350
cc)	Staat als Diskursmoderator	351
d)	Einbezug der Zivilgesellschaft	353
aa)	Ideelle Verbandsklage	353
i.	Übersicht	353
ii.	Datenschutzrechtliche Verbandsklage	353
iii.	Zivilprozessrechtliche Verbandsklage	359
bb)	Begutachtung von Algorithmen	361
cc)	Bildung	364
7.4	Zwischenfazit: effektiverer Datenschutz basierend auf Professionalisierung und Demokratisierung	364
8	Ergebnisse	369

Abkürzungsverzeichnis

A.	Auflage
ABA	American Bar Association [Vereinigung von Rechtsanwälten, Richtern und Studenten der Rechtswissenschaften in den USA]
Abb.	Abbildung(en)
AB NR	Amtliches Bulletin Nationalrat
Abs.	Absatz
AB SR	Amtliches Bulletin Ständerat
AEUV	Vertrag über die Arbeitsweise der EU (Amtsblatt der EU Nr. C326 vom 26.10.2012, 47–390)
AGB	Allgemeine Geschäftsbedingungen
AGG	Allgemeines Gleichbehandlungsgesetz der Bundesrepublik Deutschland vom 14.08.2006 (BGBl. I 1897), zuletzt geändert durch Art. 8 des Gesetzes vom 03.04.2013 (BGBl. I 610)
AI	artificial intelligence [= KI]
AIG	Bundesgesetz über die Ausländerinnen und Ausländer und über die Integration (Ausländer- und Integrationsgesetz) vom 16.12.2005 (SR 142.20)
altgr.	altgriechisch
a.M.	andere(r) Meinung
ArG	Bundesgesetz über die Arbeit in Industrie, Gewerbe und Handel (Arbeitsgesetz) vom 13.03.1964 (SR 822.11)
ArGV 3	Verordnung 3 zum Arbeitsgesetz (Gesundheitsschutz) vom 18.08.1993 (SR 822.113)
Art.	Artikel
AT	Allgemeiner Teil
AVG	Bundesgesetz über die Arbeitsvermittlung und den Personalverleih (Arbeitsvermittlungsgesetz) vom 06.10.1989 (SR 823.11)
AVV	Verordnung über die Arbeitsvermittlung und den Personalverleih (Arbeitsvermittlungsverordnung) vom 16.01.1991 (SR 823.111)
BBl	Bundesblatt

BDSG	Bundesdatenschutzgesetz der Bundesrepublik Deutschland vom 30.06.2017 (BGBl. I 2097), geändert durch Art. 12 des Gesetzes vom 20.11.2019 (BGBl. I 1626)
BeckOK	Beck'scher Online-Kommentar
BehiG	Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen (Behindertengleichstellungsgesetz) vom 13.12.2002 (SR 151.3)
BGBI.	Bundesgesetzblatt [Deutschland]
BGE	Bundesgerichtsentscheid
BGer	Schweizerisches Bundesgericht
BGSA	Bundesgesetz über Massnahmen zur Bekämpfung der Schwarzarbeit (Bundesgesetz gegen die Schwarzarbeit) vom 17.06.2005 (SR 822.41)
BK	Berner Kommentar
BMAS	Bundesministerium für Arbeit und Soziales [Deutschland]
BSK	Basler Kommentar
BT	Besonderer Teil
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18.04.1999 (SR 101)
BVGE	Bundesverwaltungsgerichtsentscheid
BVGer	Bundesverwaltungsgericht
bzgl.	bezüglich
bzw.	beziehungsweise
CCPA	California Consumer Privacy Act: Civil Code. Division 3, Obligations (1427–3273). Part 4, Obligations arising from particular transactions (1738–3273.16). Title 1.81.5. California Consumer Privacy Act of 2018 (1798.100–1798.199) (Assembly Bill no. 375, 2017–2018 session)
CEEP	European Centre of Enterprises with Public Participation and of Enterprises of General Economic Interest
CEO	Chief executive officer (Geschäftsführer)
CHF	Schweizer Franken
CHK	Handkommentar zum Schweizer Privatrecht
CMS	CMS Legal Services [Wirtschaftskanzlei, benannt nach zwei der Gründungskanzleien, Cameron McKenna und Hasche Sigle]
CO ₂	Kohlenstoffdioxid
COD	co-decision procedure [ordentliches Gesetzgebungsverfahren der EU]

COM	Commission working document [Arbeitspapier der Europäischen Kommission]
COMPAS	correctional offender management profiling for alternative sanctions [Name eines Algorithmus]
D.C.	District of Columbia
d.h.	das heisst
Diss.	Dissertation
DNA	Desoxyribonukleinsäure
DPIA	data protection impact assessment (Datenschutz-Folgenabschätzung)
DS	Datenschutz(-recht)
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1)
DSG SG	Datenschutzgesetz des Kantons St. Gallen vom 20.01.2009 (sGS 142.1)
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, Amtsblatt der EU Nr. L 119 vom 04.05.2016, 1–88) [= GDPR]
DSGVO-BDSG-K	Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar
DSRI	Deutsche Stiftung für Recht und Informatik
DSRL	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Amtsblatt der EG Nr. L 281 vom 23.11.1995, 1–50)
E.	Erwägung, Erwägungsgrund
EC	European Community [= EG]
ECLI	European Case Law Identifier
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDPB	European Data Protection Board [= EDSA]
EDPS	European Data Protection Supervisor [= EDSB]
EDSA	Europäischer Datenschutzausschuss [= EDPB]
EDSB	Europäischer Datenschutzbeauftragter [= EDPS]

E-DSG	Entwurf zum Bundesgesetz über die Totalrevision des DSG und die Änderung weiterer Erlasse zum Datenschutz (BB1 2017 7193–7276). Die in der Dissertation erwähnten Artikel beziehen sich auf diesen Entwurf zum DSG (BB1 2017 7206–7234).
EEOC	Equal Opportunity Employment Commission (Kommission für Chancengleichheit im Arbeitsleben [USA])
EG	Europäische Gemeinschaft [= EC]
EGMR	Europäischer Gerichtshof für Menschenrechte
E-GUMG	Bundesgesetz über genetische Untersuchungen beim Menschen vom 15.06.2018 [Inkrafttreten voraussichtlich im Sommer 2021]
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten (Europäische Menschenrechtskonvention), abgeschlossen in Rom am 04.11.1950, von der Bundesversammlung genehmigt am 03.10.1974, schweizerische Ratifikationsurkunde hinterlegt am 28.11.1974 (SR 0.101)
ENISA	Agentur der EU für Cybersicherheit (bis zum 28.06.2019: Europäische Agentur für Netz- und Informationssicherheit; European Network and Information Security Agency)
EntsG	Bundesgesetz über die flankierenden Massnahmen bei entsandten Arbeitnehmerinnen und Arbeitnehmern und über die Kontrolle der in Normalarbeitsverträgen vorgesehenen Mindestlöhne (Entsendegesetz) vom 08.10.1999 (SR 823.20)
ErfK	Erfurter Kommentar
et al.	et alii, et aliae (und andere)
ETUC	European Trade Union Confederation
EU	Europäische Union, European Union
EuGH	Europäischer Gerichtshof
EUR	Euro
EWK	Europäischer Wirtschaftsraum
f. (ff.)	folgende(r) Artikel
FAZ	Frankfurter Allgemeine Zeitung
FedEx	Federal Express Corporation (Unternehmen)
FES	Flight Efficiency Services
FIPP	Fair Information Practice Principles: Code of Fair Information Practices, U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Auto-

	mated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973)
FMG	Fernmeldegesetz vom 30.04.1997 (SR 784.10)
FMH	Foederatio Medicorum Helveticorum, Verbindung der Schweizer Ärztinnen und Ärzte (Berufsverband mit Sitz in Bern)
FN	Fussnote
FTC	Federal Trade Commission [USA]
FZA	Abkommen zwischen der Schweizerischen Eidgenossenschaft einerseits und der Europäischen Gemeinschaft und ihren Mitgliedstaaten andererseits über die Freizügigkeit (Freizügigkeitsabkommen), abgeschlossen am 21.06.1999, von der Bundesversammlung genehmigt am 08.10.1999, schweizerische Ratifikationsurkunde hinterlegt am 16.10.2000 (SR 0.142.112.681)
GAV	Gesamtarbeitsvertrag
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, Official Journal of the EU no. L 119 of 04.05.2016, 1–88) [= DSGVO]
GesG SG	Gesundheitsgesetz des Kantons St. Gallen vom 28.06.1979 (sGS 311.1)
GG	Grundgesetz für die Bundesrepublik Deutschland in der im BGBl. Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 1 des Gesetzes vom 15.11.2019 (BGBl. I 1546)
GlG	Bundesgesetz über die Gleichstellung von Frau und Mann (Gleichstellungsgesetz) vom 24.03.1995 (SR 151.1)
GPS	Global Positioning System (Globales Positionsbestimmungssystem)
GrCh	Charta der Grundrechte der EU (Amtsblatt der EU Nr. C 326 vom 26.10.2012, 391–407)
GUMG	Bundesgesetz über genetische Untersuchungen beim Menschen vom 08.10.2004 (SR 810.12)
Habil.	Habilitation
HArG	Bundesgesetz über die Heimarbeit (Heimarbeitsgesetz) vom 20.03.1981 (SR 822.31)
HAVE	Haftung und Versicherung [Verein]

Hg.	Herausgeber(in)
HIV	Humanes Immundefizienzvirus
HK	Handkommentar
h.M.	herrschende Meinung
HP	Hewlett-Packard Company [Unternehmen]
HR	human resources (Humankapital, Personal)
IAB	Institut für Arbeitsmarkt- und Berufsforschung
IAO	Internationale Arbeitsorganisation [= ILO]
IBM	International Business Machines Corporation [Unternehmen]
ICDPPC	International Conference of Data Protection & Privacy Commissioners
IDG BS	Gesetz über die Information und den Datenschutz (Informations- und Datenschutzgesetz) des Kantons Basel- Stadt vom 09.06.2010, SG 153.260
IDG ZH	Gesetz über die Information und den Datenschutz des Kantons Zürich vom 12.02.2007, Ordnungsnummer 170.4
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IJCAI	International Joint Conferences on Artificial Intelligence
ILO	International Labour Organisation [= IAO]
Inc.	incorporated legal entity (eingetragene juristische Person)
IoT	internet of things (Internet der Dinge)
IP	Internetprotokoll
IPBPR	Internationaler Pakt über bürgerliche und politische Rechte, abgeschlossen in New York am 16.12.1966, von der Bun- desversammlung genehmigt am 13.12.1991, schweizerische Beitrittsurkunde hinterlegt am 18.06.1992 (SR 0.103.2)
ISO	International Standards Organisation, Organisation Inter- nationale de Normalisation
IT	Informationstechnik
ITSL	Center for Information Technology, Society, and Law an der Universität Zürich
i.V.m.	in Verbindung mit
Jh.	Jahrhundert
Jr.	Junior (der Jüngere)
K	Kommentar

KG	Bundesgesetz über Kartelle und andere Wettbewerbsbeschränkungen (Kartellgesetz) vom 06.10.1995 (SR 251)
KI	Künstliche Intelligenz [= AI]
KK	Kompaktkommentar
KPMG	Klynveld Peat Marwick Goerdeler International Cooperative [Unternehmen]
KR SIX	Kotierungsreglement der Börse SIX Swiss Exchange vom 08.11.2019
KUKO	Kurzkommentar
lat.	lateinisch
lit.	litera (Buchstabe)
LL.M.	Legum Magister [«Lehrer der Rechte», juristischer Postgraduierten-Abschluss]
Madrider Übereinkommen	International Standards on the Protection of Personal Data and Privacy, The Madrid Resolution, International Conference of Data Protection and Privacy Commissioners, 05.11.2009
MedBG	Bundesgesetz über die universitären Medizinalberufe (Medizinalberufegesetz) vom 23. Juni 2006 (SR 811.11)
Mio.	Million(en)
MIT	Massachusetts Institute of Technology
MitwG	Bundesgesetz über die Information und Mitsprache der Arbeitnehmerinnen und Arbeitnehmer in den Betrieben (Mitwirkungsgesetz) vom 17.12.1993 (SR 822.14)
ML	machine learning (maschinelles Lernen)
m.w.H.	mit weiterem Hinweis/mit weiteren Hinweisen
N	Note, Randnote, Randziffer
NFP75	75. Nationales Forschungsprogramm des Schweizerischen Nationalfonds zum Thema Big Data. Zum NFP75-Projekt siehe Vorwort und S. 14–16.
NLE	non-legislative enactment (nicht rechtsetzender Akt)
no./n°/N° (nos.)	number(s), numero (numeris)
Nr.	Nummer
NZZ	Neue Zürcher Zeitung
OECD	Organisation for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)

OECD-Leitlinien 1980	OECD guidelines on the protection of privacy and trans-border flows of personal data, verabschiedet am 23.09.1980, C(80)58/FINAL
OECD-Leitlinien 2013	OECD revision of the recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data [C(80)58/FINAL], vom 20.06.2013, verabschiedet am 11.07.2013, C(2013)79
OFK	Orell-Füssli-Kommentar
OGer ZH	Obergericht des Kantons Zürich
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30.03.1911 (SR 220)
ORION	On-Road Integrated Optimization and Navigation
PC	personal computer (persönlicher Rechner)
PET	privacy-enhancing technologies (Technologien zum Privatsphäreschutz)
PETRA	pervasive technologies related to assistive environments (allgegenwärtige Technologien im Zusammenhang mit unterstützenden Umgebungen)
PIA	privacy impact assessment (Persönlichkeitsschutz-Folgenabschätzung)
PII	personally identifiable information (personenbezogene Informationen)
PK	Praxiskommentar
PLoS ONE	Public Library of Science One [Zeitschrift]
POG	Bundesgesetz über die Organisation der Schweizerischen Post (Postorganisationsgesetz) vom 17.12.2010 (SR 783.1)
rev./rev-	revised (revidiert)
rev-DSG	Bundesgesetz über den Datenschutz vom 25.09.2020 (Datenschutzgesetz) (17.059-3) – XXI – 2017-1085. Die in der Dissertation erwähnten Artikel beziehen sich auf die Vorlage der Redaktionskommission für die Schlussabstimmung im Parlament. Der Text wird voraussichtlich im Jahr 2022 in Kraft treten.
RFID	radio-frequency identification (Identifizierung mithilfe elektromagnetischer Wellen)
Richtlinie 2000/78/EG	Richtlinie 2000/78/EG des Rates vom 27.11.2000 zur Festlegung eines allgemeinen Rahmens für die Verwirklichung der Gleichbehandlung in Beschäftigung und Beruf, Amtsblatt Nr. L 303 vom 02.12.2000 0016–0022

Richtlinie 2002/58/EG	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), Amtsblatt Nr. L 201 vom 31.07.2002 0037–0047
S.	Seite(n)
SAGE	SAGE Publishing [Wissenschaftsverlag. Die Abkürzung kommt von den jeweils ersten beiden Buchstaben von «Sara» und «George», den Vornamen der Verlagsgründer: Sara Miller McCune und George D. McCune.]
SAP	Systeme, Anwendungen und Produkte in der Datenverarbeitung (Unternehmen)
SAS	Statistical Analysis Systems Institute (Unternehmen)
SBB	Schweizerische Bundesbahnen (Unternehmen)
SchKG	Bundesgesetz über Schuldbetreibung und Konkurs vom 11.04.1889 (SR 281.1)
SchlT	Schlusstitel
SDRCA	Société suisse du droit de la responsabilité civile et des assurances
SECO	Staatssekretariat für Wirtschaft
SEV	Sammlung der Europäischen Verträge des Europarats
SF-FS	Schweizer Forum für Kommunikationsrecht
SG	Systematische Gesetzessammlung des Kantons Basel-Stadt
SGB	Schweizerischer Gewerkschaftsbund
SGHVR	Schweizerische Gesellschaft für Haftpflicht- und Versicherungsrecht
SGK	St. Galler Kommentar
sGS	systematische Gesetzessammlung des Kantons St. Gallen
SHK	Stämpflis Handkommentar
sic	Lat.: Sic erat scriptum. (So stand es geschrieben.)
SO FMH	Standesordnung der FMH vom 12.12.1996
sog.	sogenannt
SR	Systematische Sammlung des Bundesrechts
StGB	Schweizerisches Strafgesetzbuch vom 21.12.1937 (SR 311.0)
StPO	Schweizerische Strafprozessordnung vom 05.10.2007 (SR 312.0)
SWR 2	Kulturprogramm des Südwestrundfunks

TET	transparency-enhancing technologies (Technologien zur Transparenzförderung)
u.a.	unter anderem
Übereinkommen 108	Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, abgeschlossen in Strassburg am 28.01.1981, von der Bundesversammlung genehmigt am 05.06.1997, schweizerische Ratifikationsurkunde hinterlegt am 02.10.1997 (SR 0.235.1) = SEV Nr. 108
Übereinkommen 111	Übereinkommen Nr. 111 über die Diskriminierung in Beschäftigung und Beruf, angenommen in Genf am 25.06.1958, von der Bundesversammlung genehmigt am 15.06.1961, schweizerische Ratifikationsurkunde hinterlegt am 13.07.1961 (SR 0.822.721.1)
UEA PME	European Association of Craft Small and Medium-Sized Enterprises
UNICE	Union of Industrial and Employers' Confederations of Europe
UNICEF	United Nations Children's Fund
UNO	United Nations Organisation (Organisation der Vereinten Nationen)
URG	Bundesgesetz über das Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz) vom 09.10.1992 (SR 231.1)
US (USA)	United States (of America) (Vereinigte Staaten (von Amerika))
UWG	Bundesgesetz gegen den unlauteren Wettbewerb vom 19.12.1986 (SR 241)
v.Chr.	vor Christus
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14.06.1993 (SR 235.11)
VGG	Bundesgesetz über das Bundesverwaltungsgericht (Verwaltungsgerichtsgesetz) vom 17.06.2005 (SR 173.32)
vgl.	vergleiche
Vicas	Virtual Career Assistant
vs.	versus
VW	Volkswagen
VwVG	Bundesgesetz über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz) vom 20.12.1968 (SR 172.021)

WP	Article 29 Data Protection Working Party (Art.-29-Datenschutzgruppe)
WSI	Wirtschafts- und Sozialwissenschaftliches Institut
WTO	World Trade Organization (Welthandelsorganisation)
WTO-Übereinkommen zum Beschaffungswesen	Übereinkommen über das öffentliche Beschaffungswesen, abgeschlossen in Marrakesch am 15.04.1994, von der Bundesversammlung genehmigt am 08.12.1994, schweize- rische Ratifikationsurkunde hinterlegt am 19.12.1995 (SR 0.632.231.422)
WWW	World Wide Web (weltweites Netz)
XAI	explainable AI (erklärbare KI)
z.B.	zum Beispiel
ZGB	Schweizerisches Zivilgesetzbuch vom 10.12.1907 (SR 210)
Ziff.	Ziffer
zit.	zitiert
ZPO	Schweizerische Zivilprozessordnung vom 19.12.2008 (SR 272)

Literaturverzeichnis

- Accenture, The future of HR: a radically different proposition, 2015, abrufbar unter <www.accenture.com> (besucht am 31.05.2020)
- AEBI-MÜLLER REGINA E., Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Bern 2005, Habil. Bern 2005
- AI now institute, Algorithmic accountability policy toolkit, 10.2018, abrufbar unter <<https://ainowinstitute.org>> (besucht am 31.05.2020)
- AJUNWA IFEOMA 2014, Genetic testing meets big data: tort and contract law issues, Ohio State Law Journal, 2014, 1225–1262
- AJUNWA IFEOMA 2017, Workplace wellness programs could be putting your health data at risk, Harvard Business Review, 19.01.2017, abrufbar unter <<https://hbr.org>> (besucht am 31.05.2020)
- AJUNWA IFEOMA / CRAWFORD KATE / FORD JOEL S., Health and Big Data: An ethical framework for health information collection by corporate wellness programs, Journal of Law, Medicine and Ethics, 2016, 474–479
- AJUNWA IFEOMA / CRAWFORD KATE / SCHULTZ JASON, Limitless worker surveillance, California Law Review, 2017, 735–776
- AJUNWA IFEOMA / FRIEDLER SORELLE A. / SCHEIDEGGER CARLOS E. / VENKATASUBARAMANIAN SURESH, Hiring by algorithm: predicting and preventing disparate impact (draft), 01.04.2016, abrufbar unter <<http://sorelle.friedler.net>> (besucht am 31.05.2020)
- AJUNWA IFEOMA / ONWUACHI-WILLIG ANGELA, Combating discrimination against the formerly incarcerated in the labor market, Northwestern University Law Review, 2018, 1385–1415
- AKHTAR PAV / MOORE PHOEBE, The psychosocial impacts of technological change in contemporary workplaces, and trade union responses, International Journal of Labour Research, 2016, 101–131
- AL CHWARIZMI MUHAMMAD IBN MUSA, Algoritmi de numero Indorum, in: Boncompagni Baldassarre / Hispalensis Johannes (Hg.): Trattati d'arimetica, Rom 1857, 1–23
- ALBERS MARION, Informationelle Selbstbestimmung, Baden-Baden 2005, Habil. Berlin 2002
- algo:aware [sic], State-of-the-art report: algorithmic decision-making, 12.2018, abrufbar unter <www.algoaware.eu> (besucht am 31.05.2020)
- ALLENSPACH BIRGIT, Wearables am Arbeitsplatz, Jusletter, 26.11.2018
- ALTMAN MICAH / WOOD ALEXANDRA / VAYENA EFFY, A harm-reduction framework for algorithmic fairness, IEEE Security & Privacy 3, 2018, 34–45
- ANANNY MIKE / CRAWFORD KATE, Seeing without knowing: limitations of the transparency ideal and its application to algorithmic accountability, New Media & Society, 2018, 973–989

- ANGRAVE DAVID / CHARLWOOD ANDY / KIRKPATRICK IAN / LAWRENCE MARK / STUART MARK, HR and analytics: why HR is set to fail the big data challenge, *Human Resource Management Journal*, 2016, 1–11
- Αρχή Προστασίας Δεδομένων, «Arché Prostasías Dedoménon» [Datenschutz-Aufsichtsbehörde von Griechenland], [Direktauskunft betreffend Urteil 26/2019] (vom 28.05.2020)
- ARNOLD CHRISTIAN / WINZER THOMAS, Flexibilisierung im individuellen Arbeitsrecht, in: Arnold Christian / Günther Jens (Hg.): *Arbeitsrecht 4.0, Praxishandbuch zum Arbeits-, IP- und Datenschutzrecht in einer digitalisierten Arbeitswelt*, München 2018, 77–157
- Art.-29-Datenschutzgruppe 2001, Opinion 8/2001 on the processing of personal data in the employment context, Brüssel 13.09.2001
- Art.-29-Datenschutzgruppe 2007, Stellungnahme 4/2007 zum Begriff «personenbezogene Daten», Brüssel 20.06.2007
- Art.-29-Datenschutzgruppe 2013, Opinion 03/2013 on purpose limitation, Brüssel 02.04.2013
- Art.-29-Datenschutzgruppe 2014, Opinion 05/2014 on anonymisation techniques (0829/14/EN WP216), Brüssel 10.04.2014
- Art.-29-Datenschutzgruppe 2017a, Guidelines on data protection impact assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of regulation 2016/679, WP 248 rev.01, Brüssel 04.04.2017
- Art.-29-Datenschutzgruppe 2017b, Opinion 2/2017 on data processing at work, Brüssel 08.06.2017
- Art.-29-Datenschutzgruppe 2017c, Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679, as last revised and adopted on 6 February 2018, WP251rev.01, Brüssel 03.10.2017
- Art.-29-Datenschutzgruppe 2017d, Guidelines on consent under Regulation 2016/679, WP259 rev.01, as last revised and adopted on 10.04.2018, Brüssel 28.11.2017
- ARYANI HEDYA, The legal implications of biodata use as an employment selection practice, *University of Pennsylvania Journal of Business Law*, 2009, 1051–1073
- AUBERT CAROLE / DELLEY RÉGINE, Utilisations des réseaux sociaux par les travailleurs et les employeurs, in: Dunand Jean-Philippe / Mahon Pascal (Hg.): *Internet au travail*, Genf 2014, 131–163
- BACHER BETTINA / DUBOIS CAMILLE, Zum Stand der Revision des Datenschutzgesetzes, Révision de la LPD: état de la situation, in: Epiney Astrid / Nüesch Daniela (Hg.): *Die Revision des Datenschutzes in Europa und die Schweiz, La révision de la protection des données en Europe et la Suisse*, Zürich/Basel/Genf 2016, 129–148
- BACON FRANCIS, *Meditationes sacrae*, London 1597
- BAERISWYL BRUNO 2010, Geschichten aus dem Wilden Westen, *digma – Zeitschrift für Datenrecht und Informationssicherheit*, 2010, 140–145
- BAERISWYL BRUNO 2013, Entwicklungen im Datenschutzrecht/Le point sur le droit de la protection des données, *Schweizerische Juristen-Zeitung*, 2013, 444–446

- BAERISWYL BRUNO 2014, Big Data zwischen Anonymisierung und Re-Individualisierung, in: Weber Rolf H. / Thouvenin Florent (Hg.): Big Data und Datenschutz – gegenseitige Herausforderungen, Zürich/Basel/Genf 2014, 45–59
- BALKIN JACK M., Information fiduciaries and the first amendment, University of California Davis Law Review, 2016, 1183–1234
- BALL KIRSTIE / MARGULIS STEPHEN T., Electronic monitoring and surveillance in call centres: a framework for investigation, New Technology, Work and Employment, 2011, 113–126
- BAMBERGER KENNETH A. / MULLIGAN DEIRDRE K. 2011, Privacy on the books and on the ground, Stanford Law Review, 2011, 247–315
- BAMBERGER KENNETH A. / MULLIGAN DEIRDRE K. 2015, Privacy on the ground, Cambridge (Massachusetts) 2015
- BAROCAS SOLON, EEOC at 50: progress and continuing challenges in eradicating employment discrimination, written testimony (Vortrag), Meetings and hearings of the EEOC, 01.07.2015, abrufbar unter <www.eeoc.gov> (besucht am 31.05.2020)
- BAROCAS SOLON / SELBST ANDREW D., Big data's disparate impact, California Law Review, 2016, 671–732
- BAUMANN MAX-OTTO, Privatsphäre als ethische und liberale Herausforderungen [sic] der digitalen Gesellschaft, Information, Wissenschaft & Praxis, 2016, 1–6
- BAUMANN ROBERT, Die Übertragung von Arbeitnehmerdaten bei Betriebsübergängen, Aktuelle Juristische Praxis, 2004, 638–648
- BeckOK DS: Wolff Heinrich Amadeus / Brink Stefan (Hg.), Beck'scher Online-Kommentar, Datenschutzrecht, 27. A., München 2019 (zit. BeckOK DS-BEARBEITER)
- BeckOK GG: Epping Volker / Hillgruber Christian (Hg.), Grundgesetz, 42. A., München 2019 (zit. BeckOK GG-BEARBEITER)
- BELSER EVA MARIA 2011a, Der grundrechtliche Rahmen des Datenschutzes, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard (Hg.): Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, 319–410
- BELSER EVA MARIA 2011b, Einführung, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard (Hg.): Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, 1–3
- BELSER EVA MARIA 2011c, Entwicklung des Datenschutzes, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard (Hg.): Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, 33–51
- BENECKE MARTINA, Kollektives Arbeitsrecht 4.0, in: Arnold Christian / Günther Jens (Hg.): Arbeitsrecht 4.0, Praxishandbuch zum Arbeits-, IP- und Datenschutzrecht in einer digitalisierten Arbeitswelt, München 2018, 257–287
- BERANEK ZANON NICOLE, Big Data und Datensicherheit, in: Weber Rolf H. / Thouvenin Florent (Hg.): Big Data und Datenschutz – gegenseitige Herausforderungen, Zürich/Basel/Genf 2014, 85–115

- BERGMAN MICHAEL K., White paper: the deep web: surfacing hidden value, The journal of electronic publishing, 2001, abrufbar unter <www.journalofelectronicpublishing.org> (besucht am 31.05.2020)
- BERNAL GUILLERMO / COLOMBO SARA / AL AI BAKY MOHAMMED / CASALEGNO FEDERICO, Safety++. [sic] Designing IoT and wearable systems for industrial safety through a user centered design approach, in: Proceedings of the 10th international conference on pervasive technologies related to assistive environments (PETRA '17), New York (New York) 06.2017, 163–170
- BERNSTEIN ETHAN S., The transparency paradox, Administrative Science Quarterly, 2012, 181–216
- BIANCHI DORIS, Mitwirkung in der Schweiz – wo drückt der Schuh?, in: Ehrenzeller Bernhard / Furer Hans / Geiser Thomas (Hg.): Die Mitwirkung in den Betrieben, St. Gallen 2009, 193–196
- BIAS SHERI K. / BOGUE KARIN L., Technology and employee privacy challenges, in: Sims Ronald R. / Sauser William I., Jr. (Hg.): Legal and regulatory issues in human resources management, Charlotte (North Carolina) 2015, 247–266
- BIEDENKOPF SEBASTIAN, Risiko- und Issues-Management als Aufgabe auch der Rechtsabteilung, in: Hambloch-Gesinn Sylvie / Hess Beat / Meier Andreas L. / Schiltknecht Reto / Wind Christian (Hg.): In-house Counsel in internationalen Unternehmen, Basel 2010, 145–154
- BIRAN OR / COTTON COURTENAY, Explanation and justification in machine learning: a survey, in: Aha David W. / Darrell Trevor / Pazzani Michael / Reid Darryn / Sammut Claude / Stone Peter (Hg.): IJCAI-17 workshop on explainable AI (XAI) proceedings, Melbourne (Australien) 20.08.2017, abrufbar unter <<https://ijcai-17.org>> (besucht am 31.05.2020), 8–13
- BISSELS ALEXANDER / MEYER-MICHAELIS ISABEL / SCHILLER JAN, Arbeiten 4.0: Big Data-Analysen im Personalbereich, Der Betrieb, 2016, 3042–3049
- BLANPAIN R., International encyclopaedia for labour law and industrial relations: European labour law, 14. A., Alphen aan den Rijn (Niederlande) 2013
- BMAS 2015, Grünbuch Arbeiten 4.0 – Arbeit weiter denken, Berlin 04.2015
- BMAS 2017, Weissbuch Arbeiten 4.0, Berlin 03.2017
- BMAS / nextpractice GmbH, Studie: «Wertewelten Arbeiten 4.0», Bremen 03.2016
- BÖCKLI PETER, Neue OR-Rechnungslegung, Zürich/Basel/Genf 2014
- BODDINGTON PAULA, Towards a code of ethics for artificial intelligence, Cham 2017
- BODIE MATTHEW T. / CHERRY MIRIAM A. / MCCORMICK MARCIA L. / JINTONG TANG, The law and policy of people analytics, University of Colorado Law Review, 2017, 961–1042
- BOEHME-NESSLER VOLKER, Die Macht der Algorithmen – Anmerkungen zum Einfluss von Big Data auf die Demokratie, in: Boehme-Nessler Volker / Rehbindner Manfred (Hg.): Big Data: Ende des Datenschutzes?, Gedächtnisschrift für Martin Usteri, Bern 2017, 111–138

- BOLLIGER CHRISTIAN / FÉRAUD MARIUS / EPINEY ASTRID / HÄNNI JULIA, Evaluation des Bundesgesetzes über den Datenschutz, Bern 10.03.2011
- BRAUN TORSTEN, Geschichte und Entwicklung des Internets, Informatik-Spektrum, 2010, 201–207
- BROWN LOUIS M., Preventive law, New York 1950
- BROY DOMINIC, Der Umgang mit Bewerberdaten aus Internetquellen, Saarbrücken 2017, Diss. Saarbrücken 2017
- BRYNJOLFFSSON ERIK / MCAFEE ANDREW, The second machine age, New York/London 2014
- BSK DSG: Maurer-Lambrou Urs / Blechta Gabor P. (Hg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. A., Basel 2014 (zit. BSK DSG-BEARBEITER)
- BSK OR I: Widmer Lüchinger Corinne / Oser David (Hg.), Basler Kommentar, Obligationenrecht I, Art. 1–529 OR, 7. A., Basel 2019 (zit. BSK OR I-BEARBEITER)
- BSK OR II: Honsell Heinrich / Vogt Nedim Peter / Watter Rolf (Hg.), Basler Kommentar, Obligationenrecht II, Art. 530–964 OR, 5. A., Basel 2016 (zit. BSK OR II-BEARBEITER)
- BSK StGB I: Niggli Marcel Alexander / Wiprächtiger Hans (Hg.), Basler Kommentar, Strafrecht I, Art. 1–110 StGB, Jugendstrafgesetz, 4. A., Basel 2018 (zit. BSK StGB I-BEARBEITER)
- BSK StGB II: Niggli Marcel Alexander / Wiprächtiger Hans (Hg.), Basler Kommentar, Strafrecht II, Art. 111–392 StGB, 4. A., Basel 2018 (zit. BSK StGB II-BEARBEITER)
- BSK UWG: Hilty Reto M. / Arpagaus Reto (Hg.), Basler Kommentar, Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Basel 2013 (zit. BSK UWG-BEARBEITER)
- BSK ZGB I: Geiser Thomas / Fountoulakis Christiana (Hg.), Basler Kommentar, Zivilgesetzbuch I, Art. 1–456 ZGB, 6. A., Basel 2018 (zit. BSK ZGB I-BEARBEITER)
- BSK ZGB II: Geiser Thomas / Wolf Stephan (Hg.), Basler Kommentar, Zivilgesetzbuch II, Art. 457–977 ZGB und Art. 1–61 SchlT ZGB, 5. A., Basel 2015 (zit. BSK ZGB II-BEARBEITER)
- BSK ZPO: Spühler Karl / Tenchio Luca / Infanger Dominik (Hg.), Basler Kommentar, Schweizerische Zivilprozessordnung, 3. A., Basel 2017 (zit. BSK ZPO-BEARBEITER)
- BUCHNER BENEDIKT / KÜHLING JÜRGEN, Die Einwilligung in der Datenschutzordnung 2018, Datenschutz und Datensicherheit, 2017, 544–548
- Bundesamt für Justiz 2006, Änderung von Art. 12 Abs. 2 Bst. a DSG: Auslegungshilfe, 10.10.2006, abrufbar unter <www.bj.admin.ch> (besucht am 31.05.2020)
- BURDON MARK / HARPUR PAUL, Re-conceptualising privacy and discrimination in an age of talent analytics, University of New South Wales Law Journal, 2014, 679–712
- BURRI MIRA / SCHÄR RAHEL, Die Reform der Datenschutzgesetzgebung der Europäischen Union: die wichtigsten Veränderungen und ihre Eignung für eine datengesteuerte Wirtschaft, Zeitschrift für Europarecht, 2016, 100–113
- BYERS PHILIPP, Mitarbeiterkontrollen, München 2016

- BYGRAVE LEE ANDREW, Data protection by design and by default: deciphering the EU's legislative requirements, *Oslo Law Review*, 2017, 105–120
- CALDAROLA MARIA CHRISTINA / SCHREY JOACHIM, *Big Data und Recht*, München 2019
- CALLAGHAN PAUL / WIGMAN DANIEL, Europe, in: Sprague Robert (Hg.): *Workplace data*, Arlington (Virginia) 2013, 16-1 – 16-98 [sic]
- CareerBuilder, One-in-four hiring managers have used internet search engines to screen job candidates; one-in-ten have used social networking sites, CareerBuilder.com survey finds, Chicago 26.10.2006
- CARUSO BRUNO, «The employment contract is dead! Hurrah for the work contract!» A European perspective, in: Stone Katherine V. W. / Arthurs Harry (Hg.): *Rethinking workplace regulation*, New York (New York) 2013, 95–111
- CASCIO WAYNE F. / MONTEALEGRE RAMIRO, How technology is changing work and organizations, *Annual Review of Organizational Psychology and Organizational Behavior*, 2016, 349–375
- CAVOUKIAN ANN 2010, Privacy by design, 05.2010, abrufbar unter <<https://iapp.org>> (besucht am 31.05.2020)
- CAVOUKIAN ANN 2011, Privacy by design in law, policy and practice. A white paper for regulators, decision-makers and policy-makers, Toronto 08.2011
- CAVOUKIAN ANN 2012, Privacy by Design, *IEEE Technology and Society Magazine* 4, 2012, 18–19
- CAVOUKIAN ANN 2013, Privacy by design and the promise of smartdata, in: Harvey Inman / Cavoukian Ann / Tomko George / Borrett Don / Kwan Hon / Hatzinakos Dimitrios (Hg.): *SmartData*, New York (New York) 2013, 1–9
- CAVOUKIAN ANN 2014, Data minding [sic]: a response to privacy pragmatism, *Foreign Affairs*, 2014, 175–176
- CAVOUKIAN ANN / DIX ALEXANDER / EL EMAM KHALED, The unintended consequences of privacy paternalism, Toronto 05.03.2014
- CAVOUKIAN ANN / TAYLOR SCOTT / ABRAMS MARTIN E., Privacy by design: essential for organizational accountability and strong business practices, *Identity in the Information Society*, 2010, 405–413
- CHARLET FRANÇOIS, Le Data Protection Officer dans le secteur privé suisse, *Jusletter*, 18.06.2018
- CHK OR AT: Furrer Andreas / Schnyder Anton K. (Hg.), *Handkommentar zum Schweizer Privatrecht, Obligationenrecht, allgemeine Bestimmungen*, Art. 1–183 OR, 3. A., Zürich 2016 (zit. CHK OR AT-BEARBEITER)
- CHK OR BT 2: Huguenin Claire / Müller-Chen Markus (Hg.), *Handkommentar zum Schweizer Privatrecht, Vertragsverhältnisse Teil 2: Arbeitsvertrag, Werkvertrag, Auftrag, GoA, Bürgschaft*, Art. 319–529 OR, 3. A., Zürich/Basel/Genf 2016 (zit. CHK OR BT 2-BEARBEITER)

- CHUI MICHAEL / MANYIKA JAMES / MIREMADI MEHDI, Four fundamentals of workplace automation, McKinsey Quarterly, 2015, abrufbar unter <www.mckinsey.com> (besucht am 31.05.2020)
- CICERO MARCUS TULLIUS, De officiis («Von den Pflichten», lateinisch und deutsch, neu übertragen und herausgegeben von Harald Merklin), Frankfurt am Main/Leipzig 1991
- CIRIGLIANO LUCA / EGGER CORINNE, Arbeitssicherheit und Gesundheitsschutz als Teil des kollektiven Arbeitsrechts, Jusletter, 03.09.2018
- CLASSEN MARTIN / GÄRTNER CHRISTIAN, Im Kampf um Big Data, personalmagazin [sic], 2016, 38–39
- COLLIER LORNA, Workplace surveillance: will new techniques spark resentment?, SAGE Business Researcher, 05.11.2018, 2–13
- Commission nationale de l'informatique et des libertés, The CNIL's restricted committee imposes a financial penalty of 50 million euros against Google LLC, 21.01.2019, abrufbar unter <www.cnil.fr> (besucht am 31.05.2020)
- COSTA GIORDANO, Internet- und E-Mail-Überwachung am Arbeitsplatz, Jusletter, 09.01.2012
- CRAWFORD KATE, The hidden biases in big data, Harvard Business Review, 01.04.2013, abrufbar unter <<https://hbr.org>> (besucht am 31.05.2020)
- CRAWFORD KATE / CALO RYAN, There is a blind spot in AI research, Nature, 2016, 311–313
- CRAWFORD KATE / SCHULTZ JASON, Big data and due process: toward a framework to redress predictive privacy harms, Boston College Law Review, 2014, 93–128
- CUKIER KENNETH / MAYER-SCHÖNBERGER VIKTOR, The rise of big data: how it's changing the way we think about the world, Foreign Affairs 3, 2013, 28–40
- CULIK NICOLAI J., Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung, Berlin 2018, Diss. Münster (Westfalen) 2018
- CUSTERS BART, Data dilemmas in the information society: introduction and overview, in: Custers Bart / Calders Toon / Schermer Bart / Zarsky Tal (Hg.): Discrimination and privacy in the information society, Data mining and profiling in large databases, Berlin/Heidelberg 2013, 3–26
- CUSTERS BART / DECHESNE FRANCIEN / SEARS ALAN M. / TANI TOMMASO / VAN DER HOF SIMONE, A comparison of data protection legislation and policies across the EU, Computer Law & Security Review, 2018, 234–243
- CUSTERS BART / URSIC HELENA, Worker privacy in a digitalized world under European law, Comparative Labor Law & Policy Journal, 2018, 323–344
- CUSTERS BART / VAN DER HOF SIMONE / SCHERMER BART, Privacy expectations of social media users: the role of informed consent in privacy policies, Policy & Internet, 2014, 268–295
- DAEDELLOW ROMY 2017, Beschäftigtendatenschutz und DSGVO, digma – Zeitschrift für Datenrecht und Informationssicherheit, 2017, 34–37
- DAEDELLOW ROMY 2018, Wenn Algorithmen (unfair) über Menschen entscheiden..., Jusletter, 26.11.2018

- DANKERT KEVIN, Verfälschung von Datenbeständen durch Social Bots, in: Hoffmann-Riem Wolfgang (Hg.): Big Data – Regulative Herausforderungen, Baden-Baden 2018, 157–165
- DARPA, Broad agency announcement: explainable artificial intelligence (XAI), Arlington (Virginia) 10.08.2016
- Datenschutzbeauftragter des Kantons Zürich, Auswirkungen der europäischen Datenschutzerlasse auf die öffentlichen Organe, 04.2018, abrufbar unter <<https://dsb.zh.ch>> (besucht am 31.05.2020)
- Datenschutzkonferenz, Hambacher Erklärung zur Künstlichen Intelligenz, Hambacher Schloss 03.04.2019
- DÄUBLER WOLFGANG, Gläserne Belegschaften, 8. A., Frankfurt am Main 2019
- DAVENPORT THOMAS H., Big data @ work [sic], München 2014
- DAVENPORT THOMAS H. / BEAN RANDY, Big companies are embracing analytics, but most still don't have a data-driven culture, Harvard Business Review, 15.02.2018, abrufbar unter <<https://hbr.org>> (besucht am 31.05.2020)
- DAVENPORT THOMAS H. / RONANKI RAJEEV, Artificial intelligence for the real world, Harvard Business Review, 2018, 108–116
- DE HERT PAUL, A human rights perspective on privacy and data protection impact assessments, in: Wright David / De Hert Paul (Hg.): Privacy impact assessment, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2012, 33–76
- DE HERT PAUL / PAPAKONSTANTINOU VAGELIS, The EDPS as a unique stakeholder in the European data protection landscape, fulfilling the explicit and non-explicit expectations, in: Hijmans Hielke / Kranenborg Herke (Hg.): Data protection anno 2014: how to restore trust?, Cambridge (Grossbritannien) 2014, 237–252
- DE MAURO ANDREA / GRECO MARCO / GRIMALDI MICHELE, A formal definition of big data based on its essential features, Library Review, 2016, 122–135
- DEBEER JEREMY, Employee privacy: the need for comprehensive protection, Saskatchewan Law Review, 2003, 383–418
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Bundesdatenschutzgesetz: Text und Erläuterungen, Bonn 01.2019
- DERRER BALLADORE RUTH, Die bestehende Regelung hat sich bewährt, in: Ehrenzeller Bernhard / Furer Hans / Geiser Thomas (Hg.): Die Mitwirkung in den Betrieben, St. Gallen 2009, 185
- DETERMANN LOTHAR, Determann's field guide to international data privacy law compliance, Cheltenham (Grossbritannien)/Northampton (Massachusetts) 2012
- DETERMANN LOTHAR / SPRAGUE ROBERT, Intrusive monitoring: employee privacy expectations are reasonable in Europe, destroyed in the United States, Berkeley Technology Law Journal, 2011, 979–1036
- DICKIE NANCY / YULE ANDREW, Privacy by design prevents data headaches later, Strategic HR Review, 2017, 100–101
- DIETRICH BRENDA L. / PLACHY EMILY C. / NORTON MAUREEN F., Analytics across the enterprise, Crawfordsville (Indiana) 2014

- DIMITROV GEORGE / ILIEVA DANIELA / MAKSHUTOVA RADOSLAVA, What data protection rights do employees have in 2018, *Privacy in Germany*, 2019, 26–29
- DIX ALEXANDER, Built-in privacy – no panacea, but a necessary condition for effective privacy protection, *Identity in the Information Society*, 2010, 257–265
- DOCHOW CARSTEN, Notwendigkeit der Datenschutz-Folgenabschätzung und Benennung eines Datenschutzbeauftragten in der Arztpraxis?, *Privacy in Germany*, 2018, 51–61
- DOMENIG BENJAMIN / MITSCHERLICH CHRISTIAN, *Datenschutzrecht für Schweizer Unternehmen*, Bern 2019
- DONAUER DANIEL / MÖRI BARBARA A., Die privatrechtliche Fürsorgepflicht des Arbeitgebers und rechtliche Konsequenzen, *Aktuelle Juristische Praxis*, 2015, 1049–1061
- DORNDORF EBERHARD, Eine Mindestmoral des Arbeitsrechts, in: Simon Dieter / Weiss Manfred (Hg.): *Zur Autonomie des Individuums, Liber amicorum Spiros Simitis*, Baden-Baden 2000, 69–90
- DRESSEL JULIA / FARID HANY, The accuracy, fairness, and limits of predicting recidivism, *Science Advances*, 2018, 1–5
- DREYER STEPHAN, Predictive Analytics aus der Perspektive von Menschenwürde und Autonomie, in: Hoffmann-Riem Wolfgang (Hg.): *Big Data – Regulative Herausforderungen*, Baden-Baden 2018, 135–143
- DREYER STEPHAN / SCHULZ WOLFGANG, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, *Gütersloh* 04.2018
- DRUEY JEAN NICOLAS 1990, «Daten-Schmutz», Rechtliche Ansatzpunkte zum Problem der Über-Information, in: Brem Ernst / Druey Jean Nicolas / Kramer Ernst A. / Schwander Ivo (Hg.): *Festschrift zum 65. Geburtstag von Mario M. Pedrazzini*, Bern 1990, 379–396
- DRUEY JEAN NICOLAS 1995, *Information als Gegenstand des Rechts*, Zürich 1995
- DRUEY JEAN NICOLAS 2015, Verantwortlichkeit und Information, in: Waldburger Robert / Sester Peter / Peter Christoph / Baer Charlotte M. (Hg.): *Law & Economics*, Festschrift für Peter Nobel zum 70. Geburtstag, Bern 2015, 3–20
- DSGVO-BDSG-K: Paal Boris P. / Pauly Daniel (Hg.), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar*, 2. A., München 2018 (zit. DSGVO-BDSG-K-BEARBEITER)
- DUISBERG ALEXANDER, Machine Learning und rechtliche Rahmenbedingungen, *Jusletter IT*, 26.09.2018
- DUNAND JEAN-PHILIPPE, Internet au travail: droits et obligations de l'employeur et du travailleur, in: Dunand Jean-Philippe / Mahon Pascal (Hg.): *Internet au travail*, Genf 2014, 33–72
- DZIDA BORIS, Big Data und Arbeitsrecht, *Neue Zeitschrift für Arbeitsrecht*, 2017, 541–546
- DZIDA BORIS / GRAU TIMON, Beschäftigtendatenschutz nach der Datenschutzgrundverordnung und dem neuen BDSG – zehn Fragen aus der Praxis, *Der Betrieb*, 2018, 189–194
- DZIDA BORIS / GROH NAEMI, Diskriminierung nach dem AGG beim Einsatz von Algorithmen im Bewerbungsverfahren, *Neue Juristische Wochenschrift*, 2018, 1917–1922

- Edelman Corporation, 2019 Edelman Trust Barometer global report, 2019, abrufbar unter <www.edelman.com> (besucht am 31.05.2020)
- EDÖB 2007, 14. Tätigkeitsbericht 2006/2007, Bern 2007
- EDÖB 2010, 17. Tätigkeitsbericht 2009/2010, Bern 2010
- EDÖB 2012, Erläuterungen zur Telefonüberwachung am Arbeitsplatz, Bern 20.02.2012
- EDÖB 2013, Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz, Bern 09.2013
- EDÖB 2014a, Schlussbericht betreffend die Datenbearbeitung im Zusammenhang mit der Datensammlung [...] von [...] AG, Bern 03.06.2014
- EDÖB 2014b, Leitfaden über die Bearbeitung von Personendaten im Arbeitsbereich, Bern 10.2014
- EDÖB 2018a, Tätigkeitsbericht 2017/2018, Bern 2018
- EDÖB 2018b, Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz, 11.2018, abrufbar unter <www.edoeb.admin.ch> (besucht am 31.05.2020)
- EDSA 2018, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version for public consultation, 16.11.2018, abrufbar unter <<https://edpb.europa.eu>> (besucht am 31.05.2020)
- EDSA 2019, First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities, 26.02.2019, abrufbar unter <www.huntonprivacyblog.com> (besucht am 31.05.2020)
- EDSB 2014, Vorläufige Stellungnahme des Europäischen Datenschutzbeauftragten, Brüssel 26.03.2014
- EDSB 2018, Opinion 5/2018, preliminary opinion on privacy by design, Brüssel 31.05.2018
- EDSB 2019a, Annual report 2018, Luxemburg 2019
- EDSB 2019b, Technology report No 1: smart glasses and data protection, Brüssel 01.2019
- EDSB 2019c, Newsletter (N°67), 25.02.2019, abrufbar unter <<https://edps.europa.eu>> (besucht am 31.05.2020)
- EDWARDS LILIAN / VEALE MICHAEL, Slave to the algorithm? Why a «right to an explanation» is probably not the remedy you are looking for, Duke Law & Technology Review, 2017, 18–84
- EGGEN MIRJAM / STENGEL CORNELIA, Wearables – eine vertragsrechtliche Betrachtung, Jusletter, 26.11.2018
- EGGIMANN PATRICK, Speichern – Verwerten – Löschen: zur zeitlichen Dimension des Informationsmanagements in Unternehmen, Zürich/St. Gallen 2015
- EGMR, Factsheet: surveillance at workplace, Strassburg 11.2018
- Eidgenössische Finanzmarktaufsicht, Rundschreiben 2017/1 Corporate Governance – Banken, Bern 22.09.2016
- ENISA, Recommendations on European data protection certification, Heraklion (Griechenland) 11.2017

- EPINEY ASTRID, Allgemeine Grundsätze, in: Belser Eva Maria / Epiney Astrid / Waldmann Bernhard (Hg.): Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, 510–558
- EPINEY ASTRID / KERN MARKUS, Zu den Neuerungen im Datenschutzrecht der Europäischen Union, Datenschutzgrundverordnung, Richtlinie zum Datenschutz in der Strafverfolgung und Implikationen für die Schweiz, in: Epiney Astrid / Nüesch Daniela (Hg.): Die Revision des Datenschutzes in Europa und die Schweiz, La révision de la protection des données en Europe et la Suisse, Zürich/Basel/Genf 2016, 39–76
- ErfK: Müller-Glöge Rudi / Preis Ulrich / Schmidt Ingrid (Hg.), Erfurter Kommentar zum Arbeitsrecht, 20. A., München 2020 (zit. ErfK-BEARBEITER)
- ETUC / UNICE / UEAPME / CEEP, Framework agreement on work-related stress, 08.10.2004, abrufbar unter <www.eurofound.europa.eu> (besucht am 31.05.2020)
- EU / Europarat, Handbook on European data protection law, Luxemburg 2018
- Europäische Kommission 2019a, A definition of AI: main capabilities and disciplines, Brüssel 08.04.2019
- Europäische Kommission 2019b, Ethics guidelines for trustworthy AI, Brüssel 08.04.2019
- Europäisches Parlament 2017, Report on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement (2016/2225(INI)), A8-0044/2017, Brüssel 20.02.2017
- Europarat 1989, Recommendation No. R (89) 2 of the committee of ministers to member states on the protection of personal data used for employment purposes, Strassburg 18.01.1989
- Europarat 2008, Application of Convention 108 to the profiling mechanism, Strassburg 11.01.2008
- Europarat 2010, Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (T-PD-BUR(2010)09), 2010, abrufbar unter <www.coe.int> (besucht am 31.05.2020)
- Europarat 2011, Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation (T-PD-BUR(2010)11 FIN), Strassburg 09.09.2011
- Europarat 2015, Recommendation CM/Rec(2015)5 on the processing of personal data in the context of employment, Strassburg 01.04.2015
- Europarat 2016a, Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, MSI-NET(2016)06rev6, 2016, abrufbar unter <<https://rm.coe.int>> (besucht am 31.05.2020)
- Europarat 2016b, The processing of personal data in the context of employment: Recommendation CM/Rec(2015)5 and explanatory memorandum, Strassburg 2016
- Europarat 2016c, «Of data and men», Fundamental rights and freedoms in a world of big data (T-PD-BUR(2015)09REV), Strassburg 11.01.2016

- Europarat 2017, Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data, 23.01.2017, abrufbar unter <<http://rm.coe.int>> (besucht am 31.05.2020)
- Europarat 2018a, Explanatory report to the protocol amending the convention for the protection of individuals with regard to automatic processing of personal data (SEV 223), Strassburg 10.X.2018 [sic]
- Europarat 2018b, 128th Session of the Committee of Ministers, Helsingør (Dänemark) 18.05.2018
- Europarat 2018c, Convention 108+ [sic], 06.2018, abrufbar unter <<http://rm.coe.int>> (besucht am 31.05.2020)
- Europarat 2019, Artificial intelligence and data protection: challenges and possible remedies, 25.01.2019, abrufbar unter <<http://rm.coe.int>> (besucht am 31.05.2020)
- FAIRFIELD JOSHUA A.T., «Do-not-track» as contract, Vanderbilt Journal of Entertainment and Technology Law, 2012, 545–602
- FASCHING GALILEO / WÖHRL MANFRED / PALECEK NORBERT, Normenkonforme Zertifizierungen zum Datenschutzbeauftragten, Jusletter IT, 22.02.2018
- FAVARETTO MADDALENA / DE CLERCQ EVA / ELGER BERNICE SIMONE, Big data and discrimination: perils, promises and solutions. A systematic review, Journal of Big Data, 2019, 1–27
- FEILER LUKAS, Die 69 Öffnungsklauseln der DSGVO (Vortrag), DSGVO ante portas, Graz 01.06.2017
- FEILER LUKAS / FORGÓ NIKOLAUS / WEIGL MICHAELA, The EU General Data Protection Regulation (GDPR): a commentary, Woking (Grossbritannien) 2018
- FINKIN MATTHEW W., Privacy in employment law, 4. A., Arlington (Virginia) 2013
- FLORIDI LUCIANO, Mature information societies – a matter of expectations, Philosophy & Technology, 2016, 1–4
- FLÜCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, Aktuelle Juristische Praxis, 2013, 837–864
- FLUECKIGER CHRISTIAN 2014, La googlelisation des employés respecte-t-elle les principes de la protection des données?, in: Dunand Jean-Philippe / Mahon Pascal (Hg.): Internet au travail, Genf 2014, 73–97
- FLUECKIGER CHRISTIAN 2017, Principes généraux de la protection des données et communications transfrontières dans le cadre des relations de travail, in: Dunand Jean-Philippe / Mahon Pascal (Hg.): La protection des données dans les relations de travail, Genf 2017, 1–23
- FORD ROGER ALLAN, Unilateral invasions of privacy, Notre Dame Law Review, 2016, 1075–1115
- FORGÓ NIKOLAUS, Big Data am Arbeitsplatz – europäische Standards (Vortrag), FAA-Tagung Big Data am Arbeitsplatz: arbeits- und datenschutzrechtliche Fragen rund um Workforce Analytics, Zürich 16.10.2018

- FOX MARIA / LONG DEREK / MAGAZZENI DANIELE, Explainable planning, in: Aha David W. / Darrell Trevor / Pazzani Michael / Reid Darryn / Sammut Claude / Stone Peter (Hg.): IJCAI-17 workshop on explainable AI (XAI) proceedings, Melbourne (Australien) 20.08.2017, abrufbar unter <<https://ijcai-17.org>> (besucht am 31.05.2020), 24–30
- FRANZEN MARTIN, Datenschutz-Grundverordnung und Arbeitsrecht, Europäische Zeitschrift für Arbeitsrecht, 2017, 311–351
- FREI NULA, Die Revision des Datenschutzgesetzes aus europarechtlicher Sicht, Jusletter, 17.09.2018
- FRITZ MAX / SCHULER CARLA, Die Mitwirkung im Arbeitsverhältnis, 2. A., Zürich 2012
- FTC 2012, Protecting consumer privacy in an era of rapid change: recommendations for businesses and policymakers, 26.03.2012, abrufbar unter <www.ftc.gov> (besucht am 31.05.2020)
- FTC 2016, Big data: a tool for inclusion or exclusion?, 01.2016, abrufbar unter <www.ftc.gov> (besucht am 31.05.2020)
- FURER HANS 2009a, Ein Vorschlag, in: Ehrenzeller Bernhard / Furer Hans / Geiser Thomas (Hg.): Die Mitwirkung in den Betrieben, St. Gallen 2009, 149–175
- FURER HANS 2009b, Interview mit Kathrin Amacker, in: Ehrenzeller Bernhard / Furer Hans / Geiser Thomas (Hg.): Die Mitwirkung in den Betrieben, St. Gallen 2009, 177–184
- GABATHULER SILVAN, Big Data Management in Theorie und Praxis aus rechtlicher Sicht, Bamberg 2018, Diss. St. Gallen 2018
- GABATHULER THOMAS, Die Mitwirkung der Arbeitnehmenden, in: SGB (Hg.): Handbuch zum kollektiven Arbeitsrecht, Basel 2009
- GÄCHTER THOMAS, Observation im Sozialversicherungsrecht: Voraussetzungen und Schranken, in: Weber Stephan (Hg.): HAVE Personen-Schaden-Forum 2011, Zürich 2011, 179–209
- GÄCHTER THOMAS / EGLI PHILIPP, Informationsaustausch im Umfeld der Sozialhilfe, Jusletter, 06.09.2010
- GAMPER LOTHAR / KASTELITZ MARKUS, Auswirkungen der Datenschutz-Grundverordnung auf die wissenschaftliche Forschung in Österreich, Jusletter IT, 22.02.2018
- GANTNER FELIX, «Code is law» aber «Is law code»? , Jusletter IT, 22.02.2018
- GASCHER LUDWIG, Zulässigkeit eines Datenabgleichs zur Aufdeckung von Straftaten von Arbeitnehmern, Hamburg 2013, Diss. Passau 2013
- GASSER URS 2001, Kausalität und Zurechnung von Information als Rechtsproblem, Bamberg 2001, Diss. St. Gallen 2001
- GASSER URS 2004, Framing information quality governance research, in: Gasser Urs (Hg.): Information quality regulation: foundations, perspectives, and applications, Baden-Baden 2004, 3–20
- GASSER URS 2016, Recoding privacy law: reflections on the future relationship among law, technology, and privacy, Harvard Law Review, 2016, 61–70

- GASSER URS / ALMEIDA VIRGILIO A.F., A layered model for AI governance, IEEE Internet Computing, 2017, 58–62
- GASSER URS / CORTESI SANDRA, Children's rights and digital technologies, Introduction to the discourse and some meta-observations, in: Ruck Martin D. / Peterson-Badali Michele / Freeman Michael (Hg.): Handbook of children's rights, Global and multidisciplinary perspectives, New York (New York)/Milton Park (Abingdon, Grossbritannien) 2017, 417–436
- GAY DARRELL S. / KAGAN ABIGAIL M., Big data and employment law: what employers and their legal counsel need to know, ABA Journal of Labor & Employment Law, 2018, 191–209
- GEISER THOMAS 2009, Aktuelle Gesetzgebung, Gerichtspraxis und internationaler Kontext, in: Ehrenzeller Bernhard / Furer Hans / Geiser Thomas (Hg.): Die Mitwirkung in den Betrieben, St. Gallen 2009, 15–58
- GEISER THOMAS 2015, Darf die Arbeitgeberin den Bewerber googeln?, in: Gschwend Lukas / Hettich Peter / Müller-Chen Markus / Schindler Benjamin / Wildhaber Isabelle (Hg.): Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, 373–385
- GERSCHWILER STEFAN / EPINEY ASTRID / NÜESCH DANIELA / NOUREDDINE HUSSEIN / WASMER CLAUDIA LEONIE, Prinzipien der Datenbearbeitung durch Privatpersonen und Behörden, in: Passadelis Nicolas / Rosenthal David / Thür Hanspeter (Hg.): Datenschutzrecht, Basel 2015, 73–120
- GILBERT FRANCOISE, Global privacy and security law, East Palo Alto (Kalifornien) 01.2019
- GLASS PHILIP, Selbstbestimmung und Designschutz, in: Schweighofer Erich / Kummer Franz / Saarenpää Ahti (Hg.): Internet of Things, Tagungsband des 22. internationalen Rechtsinformatik-Symposiums, Salzburg 21.–23.02.2019, Bern 2019, 103–112
- GLATTHAAR MATTHIAS, Automatisierte Entscheide: Rekrutierungsalgorithmen (Vortrag), SF-FS/ITSL-Tagung Automatisierte Entscheidungen, Zürich 13.11.2019
- GNEHM OLIVER, Das datenschutzrechtliche Auskunftsrecht, Nukleus zur prozeduralen Durchsetzung des datenschutzrechtlichen Persönlichkeitsschutzes, in: Epiney Astrid / Nüesch Daniela (Hg.): Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes, La mise en œuvre des droits des particuliers dans le domaine de la protection des données, Zürich/Basel/Genf 2015, 77–106
- GOLA PETER 2015, Datenschutz am Arbeitsplatz, 5. A., Heidelberg/München/Landsberg/Frechen/Hamburg 2015
- GOLA PETER 2019, Handbuch Beschäftigtendatenschutz, 8. A., Heidelberg/München 2019
- GOLA PETER / WRONKA GEORG, Handbuch Arbeitnehmerdatenschutz, 6. A., Heidelberg/München/Landsberg/Frechen/Hamburg 2013
- GOODMAN BRYCE / FLAXMAN SETH, European Union regulations on algorithmic decision-making and a «right to explanation», AI Magazine, 2017, 1–9
- GORICNIK WOLFGANG / GRÜNANGER JOSEF, Einleitung, in: Grünanger Josef / Goricnik Wolfgang (Hg.): Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle, Wien 2018, 1–7

- GRABENWARTER CHRISTOPH, European convention on human rights, commentary, München 2014
- GRABENWARTER CHRISTOPH / PABEL KATHARINA, Europäische Menschenrechtskonvention, 6. A., München 2016
- GRAF FERDINAND / KRIŽANAC MARIJA, Der Arbeitnehmerdatenschutz in der DSGVO, in: Grabenwarther Christoph / Graf Ferdinand / Ritschl Mercedes (Hg.): Neuerungen im europäischen Datenschutzrecht für Unternehmen, Wien 2017, 87–106
- GRÜNANGER JOSEF, Gesundheitskontrollen, in: Grünanger Josef / Goricnik Wolfgang (Hg.): Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle, Wien 2018, 167–202
- GUENOLE NIGEL / FERRAR JONATHAN / FEINZIG SHERI, The power of people, Glenview (Illinois) 2017
- GUIHOT MICHAEL / MATTHEW ANNE F. / SUZOR NICOLAS P., Nudging robots: innovative solutions to regulate artificial intelligence, Vanderbilt Journal of Entertainment and Technology Law, 2018, 385–456
- GUTWIRTH SERGE / HILDEBRANDT MIREILLE, Some caveats on profiling, in: Gutwirth Serge / Pouillet Yves / De Hert Paul (Hg.): Data protection in a profiled world, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2010, 31–41
- HAAS MAURITS, Die Verarbeitung besonderer Kategorien personenbezogener Daten. Gleichzeitig erste Anmerkungen zum Vorabentscheidungsersuchen EuGH C-136/17, Jusletter IT, 22.02.2018
- HACKER PHILIPP, Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law, Common Market Law Review, 2018, 1143–1186
- HÄFNER-BEIL NADJA, Datenschutz am Arbeitsplatz I.–IV., in: Wedde Peter (Hg.): Handbuch Datenschutz und Mitbestimmung, Frankfurt am Main 2016, 94–113
- HALPERN IRIS, E-discovery in the workplace: employee perspective, in: Sprague Robert (Hg.): Workplace data, Arlington (Virginia) 2013, 5-1 – 5-43 [sic]
- HAMANN CHRISTIAN, Datenschutzrecht, in: Arnold Christian / Günther Jens (Hg.): Arbeitsrecht 4.0, Praxishandbuch zum Arbeits-, IP- und Datenschutzrecht in einer digitalisierten Arbeitswelt, München 2018, 223–255
- HÄNER ISABELLE, Die Beteiligten im Verwaltungsverfahren und Verwaltungsprozess, Zürich 2000, Habil. Zürich 2000
- HÄNOLD STEFANIE, Profiling and automated decision-making: legal implications and shortcomings, in: Corrales Marcelo / Fenwick Mark / Forgó Nikolaus (Hg.): Robotics, AI and the future of law, Singapur 2018, 123–154
- HÄRTING NIKO, Internetrecht, 6. A., Köln 2017
- HARTZOG WOODROW 2013, The fight to frame privacy, Michigan Law Review, 2013, 1021–1043
- HARTZOG WOODROW 2017, The inadequate, invaluable fair information practices, Maryland Law Review, 2017, 952–982

- HARTZOG WOODROW 2018, *Privacy's blueprint: the battle to control the design of new technologies*, Cambridge (Massachusetts) 2018
- HARTZOG WOODROW / STUTZMAN FREDERIC 2013, *Obscurity by design*, *Washington Law Review*, 2013, 385–418
- HARTZOG WOODROW / STUTZMAN FREDERIC 2013, *The case for online obscurity*, *California Law Review*, 2013, 1–49
- HASKINS KEVIN J., *Wearable technology and implications for the Americans with Disabilities Act, Genetic Information Nondiscrimination Act, and health privacy*, *ABA Journal of Labor & Employment Law*, 2017, 69–78
- HAUSER CHRISTIAN, *Ethische Herausforderungen im Umgang mit Daten (Vortrag)*, Fachtagung Data Policy, Olten 15.11.2018
- HAUSHEER HEINZ / AEBI-MÜLLER REGINA E., *Das Personenrecht des Schweizerischen Zivilgesetzbuches*, 4. A., Bern 2016
- HELLER CHRISTIAN, *Post-Privacy: prima leben ohne Privatsphäre*, München 2011
- HERMSTRÜWER YOAN, *Die Regulierung der prädiktiven Analytik: eine juristisch-verhaltenswissenschaftliche Skizze*, in: Hoffmann-Riem Wolfgang (Hg.): *Big Data – Regulative Herausforderungen*, Baden-Baden 2018, 99–116
- HERMSTRÜWER YOAN / HAMANN HANJO, *Schwimmen mit Fingerabdruck?*, Göttingen 2012
- HIJMANS HIELKE / KRANENBORG HERKE, *Data protection anno 2014: how to restore trust? An introduction*, in: Hijmans Hielke / Kranenborg Herke (Hg.): *Data protection anno 2014: how to restore trust?*, Cambridge (Grossbritannien) 2014, 3–17
- HILDEBRANDT MIREILLE / KOOPS BERT-JAAP, *The challenges of ambient law and legal protection in the profiling era*, *The Modern Law Review*, 2010, 428–460
- HK: Rosenthal David / Jöhri Yvonne (Hg.), *Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen*, Zürich/Basel/Genf 2008 (zit. HK-BEARBEITER)
- HOBBS THOMAS, *Leviathan* (Erstpublikation 1651), revised student edition, edited by Richard Tuck, Cambridge (Grossbritannien) 1996
- HOEREN THOMAS 2017, *Überlegungen zu Big Data aus der Sicht der Datenschutzrechtswissenschaft*, in: Boehme-Nessler Volker / Rehbinder Manfred (Hg.): *Big Data: Ende des Datenschutzes?*, *Gedächtnisschrift für Martin Usteri*, Bern 2017, 83–109
- HOEREN THOMAS 2018, *Big Data und Zivilrecht*, in: Hoffmann-Riem Wolfgang (Hg.): *Big Data – Regulative Herausforderungen*, Baden-Baden 2018, 187–193
- HÖFER SEBASTIAN, *Algorithmen, maschinelles Lernen und die Grenzen der KI*, *Jusletter*, 26.11.2018
- HÖFFE OTFRIED, *Identität im Zeitalter der Digitalisierung*, *digma – Zeitschrift für Datenschutz und Informationssicherheit*, 2003, 98–99
- HOFFMANN-RIEM WOLFGANG, *Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data*, in: Hoffmann-Riem Wolfgang (Hg.): *Big Data – Regulative Herausforderungen*, Baden-Baden 2018, 11–80

- HOFMANN KAI, Smart Factory – Arbeitnehmerdatenschutz in der Industrie 4.0, Zeitschrift für Datenschutz, 2016, 12–17
- HÖLLER HEINZ-PETER / WEDDE PETER 2016, Neue Technik – neue Anforderungen, in: Wedde Peter (Hg.): Handbuch Datenschutz und Mitbestimmung, Frankfurt am Main 2016, 297–317
- HÖLLER HEINZ-PETER / WEDDE PETER 2018, Die Vermessung der Belegschaft, Düsseldorf 01.2018
- HOLTHAUS CHRISTIAN / PARK YOUNG-KUL / STOCK-HOMBURG RUTH, People Analytics und Datenschutz – Ein Widerspruch?, Datenschutz und Datensicherheit, 2015, 676–681
- HORNUNG GERRIT, Erosion traditioneller Prinzipien des Datenschutzrechts durch Big Data, in: Hoffmann-Riem Wolfgang (Hg.): Big Data – Regulative Herausforderungen, Baden-Baden 2018, 81–98
- HORVÁT EMÖKE-ÁGNES / HANSELMANN MICHAEL / HAMPRECHT FRED A. / ZWEIG KATHARINA A., One plus one makes three (for social networks), PLoS ONE [sic] 4, 2012, 1–8
- HORVATH SABINE, Aktueller Begriff: Big Data, Berlin 06.11.2013
- HOWARD CHRISTINE, E-discovery issues related to workplace data, in: Sprague Robert (Hg.): Workplace data, Arlington (Virginia) 2013, 3-1 – 3-36 [sic]
- HR Metrics & Analytics Summit, Workplace privacy and protection: is your employer watching your every move?, 2018, abrufbar unter <www.corporatelearningnetwork.com> (besucht am 31.05.2020)
- HUGENTOBLE MARKUS, Datenschutzfalle Assessment Center, Aktuelle Juristische Praxis, 2009, 153–156
- HUME DAVID, A treatise of human nature (reprinted from the original edition in three volumes and edited, with analytical index, by L.A. Selby-Bigge), Oxford 1896
- HURLEY MIKELLA / ADEBAYO JULIUS, Credit scoring in the era of big data, Yale Journal of Law & Technology, 2016, 148–216
- HUSI-STÄMPFLI SANDRA, Die DSGVO-Revision oder: ein Beziehungsdrama in drei Akten, Jus-letter, 07.05.2018
- HUSTINX PETER, Privacy by design: delivering the promises, Identity in the Information Society, 2010, 253–255
- IBM, What will we make of this moment?, New York 2013
- ICDPPC, Declaration on ethics and data protection in artificial intelligence, Brüssel 23.10.2018
- ILG WALO C., Kommentar über das Bundesgesetz über die Information der Arbeitnehmer in den Betrieben (Mitwirkungsgesetz), Zürich 1999
- ILO, Protection of workers' personal data, Genf 1997
- Information and Privacy Commissioner of Ontario, Privacy by design, Toronto 09.2013
- JÄGGI PETER, Fragen des privatrechtlichen Schutzes der Persönlichkeit, Zeitschrift für Schweizerisches Recht II, 1960, 133a–261a

- JAKOB RAIMUND, Big Data oder die Überforderung des Einzelnen, Psychologische Gedanken, in: Boehme-Nessler Volker / Reh binder Manfred (Hg.): Big Data: Ende des Datenschutzes?, Gedächtnisschrift für Martin Usteri, Bern 2017, 13–26
- JERVIS CLAIRE E. M., Bărbulescu v Romania: why there is no room for complacency when it comes to privacy rights in the workplace, Industrial Law Journal, 2018, 440–453
- JÖHRI YVONNE, Vorratsdatenspeicherung gemäss Bundesgericht zulässig, Digitaler Rechtsprechungskommentar, 28.09.2018
- KAINER FRIEDEMANN / WEBER CHRISTIAN, Datenschutzrechtliche Aspekte des «Talentmanagements», Betriebs-Berater, 2017, 2740–2747
- KAISER STEPHAN, Roboter statt Recruiter?, personalmagazin [sic] 8, 2014, 12–15
- KÄLIN WALTER / KÜNZLI JÖRG, Universeller Menschenrechtsschutz, 4. A., Basel 2019
- KARG MORITZ, Anonymität, Pseudonyme und Personenbezug revisited?, Datenschutz und Datensicherheit, 2015, 520–526
- KARGER MICHAEL / GAYCKEN SANDRO, Teil VI. Outsourcing und neue Technologien, Kapitel 5. Cloud Computing, C. Entnetzung, in: Forgó Nikolaus / Helfrich Marcus / Schneider Jochen (Hg.): Betrieblicher Datenschutz, Rechtshandbuch, München 2017, 663–678
- KASPER GABRIEL / WILDHABER ISABELLE, Big Data am Arbeitsplatz in Schweizer Unternehmen: datenschutz- und arbeitsrechtliche Herausforderungen von People Analytics in Schweizer Unternehmen, in: Kieser Ueli / Pärli Kurt / Uttinger Ursula (Hg.): Datenschutztagung 2018, Ein Blick auf aktuelle Rechtsentwicklungen, Zürich/St. Gallen 2019, 189–232
- KASPER SABINA, Information Governance im Arbeitsverhältnis, Bern 2008, Diss. Zürich 2008
- KEATS CITRON DANIELLE, Technological due process, Washington University Law Review, 2008, 1249–1313
- KEATS CITRON DANIELLE / PASQUALE FRANK, The scored society: due process for automated predictions, Washington Law Review, 2014, 1–33
- KELLEHER DENIS / MURRAY KAREN, EU data protection law, Dublin/Haywards Heath (Grossbritannien)/London 2018
- KERN MARKUS / EPINEY ASTRID, Durchsetzungsmechanismen im EU-Recht und ihre Implikationen für die Schweiz, in: Epiney Astrid / Nüesch Daniela (Hg.): Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes, La mise en œuvre des droits des particuliers dans le domaine de la protection des données, Zürich/Basel/Genf 2015, 19–53
- KIM PAULINE T. 2017, Auditing algorithms for discrimination, University of Pennsylvania Law Review Online, 2017, 189–203
- KIM PAULINE T. 2017, Data-driven discrimination at work, William & Mary Law Review, 2017, 857–936

- KIM PAULINE T. / HANSON ERIK A., The law and business of people analytics: People analytics and the regulation of information under the fair credit reporting act, Saint Louis University Law Journal, 2016, 17–33
- KIRPAL ALFRED / VOGEL ANDREAS, Neue Medien in einer vernetzten Gesellschaft: Zur Geschichte des Internets und des World Wide Web, International Journal of History and Ethics of Natural Sciences, Technology and Medicine, 2006, 137–147
- KK: Däubler Wolfgang / Wedde Peter / Weichert Thilo / Sommer Imke (Hg.), Kompaktkommentar EU-Datenschutz-Grundverordnung und BDSG-neu, Frankfurt am Main 2018 (zit. KK-BEARBEITER)
- KLEBE THOMAS / WEISS MANFRED, Workers’ participation 4.0 – digital and global, Comparative Labor Law & Policy Journal, 2019, 263–283
- KNAPP HANNES / HAAS MAURITS, Arbeitnehmerdatenschutz in Österreich, Privacy in Germany, 2018, 79–82
- KOOPS BERT-JAAP / LEENES RONALD, Privacy regulation cannot be hardcoded. A critical comment on the «privacy by design» provision in data-protection law, International Review of Law, Computers & Technology, 2014, 159–171
- KÖRNER MARITA, Informierte Einwilligung als Schutzkonzept, in: Simon Dieter / Weiss Manfred (Hg.): Zur Autonomie des Individuums, Liber amicorum Spiros Simitis, Baden-Baden 2000, 131–150
- KPMG, Evidence-based HR, 2015, abrufbar unter <<https://home.kpmg>> (besucht am 31.05.2020)
- KRAUSE SKADI SIIRI, Gewissens-, Glaubens-, und Religionsfreiheit, Zeitschrift für Religion, Gesellschaft und Politik, 19.12.2019, Online-Publikation
- KROENER INGA / WRIGHT DAVID, A strategy for operationalizing privacy by design, The Information Society, 2014, 355–365
- KROLL JOSHUA A. / HUEY JOANNA / BAROCAS SOLON / FELTEN EDWARD W. / REIDENBERG JOEL R. / ROBINSON DAVID G. / YU HARLAN, Accountable algorithms, University of Pennsylvania Law Review, 2017, 633–705
- KUKO ArG: Blesi Alfred / Pietruszak Thomas / Wildhaber Isabelle (Hg.), Kurzkommentar Arbeitsgesetz, Basel 2018 (zit. KUKO ArG-BEARBEITER)
- KUKO OR: Honsell Heinrich (Hg.), Kurzkommentar Obligationenrecht, Art. 1–1186, Basel 2014 (zit. KUKO OR-BEARBEITER)
- KUKO ZPO: Oberhammer Paul / Domej Tania / Haas Ulrich (Hg.), Kurzkommentar ZPO, Schweizerische Zivilprozessordnung, 2. A., Basel 2013 (zit. KUKO ZPO-BEARBEITER)
- KURER PETER, Legal and compliance risk: a strategic response to a rising threat for global business, Oxford 2015
- LE GRAND GWENDAL / BARRAU EMILIE, Prior checking, a forerunner to privacy impact assessments, in: Wright David / De Hert Paul (Hg.): Privacy impact assessment, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2012, 97–116

- LE MÉTAYER DANIEL, Privacy by design: a matter of choice, in: Gutwirth Serge / Pouillet Yves / De Hert Paul (Hg.): Data protection in a profiled world, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2010, 323–334
- LEICHT-DEOBALD ULRICH / BUSCH THORSTEN / SCHANK CHRISTOPH / WEIBEL ANTOINETTE / SCHAFFHEITLE SIMON / WILDHABER ISABELLE / KASPER GABRIEL, The challenges of algorithm-based HR decision-making for personal integrity, *Journal of Business Ethics*, 07.09.2019, Online-Publikation
- LERMAN JONAS, Big data and its exclusions, *Stanford Law Review Online*, 2013, 55–63
- LESSIG LAWRENCE, Code, 2. A., New York (New York) 2006
- LETOMBE ELODIE, Le traçage du salarié: introduction, in: Pollet-Panoussis Delphine (Hg.): *Circuler dans la société numérique: droits et limites*, Paris 2013, 25–28
- LEVENDOWSKI AMANDA, How copyright law can fix artificial intelligence's implicit bias problem, *Washington Law Review*, 2018, 579–630
- LIEDKE BERND, Big Data – Small Information: Muss der datenschutzrechtliche Auskunftsanspruch reformiert werden?, in: Taeger Jürgen (Hg.): *Big Data & Co*, Tagungsband Herbstakademie 2014 DSRI, Mainz 10.–13.09.2014, Edewecht (Niedersachsen) 2014, 133–148
- LINGEMANN STEFAN / CHAKRABARTI JOSEFINE, Neue/alternative Beschäftigungsformen, in: Arnold Christian / Günther Jens (Hg.): *Arbeitsrecht 4.0*, Praxishandbuch zum Arbeits-, IP- und Datenschutzrecht in einer digitalisierten Arbeitswelt, München 2018, 27–75
- LIPTON ZACHARY C., The mythos of model interpretability, *Communications of the Association for Computing Machinery*, 2018, 36–43
- LOCHER RETO, Der Zugang zur Justiz in Diskriminierungsfällen, Bern 07.2015
- LONG JESSICA / ROARK CHRIS / THEOFILOU BILL, The bottom line on business trust, 2018, abrufbar unter <www.accenture.com> (besucht am 31.05.2020)
- LUHMANN NIKLAS, Vertrauen, 5. A., Konstanz/Stuttgart 2014
- MACCABE KEVIN, Eigentum an digitalen Daten im sachenrechtlichen Sinne, *Jusletter IT*, 26.09.2018
- MARLER JANET H. / BOUDREAU JOHN W., An evidence-based review of HR analytics, *The International Journal of Human Resource Management*, 2017, 3–26
- MARTINI MARIO, Algorithmen als Herausforderung für die Rechtsordnung, *JuristenZeitung*, 2017, 1017–1025
- MATHYS ROLAND, Big Data in der Rechtspraxis, Ausgewählte Problemstellungen, in: Epiney Astrid / Nüesch Daniela (Hg.): *Big Data und Datenschutzrecht / Big data et le droit de la protection des données*, Zürich 2016, 95–102
- MATZNER TOBIAS, Why privacy is not enough privacy in the context of «ubiquitous computing» and «big data», *Journal of Information, Communication and Ethics in Society*, 2014, 93–106
- MAYER-SCHÖNBERGER VIKTOR, *Delete*, Princeton (New Jersey) 2009

- MAYER-SCHÖNBERGER VIKTOR / CUKIER KENNETH, *Big data*, New York (New York)/Philadelphia (Pennsylvania) 2013
- MCDONALD ALEECIA M. / CRANOR LORRIE FAITH, The cost of reading privacy policies, *A Journal of Law and Policy for the Information Society*, 2008, 543–568
- MEHRI BAHMAN, From Al-Khwarizmi to algorithm, *Olympiads in Informatics*, 2017, 71–74
- MEIER PHILIPPE, *Protection des données: fondements, principes généraux et droit privé*, Bern 2011
- MEIER REGINA, Revision des Datenschutzgesetzes: kollektive Rechtsdurchsetzung im Datenschutzrecht?, *sui generis*, 2018, 139–148
- MESSNER JOHANNES, *Das Naturrecht*, 7. A., Berlin 1984
- MÉTILLE SYLVAIN, La surveillance électronique des employés, in: Dunand Jean-Philippe / Mahon Pascal (Hg.): *Internet au travail*, Genf 2014, 99–129
- MÉTILLE SYLVAIN / ARASTEH YASMINE, Le Règlement général sur la protection des données et les assureurs privés suisses, in: Fuhrer Stephan (Hg.): *Jahrbuch SGHVR 2018, Annales SDRCA 2018*, Zürich/Basel/Genf 2018, 111–142
- MEYER-MICHAELIS ISABEL, *Die Überwachung der Internet- und E-Mail-Nutzung am Arbeitsplatz*, Hamburg 2014, Diss. Köln 2014
- Microsoft Corporation 2018a, Review of Microsoft MyAnalytics privacy, security, and compliance: technical white paper, 2018, abrufbar unter <<https://docs.microsoft.com>> (besucht am 31.05.2020)
- Microsoft Corporation 2018b, *The future computed: artificial intelligence and its role in society*, Redmond (Washington) 2018
- MILLER GEOFFREY P., The rise of risk management, in: Waldburger Robert / Sester Peter / Peter Christoph / Baer Charlotte M. (Hg.): *Law & Economics, Festschrift für Peter Nobel zum 70. Geburtstag*, Bern 2015, 473–492
- MITTELSTADT BRENT, From individual to group privacy in big data analytics, *Philosophy & Technology*, 2017, 475–494
- MITTLÄNDER SILVIA 2016a, Datenschutz am Arbeitsplatz V., in: Wedde Peter (Hg.): *Handbuch Datenschutz und Mitbestimmung*, Frankfurt am Main 2016, 113–133
- MITTLÄNDER SILVIA 2016b, Datenschutz am Arbeitsplatz VII., in: Wedde Peter (Hg.): *Handbuch Datenschutz und Mitbestimmung*, Frankfurt am Main 2016, 164–184
- MONTESQUIEU CHARLES-LOUIS DE SECONDAT, *De l'esprit des lois (Vom Geist der Gesetze)*, Auswahl, Übersetzung und Einleitung von Kurt Weigand, Stuttgart 1965
- MORSCHER LUKAS, Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, *Zeitschrift des bernischen Juristenvereins*, 2011, 177–221
- MOWBRAY ALASTAIR, *European convention on human rights*, 3. A., Oxford 2012
- MRKONICH MARKO / KING ALLAN / FLIEGEL ROD / GORDON PHILIP / JONES HARRY / LEACHMAN TAMSEN / LOTITO MICHAEL / MATHIASON GARRY / MCGUIRE MICHAEL / PIERCE NATALIE / WEINER PAUL / JACKSON CORINN / ARGENTO ZOE / FUSCHETTI DANIELLE / DAVOUDIAN SHIVA SHIRAZI / KALDOR CHAD / LEE ELAINE / LOSEY CATHERINE /

- WIENTGE JOSEPH, JR., The Littler report: the big move toward big data in employment, 08.2015, abrufbar unter <www.littler.com> (besucht am 31.05.2020)
- MUGGLIN URS, Die Mitwirkung in einem Unternehmen des Bundes – am Beispiel «Die Schweizerische Post», in: Ehrenzeller Bernhard / Furer Hans / Geiser Thomas (Hg.): Die Mitwirkung in den Betrieben, St. Gallen 2009, 119–146
- MÜLLER ROLAND A., Die Arbeitnehmervvertretung, Bern 1999, Habil. Zürich 1999
- NAHRSTEDT HARALD, Algorithmen für Ingenieure, 3. A., Wiesbaden 2018
- NEU JUDITH, Der Einsatz moderner Kommunikationsmittel am Arbeitsplatz im Spannungsverhältnis zum Arbeitnehmerdatenschutz, Frankfurt am Main 2014, Diss. Greifswald 2012
- NEUBERGER MARK J., Using big data to manage human resources, in: Kalyvas James R. / Overly Michael R. (Hg.): Big Data, A business and legal guide, Boca Raton (Florida) 2015, 157–170
- NEUNHOEFFER FRIEDRIKE, Das Presseprivileg im Datenschutzrecht, Tübingen 2005
- NIKLAS THOMAS / THURN LUKAS, Arbeitswelt 4.0 – Big Data im Betrieb, Betriebs-Berater, 2017, 1589–1596
- NISSENBAUM HELEN 2004, Privacy as contextual integrity, Washington Law Review, 2004, 119–158
- NISSENBAUM HELEN 2011, A contextual approach to privacy online, Daedalus 4, 2011, 32–48
- NISSIM KOBBI / BEMBENEK AARON / WOOD ALEXANDRA / BUN MARK / GABOARDI MARCO / GASSER URS / O'BRIEN DAVID R. / STEINKE THOMAS / VADHAN SALIL, Bridging the gap between computer science and legal approaches to privacy, Harvard Journal of Law & Technology, 2018, 687–780
- NISSIM KOBBI / WOOD ALEXANDRA, Is privacy privacy?, Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, 2018, 376–396
- NOBEL PETER, Berner Kommentar, Aktienrecht, Bern 2017
- NORDMANN DANIEL, Das schweizerische Mitwirkungsgesetz, Bern 1994
- OECD, Building blocks for smart networks, Paris 17.01.2013
- OFK: Kren Kostkiewicz Jolanta / Wolf Stephan / Amstutz Marc / Fankhauser Roland (Hg.), OR Kommentar, Schweizerisches Obligationenrecht, 3. A., Zürich 2016 (zit. OFK-BEARBEITER)
- O'ROURKE ANNE / PYMAN AMANDA / TEICHER JULIAN, The right to privacy and the conceptualisation of the person in the workplace: a comparative examination of EU, US and Australian approaches, International Journal of Comparative Labour Law and Industrial Relations, 2007, 161–194
- OSTERLOH MARGIT / WEIBEL ANTOINETTE, Investition Vertrauen, Wiesbaden 2006
- OTTO MARTA 2015, The right to privacy in employment: in search of the European model of protection, European Labour Law Journal, 2015, 343–363
- OTTO MARTA 2016, The right to privacy in employment, a comparative analysis, Portland (Oregon) 2016

- OWSCHIMIKOW PHILIP, Datenscreening zwischen Compliance-Aufgabe und Arbeitnehmerdatenschutz, Frankfurt am Main 2014, Diss. Erlangen-Nürnberg 2013
- PALFREY JOHN / GASSER URS 2008, Born digital, New York (New York) 2008
- PALFREY JOHN / GASSER URS 2012, Interop. The promise and perils of highly interconnected systems, New York (New York)/Philadelphia (Pennsylvania) 2012
- PAPA ROBERTA / PIETRUSZAK THOMAS, Datenschutz im Personalwesen, in: Passadelis Nicolas / Rosenthal David / Thür Hanspeter (Hg.): Datenschutzrecht, Basel 2015, 577–611
- PARISI J. T., Following footsteps: how federal district court jurisprudence protects health data in the workplace, Vanderbilt Journal of Entertainment and Technology Law, 2017, 319–350
- PÄRLI KURT 2005, Der Persönlichkeitsschutz im privatrechtlichen Arbeitsverhältnis, Zeitschrift für Arbeitsrecht und Arbeitslosenversicherung, 2005, 225–235
- PÄRLI KURT 2009, Vertragsfreiheit, Gleichbehandlung und Diskriminierung im privatrechtlichen Arbeitsverhältnis, Bern 2009, Habil. St. Gallen 2009
- PÄRLI KURT 2018, Datenschutz, in: Portmann Wolfgang / von Kaenel Adrian (Hg.): Fachhandbuch Arbeitsrecht, Zürich/Basel/Genf 2018, 685–724
- PÄRLI KURT 2019, Eurolohn: Berufung auf das Diskriminierungsverbot ist rechtsmissbräuchlich, Jusletter, 20.05.2019
- PEARL JUDEA, Causality, 2. A., Cambridge 2009
- PEARL JUDEA / MACKENZIE DANA, The book of why, Grossbritannien/USA/Kanada/Irland/Australien/Indien/Neuseeland/Südafrika 2018
- PELTZ-STEELE RICHARD J., The new American privacy, Georgetown Journal of International Law, 2013, 365–410
- PERRENOUD STÉPHANIE, Durées du travail et discrimination, Aktuelle Juristische Praxis, 2017, 657–682
- PHAN PHILIP / WRIGHT MICHAEL / LEE SOO-HOON, Of robots, artificial intelligence, and work, Academy of Management Perspectives, 2017, 253–255
- PK IDG BS: Rudin Beat / Baeriswyl Bruno (Hg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG), Zürich/Basel/Genf 2014 (zit. PK IDG BS-BEARBEITER)
- PK IDG ZH: Baeriswyl Bruno / Rudin Beat (Hg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Zürich (IDG), Zürich/Basel/Genf 2012 (zit. PK IDG ZH-BEARBEITER)
- PLUTARCH (ΠΛΟΥΤΑΡΧΟΣ), Dion und Brutus, übersetzt von Konrat [sic] Ziegler, Zürich 1957
- PORTMANN WOLFGANG / WILDHABER ISABELLE, Schweizerisches Arbeitsrecht, 4. A., Zürich/St. Gallen 2020
- POSNER ERIC A. / WEYL GLEN E., Radical markets, Princeton/Oxford 2018
- POULLET YVES 2010, About the E-Privacy Directive: towards a third generation of data protection legislation?, in: Gutwirth Serge / Pouillet Yves / De Hert Paul (Hg.): Data

- protection in a profiled world, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2010, 3–30
- POULLET YVES 2013, Conclusion, in: Pollet-Panoussis Delphine (Hg.): *Circuler dans la société numérique: droits et limites*, Paris 2013, 147–157
- PRIEUR YVONNE, Datenschutz durch «Big Data-Geschäfte» auf dem Prüfstand, Aktuelle Juristische Praxis, 2015, 1643–1653
- PROSSER WILLIAM L., Privacy, California Law Review, 1960, 383–423
- PURTOVA NADEZHDA N. 2011, Property rights in personal data, Oisterwijk (Niederlande) 2011
- PURTOVA NADEZHDA N. 2018, The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 2018, 40–81
- RAAB CHRISTIAN / WRIGHT DAVID, Surveillance: extending the limits of privacy impact assessment, in: Wright David / De Hert Paul (Hg.): *Privacy impact assessment*, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2012, 363–383
- RALLO LOMBARTE ARTEMI, The Madrid Resolution and prospects for transnational PIAs, in: Wright David / De Hert Paul (Hg.): *Privacy impact assessment*, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2012, 385–396
- RAM MOHAN RAO P. / MURALI KRISHNA S. / SIVA KUMAR A. P., Privacy preservation techniques in big data analytics: a survey, Journal of Big Data, 2018, 1–12
- Rat der Europäischen Union, Recommendation on addressing the deficiencies identified in the 2018 evaluation of Switzerland on the application of the Schengen acquis in the field of data protection (interinstitutional file: 2019/0024(NLE)), 08.03.2019, abrufbar unter <www.consilium.europa.eu> (besucht am 31.05.2020)
- RAY JEAN-EMMANUEL, Le traçage du salarié: mise en perspectives, in: Pollet-Panoussis Delphine (Hg.): *Circuler dans la société numérique: droits et limites*, Paris 2013, 29–40
- REHBINDER MANFRED / STÖCKLI JEAN-FRITZ, Berner Kommentar, Art. 319–330b OR, Einzelarbeitsvertrag, Bern 2010
- REICHENBACH HANS, The direction of time (edited by Maria Reichenbach, reissued with new foreword by Hilary Putnam), Berkeley/Los Angeles/Oxford 1991
- REINDL CORNELIA / KRÜGL STEFANIE, People Analytics in der Praxis, Freiburg 2017
- REINSCH ROGER W. / GOLTZ SONIA, The law and business of people analytics: Big data: Can the attempt to be more discriminating be more discriminatory instead?, Saint Louis University Law Journal, 2016, 35–63
- REISMAN DILLION / SCHULTZ JASON / CRAWFORD KATE / WHITTAKER MEREDITH, Algorithmic impact assessments: a practical framework for public agency accountability, 04.2018, abrufbar unter <<https://ainowinstitute.org>> (besucht am 31.05.2020)
- RESCH WOLFGANG, Zertifizierungen im Datenschutzbereich, in: Schweighofer Erich / Kummer Franz / Saarenpää Ahti (Hg.): *Internet of Things*, Tagungsband des 22. internationalen Rechtsinformatik-Symposiums, Salzburg 21.–23.02.2019, Bern 2019, 215–220
- RICHARDS NEIL M., Intellectual privacy, New York (New York) 2015

- RICHARDS NEIL M. / HARTZOG WOODROW 2016, Taking trust seriously in privacy law, *Stanford Technology Law Review*, 2016, 431–472
- RICHARDS NEIL M. / HARTZOG WOODROW 2017, Privacy's trust gap: a review of «Obfuscation: a user's guide for privacy and protest» by Finn Brunton and Helen Nissenbaum, *Yale Law Journal*, 2017, 1180–1224
- RICHARDS NEIL M. / KING JONATHAN H., Big data ethics, *Wake Forest Law Review*, 2014, 393–432
- RICHTER PHILIPP, Big Data, Statistik und die Datenschutz-Grundverordnung, *Datenschutz und Datensicherheit*, 2016, 581–586
- RIEDY MARIAN K. / WEN JOSEPH H., Electronic surveillance of internet access in the American workplace: implications for management, *Information & Communications Technology Law*, 2010, 87–99
- RIESELMAHN-SAXER REBECCA, *Datenschutz im privatrechtlichen Arbeitsverhältnis*, Bern 2002, Diss. Zürich 2002
- RITZER CHRISTOPH, Verhaltensregeln (Code of Conduct) im Datenschutz – Gestaltungsmöglichkeiten für Unternehmen in Verbänden, in: Taeger Jürgen (Hg.): *Big Data & Co*, Tagungsband Herbstakademie 2014 DSRI, Mainz 10.–13.09.2014, Edewecht (Niedersachsen) 2014, 501–512
- ROBERTS JESSICA L., Healthism and the law of employment discrimination, *Iowa Law Review*, 2014, 571–636
- ROESSLER BEATE / MOKROSINSKA DOROTA, Privacy and social interaction, *Philosophy & Social Criticism*, 2013, 771–791
- ROMEI ANDREA / RUGGIERI SALVATORE, A multidisciplinary survey on discrimination analysis, *The Knowledge Engineering Review*, 2014, 582–638
- ROMEIKE FRANK, Risikokategorien im Überblick, in: Romeike Frank (Hg.): *Modernes Risikomanagement*, Weinheim 2005, 17–32
- ROSENBLAT ALEX / KNEESE TAMARA / BOYD DANAH, Workplace surveillance, 08.10.2014, abrufbar unter <<https://papers.ssrn.com>> (besucht am 31.05.2020)
- ROSENBLAT ALEX / WIKELIUS KATE / BOYD DANAH / GANGADHARAN SEETA PEÑA / YU CORINE, Data & civil rights: employment primer, 30.10.2014, abrufbar unter <www.datacivilrights.org> (besucht am 31.05.2020)
- ROSENTHAL DAVID 2012, Das Bauchgefühl im Datenschutz, in: *Von der Lochkarte zum Mobile Computing*, 20 Jahre Datenschutz in der Schweiz, Zürich 2012, 69–91
- ROSENTHAL DAVID 2015, Sanktionierung von Datenschutzverstößen, in: Passadelis Nicolas / Rosenthal David / Thür Hanspeter (Hg.): *Datenschutzrecht*, Basel 2015, 203–244
- ROSENTHAL DAVID 2017a, Personendaten ohne Identifizierbarkeit?, *digma – Zeitschrift für Datenrecht und Informationssicherheit*, 2017, 198–203
- ROSENTHAL DAVID 2017b, Der Entwurf für ein neues Datenschutzgesetz, *Jusletter*, 27.11.2017
- ROSSI ARIANNA / HAAPIO HELENA, Proactive legal design: embedding values in the design of legal artefacts, in: Schweighofer Erich / Kummer Franz / Saarenpää Ahti (Hg.): In-

- ternet of Things, Tagungsband des 22. internationalen Rechtsinformatik-Symposiums, Salzburg 21.–23.02.2019, Bern 2019, 537–544
- RÖSSLER BEATE 2001, Der Wert des Privaten, Frankfurt am Main 2001, Habil. Bremen 2001
- RÖSSLER BEATE 2002, Den Wert des Privaten ergründen, *digma – Zeitschrift für Datenrecht und Informationssicherheit*, 2002, 106–113
- ROSSNAGEL ALEXANDER, Informationelle Selbstbestimmung in der Welt des Ubiquitous Computing, in: Mattern Friedemann (Hg.): *Die Informatisierung des Alltags*, Berlin/Heidelberg 2007, 265–290
- ROTH MONIKA, Kompetenz und Verantwortung: Non-Compliance als strategisches Risiko, Zürich/St. Gallen 2012
- RUBINSTEIN IRA S., Regulating privacy by design, *Berkeley Technology Law Journal*, 2011, 1409–1456
- RUDIN BEAT 1998, Kollektives Gedächtnis und informationelle Integrität, *Aktuelle Juristische Praxis*, 1998, 247–260
- RUDIN BEAT 2001, Was darf die Chefin, was die Angestellte? Arbeits- und datenschutzrechtliche Schranken der technischen Überwachung der Internet-Nutzung am Arbeitsplatz, *digma – Zeitschrift für Datenrecht und Informationssicherheit*, 2001, 4–11
- RUDIN BEAT 2002, Datenschutzaufsicht – vom Kontrolleur zum Kompetenzzentrum, in: Baeriswyl Bruno / Rudin Beat (Hg.): *Perspektive Datenschutz, Praxis und Entwicklungen in Recht und Technik*, Zürich/Basel/Genf 2002, 373–420
- RUDIN BEAT 2004a, Anonymität in einer vernetzten Welt, *digma – Zeitschrift für Datenrecht und Informationssicherheit*, 2004, 4–5
- RUDIN BEAT 2004b, Die Erosion der informationellen Privatheit – oder: Rechtsetzung als Risiko?, in: Sutter-Somm Thomas / Hafner Felix / Schmid Gerhard / Seelmann Kurt (Hg.): *Risiko und Recht, Festgabe zum Schweizerischen Juristentag 2004*, Basel 2004, 415–440
- RUDIN BEAT 2007, *Datenschutzgesetze – fit für Europa*, Zürich/Basel/Genf 2007
- RUDIN BEAT 2008, Das Recht auf Anonymität, *digma – Zeitschrift für Datenrecht und Informationssicherheit*, 2008, 6–13
- RUDIN BEAT 2010, Datenschutzkonzept auf dem Prüfstand, *digma – Zeitschrift für Datenrecht und Informationssicherheit*, 2010, 130–139
- RUDOLPH ROGER, Das Recht des Arbeitnehmers auf Einsicht in sein Personaldossier, *Aktuelle Juristische Praxis*, 2014, 1672–1683
- RUHLAND ROBERT MALTE, Big Data in mitbestimmten Unternehmen – Fallstricke und Lösungen, in: Taeger Jürgen (Hg.): *Big Data & Co, Tagungsband Herbstakademie 2014 DSRI*, Mainz 10.–13.09.2014, Edewecht (Niedersachsen) 2014, 89–102
- RULE JAMES B., *Privacy in peril: how we are sacrificing a fundamental right in exchange for security and convenience*, Oxford 2009
- RUUD FLEMMING T. / ISUFI SHQIPONJA / FRIEBE PHILIPP / STEBLER WERNER / SEHERI FATMA / EMMENEGGER MURIEL, *Wie schneiden Sie ab? Studie über Kontroll- und Prüfungsak-*

- tivitäten bei mittelgrossen Unternehmen, Spitälern und Hochschulen der Schweiz, Zürich 2008
- SAARENPÄÄ AHTI, Pseudonymous identifiability as a societal problem, in: Schweighofer Erich / Kummer Franz / Saarenpää Ahti (Hg.): Internet of Things, Tagungsband des 22. internationalen Rechtsinformatik-Symposiums, Salzburg 21.–23.02.2019, Bern 2019, 93–100
- SAURWEIN FLORIAN, Automatisierung, Algorithmen, Accountability. Eine Governance Perspektive, in: Rath Matthias / Krotz Friedrich / Karmasin Matthias (Hg.): Maschinenethik: normative Grenzen autonomer Systeme, Wiesbaden 2019, 35–56
- SBB, GAV SBB, Bern 2015
- SCHAAR PETER 2007, Das Ende der Privatsphäre, München 2007
- SCHAAR PETER 2010, Privacy by Design, Identity in the Information Society, 2010, 267–274
- SCHEFZIG JENS, Big Data = Personal Data? Der Personenbezug von Daten bei Big Data-Analysen, in: Taeger Jürgen (Hg.): Big Data & Co, Tagungsband Herbstakademie 2014 DSRI, Mainz 10.–13.09.2014, Edewecht (Niedersachsen) 2014, 103–118
- SCHERMER BART W. / CUSTERS BART / VAN DER HOF SIMONE, The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, Ethics and Information Technology, 2014, 87
- SCHIEDERMAIR STEPHANIE, Der Schutz des Privaten als internationales Grundrecht, Tübingen 2012, Habil. Mainz 2012
- SCHILLER FRIEDRICH, Don Carlos, Infant von Spanien (Uraufführung Hamburg 1787), Stuttgart 1979
- SCHINAGL WOLFGANG, Der digitale Mensch als Defizitmodell. IoT-Cyborgisierung, künstliche Intelligenz und Ich-Virtualisierung, in: Schweighofer Erich / Kummer Franz / Saarenpää Ahti (Hg.): Internet of Things, Tagungsband des 22. internationalen Rechtsinformatik-Symposiums, Salzburg 21.–23.02.2019, Bern 2019, 499–508
- SCHMIDT KIRSTEN JOHANNA, Datenschutz als Vermögensrecht, Heidelberg 2020, Diss. Basel 2019
- SCHNABL WOLFGANG, Datenschutz und Informationssicherheit – ein natürlicher Gegensatz?, Jusletter IT, 24.05.2018
- SCHRÖDER PETER, Naturrecht und absolutistisches Staatsrecht, Berlin 2001, Diss. Marburg 1999
- SCHULZ SEBASTIAN, Datenschutz-Folgenabschätzung, Privacy in Germany, 2018, 97–99
- SCHULZE MARC-OLIVER, Datenschutz am Arbeitsplatz VI., in: Wedde Peter (Hg.): Handbuch Datenschutz und Mitbestimmung, Frankfurt am Main 2016, 133–163
- SCHÜRER HANS UELI, Datenschutz im Arbeitsverhältnis, Zürich 1996
- SCHWEIZER RAINER J., Geschichte und Zukunft des Datenschutzrechts, in: Passadelis Nicolas / Rosenthal David / Thür Hanspeter (Hg.): Datenschutzrecht, Basel 2015, 3–40
- SCHWEIZER RAINER J. / RECHSTEINER DAVID, Grund- und menschenrechtlicher Datenschutz, in: Passadelis Nicolas / Rosenthal David / Thür Hanspeter (Hg.): Datenschutzrecht, Basel 2015, 41–70

- Schweizerischer Bundesrat 2012, Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 09.12.2011, Bundesblatt, 2012, 335–352
- Schweizerischer Bundesrat 2013a, Kollektiver Rechtsschutz in der Schweiz – Bestandesaufnahme und Handlungsmöglichkeiten, Bern 03.07.2013
- Schweizerischer Bundesrat 2013b, Rechtliche Basis für Social Media, Bericht des Bundesrates in Erfüllung des Postulats Amherd 11.3912 vom 29.09.2011, 09.10.2013, abrufbar unter <www.admin.ch> (besucht am 31.05.2020)
- Schweizerischer Bundesrat 2016a, Recht auf Schutz vor Diskriminierung: Bericht des Bundesrates in Erfüllung des Postulats Naef 12.3543 vom 14.06.2012, 25.05.2016, abrufbar unter <www.parlament.ch> (besucht am 31.05.2020)
- Schweizerischer Bundesrat 2016b, Rechtliche Folgen der Telearbeit, 16.11.2016, abrufbar unter <www.ejpd.admin.ch> (besucht am 31.05.2020)
- Schweizerischer Bundesrat 2017a, Bericht über die zentralen Rahmenbedingungen für die digitale Wirtschaft, 11.01.2017, abrufbar unter <www.newsd.admin.ch> (besucht am 31.05.2020)
- Schweizerischer Bundesrat 2017b, Auswirkungen der Digitalisierung auf Beschäftigung und Arbeitsbedingungen – Chancen und Risiken, 08.11.2017, abrufbar unter <www.newsd.admin.ch> (besucht am 31.05.2020)
- Schweizerischer Bundesrat 2018, Stellungnahme zur Interpellation 18.3281: Welche Auswirkungen hat der Rückstand der Schweiz beim Datenschutz?, 09.05.2018, abrufbar unter <www.parlament.ch> (besucht am 31.05.2020)
- Schweizerischer Bundesrat 2020, Zivilprozessordnung: Zugang zum Gericht soll leichter werden, 26.02.2020, abrufbar unter <www.bj.admin.ch> (besucht am 31.05.2020)
- SECO 2003, Weisungen und Erläuterungen zum Bundesgesetz über die Arbeitsvermittlung und den Personalverleih vom 06.10.1989, zur Verordnung über die Arbeitsvermittlung und den Personalverleih vom 16.01.1991 und zur Verordnung über Gebühren, Provisionen und Kautionen im Bereich des Arbeitsvermittlungsgesetzes vom 16.01.1991, Bern 01.2003
- SECO 2018, Wegleitung zur Verordnung 3 zum Arbeitsgesetz, Bern 05.2018
- SECO 2019, [Direktauskunft betreffend People Analytics] (E-Mail vom 10.01.2019)
- SEGARS ALBERT H., Seven technologies remaking the world, MIT Sloan Management Review March, 2018, 1–19
- SGB, Gewerkschaften und andere Arbeitnehmerorganisationen: Zahl der Mitglieder, 16.05.2019, abrufbar unter <www.bfs.admin.ch> (besucht am 31.05.2020)
- SGK: Ehrenzeller Bernhard / Schindler Benjamin / Schweizer Rainer J. / Vallender Klaus A. (Hg.), Die Schweizerische Bundesverfassung, St. Galler Kommentar, 3. A., Zürich 2014 (zit. SGK-BEARBEITER)
- SHK DSG: Baeriswyl Bruno / Pärli Kurt (Hg.), Datenschutzgesetz (DSG), Bern 2015 (zit. SHK DSG-BEARBEITER)

- SHOOK ELLYN / SAGE-GAVIN EVA / CANTRELL SUSAN, How companies can use employee data responsibly, Harvard Business Review, 15.02.2019, abrufbar unter <<https://hbr.org>> (besucht am 31.05.2020)
- SIEGENTHALER MARKUS, Die Effektivität der Durchsetzungsmechanismen aus der Sicht der Kantone, in: Epiney Astrid / Nüesch Daniela (Hg.): Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes, La mise en œuvre des droits des particuliers dans le domaine de la protection des données, Zürich/Basel/Genf 2015, 107–114
- SIGRIST JAN, Datensicherheit bei genetischen Untersuchungen beim Menschen, Jusletter, 28.05.2018
- SLATER DAN / ZIBLATT DANIEL, The enduring indispensability of the controlled comparison, Comparative Political Studies, 2013, 1301–1327
- SNYDER TIMOTHY M., You're fired! A case for agency moderation of machine data in the employment context, George Mason Law Review, 2016, 243–283
- SOLOVE DANIEL J., Understanding privacy, Cambridge (Massachusetts)/London (England) 2008
- SOLOVE DANIEL J. / HARTZOG WOODROW, The FTC and the new common law of privacy, Columbia Law Review, 2014, 583–676
- SOLOVE DANIEL J. / KEATS CITRON DANIELLE, Risk and anxiety: a theory of data-breach harms, Texas Law Review, 2018, 737–786
- SPIEKERMANN SARAH, The RFID PIA – developed by industry, endorsed by regulators, in: Wright David / De Hert Paul (Hg.): Privacy impact assessment, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2012, 323–346
- SPRAGUE ROBERT 2013, Workplace data and information: an introduction, in: Sprague Robert (Hg.): Workplace data, Arlington (Virginia) 2013, 1-1 – 1-6 [sic]
- SPRAGUE ROBERT 2015, Welcome to the machine: privacy and workplace implications of predictive analytics, Richmond Journal of Law & Technology 4, 2015, 1–46
- STAN OANA MARA, Steps towards sustainability – human resource capital and employee wellbeing – benchmarking evidence, Economics, Management and Financial Markets, 2018, 290–300
- STAUB LEO, Risikomanagement in der Anwaltskanzlei, Einführung und Übersicht, in: Staub Leo / Hehli Hidber Christine (Hg.): Management von Anwaltskanzleien, Zürich/Basel/Genf 2012, 695–724
- STEIGERT VERENA KAREN, Datenschutz bei unternehmensinternen Whistleblowing-Systemen, Frankfurt am Main 2013, Diss. Münster (Westfalen) 2012
- STEINAUER PAUL-HENRI, Le droit d'action des associations visant à défendre la personnalité de leurs membres, en particulier en matière de protection des données, in: Brem Ernst / Druey Jean Nicolas / Kramer Ernst A. / Schwander Ivo (Hg.): Festschrift zum 65. Geburtstag von Mario M. Pedrazzini, Bern 1990, 495–510
- STEINBUCH KARL, Masslos informiert, München/Berlin 1978
- STEINER REGINA, Aktuelle Einzelthemen, in: Wedde Peter (Hg.): Handbuch Datenschutz und Mitbestimmung, Frankfurt am Main 2016, 263–296

- STELZER HARALD / VELJANOVA HRISTINA, Why do we need both soft (post-compliance) ethics and legal compliance in the digital transformation?, in: Schweighofer Erich / Kummer Franz / Saarenpää Ahti (Hg.): Internet of Things, Tagungsband des 22. internationalen Rechtsinformatik-Symposiums, Salzburg 21.–23.02.2019, Bern 2019, 153–160
- STIEMERLING OLIVER, Löschen: Mission Impossible?, Privacy in Germany, 2018, 93–96
- STODDART JENNIFER, Auditing privacy impact assessments: the Canadian experience, in: Wright David / De Hert Paul (Hg.): Privacy impact assessment, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2012, 419–436
- STONE KATHERINE V.W., The decline of the standard contract of employment in the United States: a socio-regulatory perspective, in: Stone Katherine V. W. / Arthurs Harry (Hg.): Rethinking workplace regulation, New York (New York) 2013, 58–78
- STRAHILEVITZ LIOR JACOB 2005, A social networks theory of privacy, University of Chicago Law Review, 2005, 919–988
- STRAHILEVITZ LIOR JACOB 2013, Toward a positive theory of privacy law, Harvard Law Review, 2013, 2010–2042
- STREIFF ULLIN / VON KAENEL ADRIAN / RUDOLPH ROGER, Arbeitsvertrag, Praxiskommentar zu Art. 319–362 OR, 7. A., Zürich 2012
- STUTZ MICHÈLE / VALLONI NOEMI, Social Media im Arbeitsrecht, in: Staffelbach Oliver / Keller Claudia (Hg.): Social Media und Recht für Unternehmen, Zürich 2015, 159–187
- SUPPES PATRICK, A probabilistic theory of causality, Amsterdam 1970
- SWEENEY LATANYA, Simple demographics often identify people uniquely, Pittsburgh 2000
- TA VINH THONG, Privacy by design: on the formal design and conformance check of personal data protection policies and architectures, 15.05.2018, abrufbar unter <www.semanticscholar.org> (besucht am 31.05.2020)
- TALIDOU ZOI, Regulierte Selbstregulierung im Bereich des Datenschutzes, Frankfurt am Main 2005, Diss. Freiburg im Breisgau 2005
- TAMÒ-LARRIEUX AURELIA, Designing for privacy and its legal framework, Cham 2018, Diss. Zürich 2018
- TENE OMER / POLONETSKY JULES, A theory of creepy: technology, privacy and shifting social norms, Yale Journal of Law & Technology, 2014, 59–102
- The Kaiser Family Foundation / Health Research and Educational Trust, Employer health benefits, Menlo Park (Kalifornien)/Chicago (Illinois) 2014
- THELISSON EVA / PADH KIRTAN / CELIS ELISA L., Regulatory mechanisms and algorithms towards trust in AI/ML, in: Aha David W. / Darrell Trevor / Pazzani Michael / Reid Darryn / Sammut Claude / Stone Peter (Hg.): IJCAI-17 workshop on explainable AI (XAI) proceedings, Melbourne (Australien) 20.08.2017, abrufbar unter <<https://ijcai-17.org>> (besucht am 31.05.2020), 53–57
- THIERER ADAM, The pursuit of privacy in a world where information control is failing, Harvard Journal of Law & Public Policy, 2013, 409–455

- THOMAS RICHARD, Accountability – a modern approach to regulate the 21st century data environment, in: Hijmans Hielke / Kranenborg Herke (Hg.): Data protection anno 2014: how to restore trust?, Cambridge (Grossbritannien) 2014, 135–147
- THOUVENIN FLORENT 2014, Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data, in: Weber Rolf H. / Thouvenin Florent (Hg.): Big Data und Datenschutz – gegenseitige Herausforderungen, Zürich/Basel/Genf 2014, 61–83
- THOUVENIN FLORENT 2017, Forschung im Spannungsfeld von Big Data und Datenschutzrecht: eine Problemskizze, in: Boehme-Nessler Volker / Rehbindner Manfred (Hg.): Big Data: Ende des Datenschutzes?, Gedächtnisschrift für Martin Usteri, Bern 2017, 27–53
- THOUVENIN FLORENT / FRÜH ALFRED 2019, Automatisierte Entscheidungen: Perspektive Privatrecht (Vortrag), SF-FS/ITSL-Tagung Automatisierte Entscheidungen, Zürich 13.11.2019
- THOUVENIN FLORENT / FRÜH ALFRED 2020, Automatisierte Entscheidungen: Grundfragen aus der Perspektive des Privatrechts, Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht, 2020, 3–17
- THOUVENIN FLORENT / FRÜH ALFRED / GEORGE DAMIAN, Datenschutz und automatisierte Entscheidungen, Jusletter, 26.11.2018
- THOUVENIN FLORENT / WEBER ROLF H. / FRÜH ALFRED, Elemente einer Datenpolitik, Zürich/Basel/Genf 2019
- THÜR HANSPETER, Privatsphäre im Internetzeitalter: Möglichkeiten und Grenzen der Datenschützer, in: Boehme-Nessler Volker / Rehbindner Manfred (Hg.): Big Data: Ende des Datenschutzes?, Gedächtnisschrift für Martin Usteri, Bern 2017, 73–81
- THÜSING GREGOR / TRAUT JOHANNES, Social Media in Betrieb und Unternehmen, in: Thüsing Gregor (Hg.): Beschäftigtendatenschutz und Compliance, Effektive Compliance im Spannungsfeld von BDSG, Persönlichkeitsschutz und betrieblicher Mitbestimmung, München 2014, 1–69
- TREITL VERONIKA, The coupling ban in data protection law – a first approach, in: Schweighofer Erich / Kummer Franz / Saarenpää Ahti (Hg.): Internet of Things, Tagungsband des 22. internationalen Rechtsinformatik-Symposiums, Salzburg 21.–23.02.2019, Bern 2019, 117–124
- TRINDEL KELLY, Big data in the workplace: examining implications for equal employment opportunity law, written testimony (Vortrag), Meetings and hearings of the EEOC, 13.10.2016, abrufbar unter <www.eeoc.gov> (besucht am 31.05.2020)
- TSCHENTSCHER AXEL, Recht und Macht, in: Pichonnaz Pascal / Vogt Nedim Peter / Wolf Stephan (Hg.): Festschrift für Bruno Huwiler zum 65. Geburtstag, Bern 2007, 625–640
- TÜRK ALEX, Positionnement du débat: panorama des techniques et du champ d'application du traçage, in: Pollet-Panoussis Delphine (Hg.): Circuler dans la société numérique: droits et limites, Paris 2013, 13–22
- UNICEF, Policy guide on children and digital connectivity, New York (New York) 06.2018
- UNO, Guiding principles on business and human rights, New York (New York)/Genf 2011

- UNO Generalversammlung, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348, 29.08.2018, abrufbar unter <<https://undocs.org>> (besucht am 31.05.2020)
- UTTINGER URSULA, Verwertbarkeit von Dashcam-Aufnahmen als Beweismittel im Unfallschlichtungsprozess, Jusletter, 01.10.2018
- VAN DEN HOVEN VAN GENDEREN ROBERT, Robo sapiens and data protection, Jusletter IT, 24.05.2018
- VASELLA DAVID / ROSENTHAL DAVID, Information und Einwilligung bei HR Analytics (Vortrag), FAA-Tagung Big Data am Arbeitsplatz: arbeits- und datenschutzrechtliche Fragen rund um Workforce Analytics, Zürich 16.10.2018
- VEALE MICHAEL / BINNS REUBEN, Fairer machine learning in the real world: mitigating discrimination without collecting sensitive data, Big Data & Society 2, 2017, 1–17
- VEALE MICHAEL / BINNS REUBEN / AUSLOOS JEF, When data protection by design and data subject rights clash, International Data Privacy Law, 2018, 105–123
- VON ARNAULD ANDREAS, Big Data, Internet und das Völkerrecht, in: Hoffmann-Riem Wolfgang (Hg.): Big Data – Regulative Herausforderungen, Baden-Baden 2018, 117–123
- VON MALTZAN STEPHANIE, Informationsextraktion und die DSGVO, in: Schweighofer Erich / Kummer Franz / Saarenpää Ahti (Hg.): Internet of Things, Tagungsband des 22. internationalen Rechtsinformatik-Symposiums, Salzburg 21.–23.02.2019, Bern 2019, 207–214
- WACHTER SANDRA / MITTELSTADT BRENT, A right to reasonable inferences: re-thinking data protection law in the age of big data and AI, Columbia Business Law Review, 2019, 494–620
- WACHTER SANDRA / MITTELSTADT BRENT / RUSSEL CHRIS, Counterfactual explanations without opening the black box: automated decisions and the GDPR, Harvard Journal of Law & Technology, 2018, 841–887
- WALDMAN ARI EZRA, Privacy as trust, Cambridge (Großbritannien) 2018
- WALTER JEAN-PHILIPPE, L'effectivité des mécanismes de mise en œuvre de la protection des données, in: Epiney Astrid / Nüesch Daniela (Hg.): Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes, La mise en œuvre des droits des particuliers dans le domaine de la protection des données, Zürich/Basel/Genf 2015, 115–123
- WATL BERNHARD / VOGL ROLAND, Explainable artificial intelligence – the new frontier in legal informatics, Jusletter IT, 22.02.2018
- WARREN SAMUEL D. / BRANDEIS LOUIS D., The right to privacy, Harvard Law Review, 1890, 193–220
- WARTER JOHANNES, Löschkonzept, Jusletter IT, 22.02.2018
- WEAVER GARY R. / TREVIÑO LINDA KLEBE / CHOCHRAN PHILIP L., Corporate ethics practices in the mid-1990's: an empirical study of the fortune 1000, Journal of Business Ethics, 1999, 283–294
- WEAVER JOSHUA D., Predicting employee performance using text data from resumes, Ann Arbor (Michigan) 2017

- WEBER ROLF H. 2014, Big Data: Rechtliche Perspektive, in: Weber Rolf H. / Thouvenin Florent (Hg.): Big Data und Datenschutz – gegenseitige Herausforderungen, Zürich/Basel/Genf 2014, 17–29
- WEBER ROLF H. 2015, Big Data: Sprengkörper des Datenschutzrechts?, in: Weber Rolf H. (Hg.): Datenschutz – zum Aufstieg einer neuen Rechtsdisziplin, Bern 2015, 449–466
- WEBER ROLF H. 2018, Big Data – rechtliche Grenzen von unbegrenzten Möglichkeiten, in: Fuhrer Stephan (Hg.): Jahrbuch SGHVR 2018, Annales SDRCA 2018, Zürich/Basel/Genf 2018, 87–110
- WEBER ROLF H. / OERTLY DOMINIC, Aushöhlung des Datenschutzes durch De-Anonymisierung bei Big Data Analytics?, in: Weber Rolf H. (Hg.): Datenschutz – zum Aufstieg einer neuen Rechtsdisziplin, Bern 2015
- WEDDE PETER 2016a, Der Datenschutzbeauftragte, in: Wedde Peter (Hg.): Handbuch Datenschutz und Mitbestimmung, Frankfurt am Main 2016, 251–262
- WEDDE PETER 2016b, Einleitung: Worum geht es beim Datenschutz?, in: Wedde Peter (Hg.): Handbuch Datenschutz und Mitbestimmung, Frankfurt am Main 2016, 35–44
- WEDDE PETER 2016c, Beschäftigtendatenschutz: rechtlicher Rahmen und Handlungsmöglichkeiten für Betriebsräte (MitbestimmungsPraxis), Düsseldorf 06.2016
- WEIBEL ANTOINETTE / SCHAFHEITLE SIMON / EBERT ISABEL, Goldgräberstimmung im Personalmanagement?, Organisationsentwicklung, Zeitschrift für Unternehmensentwicklung und Change Management 3, 2019, 23–29
- WEICHERT THILO, Big Data und Datenschutz, Zeitschrift für Datenschutz, 2013, 251–259
- WESPI ANDREAS, Big Data: technische Perspektive, in: Weber Rolf H. / Thouvenin Florent (Hg.): Big Data und Datenschutz – gegenseitige Herausforderungen, Zürich/Basel/Genf 2014, 3–16
- WEST JONATHAN P. / BOWMAN JAMES S. / GERTZ SALLY, Electronic surveillance in the workplace, in: Sims Ronald R. / Sauser William I., Jr. (Hg.): Legal and regulatory issues in human resources management, Charlotte (North Carolina) 2015, 285–314
- WESTIN ALAN F., Social and political dimensions of privacy, Journal of Social Issues, 2003, 431–453
- White House, Executive Office of the President 2014, Big data: seizing opportunities, preserving values, Washington (D.C.) 01.05.2014
- White House, Executive Office of the President 2015, Big data: seizing opportunities, preserving values. Interim progress report, Washington (D.C.) 02.2015
- White House, Executive Office of the President 2016, Big data: a report on algorithmic systems, opportunity, and civil rights, Washington (D.C.) 05.2016
- WILDHABER ISABELLE 2011, Das Arbeitsrecht bei Umstrukturierungen, Zürich 2011, Habil. Zürich 2011
- WILDHABER ISABELLE 2016, Die Roboter kommen – Konsequenzen für Arbeit und Arbeitsrecht, Zeitschrift für Schweizerisches Recht, 2016, 315–352
- WILDHABER ISABELLE 2017, Robotik am Arbeitsplatz: Robo-Kollegen und Robo-Bosse, Aktuelle Juristische Praxis, 2017, 213–224

- WILDHABER ISABELLE / HÄNSENBERGER SILVIO 2015, Kündigung wegen Nutzung von Social Media, in: Gschwend Lukas / Hettich Peter / Müller-Chen Markus / Schindler Benjamin / Wildhaber Isabelle (Hg.): Recht im digitalen Zeitalter, Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, 399–430
- WILDHABER ISABELLE / HÄNSENBERGER SILVIO 2016, Internet am Arbeitsplatz, Zeitschrift des bernischen Juristenvereins, 2016, 307–341
- WILDHABER ISABELLE / HÄNSENBERGER SILVIO 2017, Social Media-Kontakte im Arbeitsverhältnis, Wem «gehören» Accounts, Kontakte und Zugangsdaten?, in: Müller Roland A. / Pärli Kurt / Wildhaber Isabelle / Geiser Thomas (Hg.): Arbeit und Arbeitsrecht, Festschrift für Thomas Geiser zum 65. Geburtstag, Zürich/St. Gallen 2017, 529–548
- WILDHABER ISABELLE / KASPER GABRIEL, Quantifizierte Arbeitnehmer: empirische Daten zu People Analytics in der Schweiz, in: Müller Roland A. / Rudolph Roger / Schnyder Anton K. / von Kaenel Adrian / Waas Bernd (Hg.): Festschrift für Wolfgang Portmann, Zürich/Basel/Genf 2020, 755–771
- WILDHABER ISABELLE / LOHMANN MELINDA F., Roboterrecht – eine Einleitung, Aktuelle Juristische Praxis, 2017, 135–140
- WILDHABER ISABELLE / LOHMANN MELINDA F. / KASPER GABRIEL, Diskriminierung durch Algorithmen – Überlegungen zum schweizerischen Recht am Beispiel prädiktiver Analytik am Arbeitsplatz, Zeitschrift für Schweizerisches Recht, 2019, 459–489
- WILSON JAMES H. / DAUGHERTY PAUL R., Human + machine: reimagining work in the age of AI, Boston 2018
- WILSON REBECCA J. / BELLIVEAU KILEY M. / GRAY LEIGH ELLEN, Busting the black box: big data, employment and privacy, Defense Counsel Journal, 2017, 2–34
- WINICK ERIN, Your boss is now more likely to train you up, thanks to a dwindling talent pool, MIT Technology Review, 07.11.2018, abrufbar unter <www.technologyreview.com> (besucht am 31.05.2020)
- WOLFER SIMON, Die elektronische Überwachung des Arbeitnehmers im privatrechtlichen Arbeitsverhältnis, Zürich 2008, Diss. Luzern 2008
- WOLTER MARC INGO / MÖNNIG ANKE / HUMMEL MARKUS / WEBER ENZO / ZIKA GERD / HELMRICH ROBERT / MAIER TOBIAS / NEUBER-POHL CAROLINE, IAB Forschungsbericht 13/2016: Wirtschaft 4.0 und die Folgen für Arbeitsmarkt und Ökonomie, Nürnberg 09.11.2016
- WOOD ALEXANDRA / ALTMAN MICAH / BEMBENEK AARON / BUN MARK / GABOARDI MARCO / HONAKER JAMES / NISSIM KOBBI / O'BRIEN DAVID R. / STEINKE THOMAS / VADHAN SALIL, Differential privacy: a primer for a non-technical audience, Vanderbilt Journal of Entertainment and Technology Law, 2018, 209–276
- World Economic Forum 2013, Unlocking the value of personal data: from collection to usage, Cologny/Genf 02.2013
- World Economic Forum 2014, Rethinking personal data: a new lens for strengthening trust, Cologny/Genf 05.2014

- WRIGHT DAVID / DE HERT PAUL 2012a, Findings and recommendations, in: Wright David / De Hert Paul (Hg.): Privacy impact assessment, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2012, 445–481
- WRIGHT DAVID / DE HERT PAUL 2012b, Introduction to privacy impact assessment, in: Wright David / De Hert Paul (Hg.): Privacy impact assessment, Dordrecht (Niederlande)/Heidelberg/London/New York (New York) 2012, 3–32
- WRIGLEY SAM, Taming artificial intelligence: «bots», the GDPR and regulatory approaches, in: Corrales Marcelo / Fenwick Mark / Forgó Nikolaus (Hg.): Robotics, AI and the future of law, Singapur 2018, 183–208
- WYBITUL TIM / SCHULTZE-MELLING JYN, Datenschutz im Unternehmen, 2. A., Frankfurt am Main 2014
- WYLER RÉMY, La responsabilité civile de l'employeur, y compris en ce qui concerne les actes de ses organes et auxiliaires, Zeitschrift für Arbeitsrecht und Arbeitslosenversicherung, 2011, 249–259
- WYLER RÉMY / HEINZER BORIS, Droit du travail, 4. A., Bern 2019
- YIN ROBERT K., Case study research and applications, 6. A., Thousand Oaks (Kalifornien) 2018
- ZARSKY TAL Z., Understanding discrimination in the scored society, Washington Law Review, 2014, 1375–1412
- ZECH HERBERT, Information als Schutzgegenstand, Tübingen 2012, Habil. Bayreuth 2012
- ZHANG WEIWEN, Videoüberwachung von Arbeitnehmern, Frankfurt am Main 2017, Diss. Passau 2016
- ZINKE MICHAELA, Eine Erweiterung der Verbandsklagebefugnisse auf datenschutzrechtliche Verstöße stärkt den Datenschutz in Zeiten von Big Data, in: Taeger Jürgen (Hg.): Big Data & Co, Tagungsband Herbstakademie 2014 DSRI, Mainz 10.–13.09.2014, Edewecht (Niedersachsen) 2014, 161–170
- ŽLIOBAITĖ INDRE / CUSTERS BART, Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models, Artificial Intelligence and Law, 2016, 183–201
- ZUBOFF SHOSHANA 2015, Big other: surveillance capitalism and the prospects of an information civilization, Journal of Information Technology, 2015, 75–89
- ZUBOFF SHOSHANA 2019, Surveillance capitalism and the challenge of collective action, New Labor Forum, 2019, 10–29
- ZÜST MARTIN, Big brother's watching you at work, Aktuelle Juristische Praxis, 1996, 1475–1487
- ZWEIG KATHARINA A. / KRAFFT TOBIAS, Qualität von algorithmischen Entscheidungen, digma – Zeitschrift für Datenrecht und Informationssicherheit, 2017, 110–115

Materialienverzeichnis

- AB NR 1991 957–982, 88.032 Datenschutzgesetz (Fortsetzung), Protection des données. Loi [sic] (suite)
- AB NR 2019 1774–1802, 17.059 Datenschutzgesetz. Totalrevision und Änderung weiterer Erlasse zum Datenschutz (Erstrat), Loi sur la protection des données. Révision totale et modification d'autres lois fédérales (premier conseil)
- AB NR 2019 1805–1844, 17.059 Datenschutzgesetz. Totalrevision und Änderung weiterer Erlasse zum Datenschutz (Fortsetzung), Loi sur la protection des données. Révision totale et modification d'autres lois fédérales (suite)
- AB NR 2020 278–279, 19.068 Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Übereinkommen (Erstrat, provisorische Fassung), Protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Convention (premier conseil, version provisoire)
- AB SR 1990 125–148, 88.032 Datenschutzgesetz, Protection de données. Loi [sic]
- AB SR 1990 149–166, 88.032 Datenschutzgesetz (Fortsetzung), Protection des données. Loi [sic] (suite)
- AB SR 1991 1063–1069, 88.032 Datenschutzgesetz (Fortsetzung), Protection des données. Loi [sic] (suite)
- AB SR 2019 1238–1252, 17.059 Datenschutzgesetz. Totalrevision und Änderung weiterer Erlasse zum Datenschutz (Zweitrat)
- BBl 1982 II 636–698, Botschaft über die Änderung des Schweizerischen Zivilgesetzbuches (Persönlichkeitsschutz: Art. 28 ZGB und 49 OR) vom 05.05.1982
- BBl 1988 II 413–534, Botschaft zum Bundesgesetz über den Datenschutz vom 23.03.1988
- BBl 1992 520–837, Botschaft II über die Anpassung des Bundesrechts an das EWR-Recht (Zusatzbotschaft II zur EWR-Botschaft) vom 15.06.1992
- BBl 1997 1–642, Botschaft über eine neue Bundesverfassung vom 20.11.1996
- BBl 2006 7221–7412, Botschaft zur Schweizerischen Zivilprozessordnung (ZPO) vom 28.06.2006
- BBl 2017 6941–7192, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.09.2017
- BBl 2017 7193–7276, Entwurf Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz
- BBl 2020 2697–2784, Botschaft zur Änderung der Schweizerischen Zivilprozessordnung (Verbesserung der Praxistauglichkeit und der Rechtsdurchsetzung) vom 26.02.2020
- Bundesamt für Justiz 2018, Erläuternder Bericht zur Änderung der Zivilprozessordnung (Verbesserung der Praxistauglichkeit und der Rechtsdurchsetzung), 02.03.2018, abrufbar unter <www.bj.admin.ch> (besucht am 31.05.2020)

Bundesamt für Justiz 2020, Revision der Zivilprozessordnung (Verbesserung der Praxis-tauglichkeit und der Rechtsdurchsetzung), 29.01.2020, abrufbar unter <www.bj.admin.ch> (besucht am 31.05.2020)

Europäisches Parlament 2014, European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading), Strassburg 12.03.2014

Abbildungsverzeichnis

Abb. 1:	Stichprobe der NFP75-Online-Umfrage nach Belegschaftsgrössen.....	15
Abb. 2:	Stichprobe der NFP75-Online-Umfrage nach Wirtschaftssektoren	16
Abb. 3:	Daten-Lebenszyklus	20
Abb. 4:	Fünf Verwendungszwecke von People Analytics entlang des Arbeitnehmer-Lebenszyklus	43
Abb. 5:	Verbreitung von People Analytics in der Schweiz nach Belegschafts- grössen	60
Abb. 6:	Verbreitung von People Analytics in der Schweiz nach Wirtschaftssektoren ..	61
Abb. 7:	Verbreitung von People Analytics in der Schweiz nach Verwendungszwecken einschliesslich der beliebtesten Technologien	62
Abb. 8:	Beliebteste und seltenste People Analytics-Technologien in der Schweiz	63
Abb. 9:	Datenlöschung in der schweizerischen People Analytics-Praxis	244
Abb. 10:	Einwilligung in der schweizerischen People Analytics-Praxis	246
Abb. 11:	«Arbeitnehmer vertrauen den Vorgesetzten stark.»	308
Abb. 12:	«Vorgesetzte vertrauen den Arbeitnehmern stark.»	309
Abb. 13:	«Es wird stets darauf vertraut, dass Versprechen eingehalten werden.»	310
Abb. 14:	«Es besteht ein sehr hohes Vertrauen im gesamten Unternehmen.»	311

Zusammenfassung

Diese juristische Dissertation widmet sich dem Thema People Analytics in privatrechtlichen Arbeitsverhältnissen. People Analytics bezeichnet das systematische Auswerten digitaler Daten, die sich auf das Humankapital beziehen, um den Unternehmenswert zu steigern. Zunächst ermittelt der Autor die Unterschiede zwischen People Analytics und älteren Überwachungsformen am Arbeitsplatz sowie die daraus resultierenden Rechtsprobleme. Nach der Betrachtung der verschiedenen relevanten Rechtsbestimmungen wird ein Schwerpunkt auf die Analyse des Arbeits- und Datenschutzrechts gesetzt. Zentrale Erkenntnisse sind folgende drei: (1) dass die überwiegend prozeduralen Datenschutzbestimmungen risikoorientiert ausgelegt werden müssen, (2) dass im Arbeitskontext die Einwilligung keinen geeigneten Rechtfertigungsgrund für Datenbearbeitungen darstellt und (3) dass Schwachstellen in der Durchsetzung des privatrechtlichen Datenschutzes bestehen. Gestützt darauf entwickelt der Autor ein Verbesserungskonzept, das auf eine Professionalisierung und Demokratisierung des Datenschutzrechts zielt. Er stellt seinen theoretischen Überlegungen die empirischen Daten gegenüber, welche er zusammen mit einem interdisziplinären Forschungsteam erhoben hat. Die Doktorarbeit berücksichtigt neben dem bestehenden schweizerischen Datenschutzgesetz auch das künftige, totalrevidierte schweizerische Datenschutzgesetz, die EU-Datenschutz-Grundverordnung und ausgewählte Aspekte des US-amerikanischen Datenschutzrechts.

Summary

This legal dissertation is dedicated to the topic of people analytics in private law employment relationships. People analytics refers to the systematic evaluation of digital data relating to human capital in order to increase the value of a company. The author begins by identifying the differences between people analytics and older forms of monitoring in the workplace as well as the resulting legal problems. After considering the various applicable fields of law, he focuses on the analysis of employment and data protection law. The three key findings are as follows: (1) data protection provisions, which are predominantly procedural in nature, must be interpreted in a risk-oriented manner; (2) in the work context, employee consent as a justification for data processing should be avoided; and (3) there are deficiencies in the enforcement of data protection in private law. Based on this, the author develops an improvement concept aimed at professionalising and democratising data protection law. He contrasts his theoretical considerations with the empirical data that he has collected as part of an interdisciplinary research project. In addition to the existing Swiss Data Protection Act, this doctoral thesis takes into account the upcoming, fully revised Swiss Data Protection Act, the EU General Data Protection Regulation and certain aspects of US data protection law.

Résumé

Cette thèse juridique traite du thème People Analytics dans le cadre des relations de travail de droit privé. People Analytics fait référence à l'évaluation systématique des données numériques relatives au capital humain afin d'augmenter la valeur de l'entreprise. L'auteur identifie d'abord les différences entre People Analytics et les anciennes formes de surveillance sur le lieu de travail ainsi que les problèmes juridiques qui en résultent. Après examen des différentes dispositions légales applicables, l'attention sera portée sur l'analyse du droit du travail et de la protection des données. L'auteur en tire trois enseignements majeurs : Premièrement, les dispositions relatives à la protection des données, principalement conçues de manière procédurale, doivent être interprétées sur la base des risques encourus par la collecte de telles données. Deuxièmement, dans le cadre du travail, le consentement ne devrait pas constituer un motif de justification pour le traitement des données. Et troisièmement, il existe des points faibles dans l'application de la protection des données en droit privé. Sur la base de ces constats, l'auteur développe un concept d'amélioration visant à professionnaliser et à démocratiser le droit de la protection des données. Il confronte ses réflexions théoriques aux données empiriques recueillies sur le terrain en collaborant avec une équipe de recherche interdisciplinaire. Quant à la législation en matière de la protection des données, la thèse prend en compte la loi fédérale suisse en vigueur, la future loi fédérale suisse entièrement révisée, le règlement général de l'UE et certains aspects du droit américain.

1 Einführung

1.1 Problemaufriss: Chancen und Risiken

Digitale Daten prägen heutzutage unser Leben stärker als je zuvor. Sie verändern alle Lebensbereiche. Auch die Personalverwaltung wird von der Umwälzung erfasst.¹ Unzählige Arbeitsplätze sind davon betroffen.

Der Begriff «People Analytics» bezeichnet die Personalentwicklungspraxis, bei der digitale Daten aus unternehmensinternen und -externen Quellen, die sich auf das Humankapital beziehen, mit Informationstechnologie analysiert werden, um Entscheidungen zur Steigerung des Unternehmenswerts zu treffen.² Jeder Arbeitnehmer erhält dabei ein digitales Etikett, das über seine Leistung, Entwicklung, gesundheitliche Verfassung und weitere Informationen Auskunft gibt. Dadurch soll der Wert des Humankapitals, das in Bilanzen als reiner Kostenfaktor ein unvollkommenes Dasein fristet, bezifferbar gemacht werden.³ Zunehmend werden auch weiche Faktoren im Unternehmen vermessen, welche früher schwierig einzuschätzen waren, wie beispielsweise die Stimmung der Mitarbeitenden.⁴ Die immer feinere Granularität und Skalierbarkeit, die People Analytics ermöglicht, sind für die Personalverwaltung so bedeutsam wie die Erfindung des Mikroskops für die Biologie.⁵

¹ «Every aspect of business is becoming more data-driven. There's no reason the people side of business shouldn't be the same», so Ben Waber, Gründer und CEO von Humanyze, einem Anbieter von People Analytics-Produkten und -Dienstleistungen: The Economist vom 28.03.2018, There will be little privacy in the workplace of the future, abrufbar unter <www.economist.com> (besucht am 31.05.2020). «Big data [...] will not easily be separated from effective human resources management»: MRKONICH *et al.*, 37.

² Zum Begriff «People Analytics» siehe auch S. 8–9. Vgl. MARLER/BOUDREAU, 15. Vgl. DIETRICH *et al.*, 21. Vgl. GUENOLE *et al.*, 87.

³ Auch im Bruttoinlandsprodukt erscheint der Wert der Bevölkerung nicht, obwohl er Schätzungen zufolge (in den USA um das Fünf- bis Zehnfache) höher liegt als der Wert aller materiellen Güter eines Landes zusammen: BRYNJOLFSSON/MCAFEE, 121.

⁴ Siehe zur Stimmungsanalyse S. 57.

⁵ REINDL/KRÜGL, 37. Vgl. zum Mikroskopeffekt der Big Data-Nutzung: LOHR STEVE, Sizing up big data, broadening beyond the internet, The New York Times vom 19.07.2013, abrufbar unter <<https://bits.blogs.nytimes.com>> (besucht am 31.05.2020).

Eine Auseinandersetzung mit People Analytics ist wichtig, weil mit dem Thema sowohl Chancen als auch Risiken verbunden sind.⁶ Zu den Chancen zählt vorderhand, dass die Arbeitgeberin einen Wettbewerbsvorteil durch Effizienzsteigerung,⁷ Kostenreduktion⁸ und mehr Innovation⁹ erlangen will. People Analytics soll ebenso zum Wohle der Arbeitnehmer Transparenz¹⁰ und Objektivität¹¹ in die Personalentscheidungen bringen, wodurch Diskriminierungen abgebaut¹² und die Diversität im Unternehmen angereichert werden können.¹³ Beispielsweise werden

-
- ⁶ Etwas allgemeiner: Digitalisierung sei für den Schweizer Arbeitsmarkt sowohl mit Chancen als auch mit Risiken verbunden: Schweizerischer Bundesrat 2017b, 6.
- ⁷ CUSTERS/URSIC, 333; NIKLAS/THURN, 1590; DIETRICH *et al.*, 9, m.w.H.; KPMG, 23–24. «Employers [...] need to [...] assess corporate wellbeing [...] for overall performance outcome»: STAN, 295. A.M. RIEDY/WEN, 90: Die Überwachung am Arbeitsplatz beeinträchtigt die Produktivität.
- ⁸ Z.B. betragen die Recruiting-Kosten bei Neubesetzungen bis zu 40 Prozent eines Jahresgehalts, weshalb eine ideale Auswahl der Mitarbeiter umso wichtiger ist: REINDL/KRÜGL, 198, m.w.H.; ebenso BRYNJOLFSSON/MCAFEE, 217. Zwar sind nach a.M. auch höhere Kosten der Digitalisierung denkbar: WOLTER *et al.*, 63. Doch erwarten die Unternehmen, dass der mögliche Gewinn die Investitionskosten für die Entwicklung von KI und Big Data deutlich übertreffen wird: WILSON/DAUGHERTY, 209; HÄNOLD, 124.
- ⁹ AJUNWA/CRAWFORD/SCHULTZ, 743. Die Innovation steigt, weil durch allgegenwärtige Aufzeichnungen Ideen schon im Ansatz festgehalten werden können und nicht verloren gehen: BRYNJOLFSSON/MCAFEE, 71. Vgl. aus dem Volksmund: «Wer schreibt, der bleibt.»
- ¹⁰ Algorithmen (zum Begriff: S. 29) arbeiten im Vergleich zu Menschen transparenter, weil sie ihre Tätigkeit protokollieren: GOODMAN/FLAXMAN, 7. Es ist leichter, einen standardisierten Computerprozess zu beaufsichtigen als einen Menschen: ZARSKY, 1412.
- ¹¹ SNYDER, 251–252; informierte und faktenbasierte Entscheidungsprozesse im Gegensatz zur Entscheidungsfindung nach Bauchgefühl: DAVENPORT, 27. Vgl. DIETRICH *et al.*, 2, 9. RIEDY/WEN, 91. «Technology and data are neutral»: World Economic Forum 2013, 3. «Surveillance technology itself is value neutral»: WEST *et al.*, 309. Zu den Versprechungen des auf prädiktive Analyse im Bewerbungsprozess spezialisierten amerikanischen Unternehmens Gild: KIM 2017, 868. Vgl. ALTMAN *et al.*, 39.
- ¹² Reduktion von Vorurteilen: REINSCH/GOLTZ, 46. Vgl. The Bath Chronicle vom 13.10.2016, Calling on his people skills: Reduktion von subjektiven Eindrücken und Vorurteilen der Arbeitgeberin durch den Algorithmus von Cognisess Deep Learn. HÄNOLD, 129; GAY/KAGAN.
- ¹³ WILSON *et al.*, 32; KIM 2017, 872. Eine Rekrutierungsmethode, bei der das Verhalten von Bewerbern bei einem Spiel mit KI und Neurowissenschaft ausgewertet wird, um eine bessere Auswahl zu treffen, führt dazu, dass 39 Prozent mehr Frauen angestellt werden: SHOOK *et al.*

bei automatisierten Einzelentscheidungen die Modellparameter bewusst ausgewählt und die Entscheidungslogik hernach konsistent auf alle Fälle gleich angewendet, um das mit subjektiven Vorurteilen behaftete menschliche Ermessen zu minimieren.¹⁴ Auch die Mitarbeiterzufriedenheit soll durch People Analytics steigen, etwa weil die Analyse von Gesundheitsdaten sie dazu motiviert, Krankheiten gezielt vorzubeugen.¹⁵ Über-Fahrer fühlen sich sicherer, wenn sie wissen, dass sie überwacht werden, als wenn sie dessen ungewiss sind.¹⁶ Im Endeffekt können durch die Kosteneinsparungen die Arbeitsplätze gesichert werden,¹⁷ und der Mensch kann sich dank neuer Technologien, die automatisierbare Prozesse übernehmen, auf die kreativen Tätigkeiten fokussieren, was in einer «Rehumanisierung» der Arbeit resultiert.¹⁸ Die meisten Arbeitnehmer scheinen sich nicht an den intensiver werdenden Verhaltens- und Leistungskontrollen im beruflichen Kontext zu stören.¹⁹

Doch People Analytics ist auch mit Risiken verbunden. Denn die Datenanalysen können zum «Mikromanagement» von Arbeitskräften, d.h. für intensive Arbeitskontrollen mit übertriebener Detailorientierung, verwendet werden.²⁰ Im Wesent-

¹⁴ HACKER, 1185; DREYER/SCHULZ, 7; ZARSKY, 1412.

¹⁵ «*Modern data analytics [...] helps workers keep healthy bodies and sane minds*»: CUSTERS/URSIC, 333. «*Employer and employee share an interest in the health of the employee*»: AJUNWA/CRAWFORD/FORD, 479. Gesundheitsprogramme (siehe hierzu S. 48–49) stellen einen Wettbewerbsvorteil im Kampf um die Rekrutierung von Talenten dar: STAN, 291. Ein Arbeitnehmer des texanischen Unternehmens Regal Plastics sagt über seinen Vorgesetzten, der die Fitness der Angestellten überwacht und sie regelmässig daran erinnert, mehr dafür zu tun: «*He's a real motivator*»: ROWLAND CHRISTOPHER, With fitness trackers in the workplace, bosses can monitor your every step – and possibly more, The Washington Post vom 16.02.2019, abrufbar unter <www.washingtonpost.com> (besucht am 31.05.2020).

¹⁶ KATZ MIRANDA, The creative ways your boss is spying on you, 08.12.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020).

¹⁷ COLLIER, 7.

¹⁸ KI führe dazu, dass «*people work more like humans and less like robots*»: WILSON/DAUGHERTY, 20. KI «*has the potential to rehumanize work*»: WILSON/DAUGHERTY, 214.

¹⁹ So WEDDE 2016c, 3. Siehe auch die empirischen Befunde des NFP75-Projekts später auf S. 308–313: Demnach herrscht in Unternehmen, die People Analytics anwenden, ein stabiles Vertrauensklima, und die Analysetechniken üben kaum einen Einfluss auf das Vertrauen der Arbeitnehmer in die Arbeitgeberin aus.

²⁰ AKHTAR/MOORE, 106. Die Befürchtung des Mikromanagements nährt sich von negativen Erfahrungen mit dem «Mikrotargeting» im Marketing, das zur Manipulation von

lichen stellt People Analytics den Persönlichkeitsschutz der einzelnen Arbeitnehmer zur Debatte, welcher durch das Arbeits-, Datenschutz- und Diskriminierungsschutzrecht gewahrt wird.²¹ Auch die Mitwirkungsrechte der Belegschaft können von People Analytics betroffen sein.²² Schliesslich schürt der Umstand, dass Daten in immer mehr Arbeitsbereichen und darüber hinaus im Privatleben anfallen, ein gesellschaftliches Interesse an einem effektiven Datenschutz.²³

Im Folgenden ist zu klären, inwiefern sich die Forschung und Praxis mit den beschriebenen Chancen und Risiken bisher auseinandergesetzt hat und wo allenfalls Forschungslücken bestehen.

1.2 Forschungsstand und Forschungslücke

1.2.1 Vorbemerkung: Berücksichtigung internationaler Quellen

Für die vorliegende Arbeit sind das Datenschutzrecht und das Arbeitsrecht wichtig. Bzgl. datenschutzrechtlicher Fragen sind neben den schweizerischen Quellen auch diejenigen zum Datenschutzrecht der Europäischen Union und die entsprechende Literatur aus den Mitgliedstaaten zu konsultieren. Denn einerseits entfalten die europäischen Normen in gewissen Fällen eine extraterritoriale Wirkung auf die Schweiz;²⁴ andererseits ist die Rechtslage hier wie dort relativ ähnlich, was nicht zuletzt darauf zurückzuführen ist, dass sowohl das schweizerische DSG als auch die europäische DSGVO inhaltlich durch die OECD-Leitlinien 1980 geprägt sind.²⁵ Ferner sind Blicke auf die Rechtslage jenseits der europäischen Grenzen hilfreich, weil rund um den Erdball vergleichbare Datenschutz-Grundsätze gelten.

Konsumenten und Wählern durch personalisierte Werbung geführt hat: UNO Generalversammlung, 9.

²¹ Siehe S. 82–99.

²² Siehe S. 99–105.

²³ Siehe S. 235–237.

²⁴ Siehe zur Anwendbarkeit der DSGVO und der Datenschutznormen von EU-Mitgliedstaaten auf schweizerische Sachverhalte S. 109–114.

²⁵ Die OECD-Leitlinien 1980 haben nachhaltig zur Harmonisierung der unterschiedlichen nationalen Datenschutzniveaus beigetragen: BBl 2017, 6968. Die Schweiz ist Mitglied der OECD. Die EU nimmt an deren Beratungen teil, ohne stimmberechtigt zu sein.

Es haben sich schon früh internationale Standards zur Regulierung des Datenschutzrechts, einer relativ jungen Rechtsmaterie, durchgesetzt.²⁶

Das Arbeitsrecht gehört dagegen traditionell zur Regelungshoheit des betreffenden Staats. Bzgl. arbeitsrechtlicher Fragen ist daher vorwiegend auf nationale Quellen abzustellen.

1.2.2 Behördliche Verlautbarungen

Auf Seiten der Behörden setzte sich der EDÖB zunächst mit Datenbearbeitungen beim Einsatz spezifischer Technologien auseinander: Er veröffentlichte 2012 die «Erläuterungen zur Telefonüberwachung am Arbeitsplatz»²⁷ und 2013 den «Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz (für die Privatwirtschaft)».²⁸ Der im darauffolgenden Jahr erschienene «Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich (Bearbeitung durch private Personen)» erweitert den Blickwinkel, indem er einen von konkreten Technologien losgelösten generellen Überblick zur Datenbearbeitung in Arbeitsverhältnissen und insbesondere zu Überwachungs- und Kontrollsystemen am Arbeitsplatz bietet.²⁹

Das SECO, das für die Oberaufsicht über den Vollzug des ArG und der ArGV 3 zuständig ist (vgl. Art. 42 Abs. 3 ArG), hat sich gemäss eigener Auskunft direkt an den Autor der vorliegenden Arbeit bislang nicht zum Thema People Analytics geäußert.³⁰

Aus der Tätigkeit des Europarats resultierte bereits 1989 die Empfehlung No. R (89) 2 zur Bearbeitung von Personendaten, die für Anstellungszwecke verwendet werden.³¹ Im Jahr 2015 schob der Europarat die überarbeitete Empfehlung CM/Rec(2015)5 zur Bearbeitung von Personendaten im Arbeitskontext³² und im

²⁶ In Hessen wurde 1970 das weltweit erste Datenschutzgesetz erlassen, und im Jahr 1973 folgte in Schweden das erste nationale Datenschutzgesetz: SCHIEDERMAIR, 44. Bereits im Jahr 1980 entstand mit den OECD-Leitlinien das erste internationale Regelwerk für den Datenschutz: SCHIEDERMAIR, 141; KROENER/WRIGHT, 359. Das schweizerische DSG stammt aus dem Jahr 1992.

²⁷ EDÖB 2012.

²⁸ EDÖB 2013.

²⁹ EDÖB 2014b.

³⁰ SECO 2019. Immerhin existieren allgemeine Erläuterungen zur Überwachung am Arbeitsplatz (vgl. Art. 26 ArGV 3): SECO 2018, 326–1 – 326–7 [sic].

³¹ Europarat 1989.

³² Europarat 2015.

Jahr 2016 das dazugehörige erklärende Memorandum³³ nach. Das Memorandum ist sowohl an öffentliche als auch an private Arbeitgeberinnen gerichtet.³⁴ 2018 hat der Europarat gemeinsam mit der EU das Handbuch zum europäischen Datenschutzrecht, worin ein Unterkapitel den arbeitsplatzbezogenen Daten gewidmet ist, herausgegeben.³⁵ Der EGMR fasst die EMRK-Rechtsprechung zur Überwachung am Arbeitsplatz in einem Faktenblatt von 2018 zusammen.³⁶

1.2.3 Literatur

Bzgl. Fachliteratur sollen zunächst grundlegende Werke erwähnt werden. RIESELMANN-SAXER setzt sich in ihrer Dissertation von 2002 umfassend mit dem Thema Datenschutz im privatrechtlichen Arbeitsverhältnis auseinander.³⁷ Die Autorin analysiert zunächst die rechtlichen Grundlagen, um diese am Ende auf vier bestimmte Technologien anzuwenden (Telefon-, Internet-, E-Mail- und Videoüberwachung). In ihrem Werk finden sich empirische Daten zum Thema; zwischen diesen Erhebungen und den gegenwärtigen Verhältnissen am Arbeitsplatz liegen jedoch beinahe zwei Jahrzehnte.

Im Jahr 2007 widmete auch WOLFER seine Doktorarbeit dem Thema der elektronischen Überwachung des Arbeitnehmers im privatrechtlichen Arbeitsverhältnis.³⁸ Hier finden sich eine Auseinandersetzung mit den betroffenen Persönlichkeitsaspekten, insbesondere mit der psychischen Integrität und der Privatheit,³⁹ sowie eine Besprechung der gegenläufigen Interessen von Arbeitnehmer und Arbeitgeberin, welche bei der Frage der Rechtfertigung einer Persönlichkeitsverletzung abzuwägen sind. Gestützt darauf begutachtet der Autor die rechtliche Zulässigkeit von vier ausgewählten Überwachungssystemen (Videoüberwachung, elektronische Zeiterfassung und Zugangskontrolle, elektronische Standortermittlung ausserhalb des Betriebsgeländes sowie Überwachung der elektronischen Kommunikation).

³³ Europarat 2016b.

³⁴ Europarat 2016b, 22.

³⁵ EU/Europarat.

³⁶ EGMR.

³⁷ RIESELMANN-SAXER.

³⁸ WOLFER.

³⁹ Siehe zum Begriff der «Privatheit» S. 267.

Im deutschen Schrifttum scheinen zwei aktuellere Publikationen auf, die das komplexe Thema «People Analytics» bis in spitze Winkel abtasten: Zum einen trägt CULIKS Promotionsschrift von 2018 den Titel «Beschäftigtendatenschutz nach der EU-Datenschutz-Grundverordnung – Möglichkeit und Grenzen für Big Data-Anwendungen im Personalwesen».⁴⁰ CULIK verwendet den Begriff «Big HR Data» und schildert das Zusammenspiel der DSGVO mit dem Arbeitsrecht und dem Diskriminierungsschutzrecht. Im Unterschied zu RIESELMANN-SAXER und WOLFER behandelt er die auftretenden Rechtsfragen technikneutral. CULIK kritisiert, dass die europäischen und deutschen Rechtsnormen zu unbestimmt seien, um in der Praxis die erwünschte Wirkung zu erzielen.⁴¹

Zur grundlegenden deutschsprachigen Literatur zählt zum andern DÄUBLERS Werk «Gläserne Belegschaften», das 2019 in der 8. Auflage erschienen ist.⁴² Dieses Handbuch zum Beschäftigtendatenschutz enthält ein Kapitel zu Big Data am Arbeitsplatz und stellt fest, dass dieses Problem «nicht bewältigt» sei, insbesondere weil man von einer informationellen Gewaltenteilung «meilenweit entfernt» sei.⁴³

Die Konsultation rechtsvergleichender Beiträge lohnt sich, weil Datenbearbeitungen häufig Bezüge zu verschiedenen Rechtsordnungen aufweisen und Rechtsordnungen weltweit mit den gleichen Technologien umgehen müssen. OTTO vergleicht das US-amerikanische, das europäische und das kanadische Modell des Datenschutzes in Arbeitsverhältnissen in ihrer 2016 erschienenen Monografie.⁴⁴ Einen Blick auf die australische Rechtsordnung gewähren O'ROURKE, PYMAN und TEICHER im Aufsatz «*The right to privacy and the conceptualisation of the person in the workplace: a comparative examination of EU, US and Australian approaches*» von 2007.⁴⁵

Diverse Autoren betrachteten in der jüngeren Vergangenheit einzelne Segmente von People Analytics, seien es bestimmte verwendete Technologien oder gewisse Verwendungszwecke. Zu erwähnen sind namentlich die rechtswissenschaftlichen Dissertationen von: NEU (Der Einsatz moderner Kommunikationsmittel am Arbeitsplatz im Spannungsverhältnis zum Arbeitnehmerdatenschutz, 2012; mit

⁴⁰ CULIK.

⁴¹ «Konkretisierungsdefizit»: CULIK, 298.

⁴² DÄUBLER.

⁴³ DÄUBLER, N 389–435, 952 und 954.

⁴⁴ OTTO 2016.

⁴⁵ O'ROURKE *et al.*

einem Schwerpunkt auf Telefon-, Internet- und E-Mail-Daten),⁴⁶ STEIGERT (Datenschutz bei unternehmensinternen Whistleblowing-Systemen, 2012),⁴⁷ GASCHER (Zulässigkeit eines Datenabgleichs zur Aufdeckung von Straftaten von Arbeitnehmern, 2013),⁴⁸ OWSCHIMIKOW (Datenscreening zwischen Compliance-Aufgabe und Arbeitnehmerdatenschutz, 2013),⁴⁹ MEYER-MICHAELIS (Die Überwachung der Internet- und E-Mail-Nutzung am Arbeitsplatz, 2014; unter Berücksichtigung der Rechtslage in den USA),⁵⁰ ZHANG (Videoüberwachung von Arbeitnehmern, 2016; einschliesslich eines Rechtsvergleichs zwischen Deutschland und China)⁵¹ und BROY (Der Umgang mit Bewerberdaten aus Internetquellen, 2017).⁵² Ferner darf die Monografie von BYERS (Mitarbeiterkontrollen, Praxis im Datenschutz und Arbeitsrecht, 2016) nicht vergessen werden.⁵³ Die Forschungsergebnisse von HÖLLER und WEDDE (Die Vermessung der Belegschaft, 2018; mit einem Fokus auf dem unternehmensinternen sozialen Graphen)⁵⁴ sowie diejenigen von CUSTERS und URSIC (*Worker privacy in a digitalized world under European law*, 2018)⁵⁵ runden den Spiegel der Spezialliteratur ab.

Die Literaturanalyse zeigt, dass sich für das Phänomen der Personalanalysen mit neuen Technologien – wohl gerade wegen der jungen Entwicklung dieser Technologien – noch kein einheitlicher Begriff durchgesetzt hat.⁵⁶ Am häufigsten anzutreffen sind die Bezeichnungen «*People Analytics*» und «*HR Analytics*».⁵⁷ Aber auch «*Workforce Analytics*», «*Talent Analytics*», «*Human Capital Analytics*»,

⁴⁶ NEU.

⁴⁷ STEIGERT.

⁴⁸ GASCHER.

⁴⁹ OWSCHIMIKOW.

⁵⁰ MEYER-MICHAELIS.

⁵¹ ZHANG.

⁵² BROY.

⁵³ BYERS.

⁵⁴ HÖLLER/WEDDE 2018.

⁵⁵ CUSTERS/URSIC.

⁵⁶ GUENOLE *et al.*, 16; Zahlen zur Häufigkeit der Begriffsverwendungen: KASPER/WILDHABER, 191.

⁵⁷ «HR Analytics» schränkt das Phänomen ungebührlich ein, da im Zuge der Interoperabilität und des immer häufigeren Zusammenführens von verschiedenen Datenquellen weit mehr als die traditionellen Daten der Personalverwaltungsabteilung ausgewertet werden und Analysten ausserhalb der HR-Abteilung einbezogen werden können. KASPER/WILDHABER, 191.

«*Workplace Analytics*» und weitere Namensgebungen⁵⁸ sind im Umlauf. Der Wortteil «*Analytics*», zu Deutsch «Analytik», bedeutet wörtlich die «Kunst des AuflöSENS» (altgr. ἀναλύτική (τέχνη), «*analytikḗ [téchnē]*») und bezeichnet vorliegend das Sezieren und Interpretieren von Datensätzen.⁵⁹ Angesichts der starken Verbreitung des Ausdrucks «*People Analytics*» wird in der vorliegenden Arbeit dieser Begriff in der Einzahl verwendet. Nichtsdestotrotz trifft «*Workforce Analytics*» den Vorgang der Big Data-Analysen am Arbeitsplatz wohl präziser, weil die «*Workforce*» (im Gegensatz zu «*People*») einen spezifischen Bezug zum Arbeitsplatz herstellt. Ausserdem umfasst sie die Auswertung der gesamten Arbeitskraft, die zum Erfolg des Unternehmens beiträgt (Festangestellte, Temporärmitarbeiter, Talente, nicht angestellte Vertragspartner, Freelancer, Outsourcing-Dienstleister), einschliesslich der künftig zu erwartenden wachsenden Zahl von Robotern am Arbeitsplatz.⁶⁰ Deutsche Übersetzungen, etwa «Personalanalytik», sind ungleich seltener als die englischen Termini anzutreffen.

1.2.4 Forschungslücke

Es besteht erheblicher Diskussionsbedarf zu People Analytics.⁶¹ Forschungslücken zeigen sich in folgenden Bereichen:

Die beiden am schweizerischen Recht orientierten Dissertationen von RIESSELMANN-SAXER und WOLFER sind zu Beginn des 21. Jh. entstanden. Begriffe wie «People Analytics», «Algorithmen» oder «Big Data», die mittlerweile das Forschungsfeld prägen, fehlen dort noch. Auch neu hinzuge tretene technologische Ausstattungen wie RFID, Roboter oder Wearables bleiben weitgehend ausgeklam-

⁵⁸ Anzutreffen sind auch: «Electronic Performance Monitoring» (etwa bei AKHTAR/MOORE, 105–106. Dieser Begriff zielt auf die Leistungssteuerung und lässt andere verfolgte Ziele ausser Acht), «Electronic Surveillance» (etwa bei RIEDY/WEN, 87; «elektronische Überwachung» bei WOLFER), «Human Resource Intelligence», «New Control» (im Gegensatz zu klassischer Kontrolle), «Performance Management», «Workforce Science» (etwa bei SPRAGUE 2015, 30), «Workplace Surveillance» und, etwas genereller, «Monitoring» und «New Normal» (Letzteres als Bezeichnung der allgemeinen Digitalisierung der Gesellschaft). KASPER/WILDHABER, 191.

⁵⁹ Analytik bezeichnet jede fortgeschrittene mathematische Methode der Datenanalyse, bei der in der Regel ein ganzer Satz von Rechenwerkzeugen zum Einsatz kommt: DIETRICH *et al.*, 1. Analytik kann sich auf jeden Unternehmensbereich beziehen: DIETRICH *et al.*, 2.

⁶⁰ GUENOLE *et al.*, 6, 16–17; KASPER/WILDHABER, 191.

⁶¹ Aus deutscher Sicht: BMAS 2017, 146.

mert.⁶² Vorliegend ist für den Einstieg ins Thema eine aktualisierte Übersicht zu den Überwachungstechnologien geboten. Diese ist idealerweise beständiger und umfassender als bei den erwähnten beiden Autoren, die sich je auf vier damals verbreitete Technologien beschränken. Das Vorhaben soll gelingen, indem nicht primär die Technologien an sich beschrieben werden, sondern zu welchen Zwecken sie im Verlauf eines Arbeitnehmer-Lebenszyklus Verwendung finden.⁶³

Zudem sind empirische Zahlen zur praktischen Verbreitung und Anwendung von People Analytics in schweizerischen Unternehmen notwendig. Seit RIESSELMANN-SAXER (2002) hat, soweit ersichtlich, niemand mehr eine systematische Erhebung vorgenommen.

Die beiden schweizerischen Doktorarbeiten von RIESSELMANN-SAXER und WOLFER sind lange vor Inkrafttreten der DSGVO und des rev-DSG entstanden. Die geänderten Rechtsgrundlagen (die DSGVO und die sich abzeichnenden Bestimmungen gemäss dem E-DSG bzw. rev-DSG) sind in die vorliegende Untersuchung von People Analytics einzubeziehen.

Die jüngeren Werke, namentlich diejenigen von CULIK und DÄUBLER sowie die zahlreichen segmentalen Titel,⁶⁴ ergeben zusammengekommen relativ vollständig Auskunft zu den Rechtslagen in allen Situationen, die durch People Analytics entstehen können. Doch der grosse Umfang der einschlägigen Fachliteratur zu diesem Thema zeigt, dass das Datenschutzrecht nicht selbsterklärend ist und daher auch nicht konsequent durchgesetzt werden kann. Dies ist problematisch, weil Datenaufzeichnungen zunehmend das gesamte Arbeitsverhältnis mitbestimmen. Gesucht ist ein Rezept zur besseren Durchsetzung des Datenschutzrechts.

Während seines Forschungsaufenthalts am Berkman Klein Center for Internet & Society an der Harvard University in Cambridge (Massachusetts, USA) im Frühjahr 2019 hat der Autor zudem den Eindruck erhalten, dass People Analytics im angloamerikanischen Raum weiter fortgeschritten ist als in Festlandeuropa. Beispielsweise gehören Programme zur Analyse der Gesundheit der Arbeitnehmer in amerikanischen Grossunternehmen zum Standard.⁶⁵ Doch hat sich auch ergeben, dass die Rechtsprobleme, die People Analytics verursacht, weltweit ähnlich sind, und vor allem, dass den Datenschutz-Idealen in der Praxis überall mangelhaft

⁶² Siehe zu den Begriffen der Wearables und Roboter S. 25–27 und zur RFID-Technik FN 418.

⁶³ Siehe S. 42–58.

⁶⁴ Siehe S. 7–8.

⁶⁵ Siehe S. 65.

nachgelebt wird. So wurde etwa Facebook im Jahr 2019 in den USA eine rekordhohe Busse von USD 5 Milliarden auferlegt wegen des Cambridge Analytica-Datenskandals, der weltweit Bekanntheit erlangt hat.⁶⁶

1.3 Zielsetzung und Forschungsfrage

Vor dem skizzierten Hintergrund verfolgt die Abhandlung das folgende Ziel: Es sollen Vorschläge aufgezeigt werden, wie in der privatrechtlichen People Analytics-Praxis die Einhaltung des Datenschutzrechts sichergestellt werden kann.

Zur Zielgruppe gehört zunächst die Rechtswissenschaft. Für sie ist Grundlagenforschung zu betreiben, da es sich bei der mangelhaften Durchsetzung des Datenschutzrechts um ein strukturelles Problem handelt. Die Grundlagenforschung ist auch angezeigt, weil sich der Rechtsrahmen für Datenbearbeitungen ständig ändert⁶⁷ und somit nur die grundlegenden Bestimmungen von Dauer sind. Ganz offensichtlich richtet sich die Doktorarbeit an die Personalverantwortlichen in den Betrieben, da sie letztlich das Datenschutzrecht anwenden. Um ihre Lage zu verstehen und sie in ihrer Sprache anzureden, müssen empirische Daten zu People Analytics in die Arbeit einfließen. Ebenso wird die Politik angesprochen, die im Begriff ist, das DSG zu revidieren. Diesem breiten Publikum dienen die konzisen Zwischenergebnisse und Ergebnisse dazu, mit wenig Zeit den Einstieg in die komplexe Thematik zu finden und die zentralen Botschaften mitzunehmen.

Aufgrund des Forschungsziels lautet die zentrale, übergeordnete Forschungsfrage:

FORSCHUNGSFRAGE: Wie könnte eine künftige Neuausrichtung des privatrechtlichen Datenschutzrechts aussehen, bei welcher die Rechtsdurchsetzung ex ante und ex post im Zusammenhang mit People Analytics besser gewährleistet wäre als heute?

Um diese Hauptfrage zu beantworten, werden vorgängig in kausal zusammenhängender Reihenfolge die nachstehenden untergeordneten acht Vorfragen angegangen:

- (1) *Was ist People Analytics und was ist daran neu im Vergleich zu früheren Überwachungspraktiken an den Arbeitsplätzen?*

⁶⁶ FTC, FTC imposes \$5 billion penalty and sweeping new privacy restrictions on Facebook, 24.07.2019, abrufbar unter <www.ftc.gov> (besucht am 31.05.2020).

⁶⁷ Siehe dazu das Vorwort dieser Arbeit.

- (2) *Welche Rechtsprobleme ergeben sich aus People Analytics?*
- (3) *Welche Rechtsgebiete sind für People Analytics relevant?*
- (4) *Welchen Zweck verfolgt das DSG im Hinblick auf People Analytics?*
- (5) *Welche People Analytics-Anwendungen erfasst das DSG und welche Datenbearbeitungsregeln stellt es für People Analytics in privatrechtlichen Arbeitsverhältnissen auf?*
- (6) *Welche Rechtfertigungsmöglichkeiten bestehen für allfällige Datenschutzverletzungen?*
- (7) *Warum hat die zivilrechtliche Individualklage ihre Rolle bei der Durchsetzung des Datenschutzrechts bis heute nicht erfüllen können?*
- (8) *Wie können Gruppen und/oder Behörden ihre Interessen beim Datenschutz wirksam einbringen, um zur Rechtsdurchsetzung beizutragen?*

1.4 Abgrenzung der Forschungsfrage

Die vorliegende Arbeit untersucht in sachlicher Hinsicht die rechtlichen Rahmenbedingungen für People Analytics. Gegenstand der Analyse sind privatrechtliche Arbeitsverhältnisse. Öffentlich-rechtliche Anstellungsverhältnisse werden ausgeklammert.⁶⁸ Vertragsverhältnisse, in denen arbeitnehmerähnliche Stellungen vorkommen, wie beispielsweise mit freien Mitarbeitern (Freelancer), werden nur beachtet, soweit sich daraus Erkenntnisse für den Arbeitsvertrag unter Privaten gewinnen lassen.⁶⁹

⁶⁸ Einige der vorliegenden datenschutzrechtlichen Ausführungen dürften jedoch auch für öffentlich-rechtliche Arbeitsverhältnisse gelten, weil die allgemeinen Grundsätze des DSG gleichermassen für Datenbearbeitungen von Privaten wie von Behörden gelten: SGK-SCHWEIZER, Art. 13 Abs. 2 BV, N 84. Die Konzeption des Einheitsgesetzes aus privat- und öffentlich-rechtlichem Datenschutz ist unüblich im Vergleich zu andern Rechtsgebieten und stösst auf Kritik. Dadurch sei etwa der Begriff der Verhältnismässigkeit in das Privatrecht überführt worden, was Interpretationsschwierigkeiten zur Folge habe: AEBI-MÜLLER, N 556. BAERISWYL 2010, 141; kritisch auch THOUVENIN 2014.

⁶⁹ Viele der vorliegenden Ausführungen dürften sinngemäss in arbeitsähnlichen Vertragsverhältnissen gelten, denn z.B. das EU-Recht legt den Begriff des Arbeitnehmers (*worker*) breit aus: Darunter ist jede Person zu verstehen, die während eines bestimmten Zeitraums für eine andere Person und nach deren Weisung Leistungen erbringt, für die sie typischerweise eine Vergütung erhält: Urteil EuGH vom 17.07.2008, Raccanelli, C-94/07, EU:C:2008:425, N 33, m.w.H.; Europarat 2016b, 28. Der deutsche Beschäftigtendatenschutz erfasst auch arbeitnehmerähnliche Stellungen, wie z.B. freie

Räumlich bezieht sich die Abhandlung auf Rechtsverhältnisse in der Schweiz, d.h., das arbeitgebende Unternehmen hat Sitz in der Schweiz und der Arbeitsort liegt ebenfalls innerhalb dieses nationalen Territoriums.

In personeller Hinsicht fallen die Hauptrollen bei People Analytics dem Arbeitnehmer und der Arbeitgeberin zu. Unter dem Begriff des Arbeitnehmers wird vorliegend der Angestellte in einem Arbeitsvertrag (Art. 319 ff. OR) verstanden. In die Betrachtung eingeschlossen werden auch Stellenbewerber und ehemalige Mitarbeiter, da sie sich weitgehend auf den Datenschutz von Arbeitnehmern berufen können.⁷⁰ Als «Arbeitgeberin» fallen sowohl eine natürliche (Art. 11 ff. ZGB) als auch eine juristische Person (Art. 52 ff. ZGB) in Betracht. Datenschutzrechtlich wird die Arbeitgeberin als verantwortliche Stelle mit Entscheidungsgewalt angesehen (vgl. Art. 4 lit. i E-DSG, Art. 5 lit. j rev-DSG, Art. 4 Nr. 7 DSGVO), unabhängig davon, ob sie die eigentliche Datenbearbeitung vornimmt.⁷¹ Folglich wird nicht näher auf Konstellationen eingegangen, bei denen Dritte an Stelle der Arbeitgeberin handeln, wie beispielsweise bei der Auftragsdatenbearbeitung und beim Outsourcing (vgl. hierzu Art. 10a DSG, Art. 8 E-DSG, Art. 9 rev-DSG). Der Begriff der Arbeitgeberin schliesst vorliegend Unternehmen jeder Grösse ein. People Analytics findet zwar vorwiegend in grossen Unternehmen statt.⁷² Jedoch gelten die Datenschutz-Grundsätze auch für Familienbetriebe, da dort die gleichen Datenschutzprobleme auftreten können.⁷³

Mitarbeiter, Beschäftigte im Rahmen von Werkverträgen, Einfirmenvertreter und Heimarbeiter: MITTLÄNDER 2016a, 115.

⁷⁰ Siehe S. 182–183.

⁷¹ MEIER PHILIPPE, N 2065; HÄFNER-BEIL, 110.

⁷² Z.B. sind technische Hilfsmittel für die Kontrolle der Präsenzzeit in grösseren Betrieben erforderlich, weil dort die Arbeitgeberin die Arbeitnehmer nicht persönlich empfangen und verabschieden kann: WOLFER, N 382. Etwas allgemeiner ausgedrückt lohnt sich die ökonometrische Kontrolle in allen Prinzipal-Agenten-Beziehungen, in denen der Prinzipal (z.B. eine Versicherung) das Verhalten des Agenten (z.B. des Versicherungsnehmers) nicht unmittelbar mitverfolgen kann: HERMSTRÜWER, 107.

⁷³ Europarat 2016b, 31.

1.5 Methodik der begleitenden empirischen Datenerhebung

Die vorliegende theoretische Auseinandersetzung mit People Analytics, die auf einer Analyse von Gesetz, Materialien, Literatur und Rechtsprechung beruht, wird an den geeigneten Stellen durch die empirischen Daten ergänzt, die der Autor zusammen mit dem Forschungsteam des NFP75-Projekts erhoben hat.⁷⁴ Dieses basierte auf einem Forschungsdesign mit gemischten Methoden verteilt über mehrere Module (*mixed methods research design*).⁷⁵

Das erste Modul widmete sich der Frage «Welche People Analytics-Technologien kommen in der Praxis vor?» und begann mit einer qualitativen Untersuchung, bei der insgesamt 27 Experten zu People Analytics in der Schweiz befragt wurden. Es kam Interviewmaterial von 30 Stunden zusammen. Daraus resultierte eine Beschreibung des Phänomens, und die verschiedenen Anwendungen wurden in Kategorien eingeteilt.

Im zweiten Modul galt es, herauszufinden, wie verbreitet People Analytics in der Schweiz ist. Auch war es von Interesse, zu erfahren, wie stark sich die Personalverantwortlichen der rechtlichen Schranken von People Analytics bewusst sind und wie sie damit umgehen. Weiter sollte festgestellt werden, wie verschiedene Stakeholdergruppen am Prozess mitwirken und welche ethischen Fragestellungen auf welche Weise diskutiert werden. Methodisch eignete sich hierfür eine quantitative Online-Umfrage.⁷⁶ Diese stand während eines Zeitraums von zwei Monaten zur Teilnahme offen (15.05. bis 13.07.2018). Angeschrieben wurden 1'185 Personalverantwortliche von Unternehmen mit Sitz in der Schweiz. Von ihnen haben 158 die Fragen vollständig beantwortet. Diese Stichprobe setzt sich zu zwei Dritteln aus Angehörigen des Top- oder Senior-Managements und zu einem Drittel aus Personen des Middle- oder Junior-Managements zusammen. Überwiegend sind grosse Unternehmen dabei (siehe Abb. 1).⁷⁷ Die Branchenstruktur ist unge-

⁷⁴ Siehe zum NFP75-Projekt das Vorwort dieser Arbeit.

⁷⁵ YIN, 63 und 235; auch «*methodological mix*» oder «*multimethod*»: SLATER/ZIBLATT, 1303–1304.

⁷⁶ Die Umfrage-Ergebnisse, die im Verlauf der vorliegenden Arbeit präsentiert werden, finden sich in geraffter Form teilweise bereits bei WILDHABER/KASPER.

⁷⁷ Vgl. auch die Abb. bei WEIBEL *et al.*, 25, und bei WILDHABER/KASPER, 761.

fähr repräsentativ für die Schweiz, wobei das Finanz- und Versicherungswesen etwas überrepräsentiert ist (siehe Abb. 2).⁷⁸

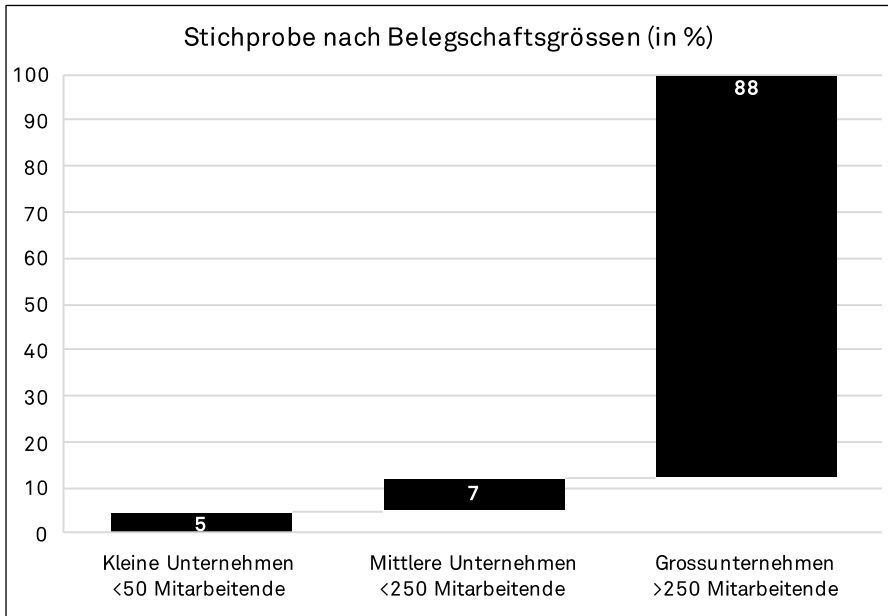


Abb. 1: Stichprobe der NFP75-Online-Umfrage nach Belegschaftsgrössen

⁷⁸ Vgl. die regelmässig aktualisierten Statistiken des Bundesamts für Statistik: Bundesamt für Statistik, Bruttoinlandprodukt, abrufbar unter <www.bfs.admin.ch> (besucht am 31.05.2020). Vgl. auch die Abb. bei WEIBEL *et al.*, 25, und bei WILDHABER/KASPER, 762.

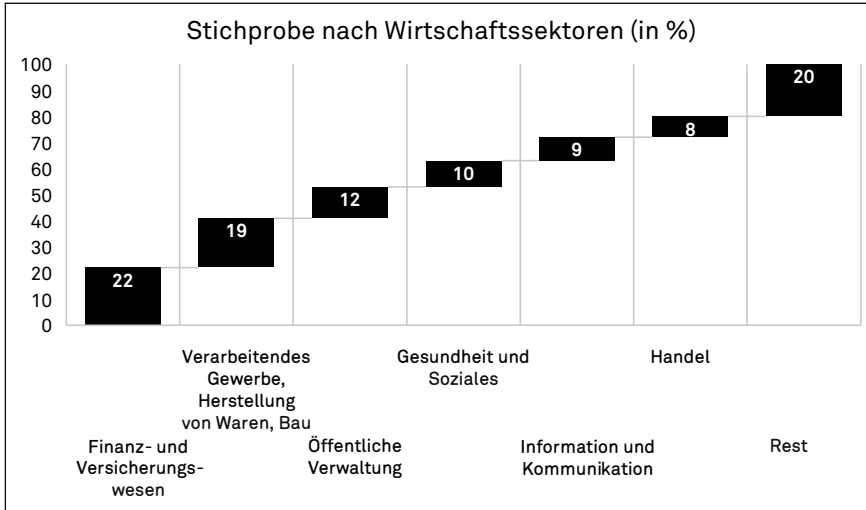


Abb. 2: Stichprobe der NFP75-Online-Umfrage nach Wirtschaftssectoren

Das dritte Modul des Forschungsprojekts ging der Frage nach, wie sich der Einsatz von People Analytics kausal auf das Vertrauensklima im Unternehmen auswirkt. Es gab bislang zu wenig empirische Daten zu den Auswirkungen von Überwachungen am Arbeitsplatz.⁷⁹ Deshalb beinhaltete das NFP75-Projekt qualitative Fallstudien mit fünf Unternehmen, die People Analytics betreiben. Insgesamt wurden rund 100 halbstrukturierte⁸⁰ Interviews mit Angestellten aus verschiedenen Abteilungen der fünf Unternehmen geführt, niedergeschrieben und analysiert.

⁷⁹ Fehlende Daten zu den gesundheitlichen Auswirkungen von People Analytics: RIEDY/WEN, 90; mangelnde Nachweise, ob prädiktive Analytik zu diskriminierenden Praktiken führt: FAVARETTO *et al.*, 23–24.

⁸⁰ Halbstrukturiert bedeutet, dass die Interviews einem Leitfaden folgten, der die groben Themen vorgab, sodass eine Vergleichbarkeit der Gespräche möglich war. Gleichzeitig bestand Raum für individuelle Schwerpunktsetzungen, um gegenüber dem Interviewpartner offen für Neues zu sein.

1.6 Aufbau

Aufgrund ihrer Ziele und Fragen gliedert sich die Arbeit in acht Teile und beginnt mit der vorliegenden (1) Einführung.

(2) Anschliessend gilt es, das Phänomen People Analytics zu beschreiben, d.h. aufzuzeigen, was daran im Vergleich zu früheren Überwachungen am Arbeitsplatz neu ist und dass es bereits eine Verbreitung erlangt hat, die es zu einem relevanten Thema macht. Im Unterkapitel 2.2 findet der Leser die Erklärungen der technischen Begriffe, die in dieser Arbeit vorkommen.

(3) Im dritten Teil sind die Rechtsprobleme, die People Analytics aufwirft, darzulegen. Sie geben den Anstoss für die nachfolgende juristische Untersuchung des Phänomens.

(4) Die rechtliche Untersuchung beginnt mit einer Übersicht der relevanten Rechtsbestimmungen und der Schutzlücken in den Geltungsbereichen der Rechtserrlasse.

(5) Im fünften Kapitel wird auf das Datenschutzrecht näher eingegangen, das bei People Analytics eine eminente Stellung einnimmt. Hierzu gehören eine Ergründung des Zwecks des DSG und die Betrachtung der Pflichten der Arbeitgeberin, welche sich aus den Datenbearbeitungsregeln und -rechtfertigungsgründen ergeben.

(6) Spiegelbildlich zu den Pflichten der Arbeitgeberin stehen die Rechte der Individuen, der Arbeitnehmervertretung und der Behörden zur Durchsetzung des Datenschutzrechts.

(7) Das siebte Kapitel widmet sich ganz der Beantwortung der Forschungsfrage. Es wird sich zeigen, dass das Datenschutzrecht weder von der Arbeitgeberin *ex ante* genügend umgesetzt noch von der Gegenseite *ex post* durchgesetzt wird. Damit hat das Datenschutzrecht ein Glaubwürdigkeitsproblem, weil es in der Praxis nicht gelebt wird. Nach der vorliegend entwickelten These könnten eine Professionalisierung und eine Demokratisierung zur wirksameren Durchsetzung des Datenschutzrechts führen. Diese These wird im siebten Kapitel erklärt.

(8) Am Schluss werden alle essenziellen Ergebnisse, die einen neuen Beitrag zur Forschung darstellen, auf den Punkt gebracht.

2 Phänomenbeschreibung

2.1 Übersicht

Als Einstieg ins Thema gilt es, den Forschungsgegenstand, People Analytics, zu beschreiben. Zunächst wird der zweite Wortteil – «Analytics» – erörtert, um jene technischen Begriffe zu erläutern, die in den späteren Kapiteln fallen werden (dazu sogleich, Unterkapitel 2.2, S. 19–41). Sodann wird mit Bezug auf den ersten Wortteil – «People» – dargelegt, zu welchen Zwecken die Technologien verwendet werden und wie dabei Mensch und Technik interagieren (Unterkapitel 2.3, S. 42–59). Die Analyse der gegenwärtigen und möglichen künftigen Verbreitung von People Analytics wird die praktische Relevanz des Themas unterstreichen (Unterkapitel 2.4, S. 60–68). Basierend auf diesen einleitenden Beobachtungen sind die Kernelemente herauszuschälen, durch die sich People Analytics von früheren Überwachungspraktiken an den Arbeitsplätzen unterscheidet (Unterkapitel 2.5, S. 69–77).

2.2 Technische Begriffserklärungen

2.2.1 Daten-Lebenszyklus

Als Gedankenstütze bei der Betrachtung der technischen Aspekte von People Analytics dient der Daten-Lebenszyklus. Dieser besteht aus vier Phasen, (1) angefangen bei der Datenbeschaffung, (2) über die Datenanalyse und (3) die Nutzung der Daten mit deren Wirkung auf die Umwelt bis hin zur (4) Löschung oder gegebenenfalls Wiederverwendung der Daten (siehe Abb. 3).⁸¹

⁸¹ Die Unterteilung in vier Phasen lehnt sich an die Darstellung der Schweizer Juristin TAMÒ-LARRIEUX an: TAMÒ-LARRIEUX, 6–7. Vergleichbare Konzepte finden sich in der deutschen Rechtswissenschaft (CALDAROLA/SCHREY, N 209), in der EU (*lifecycle data protection management*): Europäisches Parlament 2014, Section 3 Art. 33) und bei der amerikanischen FTC (Unterteilung in Datenerhebung, Zusammenstellung und Konsolidierung, Analyse sowie Nutzung von Big Data: FTC 2016, i) sowie in der Computerwissenschaft (Unterteilung in Trainingsdatenerfassung, Gestaltung (*design*) des Algorithmus, Modell-Training, Einsatz von Daten und Algorithmus: THELISSON *et al.*, 56).

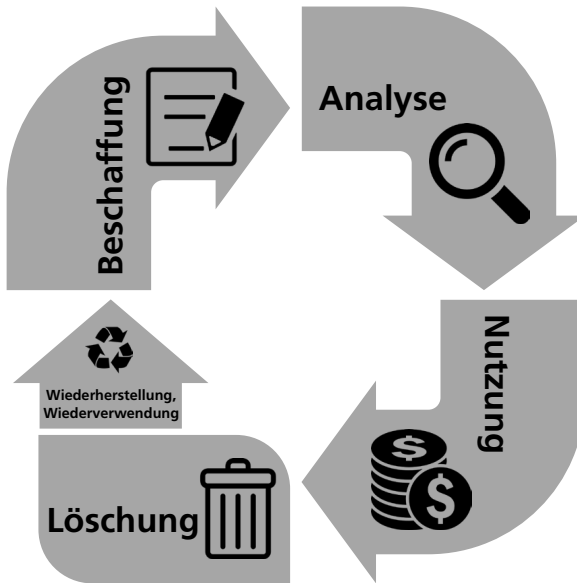


Abb. 3: Daten-Lebenszyklus

Im Folgenden ist in Bezug auf die Datenbeschaffung zu klären, was überhaupt Daten sind. Zudem sind die für die Datenerhebung erforderlichen physischen Komponenten (Hardware) zu beschreiben. In der Phase der Datenanalyse stehen die verwendeten Algorithmen bzw. Programme (Software) im Zentrum. Bei der Datennutzung leuchtet der Begriff «Big Data» auf, welcher auch Ausgangspunkt des NFP75-Projekts war.⁸² Schliesslich gibt es in der vierten Phase zwei Alternativen: Entweder werden die Daten gelöscht oder aber sie werden wiederverwendet, wodurch der Daten-Lebenszyklus von Neuem beginnt.

2.2.2 Daten

a) Daten und Information

Das Wort «Datum» bedeutet wörtlich «das Gegebene».⁸³ Diese etymologische Herkunft widerspiegelt sich im deutschen Wortlaut des DSG, wonach Daten «An-

⁸² Siehe Vorwort.

⁸³ Von lat. *dare*: geben (*datum* = Partizip Perfekt, Passiv, Nominativ, Singular, Neutrum).

gaben» bezeichnen (Art. 3 lit. a DSGVO, Art. 4 lit. a E-DSG, Art. 5 lit. a rev-DSG). Datenschutzrechtlich relevant sind die Angaben, wenn sie sich auf eine bestimmte oder bestimmbare Person beziehen (vgl. Art. 3 lit. a DSGVO, Art. 4 lit. a E-DSG, Art. 5 lit. a rev-DSG).⁸⁴

In der französischen und der italienischen Fassung des DSGVO sind Daten gleichbedeutend mit Informationen (*«informations»*, *«informazioni»*). Auch das europäische Recht setzt «Daten» und «Informationen» gleich (Art. 4 Nr. 1 DSGVO). Die Rechtswissenschaft und Rechtspraxis kennen keine eigenen, einheitlichen Begriffe des Datums und der Information, sondern verwenden diese Termini gemäss dem üblichen, alltäglichen und mehrdeutigen Sprachverständnis.⁸⁵

Ein Teil der Lehre unterscheidet die beiden Begriffe «Daten» und «Information» qualitativ, indem Daten als das Rohmaterial und Information als das bearbeitete, nutzbare Wissen bezeichnet werden.⁸⁶ Information schliesst dabei den Sinn ein, der den Daten durch eine Analyse verliehen wird.⁸⁷ Gemäss DRUEY erhält Information erst rechtliche Relevanz, wenn unter ihrem Empfänger ein Mensch verstanden wird.⁸⁸ Nach der hier vertretenen Auffassung können sich aber auch rechtliche Fragen ergeben, wenn eine Maschine Informationsempfängerin und -verarbeiterin ist. Dieses breitere Informationsverständnis wird mit Blick auf das aufkommende Internet der Dinge⁸⁹ künftig an Bedeutung gewinnen.⁹⁰

Eine Information ist in sich noch kein Wert.⁹¹ Information ist als Wertchance zu verstehen, die sich je nach Ausgestaltung der Information im Verhältnis zu ihrem Adressaten verwirklicht.⁹² Für die Realisierung des Werts ist somit ein geeigneter

⁸⁴ Zur Unterscheidung der Personendaten von anderen Daten später, S. 155–173.

⁸⁵ DRUEY 1995, 3; GASSER 2001, 52; THOUVENIN/WEBER/FRÜH, 4. «Daten» und «Informationen» werden teils auch als Synonyme erachtet, so etwa bei GILBERT, 264, und SPRAGUE 2013, 1–1.

⁸⁶ Vgl. CUSTERS, 10, und HOFFMANN-RIEM, 16.

⁸⁷ *«Information is data + meaning»*: PURTOVA 2018, 50. GILBERT, 263. Besonders die angelsächsische Sprache verwendet *«information»* für Wissensinhalte: KASPER, N 10; ALBERS, 89. Vgl. SCHEFZIG, 105. Vgl. DRUEY 1995, 21.

⁸⁸ DRUEY 1995, 3. Ähnlich äussert sich ALBERS, 88.

⁸⁹ Siehe zum Begriff «Internet der Dinge» S. 28.

⁹⁰ Z.B. stellen sich Fragen zum Schutz der Freiheit und Selbstbestimmung, wenn Maschinen beginnen, über ihren Besitzer zu erzählen: RUDIN 2008, 13.

⁹¹ DRUEY 1995, 437. Vgl. HOFFMANN-RIEM, 15. Macht resultiere nicht aus den Daten, sondern aus dem Wissen, das aus ihnen gezogen werde: EGGIMANN, 7.

⁹² DRUEY 1995, 73; KASPER, N 93.

Empfänger erforderlich, der die Chance nutzt. Um die im Zusammenhang mit Daten oft anzutreffende Wasser-Metapher⁹³ aufzugreifen: Ein Stausee enthält Wasser (Daten) mit einer physikalischen Lageenergie (Wertchance); Letztere kann aber nur jemand freisetzen, der das Kraftwerk betätigen und Wasser durch die Turbinen schnellen lassen kann.⁹⁴ Das Verständnis von Information als Wertchance ist relevant bei der Bestimmung des Geltungsbereichs des DSG. Für dessen Anwendbarkeit kann es entscheidend sein, ob eine Datenbearbeiterin zum Zweck der Wertschöpfung gewisse anonyme Daten durch Re-Identifizierung einer Person zuordnen will oder nicht.⁹⁵

Es gibt weitere Ausprägungen der Begriffe «Daten» und «Information», die vorliegend nur in Kürze zu erwähnen sind. In der Diskussion um ein mögliches Dateneigentum wird Information als Objekt beschrieben, das als strukturelle, syntaktische oder semantische Information existieren kann.⁹⁶ Auf diese Dreiteilung muss jedoch nicht näher eingegangen werden, weil vorliegend ein Dateneigentum für das Schweizer Recht abgelehnt wird.⁹⁷ Ferner kann Information als Vorgang zwischen einem Sender und einem Empfänger dargestellt werden und kommt dabei dem Begriff «Kommunikation» nahe.⁹⁸ Weniger verbreitet ist das Verständnis von Information als Zustand der Kenntnis; es kommt in der Wendung «Stand der In-

⁹³ Daten als Salzwasser, das erst nach der Destillierung trinkbar wird: LOHR STEVE, Sizing up big data, broadening beyond the internet, The New York Times vom 19.07.2013, abrufbar unter <<https://bits.blogs.nytimes.com/>> (besucht am 31.05.2020); «data lakes», «data pools», Big Data als «reissender Strom» von Daten: S. 38. Vgl. auch WEDDE 2016b, N 2: Daten als Öl, das durch die Raffinerie geht.

⁹⁴ So wie die Physik von «potenzieller Energie» spricht, verwendet die Informationsrechtswissenschaft den Begriff «potenzielle Information»: ZECH, 16; ALBERS, 89. Vgl. MAYER-SCHÖNBERGER/CUKIER, 104.

⁹⁵ Siehe zur Rechtsprechung bzgl. des Interesses an einer Re-Identifizierung später, S. 157–159.

⁹⁶ Diese Dreiteilung geht namentlich zurück auf: ZECH, 35–45. Siehe auch SCHMIDT, 27–30, und THOUVENIN/WEBER/FRÜH, 5–6. Dabei werden Daten als maschinell lesbar kodierte Information definiert: ZECH, 32. Umstritten ist aber, ob Daten als verkörperte Information angesehen werden sollen bzw. ob die Verkörperung ein Tatbestandsmerkmal für den Begriff der Daten sein soll: ZECH, 32 FN 90.

⁹⁷ Siehe dazu später, S. 265–266. Ohnehin werden die vorliegend interessierenden Personendaten nur über die semantische Ebene abgegrenzt, d.h. über ihre Bedeutung bzw. ihren Bezug auf eine bestimmte oder bestimmbare Person: SCHMIDT, 31.

⁹⁸ KASPER, N 10. Vgl. DRUEY 1995, 27. Vgl. STEINBUCH, 55, der Information als Signalvermittlung beschreibt: «Information ist die durch Signale veranlasste Strukturveränderung in einem Empfänger.»

formation» zum Ausdruck.⁹⁹ Schliesslich differenziert ein Teil der Rechtsliteratur quantitativ, indem ein Datum die kleinste Einheit von Information darstelle.¹⁰⁰

Der doppeldeutige Begriff des «Informationsrechts» kann sowohl das «Recht auf Information» als auch das «Recht der Information» bezeichnen. Ersteres meint den subjektiven Anspruch darauf, informiert zu werden, und steht somit gegensätzlich zum Recht auf Geheimhaltung. Dieses Verständnis von «Informationsrecht» wird bei der Besprechung der Mitwirkungsrechte der Arbeitnehmer bedeutsam werden.¹⁰¹ Das Recht der Information betrifft dagegen das Recht im objektiven Sinn, das sich in seiner Gesamtheit mit Information befasst.¹⁰² Die Informations-Rechtswissenschaft befasst sich einerseits mit der Analyse der rechtlichen Rahmenbedingungen und Bestimmungen zu Informationserzeugung, -verteilung, -austausch, -zugang und -nutzung in einem bestimmten gesellschaftlichen (z.B. dem wirtschaftlichen, kulturellen oder politischen) Subsystem. Andererseits erforscht die Informations-Rechtswissenschaft die dynamischen Veränderungen der Informations- und Kommunikationstechnologien und -prozesse sowie deren Auswirkungen auf das Recht.¹⁰³ Auch dieses zweite Verständnis von Informationsrecht interessiert vorliegend, und zwar mit Blick auf das Subsystem Arbeitsplatz.

b) Digitalisierung und Datafizierung

Im Lichte der vorstehenden Ausführungen sind Daten nicht zwingend digitale Einheiten (Bits) im Sinne der Informatik, weil auch andere Repräsentationen von Information möglich sind.¹⁰⁴ Es ist jedoch eine Tatsache, dass heutzutage schätzungsweise über 98 Prozent der Daten digital aufgezeichnet werden.¹⁰⁵

Die Digitalisierung (*digita(li)sation*) bezeichnet die Verwandlung analoger Daten zu digitalen, die in einer maschinell lesbaren, binären Sprache aus Nullen und Ein-

⁹⁹ KASPER, N 10.

¹⁰⁰ DRUEY 1995, 20. Daten seien «*items of information*»: GILBERT, 263.

¹⁰¹ Siehe S. 101–103.

¹⁰² Zum Informationsrecht im subjektiven und objektiven Sinn: KASPER, N 12.

¹⁰³ GASSER 2004, 4.

¹⁰⁴ Z.B. Gruben (*pits*) und Flächen (*lands*) in der Spiralspur einer CD: THOUVENIN/WEBER/FRÜH, 5.

¹⁰⁵ SPRAGUE 2013, 1–2; CUKIER/MAYER-SCHÖNBERGER, 29. Noch im Jahr 2000 war erst ein Viertel der weltweit von Menschen gespeicherten Informationen digital: CUKIER/MAYER-SCHÖNBERGER, 28.

sen gefasst sind.¹⁰⁶ Die Digitalisierung bedeutet noch nicht, dass die Daten kategorisiert sind: Eine eingescannte Buchseite ist zwar digital, der Text aber lässt sich noch nicht auf bestimmte Stichwörter hin automatisch durchsuchen.¹⁰⁷

Die Datafizierung (*datafication*) ist der nächste Schritt, der zur Verwertung von Daten erforderlich ist.¹⁰⁸ Datafizieren bedeutet, Daten in ein quantifiziertes Format zu setzen, sodass sie kategorisiert und interpretiert werden können.¹⁰⁹ Um beim obigen Beispiel zu bleiben: Der eingescannte Text ist erst datafiziert, wenn ein Texterkennungs-Programm (*optical character-recognition, OCR*) das digitale Bild in einzelne Buchstaben zerlegt hat. In einem datafizierten Datensatz lässt sich, wie in einem Register, nach Suchbegriffen nachschlagen.¹¹⁰ Die Tatsache, dass sich die Menschheit zusehends dem «*onlife*» nähert, d.h. einer Existenz, die durch Informationstechnologie vermittelt wird,¹¹¹ führt dazu, dass das gesamte Leben datafiziert und durchsuchbar werden wird.¹¹²

Die Datafizierung steht als Begriff unabhängig von Digitalisierung¹¹³ und ist ihrem Wesen nach auch älter: Eine Ausprägung von Datafizierung ist beispielsweise das Koordinatensystem aus Längen- und Breitengraden der Erde, dessen Erfindung auf Eratosthenes von Kyrene (276/273–194 v.Chr.) zurückgeht: Über ein System von Gitterlinien zur Standortbestimmung wird es möglich, jede Position in einem numerischen Format aufzuzeichnen, zu kategorisieren oder zu suchen.¹¹⁴

¹⁰⁶ HOFFMANN-RIEM, 15; MAYER-SCHÖNBERGER/CUKIER, 78.

¹⁰⁷ Vgl. CUKIER/MAYER-SCHÖNBERGER, 35.

¹⁰⁸ Zum Begriff der «Datafizierung»: WILDHABER/KASPER, 756.

¹⁰⁹ MAYER-SCHÖNBERGER/CUKIER, 78; CUKIER/MAYER-SCHÖNBERGER, 29.

¹¹⁰ MAYER-SCHÖNBERGER/CUKIER, 84. Die Suche erfolgt entweder in strukturierter Abfragesprache (*structured query language, SQL*) oder auf andere Arten der Leseanfrage (*not only SQL, NoSQL*): GABATHULER SILVAN, 22.

¹¹¹ PURTOVA 2018, 41.

¹¹² ZUBOFF 2019, 14.

¹¹³ CUKIER/MAYER-SCHÖNBERGER, 35.

¹¹⁴ In der Renaissance hat der Kartograf und Globenhersteller Gerhard Mercator (1512–1594) das Meridiansystem wieder aufgegriffen und vorangetrieben. Eine Einigung auf ein globales, standardisiertes Koordinatensystem zum weltweiten Teilen von Ortungsdaten gelang erst ab den 1940er-Jahren mit dem Universal-Transverse-Mercator-(UTM-)Koordinatensystem: MAYER-SCHÖNBERGER/CUKIER, 87.

Nach der im Wesentlichen immer noch gleichen Logik überwachen Arbeitgeberinnen heute ihre Fahrzeugflotten und die Aufenthaltsorte ihrer Arbeitnehmer.¹¹⁵

Die Datafizierung wirkt als Katalysator bei der Realisierung der Wertchancen, die in Informationen stecken.¹¹⁶ Daten kommen nun aufbereitet als «Mahlgut für die Analysemühle» daher.¹¹⁷ Wirtschaftliche Impulse entstehen, wenn Bewegung in die Daten kommt. Johannes Gutenbergs (1400–1468) Buchdruckerfindung hat gezeigt, wie einflussreich gedruckte Information sein kann, wenn sie weit durch die Gesellschaft gestreut wird.¹¹⁸ Der durch die Datafizierung in Gang gesetzte Informationsfluss ist historisch vergleichbar mit Gütertransportachsen, die Volkswirtschaften zum Erlblühen brachten, wie die Seidenstrasse, das römische Fernstraßennetz ausgehend von der Via Appia oder die britische Flotte.¹¹⁹

2.2.3 Ausgewählte physische Komponenten und Computerinfrastruktur

a) Sensoren, Wearables und Roboter zur Datenbeschaffung

Die Beschaffung der für People Analytics erforderlichen Daten gelingt mit sog. Sensoren (von lat. *sentire*: fühlen, empfinden, wahrnehmen). Es handelt sich dabei um technische Bauteile, die bestimmte physikalische oder chemische Eigenschaften der Umgebung erfühlen und in ein elektrisches Signal umformen. Beispielsweise registrieren Infrarot-Kameras die Wärme und GPS-Sensoren empfangen Radiowellen von Satelliten. Mit beiden Techniken lassen sich auch Arbeitnehmer orten.¹²⁰

Vermehrt kommen Sensoren vor, die am oder im Körper getragen werden (*wearables* bzw. *wearable computers*).¹²¹ Wearables können die Form von Acces-

¹¹⁵ Siehe S. 48. Vgl. MAYER-SCHÖNBERGER/CUKIER, 89.

¹¹⁶ Vgl. MAYER-SCHÖNBERGER/CUKIER, 83. Ist erst die ganze Welt datafiziert, begrenzt einzig der persönliche Einfallsreichtum die möglichen Verwendungen von Information: MAYER-SCHÖNBERGER/CUKIER, 96.

¹¹⁷ «Grist for the analytics mill»: BAROCAS.

¹¹⁸ MAYER-SCHÖNBERGER/CUKIER, 172.

¹¹⁹ EGGIMANN, 6–7.

¹²⁰ BIAS/BOGUE, 259.

¹²¹ EGGEN/STENGEL, N 4.

soires (z.B. Kopfhörer,¹²² Armbänder, Brillen,¹²³ oder Zahnbürsten¹²⁴) annehmen oder in die Kleidung eingenäht werden. Teils werden sie als Tattoo oder Folie auf der Haut getragen oder als Implantate unter die Haut gespritzt.¹²⁵ Die Arbeitgeberin kann Wearables grundsätzlich als Arbeitsmittel oder Fitnesstracker einsetzen.¹²⁶ Wertvoll sind Wearables für die Arbeitgeberin, weil sie Informationen direkt von den Mitarbeitern liefern (*user data*).¹²⁷ Dies vermittelt eine grössere Einsicht in das Humankapital als mittelbare Daten, etwa dazu, wie eine Maschine bedient wurde (*use data*). Das Speichersystem eines Wearable setzt sich aus dem lokalen (dem Wearable selbst) und einem externen Speicherort (Smartphone, Computer, Cloud) zusammen.¹²⁸ Die externe Komponente zeigt in der Regel über ein Anwendungsprogramm (Applikation, App) die Datenauswertung an. Beispielsweise stellt die App «Happiness Planet» auf dem Mobiltelefon die Daten dar, die das noch näher vorzustellende «Happiness Meter»-Halsband von Hitachi aufzeichnet.¹²⁹

Menschen arbeiten zusehends mit Robotern zusammen. Dies erfordert einen Informationsaustausch über die Sensoren der Roboter. Exosuits und Exoskelette ertasten so die anthropometrischen Merkmale jedes individuellen Arbeitnehmers, um sich dessen Schritt-, Arm- und Rückenlänge anzupassen.¹³⁰ Roboter haben aber nicht nur Sensoren zur Wahrnehmung; sie können diese Wahrnehmung auch

¹²² Eine frühe Erscheinung von Wearables waren die tragbaren Hörgeräte, die in der ersten Hälfte des 20. Jh. aufkamen. Die Erfindung des ersten tragbaren Hörgeräts datiert aus dem Jahr 1938 und wird dem Chicagoer Elektronikhersteller Aurex Corporation zugeschrieben: EGGEN/STENGEL, N 6. Heutzutage überwachen Kopfhörer von Apple die elektrische Herzfrequenz und das Herzschlagvolumen: PARISI, 323.

¹²³ Google und Snap produzieren intelligente Brillen (*smart glasses*): EDSB 2019b, 10–11. Facebook, Apple und Amazon haben die Produktion angekündigt: EDSB 2019b, 3.

¹²⁴ Elektronische Zahnbürsten lassen nachverfolgen, wie oft und lang jemand die Zähne putzt: CUSTERS/URSIC, 330.

¹²⁵ Tattoo: ALLENSPACH, N 3; Folie, die auf Oberflächen geklebt wird: HARTZOG 2018, 267; Implantat: S. 53.

¹²⁶ ALLENSPACH, N 44.

¹²⁷ GAY/KAGAN.

¹²⁸ ALLENSPACH, N 2.

¹²⁹ Siehe dazu später, S. 56.

¹³⁰ Siehe zu den Begriffen Exosuit und Exoskelett später, S. 54. Vgl. zu sog. «Cobots», die anthropomorphe Merkmale von Arbeitern erfassen und Werkstücke so positionieren, dass ergonomisch angenehm gearbeitet werden kann: WILDHABER 2017, 220, und HOFMANN, 13.

mittels Datenanalyse prozessieren (*think*) und gestützt darauf physisch handeln (navigieren, etwas bewegen) oder nichtphysische Funktionen ausführen (warnen, empfehlen, entscheiden) (*act*).¹³¹ Beispielsweise die Kiva-Roboter in den Warenlagern von Amazon transportieren Kunststoffbehälter voller Artikel zu Arbeitnehmern, die darauf die Bestellung ausführen.¹³²

b) Internet als Medium zur Datenübertragung

Der Begriff des Internets bedeutet «miteinander verbundene Netzwerke» (*inter-connected networks*).¹³³ Als Geburtsstunde des Internets gilt das Jahr 1969.¹³⁴ Den Durchbruch zum populären Massenmedium schaffte das Internet aber erst rund zwanzig Jahre später dank zweier Entwicklungen: Einerseits gelang Ende der 1980er-Jahre die Verbindung des Internets mit den E-Mail-Diensten, wodurch der Nachrichtenversand für die breite Öffentlichkeit zu kommerziellen Zwecken möglich wurde.¹³⁵ Andererseits präsentierte der Informatiker Tim Berners-Lee 1989 den Internetdienst World Wide Web (WWW), dessen disruptive Neuerung darin bestand, dass es ausser Text auch beliebige andere Informationen wie Zeichnungen oder Bilder transportieren konnte.¹³⁶ Heute fungiert das Internet als das Medium, worüber aufgezeichnete Daten in breitem Stil ausgetauscht werden.¹³⁷

¹³¹ WILDHABER 2016, 316.

¹³² WILSON/DAUGHERTY, 31.

¹³³ Das Internet bezeichnet das grösste und bekannteste globale und dezentrale Computernetzwerk, das wiederum aus vielen miteinander verbundenen lokalen und nationalen Netzen besteht: NEU, 3. Da das Internet offen konzipiert ist und sich potenziell jedermann als Anbieter oder als Nutzer anschliessen kann, ist es in seiner Grundstruktur keine feste physikalische Grösse: MEYER-MICHAELIS, 29.

¹³⁴ Ende 1969 konnten vier räumlich distanzierte Rechner miteinander verbunden werden, welche sich an den Standorten der University of California in Los Angeles und Santa Barbara sowie am Stanford Research Institute und an der University of Utah befanden: BRAUN, 202–203. Vgl. KIRPAL/VOGEL, 140.

¹³⁵ EDSB 2018, E. 6.

¹³⁶ Die Übertragung von multimedialen, nicht nur textuellen Elementen war möglich, weil das WWW auf dem Hypertext-Übertragungsprotokoll (*hyper text transfer protocol*, HTTP) basierte. Vgl. MEYER-MICHAELIS, 31–32. NEU, 4; EDSB 2018, E. 6; HÖLLER/WEDDE 2016, 301; THIERER, 432. Vgl. NISSENBAUM 2011, 33.

¹³⁷ MEYER-MICHAELIS, 27; «*mediation by the net*»: NISSENBAUM 2011, 38; Internet als wichtigstes Kommunikationsmittel: WOLFER, N 449.

Das Internet der Dinge (*internet of things, IoT*) beschreibt ein drahtgebundenes oder drahtloses Netzwerk von Geräten, die über eingebettete Sensoren miteinander kommunizieren, wobei die Daten via Internet übertragen werden.¹³⁸ Mittlerweile gibt es mehr ans Internet gebundene Geräte als Menschen auf der Erde.¹³⁹ Ruft man sich die Wearables, die Arbeitnehmende an und in sich tragen (werden), in Erinnerung, so weitet sich das Phänomen zu einer digitalen Vernetzung aller Werker, Werkzeuge und Werkstücke im Produktionsprozess und über Unternehmensgrenzen hinweg aus. Dies generiert ein «Internet der Dinge und der Menschen».¹⁴⁰ Diese netzwerkartige Architektur führt dazu, dass Daten über die Mitarbeiter in exponentiellem Ausmass zunehmen werden.¹⁴¹ Wir erleben eine vierte industrielle Revolution; in der Welt des sog. Arbeitens 4.0 verschmelzen die physische und die digitale Sphäre miteinander.¹⁴²

c) Cloud-Computing

Die Rechnerwolke (Cloud-Computing) ist eine IT-Infrastruktur, die als Dienstleistung angeboten wird. Die Infrastruktur besteht aus einem Netzwerk von Servern. Die Kunden beziehen Speicherplatz, Rechenleistung oder Anwendungssoftwares. Diese Dienstleistungen sind über eine technische Schnittstelle verfügbar, beispielsweise über das WWW und einen zugehörigen Webbrowser. Charakteristisch

¹³⁸ White House, Executive Office of the President 2014, 2. Es kommt zu einer Vernetzung von Informationen und Gegenständen: Schweizerischer Bundesrat 2017b, 11.

¹³⁹ Zwischen 2008 und 2009 hat die Zahl der ans Internet angeschlossenen Geräte diejenige der Menschen auf der Erde überschritten. Im Jahr 2020 sollen mehr als drei solcher Geräte pro Person oder insgesamt 26 Milliarden existieren: DE MAURO *et al.*, 125. Eine durchschnittliche vierköpfige Familie aus einem OECD-Land wird im Jahr 2022 rund 50 ans Internet angeschlossene Geräte besitzen, dies gegenüber zehn im Jahr 2013: OECD, 4. Mehr mobile Internetgeräte als Menschen auf der Erde Ende 2015: AKHTAR/MOORE, 105.

¹⁴⁰ BMAS 2017, 68.

¹⁴¹ GUENOLE *et al.*, 11–12.

¹⁴² «Vierte industrielle Revolution»: AKHTAR/MOORE, 102; «Arbeiten 4.0»: BMAS 2015, 32. Arbeiten 3.0 umfasst die beginnende soziale Marktwirtschaft mit Konsolidierung des Sozialstaats und der Arbeitnehmerrechte. Arbeiten 2.0 bezeichnet die Zeit der Massenproduktion und die Anfänge des Wohlfahrtsstaats am Ende des 19. Jh. Arbeiten 1.0 umfasst die beginnende Industriegesellschaft und die ersten Organisationen von Arbeitern: BMAS 2015, 34. KI und Cloud-Computing sind ebenfalls treibende Kräfte hinter der vierten industriellen Revolution: Microsoft Corporation 2018b, 91.

für Cloud-Computing ist, dass die Daten von überall her bzw. von irgendeinem Gerät aus bezogen werden können.¹⁴³

2.2.4 Algorithmen

a) Zum Begriff «Algorithmus»

Als Algorithmus gilt allgemein die mathematische Logik hinter jeder Art von System, das Aufgaben ausführt oder Entscheidungen trifft.¹⁴⁴ Algorithmen gab es lange vor der Digitalisierung, etwa zur technischen Steuerung von Maschinen.¹⁴⁵ Das Wort «Algorithmus» ist eine Verballhornung von «al Chwarizmi», dem Familiennamen des persischen Rechenmeisters und Astronomen Muhammad ibn Musa al Chwarizmi (780–835/850 nach julianischem Kalender).¹⁴⁶ Von seinem Werk ist die lateinische Übersetzung erhalten geblieben, die den Titel *Algoritmi de numero Indorum* trägt («al Chwarizmi über die indische Zahlschrift».)¹⁴⁷

Im heutigen digitalen Zeitalter sind Algorithmen unverzichtbar, um Erkenntnisse aus den immensen Datensätzen zu gewinnen.¹⁴⁸ Algorithmen müssen in maschinell bearbeitbarer Programmiersprache formuliert werden, damit ein Computer die Rechenoperationen anwenden kann.¹⁴⁹

b) Abgestufte Fähigkeiten von Algorithmen

Algorithmen zur Entscheidungsunterstützung (*decision-support algorithms*) helfen bei einer Entscheidung, ohne jedoch den Entscheid selbst auszuführen.¹⁵⁰ Die folgenden drei Stufen von Finesse des Analyseresultats lassen sich unterscheiden:¹⁵¹

¹⁴³ GILBERT, 260; BMAS 2017, 199. Die Wolke erleichtert auch das Zusammenführen von Daten aus unterschiedlichen Quellen: BMAS 2017, 66.

¹⁴⁴ AI now institute, 2.

¹⁴⁵ HOFFMANN-RIEM, 13; ältester bekannter Algorithmus um 1'700 v.Chr. in babylonisch-sumerischer Keilschrift festgehalten: NAHRSTEDT, 1. Nach **a.M.** reichten die ersten Algorithmen [nur] rund 2'000 Jahre zurück: HÄNOLD, 126. Der erste für einen Computer gedachte Algorithmus wurde 1842 skizziert: NAHRSTEDT, 2.

¹⁴⁶ NAHRSTEDT, 1; MEHRI, 71.

¹⁴⁷ AL CHWARIZMI; NAHRSTEDT, 1. Vgl. MEHRI, 72.

¹⁴⁸ HÄNOLD, 126.

¹⁴⁹ HÖFER, N 3; HOFFMANN-RIEM, 13. Vgl. BMAS 2017, 198.

¹⁵⁰ Algo:aware [sic], 11.

¹⁵¹ Zu den drei Stufen von Algorithmen: DAVENPORT, 194, SNYDER, 249, und DIETRICH *et al.*, 5.

(1) Deskriptive Algorithmen beschreiben bisher unbekannte Beziehungen innerhalb von gegenwarts- und vergangenheitsbezogenen Datensätzen.¹⁵² Beispielsweise kann die Arbeitgeberin durch den Vergleich von Gehaltsabrechnungsinformationen und Arbeitsleistung feststellen, wie die Dauer der Ferien die Produktivität in den umliegenden Arbeitswochen beeinflusst.¹⁵³ (2) Prädiktive Analytik dient dazu, die Wahrscheinlichkeit künftiger Ereignisse oder Ausgänge anhand bestimmter Indikatoren und statistischer Regelmässigkeiten in den Datensätzen vorherzusagen.¹⁵⁴ (3) Präskriptive Algorithmen versorgen den Anwender mit Handlungsempfehlungen zur Erreichung seiner Ziele.¹⁵⁵

Entscheidfällende Algorithmen (*decision-making algorithms*) generieren eine Entscheidung oder führen eine Massnahme gegenüber einem sozialen oder physikalischen System aus.¹⁵⁶ Beispielsweise kann ein entscheidfällender Algorithmus eine Person von internationalen Flugreisen direkt ausschliessen.¹⁵⁷

c) Künstliche Intelligenz

Die Geburtsstunde der Forschung nach KI wird auf eine Konferenz von 1956 datiert, die der Computerwissenschaftler John McCarthy am Dartmouth College (New Hampshire, USA) organisiert hat.¹⁵⁸ KI-Systeme sind Software- und gegebenenfalls auch Hardware-Systeme, die ihre Umwelt über Sensoren wahrnehmen.¹⁵⁹ Darauf interpretieren sie die Daten in algorithmischen Rechenoperationen und bestimmen zur Erreichung des vorgegebenen Ziels die besten Massnahmen, die sie in der physischen oder digitalen Dimension umsetzen. KI-Systeme können ihr Verhalten anpassen, wenn sie spüren, dass sich die Umwelt durch ihre Hand-

¹⁵² Vgl. GAY/KAGAN und HOFFMANN-RIEM, 19.

¹⁵³ GAY/KAGAN.

¹⁵⁴ WILDHABER *et al.*, 461; AI now institute, 30.

¹⁵⁵ HOFFMANN-RIEM, 20.

¹⁵⁶ Algo:aware [sic], 7. Dabei können Menschen zu einem variablen Grad in die algorithmische Entscheidfällung einbezogen werden: Befehlsausführende Systeme befolgen ausschliesslich bestimmte menschliche Anweisungen (*human-in-the-loop*). Beaufsichtigte Systeme kann ein Mensch überwachen und übersteuern (*human-on-the-loop*). Vollkommen selbständige (*fully autonomous*) Systeme arbeiten ohne menschliche Überwachung: algo:aware [sic], 11–12.

¹⁵⁷ DREYER, 136.

¹⁵⁸ WILSON/DAUGHERTY, 40.

¹⁵⁹ Europäische Kommission 2019a, 1.

lungen verändert.¹⁶⁰ Zur KI gehört der Versuch, die neuronale Struktur des menschlichen Gehirns mit den Mitteln der Informatik nachzubauen.¹⁶¹ Die einzelnen Schritte in Vorgängen wie Lernen, Kreativität und Aufgabenerledigung mit «gesundem Menschenverstand» sollen in mathematische Modelle übersetzt werden, sodass Maschinen sie replizieren können.¹⁶² Trotz dieser Kennzeichen fehlt jedoch eine klare Begriffsdefinition von KI.¹⁶³

Es wird zwischen schwacher (*weak* oder *narrow*) und starker (*strong* oder *general*) KI unterschieden. Die gegenwärtigen Anwendungen von KI gehören zu ersterer Kategorie; sie können beispielsweise ein Spiel gewinnen, eine Stimme erkennen oder auf Muster in einem Computertomografie-(CT-)Scan hinweisen. Starke KI hingegen beschreibt Maschinen von höherer Intellektualität, einer Eigenwahrnehmung und Selbstkontrolle, sodass sie irgendein Problem in beliebigem Kontext lösen können.¹⁶⁴ Selbst Probleme, die im Zeitpunkt der Schaffung der KI noch nicht existierten, kann starke KI erledigen.¹⁶⁵

Maschinelles Lernen ist die hauptsächliche Form der (gegenwärtig noch schwachen) KI.¹⁶⁶ Den Begriff des maschinellen Lernens prägte im Jahr 1959 der IBM-Ingenieur Arthur Samuel, der seinerseits an John McCarthys KI-Konferenz teilge-

¹⁶⁰ Europäische Kommission 2019a, 6. KI ist fähig, Objekte in der Umwelt zu beeinflussen bzw. zu manipulieren: GUIHOT *et al.*, 394.

¹⁶¹ Mit Bezug auf maschinelles Lernen: THOUVENIN/FRÜH/GEORGE, N 7. Neuronale Netzwerke schreiben eigene Programme unabhängig vom menschlichen Programmierer: HÄNOLD, 126.

¹⁶² WILSON/DAUGHERTY, 40; WRIGLEY, 186–187; GAY/KAGAN.

¹⁶³ DREYER/SCHULZ, 45. KI umfasst einen Fächer von Unterdisziplinen: GASSER/ALMEIDA, 59. Die Unterdisziplinen reichen vom maschinellen Lernen (*machine learning*) über das maschinelle Denken (*machine reasoning*, das im Gegensatz zu maschinellern Lernen auch neue Probleme angeht) bis zur Robotik (Integration der Techniken in cyber-physikalische Systeme): Europäische Kommission 2019a, 6. Zur KI zählt auch die Kognitionswissenschaft (*cognitive computing*); näher zu diesem Begriff: MRKONICH *et al.*, 2. Dabei schliesst KI auch Arten von Intelligenz ein, die mehr Rechenleistung abverlangen, als das menschliche Gehirn bietet: GUIHOT *et al.*, 394.

¹⁶⁴ Zur Begriffsverwendung und Unterscheidung zwischen schwacher und starker KI: GASSER/ALMEIDA, 59.

¹⁶⁵ GUIHOT *et al.*, 396; Ableitung von Algorithmen aus unstrukturierten Informationen ohne vorgängige Programmierung: Schweizerischer Bundesrat 2017b, 11.

¹⁶⁶ UNO Generalversammlung, 4. Maschinelles Lernen verursache gegenwärtig eine «Explosion» von KI: AI now institute, 2.

nommen hatte.¹⁶⁷ Unter dem Sammelbegriff des maschinellen Lernens existieren verschiedene Technologien.¹⁶⁸ Allgemein geht es darum, ein Computerprogramm darauf hin zu trainieren, in einem Datensatz selbständig Muster zu erkennen, ohne zu verstehen, was die Muster bedeuten.¹⁶⁹ Der Clou am maschinellen Lernen ist die Fähigkeit, zu generalisieren: Muster werden nachher auch in Daten erkannt, die nicht Teil der Trainingsdaten bildeten.¹⁷⁰ Hierdurch hebt sich das maschinelle Lernen von sog. Expertensystemen ab, die über Wissen in Form von im Voraus abgespeicherten «wenn-dann»-Regeln verfügen.¹⁷¹ Von (starker) KI unterscheiden sich Systeme des maschinellen Lernens dadurch, dass sie nicht autonom handeln, sich nicht an Veränderungen anpassen und sich keine eigenen Ziele stecken.¹⁷²

d) Korrelationen und Kausalitäten

Algorithmen gewinnen Erkenntnisse nach heutigem Stand der Technik hauptsächlich durch das Aufdecken von Korrelationen in Datensätzen. Eine Korrelation (von lat. *cum relatione*: «mit Wiederholung», und mittellat. *correlatio*: «Wechselbeziehung») beschreibt eine statistische Beziehung zwischen zwei Variablen A und B, ohne den Grund für die Beziehung – welcher in einer Kausalität oder einem Zufall bestehen kann – zu nennen. Es handelt sich somit um eine rein deskriptive Erkenntnis, die weitgehend von einem Verstehensprozess losgelöst ist und jegli-

¹⁶⁷ Arthur Samuel entwickelte damals ein Computerprogramm, das Dame spielte: WILSON/DAUGHERTY, 41.

¹⁶⁸ AI now institute, 2. Drei dieser Technologien sind das überwachte Lernen (*supervised learning*), das verstärkende Lernen (*reinforcement learning*) und das tiefgehende Lernen (*deep learning*): algo:aware [sic], 9, m.w.H.

¹⁶⁹ AI now institute, 2. Daten werden dem Computer zur Verfügung gestellt, damit er selbständig lernen kann: GAY/KAGAN. In älterer sozialwissenschaftlicher Literatur findet sich teilweise der Begriff «Data Mining» zur Beschreibung des Herauslesens von Mustern aus Datensätzen.

¹⁷⁰ HÖFER, N 20. Die Generalisierungsfähigkeit bleibt zurzeit noch weit unter dem, was man intuitiv erwarten würde: HÖFER, N 40.

¹⁷¹ Expertensysteme entscheiden z.B.: «Wenn X ein Vogel ist, kann es fliegen»: THOUVENIN/FRÜH/GEORGE, N 6. Anders als Expertensysteme könne maschinelles Lernen auch viel besser mit Spezial- und Härtefällen umgehen: THOUVENIN/FRÜH/GEORGE, N 31.

¹⁷² GUIHOT *et al.*, 394–395. Die fehlende Fähigkeit zur Anpassung an Veränderungen zeigt sich, wenn ein Modell des maschinellen Lernens überlistet wird, indem es auf Daten angewendet wird, die sich deutlich von den Trainingsdaten unterscheiden: HÖFER, N 31. Eine zu starke Ausrichtung an den Trainingsdaten (*overfitting*) stellt eine Gefahr für das System des maschinellen Lernens dar: HÖFER, N 20.

cher individuell nachvollziehbaren Begründungsleistung entbehrt.¹⁷³ Eine Korrelation vermittelt ein vergleichsweise oberflächliches Wissen, weil sie nicht Licht ins Innere einer Variablen bringt.¹⁷⁴ Stattdessen identifiziert sie eine andere nützliche, sog. stellvertretende oder Proxy-Variable: Wenn die gesuchte Variable A mit dem Stellvertreter B korreliert, genügt es, nach B Ausschau zu halten, um vorherzusagen, was höchstwahrscheinlich mit A passieren wird.¹⁷⁵ Als Beispiel für eine arbeitsplatzbezogene Korrelation (die sich jedoch als falsch herausgestellt hat) mag diejenige zwischen Lohn und Lebensglück dienen: Ökonomen und Politikwissenschaftler glaubten über Jahre, dass ein Einkommensanstieg zu mehr Zufriedenheit führe. Diese Annahme stimmt jedoch nur für Einkommen bis zu einer bestimmten Schwelle; ein Lohnanstieg darüber hinaus verbessert die Glücksgefühle kaum mehr.¹⁷⁶

Eine Kausalität ist die Beziehung zwischen Ursache und Wirkung (von lat. *causalis*: «die Ursache angehend», und mittellat. *causalitas*: «Ursächlichkeit»). Im Gegensatz zur Korrelation wird hier der Grund, warum aus Ursache A die Wirkung B folgt, erklärt.

Menschen haben beim Anblick einer Korrelation einen «intuitiven Hang dazu, eine kausale Beziehung zu sehen, obschon es keine gibt».¹⁷⁷ Tatsächlich bestehen zwischen Korrelation und Kausalität Gemeinsamkeiten. Eine Korrelation kann ein Indiz für einen möglichen Kausalzusammenhang darstellen. Der Wahrheitsgehalt einer Kausalität kann, ähnlich wie bei einer Korrelation, selten bewiesen werden; es kann bloss festgestellt werden, dass er mit einem hohen Grad an Wahrscheinlichkeit vorliegen muss.¹⁷⁸ Die Philosophie versucht, die Ursächlichkeit mithilfe der Wahrscheinlichkeitssteigerung zu definieren: A verursacht B kausal, wenn A die Wahrscheinlichkeit von B erhöht.¹⁷⁹ Beispielsweise mag Einigkeit darüber bestehen, dass Uber-Chauffeure, die rücksichtslos fahren, Unfälle provozieren, ob-

¹⁷³ HOFFMANN-RIEM, 19; HERMSTRÜWER, 103; GOODMAN/FLAXMAN, 6.

¹⁷⁴ CUKIER/MAYER-SCHÖNBERGER, 32.

¹⁷⁵ MAYER-SCHÖNBERGER/CUKIER, 53.

¹⁷⁶ MAYER-SCHÖNBERGER/CUKIER, 61–62.

¹⁷⁷ MAYER-SCHÖNBERGER/CUKIER, 63.

¹⁷⁸ MAYER-SCHÖNBERGER/CUKIER, 66.

¹⁷⁹ PEARL/MACKENZIE, 47; «*Philosophers [...] are oblig'd [sic] to comprehend all our arguments from causes or effects under the general term of probability*»: HUME, 124; «*transition from strictly causal relations to probability relations*»: REICHENBACH, 25–26. Vgl. SUPPES, 8.

wohl dieses Vorzeichen bloss dazu neigt, eine Kollision wahrscheinlicher, nicht absolut sicher zu machen.¹⁸⁰

Richtigerweise sind Korrelation und Kausalität aber bewusst auseinanderzuhalten.¹⁸¹ Die Wahrscheinlichkeiten einer Korrelation beziehen sich auf eine statische Welt. Kausalität erklärt dagegen, wie sich die Wahrscheinlichkeiten ändern, wenn sich die Welt um die Variablen A und B herum wandelt.¹⁸² In der dynamischen Welt, in der wir leben, müssen Korrelationen somit ein Ablaufdatum tragen; ihr Wert ist zeitlich limitiert.¹⁸³ Demgegenüber bewahren Kausalitäten Beständigkeit. Es handelt sich um autonome «Eltern-Kind-Beziehungen» zwischen Variablen.¹⁸⁴ Wenn sich Umweltbedingungen ändern, beeinflusst dies in der Regel nur einige wenige kausale Beziehungen, während die übrigen stabil bleiben.¹⁸⁵

Die Frage steht im Raum, wann sich welche Methode besser für die Wissensgewinnung eignet. Bei gewissen Autoren geniesst die Kausalität generell einen höheren Stellenwert als die Korrelation, weil sie beständig ist und direkten Einblick in die innere Beziehung zwischen Ursache und Wirkung gewährt.¹⁸⁶ Demokrit von Abdera (460/459–370 v.Chr.) wäre es eigener Aussage zufolge lieber gewesen, eine einzige Ursachenerklärung zu finden als König von Persien zu werden. Es wird kritisiert, dass die Wissenschaft auf dramatische Art ihre Identität opfere, wenn sie nicht mehr nach Ursache und Wirkung suche.¹⁸⁷ Zudem können sich nicht begründbare Entscheidungen auf die Wirklichkeit auswirken: Beispielsweise erscheint das Handeln desjenigen Algorithmus uninformatiert, der Arbeitnehmer aus entfernten Wohnorten nicht zur Beförderung vorschlägt, weil eine Korrelation zwischen langem Arbeitsweg und kurzer Verweildauer im Unternehmen be-

¹⁸⁰ Vgl. SUPPES, 7.

¹⁸¹ Vgl. PEARL, 331.

¹⁸² Vgl. PEARL/MACKENZIE, 51. Kausalität ist in der Lage, externe und spontane Änderungen abzubilden und darauf zu antworten: PEARL, 22.

¹⁸³ Entscheidend ist die Dauer der Korrelation: MRKONICH *et al.*, 21. Die Korrelation ist am Anfang bei der Kalibrierung des Algorithmus am grössten und nimmt mit der Zeit ab: MRKONICH *et al.*, 21.

¹⁸⁴ PEARL, 22.

¹⁸⁵ PEARL, 31.

¹⁸⁶ So etwa bei PEARL, 22. Vgl. die Kritik am «beinahe religiösen Glauben» an Daten, die jedoch «niemals» kausale Fragen beantworten könnten: PEARL/MACKENZIE, 351.

¹⁸⁷ HARTNETT KEVIN, How a pioneer of machine learning became one of its sharpest critics, *The Atlantic* vom 19.05.2018, abrufbar unter <www.theatlantic.com> (besucht am 31.05.2020).

steht.¹⁸⁸ Die Weglänge ist jedoch möglicherweise nicht kausal für den Jobwechsel, sondern der Stress aufgrund überfüllter Verkehrsmittel.¹⁸⁹ Wären die Arbeitszeiten flexibel, könnte der Angestellte einen weniger dicht besetzten Zug nehmen und bliebe der Stelle länger treu. Arbeitnehmer mit langem Arbeitsweg hätten plötzlich eine Chance, befördert zu werden.

Korrelationen sollten jedoch nicht als unnütz abgetan werden. In Rechnung zu ziehen ist, dass die Digitalisierung zu einer regelrechten Schwemme an Daten führt.¹⁹⁰ Dies spielt der Wissensgewinnung durch Korrelationen in die Karten: *«Correlations are useful in a small-data world, but in the context of big data they really shine.»*¹⁹¹ Korrelationsanalysen sind schneller und billiger als das Suchen nach Kausalitäten in grossen Datensätzen.¹⁹² Für viele Fragen genügt es, bloss zu wissen, dass sich zwei Variablen dauerhaft auf eine bestimmte Weise verhalten, ohne dass es nötig wäre, zu verstehen, warum dies so ist.¹⁹³ MAYER-SCHÖNBERGER und CUKIER mutmassen sogar, dass Kausalität künftig nicht mehr die primäre Quelle der Wissensgewinnung sein werde.¹⁹⁴

Nach vorliegend vertretener Ansicht tragen Kausalitäten und Korrelationen komplementär zum Weltverständnis bei. Korrelationen sind umso zuverlässiger, je grösser die Datenmenge ist.¹⁹⁵ Hierin liegt ein grosses Potenzial im Vergleich zum menschlichen Denken, droht doch dem Gehirn bei grossen Mengen an Informationen die Überforderung.¹⁹⁶ Allerdings sind Algorithmen nach dem Stand der Technik noch nicht imstande, kausale Beziehungen zwischen Daten zu verste-

¹⁸⁸ Siehe zu diesem Algorithmus auch noch später, S. 43–44.

¹⁸⁹ TRINDEL.

¹⁹⁰ MAYER-SCHÖNBERGER/CUKIER, 70.

¹⁹¹ MAYER-SCHÖNBERGER/CUKIER, 52.

¹⁹² Die Suche nach Kausalitäten bringe zudem ethische Herausforderungen mit sich: MAYER-SCHÖNBERGER/CUKIER, 66.

¹⁹³ MAYER-SCHÖNBERGER/CUKIER, 191. *«Petabytes allow us to say: correlation is enough»*: ANDERSON CHRIS, The end of theory: the data deluge makes the scientific method obsolete, 23.06.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020).

¹⁹⁴ MAYER-SCHÖNBERGER/CUKIER, 68.

¹⁹⁵ Vgl. zu kognitiven Rechensystemen, die erst ab einer bestimmten Grösse des Datensatzes selbständig zu lernen beginnen: MRKONICH *et al.*, 2.

¹⁹⁶ Ebenso HÄRTING, N 240. Vgl. RICHARDS/KING, 394: Gewisse Erkenntnisse können nur gewonnen werden, wenn Daten im grossen Stil zur Verfügung stehen.

hen.¹⁹⁷ Sie können die entdeckten Korrelationen nicht auf ihre Ursächlichkeit hin anzweifeln in der Art: «Dieses Resultat macht keinen Sinn; ich werde es nochmals ausrechnen.»¹⁹⁸ Daher ist menschliches, kausales Denken nach wie vor zur Überprüfung der Stichhaltigkeit einer Korrelation erforderlich.

2.2.5 Big Data

a) Fehlende Legaldefinition

Das Phänomen «Big Data» ist relativ jung.¹⁹⁹ Es gibt keine Legaldefinition des Begriffs,²⁰⁰ und er erscheint weder im DSG noch in der DSGVO. Auf Englisch kommt «Big Data» deutlich häufiger vor als in jeder deutschen Übersetzungsvariante. Sowohl in der Einzahl²⁰¹ als auch in der Mehrzahl²⁰² ist «Big Data» anzutreffen. Vorliegend wird der Singular bevorzugt, weil die Daten erst als Masse wertvoll werden und sich rechtliche Überlegungen auf das Phänomen als Ganzes beziehen.

b) Die (mindestens) drei V-Eigenschaften

Die Versuche der Literatur, «Big Data» zu definieren, beginnen häufig mit den drei V-Eigenschaften (*volume*, *variety*, *velocity*), die, soweit ersichtlich, erstmals LANEY (2001) beschrieben hat.²⁰³ Big Data beschreibt demnach Datenbestände, die aufgrund ihres Umfangs (*volume*), ihrer Unterschiedlichkeit (*variety*) oder ih-

¹⁹⁷ PEARL/MACKENZIE, 21. Wegen des mangelnden Verständnisses entstehen Bedenken gegen die Qualität der Erkenntnisse: Europarat 2016a, 7.

¹⁹⁸ Bzgl. KI: SMITH ANDREW, Franken-algorithms: the deadly consequences of unpredictable code, The Guardian vom 30.08.2018, abrufbar unter <www.theguardian.com> (besucht am 31.05.2020). «Today's predictive models are not capable of reasoning at all»: LIPTON, 36.

¹⁹⁹ Z.B. ist die Zahl sozialwissenschaftlicher Publikationen zu Big Data erst seit 2010 sprunghaft angestiegen: HAUSER, 9.

²⁰⁰ Vgl. zum amerikanischen Recht: White House, Executive Office of the President 2014, 2; ZUBOFF 2015, 75.

²⁰¹ Z.B. bei: DAVENPORT; DIETRICH *et al.*

²⁰² Vgl. ROGERS SIMON, Data are or data is?, The Guardian vom 08.07.2012, abrufbar unter <www.theguardian.com> (besucht am 31.05.2020).

²⁰³ LANEY verwendete damals jedoch noch nicht den Begriff «Big Data»: LANEY DOUG, 3D data management: controlling data volume, velocity and variety, 06.02.2001, abrufbar unter <www.bibsonomy.org> (besucht am 31.05.2020).

rer Schnelllebigkeit (*velocity*) nur begrenzt mit herkömmlichen Tools bearbeitet werden können.²⁰⁴

Wie aus dem Begriff «Big» Data erhellt, ist das Datenvolumen (*volume*) im Grundsatz unbegrenzt.²⁰⁵ Im Jahr 2021 werden in jeder Stunde mehr Daten aufgezeichnet werden als in den letzten 30'000 Jahren.²⁰⁶ Das Wachstum ist exponentiell.²⁰⁷ Das Bundesgericht führt das Stichwort Big Data, soweit ersichtlich, nur in einem einzigen Entscheid aus dem Jahr 2014 explizit auf.²⁰⁸ Dort bezeichnen die Beschwerdeführerin und die Vorinstanz den Sachverhalt als «Big Data-Fall», d.h. als Fall «mit einer immensen Datenmenge». Streitgegenstand sind unter anderem «ein Datenvolumen von 22 Gigabytes bzw. 89'000 Dateien in 11'000 Verzeichnissen» sowie «65'345 Dateien in 346 Unterverzeichnissen» und «521'721 Wörter, die ausgedruckt 1'449 A4-Seiten» füllen.²⁰⁹ Das Bundesgericht widerspricht dieser Beschreibung von Big Data nicht.²¹⁰ Doch «*big*» im Gegensatz zu «*small*» in absoluten Zahlen auszudrücken, ist schwierig, da das Verständnis der Grösse von Unternehmen zu Unternehmen relativ ist und sich über die Zeit ändern kann.²¹¹ Die Zahlen im zitierten Bundesgerichtsentscheid erscheinen dem Autor ob der immer intensiveren Datenaufzeichnungen an Büroarbeitsplätzen als gering.

²⁰⁴ WILDHABER/KASPER, 756; CULIK, 53.

²⁰⁵ PRIEUR, 1644.

²⁰⁶ FREELAND CHRYSTIA, Yuri Milner on the future of the internet, 23.09.2011, abrufbar unter <<http://blogs.reuters.com>> (besucht am 31.05.2020). Vgl. auch die Schätzungen bei WESPI, 4, und THOUVENIN 2017, 28.

²⁰⁷ Ungefähr alle zwei Jahre verdoppelt sich die weltweit vorhandene Datenmenge: HORVATH, 1. Vgl. auch die Schätzungen bei BRYNJOLFSSON/MCAFEE, 66–67, White House, Executive Office of the President 2014, 1–2, Microsoft Corporation 2018b, 32, und CALDAROLA/SCHREY, N 3.

²⁰⁸ Und der europäische Gerichtshof hat das Stichwort «Big Data» bis anhin (31.05.2020) nicht verwendet (vgl. auch bereits GABATHULER SILVAN, 31).

²⁰⁹ Urteil BGer 1B_195/2014 vom 09.09.2014 E. 3.1.

²¹⁰ GABATHULER SILVAN, 31.

²¹¹ DAVENPORT, 7.

Mit der Vielfalt der Daten (*variety*) ist gemeint, dass die Art der Daten (strukturiert und unstrukturiert;²¹² Inhalte und Metadaten)²¹³ und ihre Herkunft (unternehmensintern oder aus dem Internet) irrelevant und im Grundsatz unbegrenzt sind.²¹⁴ Die Arbeitgeberin kann bisher nicht aufeinander bezogene Daten, beispielsweise traditionelle und nichttraditionelle Arbeitnehmerdaten, zusammenführen. Zu Ersteren zählen die Angaben im Lebenslauf über frühere Berufserfahrung und Ausbildungen. Letztere sind in der Regel nicht in der Datenbank der Personalabteilung gespeichert und betreffen etwa Daten der produzierenden oder der Finanzabteilung, aber auch der öffentlichen Register, Daten über Aktivitäten in sozialen Netzwerken, Sensordaten, Kommunikations-Metadaten oder den Browserverlauf.²¹⁵ Durch die Kombination entstehen Ergebnisse von neuer Qualität.²¹⁶

Die Daten liegen nicht einfach auf Speicherplatten herum: «Alles fließt» (altgr. *πάντα ῥεῖ*, «*pánta rhei*», Heraklit von Ephesos um 520–460 v.Chr.). Big Data zieht als schnelllebig, «reissender Strom» vorbei (*velocity*).²¹⁷ Der weltweite Internetdaten-Verkehr hat sich in den fünf Jahren zwischen 2006 und 2011 verzehnfacht.²¹⁸ Die Datenerfassung und -analyse erfolgen in Echtzeit, um Massnahmen

²¹² Unstrukturiert ist z.B. der E-Mail-Text, während die E-Mail-Adressen strukturiert sind, weil sie in standardisierter Form in das Empfänger- und Absenderfeld eingegeben werden. Folglich handelt es sich bei einer E-Mail insgesamt um einen halbstrukturierten Datensatz. Unstrukturierte Daten machen weltweit vier Fünftel der Daten aus: MRKONICH *et al.*, 2. Vgl. WESPI, 4, und PRIEUR, 1644.

²¹³ Metadaten sind «Daten über Daten». Sie kommen einem Etikett gleich, das die Bearbeitungshistorie festhält, etwa den Zeitpunkt der Datenerhebung oder den Bearbeitungszweck: World Economic Forum 2013, 23. Vgl. HOWARD, 3–4 [sic].

²¹⁴ WEBER 2015, N 3.

²¹⁵ TRINDEL.

²¹⁶ HORVATH, 2. Es kommt zur «totalen Vernetzung aller Bereiche»: KARGER/GAYCKEN, N 174. Vor allem aus unstrukturierten Daten werden neue Erkenntnisse gewonnen: IBM, 13. Vgl. THÜR, 78.

²¹⁷ DAVENPORT, 16; «*data in motion*»: WESPI, 6.

²¹⁸ BRYNJOLFSSON/MCAFFEE, 66–67.

mit unmittelbarer Auswirkung auf das Leben von Personen zu treffen.²¹⁹ Dazu braucht es spezielle Analyse-Algorithmen und hochleistungsfähige Hardware.²²⁰

Teilweise führt die Literatur weitere V-Eigenschaften auf, die über die drei von LANEY erwähnten hinausgehen: DE MAURO, GRECO und GRIMALDI folgern aus einer systematischen Literaturanalyse, dass Big Data einen Wertschöpfungsprozess einschliesse (sozusagen als viertes V: *value*).²²¹ Für Big Data ist somit essenziell, dass in der dritten Phase des Daten-Lebenszyklus die in Daten steckende Wertchance genutzt wird.²²² Um den Unterschied zwischen den Daten als Rohstoff und dem Wertschöpfungsprozess hervorzuheben, tritt mancherorts der Zusatz «Analytik» hinzu («Big Data-Analytik» bzw. «*big data analytics*»).

Um die V-Reihe um ein fünftes Glied zu erweitern, sei vorliegend auch die Richtigkeit der Daten (*veracity*) angesprochen. Sie lässt sich aufgrund des Volumens von Big Data, der Entstehungsgeschwindigkeit und Vielfalt kaum überprüfen, jedoch sollen die Ungenauigkeiten dank der grossen Datenmenge und geeigneter Analyse-Werkzeuge vergleichsweise gut auszumergen sein.²²⁴

²¹⁹ White House, Executive Office of the President 2014, 5. Vgl. WESPI, 4. WEBER 2015, N 1. Z.B. hat Google eine Zeit lang Grippe-Epidemien in 29 Ländern in Echtzeit vorausgesagt: Google LLC, Google flu trends and Google dengue trends, abrufbar unter <<https://www.google.org/flutrends>> (besucht am 31.05.2020).

²²⁰ CRAWFORD/SCHULTZ, 96. Näheres zu den Big Data-Programmiermodellen *MapReduce* von Google und *Hadoop* von Apache: KRILL PAUL, Hadoop becomes critical cog in the big data machine, 19.06.2012, abrufbar unter <www.infoworld.com> (besucht am 31.05.2020). Weiterführend zu den Big Data-Bearbeitungsmethoden: DE MAURO *et al.*, 126; BISSELS *et al.*, 3042; JAKOB, 13.

²²¹ DE MAURO *et al.*, 122. Vgl. ebenso PRIEUR, 1644, BISSELS *et al.*, 3042, EU/Europarat, 349, TRINDEL und White House, Executive Office of the President 2014, 15.

²²² Siehe zum Begriff der Wertchance S. 21–22. Siehe zum Daten-Lebenszyklus S. 19–20.

²²³ Europarat 2017, 2; HOFFMANN-RIEM, 19; RICHARDS/KING, 394; zur Betonung der mit Big Data verbundenen Technologien und Methoden entsprechend «*big data technology*» und «*big data methods*»: DE MAURO *et al.*, 131.

²²⁴ WESPI, 5. Z.B. funktioniert die Big Data-Übersetzungsmaschine von Google besser als diejenige von IBM, welche auf einem kleineren, aber bereinigten Datensatz basiert: CUKIER/MAYER-SCHÖNBERGER, 31. A.M., unter Hinweis auf mögliche Qualitätsmängel: HOFFMANN-RIEM, 18.

c) Kritik am Begriff «Big Data»

Die Verwendung des Begriffs «Big Data» stösst teilweise auf Kritik.²²⁵ Diese zielt auf den ersten Wortteil, «Big». Vergessen gehe dabei, dass auch gestützt auf kleine Datensätze wichtige Entscheide gefällt würden.²²⁶ Ausserdem sei die Vielfalt der Daten wesentlich prägender als das Volumen und biete insbesondere im Bereich der Personalverwaltung mehr Innovationspotenzial.²²⁷ Auch der Aspekt der Geschwindigkeit, das dritte V, dürfte im statischen Ausdruck «Big» zu kurz kommen. Vermehrt taucht daher der Begriff «*Smart Data*» auf, der die Wissensgewinnung ins Zentrum rückt.²²⁸

d) Verhältnis zu People Analytics

An gewissen Stellen wird People Analytics als ein Teilbereich von Big Data beschrieben, in welchem es um Big Data-Analysen geht, die auf den Arbeitsplatz bezogen sind.²²⁹ Richtigerweise ist jedoch zu differenzieren: People Analytics funktioniert mit oder ohne Big Data.²³⁰ Ist die Datenmenge klein, aber sind andere beschriebene Aspekte erfüllt, insbesondere der Einsatz von Algorithmen, so handelt es sich ebenfalls um People Analytics. Beispielsweise kann es sowohl für ein Gross- als auch für ein Kleinunternehmen sinnvoll sein, die E-Mail-Prozesse zu optimieren.²³¹ Bei wenigen Angestellten wird die Datenmenge jedoch kleiner bleiben.

²²⁵ DAVENPORT, 6–7; FEW STEPHEN, Basta, big data: it's time to say arrivederci, 27.06.2017, abrufbar unter <www.perceptualedge.com> (besucht am 31.05.2020).

²²⁶ RICHARDS/KING, 394.

²²⁷ CULIK, 59. «*Variety, not volume or velocity, drives Big Data investments*»: Tableau Software, Top 10 big data trends 2017, abrufbar unter <www.tableau.com> (besucht am 31.05.2020). GOLA 2019, N 1103.

²²⁸ CULIK, 59; ANGRAVE *et al.*, 2; HARVEY *et al.* Smart Data sind ihrerseits die Grundlage für Smart Services: BMAS 2017, 202.

²²⁹ People Analytics als Teilbereich von Big Data: BODIE *et al.*, 962. Vgl. auch: TRINDEL. «*Big data in employment is referred to [...] as [...] human resources analytics*»: MRKONICH *et al.*, 12.

²³⁰ DZIDA/GROH, 1917.

²³¹ Etwa mithilfe der noch vorzustellenden Software MyAnalytics von Microsoft. Siehe dazu S. 50.

2.2.6 Zwischenfazit: zusammenhängende technische Konzepte

Hinter dem Wort «Analytics» steckt ein Daten-Lebenszyklus. Der Daten-Lebenszyklus besteht aus den vier Phasen der Beschaffung, Analyse, Nutzung und Löschung oder Wiederverwertung der Daten. Betreffend die erste Phase – Beschaffung – wurden sowohl der Begriff des Datums als auch die Hardware und Infrastruktur zur Aufzeichnung der Daten beschrieben.²³² In der zweiten Phase – Analyse – kommen Algorithmen zum Einsatz, die gegenwärtig noch relativ einfältig nach Korrelationen suchen, aber durch KI immer intelligenter werden.²³³ In der dritten Phase – Nutzung – zeigt sich, dass die Big Data-Wirtschaft ein Wertschöpfungsprozess und kein Selbstzweck ist.²³⁴ Kommt es in der vierten Phase zu einer Wiederverwendung, erlangen alle diese Begriffe erneut Relevanz.

Rechtlich und für die vorliegende Forschungsfrage²³⁵ relevant ist das Gesamtbild: Hinter People Analytics steckt eine enorme technische Apparatur. Es wächst eine datafizierte Welt heran, in der immer und überall Datenerhebungen und -analysen geschehen können und in der sich der Arbeitnehmer zurechtfinden muss. In dieser Welt hängen Begriffe wie «Sensoren», «Algorithmen» und «Big Data» zusammen.²³⁶ Sie bedingen und stimulieren sich gegenseitig in Wechselwirkung: Daten, Computerinfrastruktur und Algorithmen sind Voraussetzungen für eine Big Data-Wirtschaft; umgekehrt wird der gewonnene Mehrwert Investitionen in die Erhebung weiterer Daten mit verbesserter Hardware, höherer KI und erweiterter Zwecksetzung ermöglichen. Die konkreten wirtschaftlichen Verwendungszwecke von People Analytics werden sogleich dargestellt.

²³² Siehe einerseits zu den Daten S. 20–25, andererseits zur Hardware und Infrastruktur S. 25–28.

²³³ Siehe S. 29–36.

²³⁴ Siehe S. 36–40.

²³⁵ Siehe S. 11.

²³⁶ Vgl. algo:aware [sic], 10. Big Data und KI bewegen sich in einem «Kontinuum»: DAVENPORT/BEAN. Big Data als Teilelement der Digitalisierung: HOFFMANN-RIEM, 13.

2.3 Verwendungszwecke

2.3.1 Arbeitnehmer-Lebenszyklus

Nachdem der Wortteil «Analytics» und der Daten-Lebenszyklus vorgestellt worden sind, soll nun der erste Wortteil – «People» – in den Vordergrund rücken. Es ist zu erklären, inwiefern die Menschen von dem Phänomen betroffen sind und wie sich die Interaktion zwischen Mensch und Technik gestaltet. Darzustellen sind die Verwendungszwecke von People Analytics.²³⁷ Die Wissensgewinnung durch Datenanalysen ist kein Selbstzweck, sondern das Ziel ist stets, das gewonnene Wissen auf die Wirklichkeit anzuwenden.²³⁸ Der Nutzen von People Analytics besteht beispielsweise darin, Schulungsressourcen bei den richtigen Gruppen von Arbeitnehmern zu allozieren oder sich von Praktiken oder Personen zu trennen, die hohe Kosten verursachen.²³⁹

Die Zwecke von People Analytics können entlang des Lebenszyklus eines Arbeitnehmers in eine zeitliche Ordnung gesetzt werden: Arbeitnehmende begegnen Datenbearbeitungen erstmals in der Bewerbungsphase, später während der gesamten Dauer des Arbeitsvertrags und auch nach dessen Beendigung.²⁴⁰ Orientiert am Arbeitnehmer-Lebenszyklus können die mit Personalanalysen verfolgten Zwecke grob in fünf Kategorien unterteilt werden: Rekrutierung, Leistungssteuerung, Compliance-Management, Gestaltung von Arbeit und Arbeitsplatz sowie Mitarbeiterbindung (siehe Abb. 4).²⁴¹

²³⁷ Mit der Betrachtung der Verwendungszwecke zielt die vorliegende Arbeit auf Beständigkeit und bricht mit den Darstellungen bei RIESSELMANN-SAXER, WOLFER sowie CUSTERS und URSIC (siehe zu diesen Autoren: S. 6–8), die alle einzelne Technologien analysieren, die in einigen Jahren möglicherweise überholt sein werden.

²³⁸ VASELLA/ROSENTHAL, 4. «*Profiling is not a goal in itself but a technical means of achieving a particular result*»: Europarat 2008, 32.

²³⁹ TRINDEL.

²⁴⁰ Eine bei Personalverantwortlichen verbreitete Betrachtung unterteilt den Mitarbeiter-Lebenszyklus weiter in sechs Phasen: Anziehung durch Aufbau einer geeigneten Marke und Unternehmenskultur (*attraction*), Bewerbungsphase (*recruitment*), Eingliederung in die Unternehmenskultur (*onboarding*), Weiterentwicklung der Fähigkeiten und der Karriere (*development*), Mitarbeiterbindung (*retention*) und Beendigungsphase (*separation*): FRENCH MATTHEW, Automating employee lifecycle management: six steps to success, 02.07.2019, abrufbar unter <www.subscribe-hr.com> (besucht am 31.05.2020).

²⁴¹ Vgl. auch die Abb. bei WEIBEL *et al.*, 26, und bei WILDHABER/KASPER, 760.



Abb. 4: Fünf Verwendungszwecke von People Analytics entlang des Arbeitnehmer-Lebenszyklus

2.3.2 Rekrutierung

In der Bewerbungsphase müssen die eingehenden Kandidatenprofile mit der Stellenbeschreibung abgeglichen (*matching*) und der Wunschkandidat (der *perfect match*)²⁴² herausgefiltert werden (*shortlisting*). So gleicht beispielsweise die Funktion Talent Match von LinkedIn die von Unternehmen gesuchten Profile in Echtzeit mit den Profilen der Netzwerk-Mitglieder ab.²⁴³ Watson von IBM eruiert, welches Profil voraussichtlich die höchste persönliche Arbeitnehmerleistung erbringen wird.²⁴⁴ Die Software Kenexa prognostiziert die Verweildauer im Unternehmen und die Eignung für eine Führungsposition.²⁴⁵ Auf eine längerfristige Bindung von Arbeitnehmenden will das Analytik-Unternehmen Evolv (heute Cornerstone OnDemand) aus der Aktivität in einem sozialen Netzwerk wie Facebook, einer kurzen Distanz zwischen Wohn- und Arbeitsort sowie einer kreativen Per-

²⁴² BISSELS *et al.*, 3043.

²⁴³ BRYNJOLFSSON/MCAFEE, 217.

²⁴⁴ FAZ vom 01.03.2018, Lieber Roboter als Personaler, abrufbar unter <www.faz.net> (besucht am 31.05.2020). Vgl. WEAVER, 3: «Biodata [...] predict job performance.»

²⁴⁵ DIETRICH *et al.*, 23.

sönlichkeit schliessen – nicht entscheidend seien Berufserfahrung und Ausbildung.²⁴⁶ Zudem verzeichnen Bewerber, die eine eigene Internet-Suchmaschine installiert haben, 15 Prozent weniger Fehltage und erzielen eine höhere Kundenzufriedenheit als solche, die einen vorinstallierten Browser benützen.²⁴⁷

In Zeiten des Fachkräftemangels ist es nicht immer eine Option, sich mit den passiv empfangenen Bewerbungen zu begnügen. Stattdessen ermittelt die Arbeitgeberin – mit Firmen wie Entelo, Talentwunder oder Joberate im Rücken – aus Webdaten und aktuellem Userverhalten aktiv, ob Kandidaten latent bereit wären, für eine neue Stelle die bestehende zu kündigen und umzuziehen (*active sourcing*).²⁴⁸ Anzeichen für eine Wechselbereitschaft bestehen, wenn eine Person nach längerer Zeit ihr Profil in den sozialen Netzwerken auf den neusten Stand bringt, oder je nachdem, welche ihr zugesandten Inhalte sie liest und welche nicht.²⁴⁹ Auf die Personensuche spezialisierte Suchmaschinen²⁵⁰ erleichtern das Finden von Informationen über Individuen.

Ist eine engere Auswahl von passenden Profilen getroffen worden, kann der Algorithmus direkt das Bewerbungsgespräch führen. Das Kosmetikunternehmen L'Oréal verwendet einen Chabot mit Namen Mya, der Fragen stellen und beantworten sowie Qualifikationen, Wohnort und Gehalt überprüfen kann. Geplant ist aber auch die Berücksichtigung weicher Faktoren, etwa ob der Bewerber zu den Unternehmenswerten von L'Oréal passt.²⁵¹ Weitergehende Lösungen messen physiologische Reaktionen und passive Verhaltenscharakteristika wie Herzschlag,

²⁴⁶ So die Ergebnisse aus einer Zusammenarbeit von Evolv mit dem Call-Center Xerox: LEBER JESSICA, The machine-readable workforce, 27.05.2013, abrufbar unter <www.technologyreview.com> (besucht am 31.05.2020); WALKER JOSEPH, Meet the new boss: big data, The Wall Street Journal vom 20.09.2012, abrufbar unter <www.wsj.com> (besucht am 31.05.2020); NEUBERGER, 160. Siehe zur Korrelation zwischen Arbeitsweg und Verbleibedauer bereits S. 34.

²⁴⁷ SPRAGUE 2015, 32, m.w.H.; ROSENBLAT/WIKELIUS *et al.*, 1.

²⁴⁸ KAINER/WEBER, 2743; Entelo: REINSCH/GOLTZ, 37; Joberate und Talentwunder: BRAEHMER BARBARA, Ab wann werden viele Daten im Personalwesen HR-Big-Data?, 12.08.2016, abrufbar unter <https://intercessio.de> (besucht am 31.05.2020).

²⁴⁹ So die Personaldienstleister Hays und Manpower: GRATWOHL NATALIE, Wie Personalvermittler auf LinkedIn und Xing nach Talenten suchen, NZZ vom 08.01.2018, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

²⁵⁰ Z.B. LittleSis oder Yasni.

²⁵¹ Mya arbeitet mithilfe von KI und Sprachbearbeitung: SHARMA ANUSHREE, How AI reinvented hiring practice at L'Oréal, 16.08.2018, abrufbar unter <www.peoplematers.in> (besucht am 31.05.2020).

Augenbewegungen und Gesichtsausdruck eines Bewerbers während seiner Vorstellung.²⁵²

Eine strategische Personalplanung ermöglichen das Schweizer Unternehmen People Analytix oder die Software Jobfeed von Textkernel, indem sie vorhersagen, wie sich der Personalmarkt entwickeln wird.²⁵³ IBM-Analysten erfassen zur Bestimmung des künftigen unternehmensinternen Fachkräftebedarfs die Fähigkeiten und Erfahrungen der gesamten IBM-Belegschaft.²⁵⁴ Der amerikanische Lebensmittelfabrikant Conagra Foods sah sich mit dem Problem konfrontiert, dass über die Hälfte seiner Angestellten in den nächsten zehn Jahren in Pension gehen wird, weshalb er neues Personal brauchte, das fähig und willens war, schnell neue Aufgaben zu lernen. Eine Datenanalyse ergab, dass diese Fähigkeit über alle Altersklassen verteilt war und Conagra Foods bei der Rekrutierung nicht nur auf junge Leute beschränkt war.²⁵⁵ Mit People Analytics kann die Arbeitgeberin somit Lücken im Unternehmenswissen schliessen bzw. ihr Nichtwissen bewirtschaften, was genauso wichtig ist wie die Kultivierung des Wissens.²⁵⁶

2.3.3 Leistungssteuerung

Zunächst ist im Rahmen der Leistungssteuerung an die elektronische Überwachung (*electronic surveillance*) zu denken im Hinblick darauf, ob der Mitarbeiter seine arbeitsvertraglich geschuldete Leistung überhaupt erbringt. Besonders wenn die Arbeitgeberin das Arbeiten von zu Hause aus zulässt, wird die Leistungsüberprüfung schwieriger. Das Zeiterfassungssystem Work Diary von Upwork zählt deshalb die Tastenanschläge im Homeoffice, erstellt alle zehn Minuten eine Bildschirmfotografie und enthält einen Sofortnachrichtendienst, um den Arbeitnehmer

²⁵² Sog. *hireobotics solutions* wie z.B. der Roboter Sophie: WILDHABER 2017, 216. Vgl. auch die Plattform HireIQ und die Software Infor Talent Science: SNYDER, 253.

²⁵³ People Analytix berücksichtigt die Trends für künftig entscheidende Fähigkeiten von Mitarbeitenden: People-Analytix, abrufbar unter <<https://people-analytix.com/>> (besucht am 31.05.2020). Bei Jobfeed sehen Arbeitgeberinnen, wo welche Talente verfügbar werden (*talent mapping*), und Arbeitnehmer, wo welche Stellen entstehen: BRAEHMER BARBARA, Ab wann werden viele Daten im Personalwesen HR-Big-Data?, 12.08.2016, abrufbar unter <<https://intercessio.de>> (besucht am 31.05.2020).

²⁵⁴ SPRAGUE 2015, 33.

²⁵⁵ NEUBERGER, 161.

²⁵⁶ Vgl. DRUEY 2015, 6.

zu kontaktieren.²⁵⁷ Im Einsatz sind auch Softwares, die über eine Webcam alle zehn Minuten eine Foto des Mitarbeiters persönlich im Homeoffice erstellen²⁵⁸ und den E-Mail-Verlauf und die Kalendereinträge kontrollieren.²⁵⁹

Der US-Postzulieferer FedEx setzt in seinen Logistikzentren auf einen Paketscanner, den der Arbeitnehmer am rechten Unterarm trägt. Der Scanner erfasst die Pakete und zeichnet dabei die Arbeitsgeschwindigkeit auf. Ein Countdown gewährt dem Arbeitnehmer eine bestimmte Anzahl Sekunden bis zum Scannen des nächsten Pakets. Gerät der Arbeitnehmer in Verzug, weil er beispielsweise in einen falschen Korridor im Lager eingebogen ist, ergeht eine Benachrichtigung an eine Aufsichtsperson.²⁶⁰ Der Detailhändler Tesco senkt mit vergleichbaren Geräten seinen Bedarf an Vollzeitstellen in den Warenhäusern um 18 Prozent.²⁶¹ Amazon arbeitet mit einem Ultraschall-Armband, das vibriert, wenn der Arbeitnehmer die falsche Ware verpackt.²⁶² Intelligente Arbeitshandschuhe dokumentieren die Arbeitsschritte, indem sie Informationen von Maschinen, die der Arbeitnehmer bedient, lesen.²⁶³

Das Elektroenzephalografie-Stirnband (*EEG headband*) mit Namen «Muse» misst die Gehirnwellen des Angestellten und damit seine aktuelle Leistungsfähigkeit und Aufmerksamkeit bzw. seinen Müdigkeitsgrad und schlägt ihm gegebenenfalls

²⁵⁷ AKHTAR/MOORE, 113. Vergleichbare Produkte sind: RescueTime, Toggl, ATracker, My Minutes (AKHTAR/MOORE, 106) oder Hubstaff (KATZ MIRANDA, The creative ways your boss is spying on you, 08.12.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020)).

²⁵⁸ COLLIER, 3.

²⁵⁹ RIEDY/WEN, 89. In einem anderen Fall wurde heimlich ein sog. Trojaner (Spyware) beim Computer eines deutschen Betriebsratsmitglieds installiert. Die Software aktivierte das Mikrofon im PC, was ein problemloses Mithören ermöglichte, und erstellte fünf Minuten lang jede Sekunde einen Screenshot: DÄUBLER, N 315.

²⁶⁰ BRUDER JESSICA, These workers have a new demand: stop watching us, 27.05.2015, abrufbar unter <www.thenation.com> (besucht am 31.05.2020).

²⁶¹ AKHTAR/MOORE, 116.

²⁶² COLLIER, 4; HURTZ SIMON, Diese Technologien können Angst machen, Süddeutsche Zeitung vom 27.12.2018, abrufbar unter <www.sueddeutsche.de> (besucht am 31.05.2020); Patentierung des Ultraschall-Armbands 2018: KATZ MIRANDA, The creative ways your boss is spying on you, 08.12.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020).

²⁶³ KLEBE/WEISS, 265.

eine Pause vor.²⁶⁴ Intelligente Brillen (*smart eyeglasses*) mit eingebauten Kameras zur Blickverfolgung (*eye tracking*) registrieren nicht nur, was der Angestellte sieht, sondern auch, ob er darauf fokussiert oder abgelenkt ist.²⁶⁵ Das Unternehmen Schlumberger, ein Dienstleister für Erdölfelder, gewährt seinen Angestellten häufigere kurze Pausen, weil eine systematische Videoanalyse ergeben hat, dass so die Produktivität steigt.²⁶⁶

Zur Auswertung von Kundengesprächen überprüfen Callcenter mit einer Stichwortsuche (*keyword spotting*), wie oft der Agent das zu verkaufende Produkt oder das Preis-Leistungs-Verhältnis erwähnt,²⁶⁷ und mit einer Stimmanalyse, ob Mitarbeiter (oder Kunden) zu langsam sprechen²⁶⁸ und welche Emotionen mitschwingen.²⁶⁹ Diese in Telefonzentralen heimische Technologie verlässt nun ihr Stammgebiet: Auch bei Hostessen, Kellnern und Verkäuferinnen in Supermärkten wird gemessen, wie oft sie ihren Kunden ein Lächeln schenken.²⁷⁰ Laut dem Unternehmen Affectiva aus Boston, das Emotionsmesstechnik produziert und Gesichtsausdrücke scannt, neigen Frauen in alltäglichen Gesprächen dazu, häufiger zu lächeln als Männer.²⁷¹

²⁶⁴ SCHINAGL, 508. Solche Kopfbedeckungen sind z.B. in chinesischen Unternehmen im Einsatz: COLLIER, 5. Vgl. das britische Bahnunternehmen, das seinen Angestellten ein Wearable verteilt (zu diesem Begriff siehe S. 25–26), das ihren Energiestand misst: KATZ MIRANDA, The creative ways your boss is spying on you, 08.12.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020).

²⁶⁵ COLLIER, 5.

²⁶⁶ SHOOK *et al.* Vgl. HURTZ SIMON, Diese Technologien können Angst machen, Süddeutsche Zeitung vom 27.12.2018, abrufbar unter <www.sueddeutsche.de> (besucht am 31.05.2020): In chinesischen Schulen benachrichtigt ein Gesichtserkennungssystem, bestehend aus Kameras, den Lehrer, wenn es ein unaufmerksames Kind identifiziert.

²⁶⁷ GOLA 2015, N 420.

²⁶⁸ BRUDER JESSICA, These workers have a new demand: stop watching us, 27.05.2015, abrufbar unter <www.thenation.com> (besucht am 31.05.2020).

²⁶⁹ AKHTAR/MOORE, 105. Den Callcenter-Agenten wird die Vermittlung einer positiven Stimmung antrainiert: GOLA 2015, N 421.

²⁷⁰ KIULIAN ARTUR, Why your next boss will be a robot, 18.09.2017, abrufbar unter <www.linkedin.com> (besucht am 31.05.2020). Der Detailhändler Walmart besitzt ein Patent für eine Erfindung zur Verfolgung der Gespräche zwischen Kunden und Mitarbeitern an der Kasse: COLLIER, 4.

²⁷¹ CHENG MICHELLE, How do you design a robot that isn't sexist or racist? It's harder than you think, 28.02.2018, abrufbar unter <www.inc.com> (besucht am 31.05.2020).

Das Telematik-System On-Road Integrated Optimization and Navigation (ORION) des Postzulieferers UPS optimiert die Bewegungsmuster von Postboten anhand ihrer Geolokalisationsdaten: ORION berechnet die kürzeste und hinsichtlich Benzinverbrauch billigste Fahrstrecke, lenkt die Autos an Staus und schlechtem Wetter vorbei und ermöglicht personalisierte Lieferungen (z.B. in Bezug auf die Lieferzeit).²⁷² Solche Flottenanalyse-Systeme kommen auch im Flugverkehr vor.²⁷³ Möglich ist darüber hinaus die Verfolgung der Position und der Bewegungen der Mitarbeiter persönlich durch Computerchips, die in die Arbeitskleidung eingenäht sind:²⁷⁴ Ein Spital in Florida hat die Heilmittelvorräte besser auf die Krankenstationen verteilt, nachdem es realisiert hatte, wie viel Zeit die Krankenschwestern damit verloren, zusätzliche Medikamente aufzuspüren.²⁷⁵ Das Medizinalunternehmen Propeller Health (zuvor Asthmapolis) deckt Umweltauslöser für Asthmaanfälle der Arbeitnehmer auf (z.B. die Aufenthaltsnähe zu bestimmten Pflanzenkulturen), indem es Ortungsdaten aus einem GPS-Sensor und Atmungsdaten aus einem Asthma-Inhalator zusammenführt.²⁷⁶

Gesundheitsprogramme (*wellness programmes*) sind Datenbearbeitungen zur Bekämpfung von Übergewicht, Rauchen, hohem Blutdruck und weiteren physischen Beschwerden.²⁷⁷ Der Detailhändler Walmart identifiziert Arbeitnehmer mit erhöhtem Diabetesrisiko und legt ihnen nahe, einen Arzt aufzusuchen oder sich einem

²⁷² KONRAD ALEX, Meet Orion, software that will save UPS millions by improving drivers' routes, Forbes vom 01.11.2013, abrufbar unter <www.forbes.com> (besucht am 31.05.2020); ZAX DAVID, Brown down: UPS drivers vs. the UPS algorithm, 01.03.2013, abrufbar unter <www.fastcompany.com> (besucht am 31.05.2020). ORION erinnert zudem im Voraus, wann gewisse Fahrzeugteile ersetzt werden müssen (*preventative maintenance*): MAYER-SCHÖNBERGER/CUKIER, 59. Vgl. zu einem verwandten System des Logistikunternehmens Schneider National: DAVENPORT, 191.

²⁷³ Mit den Flight Efficiency Services (FES) von General Electric kann ein Pilot seine Entscheidungen betreffend Flugplanung und Kerosinladung optimieren: General Electric and Business Insider Studios, How big data and the industrial internet can help southwest save \$100 million on fuel, 15.10.2015, abrufbar unter <www.businessinsider.com> (besucht am 31.05.2020).

²⁷⁴ Europarat 2016b, 54.

²⁷⁵ COLLIER, 6; SHOOK *et al.*

²⁷⁶ MAYER-SCHÖNBERGER/CUKIER, 95.

²⁷⁷ The Economist vom 05.01.2019, The spy who hired me, abrufbar unter <www.economist.com> (besucht am 31.05.2020). Ein Vergleich von Gesundheitsprogrammen in zwölf multinationalen Unternehmen mit Sitz in Rumänien findet sich bei: STAN.

Programm gegen Fettleibigkeit und für gesunde Ernährung zu unterziehen.²⁷⁸ Mitarbeiterinnen, die auf der Walmart-Gesundheits-App Arztrezepte zur Empfängnisverhütung nicht mehr einlösen und nach Themen über Fruchtbarkeit suchen, erhalten Informationen zur Schwangerschaftsvorsorge und Kontakte zu Hebammen.²⁷⁹ Mit besseren Gesundheitswerten steigt die Leistungsfähigkeit der Arbeitnehmer.²⁸⁰ Zusätzliche Profite locken in den USA, wo sich die Arbeitgeberin oft an den Krankenversicherungskosten der Arbeitnehmer beteiligt.²⁸¹ Die Arbeitnehmer, die sich immer besserer Gesundheit erfreuen, stellen seltener Versicherungsfälle in Rechnung,²⁸² wodurch Prämienverbilligungen möglich werden.²⁸³

Den Vermittlungsplattformen ist die jederzeitige Aufrechterhaltung ihres Systems für die Kunden wichtig. Der Essenszulieferer Deliveroo aus London beispielsweise wertet aus, wie lange seine Kuriere benötigen, um eine Bestellung zu bestätigen, und ob sie Bestellungen ablehnen. Erreicht der Kurier die vereinbarte Leistung nicht, blockiert ihn das System.²⁸⁴ Im gleichen Stil operiert der Taxivermittler Uber: Hat sich ein Taxichauffeur ins System eingeloggt, muss er Aufträge innert zwanzig Sekunden akzeptieren. Verpasst er drei Gelegenheiten in Folge, wird er

²⁷⁸ Walmart kooperiert hierfür mit Castlight Healthcare: AJUNWA/CRAWFORD/FORD, 474.

²⁷⁹ AJUNWA/CRAWFORD/FORD, 475; WILSON *et al.*, 24–25.

²⁸⁰ Vgl. PARISI, 320.

²⁸¹ Vgl. PARISI, 320. Schweizerische Arbeitgeberinnen haben weniger solche finanziellen Anreize, weil Arbeitnehmende die Krankenversicherungsprämien hierzulande direkt bezahlen und eine Krankentaggeldversicherung der Arbeitgeberin freiwillig ist. Im Bereich der (obligatorischen) Unfallversicherung könnten aber vergleichbare Interessenkonstellationen entstehen.

²⁸² Reduktion der Entschädigungsansprüche von Arbeitnehmern um rund zwei Drittel beim Entsorgungsunternehmen Richfield Management LLC, seit Bewerber, die aufgrund eines Einstellungstests ein hohes Invaliditätsrisiko aufweisen, systematisch abgelehnt werden: ROSENBLAT/WIKELIUS *et al.*, 5.

²⁸³ Das US-Beratungsunternehmen Appirio kommt in den Genuss von USD 300'000 Prämienverbilligung bei total USD 5 Mio. Prämien, weil es die Gesundheitsdaten der Arbeitnehmer mit dem Versicherer teilt: PARISI, 324. A.M., keine Prämieinsparungen beim Plastikbearbeitungsunternehmen Regal Plastics aus Texas: ROWLAND CHRISTOPHER, With fitness trackers in the workplace, bosses can monitor your every step – and possibly more, The Washington Post vom 16.02.2019, abrufbar unter <www.washingtonpost.com> (besucht am 31.05.2020).

²⁸⁴ KIULIAN ARTUR, Why your next boss will be a robot, 18.09.2017, abrufbar unter <www.linkedin.com> (besucht am 31.05.2020).

automatisch für einige Minuten ausgeloggt. Im Wiederholungsfall wird sein Konto gelöscht.²⁸⁵

Einen alternativen Ansatz verfolgt Microsoft mit dem Programm MyAnalytics. Es geht hier darum, den Mitarbeitern die Mittel zu verschaffen, um sie zu höherer Leistung basierend auf Selbständigkeit zu befähigen (*empowering employees*).²⁸⁶ Ein personalisiertes Übersichtsfenster (Dashboard) zeigt dem Arbeitnehmer einen wöchentlichen E-Mail-Zusammenschnitt an²⁸⁷ und, zum Ansporn, die Durchschnittswerte des Unternehmens betreffend E-Mail-Erledigung.²⁸⁸ Nur die Arbeitnehmer selbst können ihre personenbezogenen Daten einsehen.²⁸⁹

2.3.4 Compliance-Management

«Compliance» bedeutet wörtlich die «Befolgung» und bezieht sich auf alle für ein Unternehmen verbindlichen Normen.²⁹⁰ Die Arbeitgeberin haftet für die Nichtbefolgung durch ihre Angestellten.²⁹¹

Dem Vermögensschutz der Arbeitgeberin dienen Videoüberwachungsanlagen und die Aufzeichnung der Tastenanschläge bei der Kasse.²⁹² Ein japanischer Antidiebstahlsitz kontrolliert, ob der berechtigte Fahrer, dessen individueller Abdruck über 360 eingebaute Drucksensoren ertastet wird, im Firmenauto Platz nimmt.²⁹³ Die Geschäftsgeheimnisse schützt das System Teramind, das bei der Bank BNP Pa-

²⁸⁵ KIULIAN ARTUR, Why your next boss will be a robot, 18.09.2017, abrufbar unter <www.linkedin.com> (besucht am 31.05.2020).

²⁸⁶ Microsoft Corporation 2018a, 4.

²⁸⁷ Microsoft Corporation 2018a, 4.

²⁸⁸ Microsoft Corporation 2018a, 11.

²⁸⁹ Microsoft Corporation 2018a, 4.

²⁹⁰ Die Funktion Compliance überprüft die Einhaltung von Regeln im weitesten Sinne (Gesetze, regulatorische und interne Vorschriften, marktübliche Standards, Standesregeln und ethische Grundsätze): Eidgenössische Finanzmarktaufsicht, N 7; NOBEL, § 9 N 118; Compliance-Officers setzen sich hauptsächlich mit den folgenden Gebieten auseinander: Geldwäscherei, neue Regulierungen, Korruption, Kartellrecht, Datenschutz, neue Produkte und Dienstleistungen, Cross-Border-Fragen und Interessenkonflikte: ROTH, 133. DÄUBLER, N 427k.

²⁹¹ RIEDY/WEN, 87.

²⁹² COLLIER, 6; NEUBERGER, 162.

²⁹³ CUKIER/MAYER-SCHÖNBERGER, 34.

ribas und dem Mobilfunknetzbetreiber Salt (vormals Orange) im Einsatz ist:²⁹⁴ Es filtert alle E-Mails einschliesslich Anhängen und Bildern sowie äusseren Verbindungsdaten (Randdaten) beispielsweise auf Namen von Konkurrenten (sog. Datenscreening)²⁹⁵ und warnt die Arbeitgeberin, wenn Angestellte vertrauliche Dokumente teilen. Der Lügendetektor des Schweizer Beratungsunternehmens 1-prozent GmbH entlarvt Hochstapler dadurch, dass sie in ihre unwahren Aussagen immer gerade so viel Wahrheit einflechten, dass ihr Gegenüber unablässig verwirrt wird.²⁹⁶ Ein britisches Pendant deutet die unbewusste Unsicherheit in einer Stimme als Zeichen möglicher betrügerischer Absichten.²⁹⁷

Die US-Investmentbank JP Morgan verwendet das Datenscreening zur Aufdeckung von Verstössen gegen finanzmarktrechtliche Verhaltenspflichten wie beispielsweise Betrug (*fraud detection*) oder Insider-Handel.²⁹⁸

Zur Kontrolle von Berechtigungen sind biometrische Zutritts- oder Kassensysteme, bei denen die Mitarbeitenden sich mit ihrem Fingerabdruck identifizieren müssen, weit verbreitet, so etwa in der Gastronomie.²⁹⁹

Auf die Einhaltung von Arbeitssicherheits-Richtlinien zielen die intelligenten Teppiche der Lausanner Firma Technis, die registrieren, wer wo hintritt.³⁰⁰ Andernorts warnen smarte Socken den Arbeitnehmer vor Stürzen.³⁰¹ Die Software Intelligent Edge von Microsoft ermittelt via Videokameras, ob ein Mitarbeiter die Schutzbrille nicht aufsetzt oder ein Fass mit einer gefährlichen Chemikalie ausleert.³⁰² Arbeitsschuhe mit einem integrierten Drucksensor vibrieren, wenn der

²⁹⁴ Vgl. KATZ MIRANDA, The creative ways your boss is spying on you, 08.12.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020).

²⁹⁵ Zum Begriff des Datenscreenings: OWSCHIMIKOW, 3. Vgl. RIEDY/WEN, 88.

²⁹⁶ Zum Einsatz kommt dabei die Technik Aachener Firma Precire Technologies: GENOVA MICHAEL, Mit Robotern gegen Hochstapler: Firmen jagen unehrliche Mitarbeiter, Tagblatt vom 22.07.2018, abrufbar unter <www.tagblatt.ch> (besucht am 31.05.2020).

²⁹⁷ Entsprechende Personen werden von Betrugsspezialisten ins Kreuzverhör genommen: DÄUBLER, N 378j.

²⁹⁸ DÄUBLER, N 429b.

²⁹⁹ EDÖB 2018a, 28.

³⁰⁰ Die Teppiche registrieren z.B. in Altersheimen Stürze: Bilanz vom 15.11.2016, Ein intelligenter Teppich sorgt für Hightech, abrufbar unter <www.bilanz.ch> (besucht am 31.05.2020).

³⁰¹ Vgl. ALLENSPACH, N 4.

³⁰² Oder die Software beauftragt eine Krankenschwester, einem erkennbar müden Patienten einen Rollstuhl zu bringen: SULLIVAN MARK, At build, Microsoft's vision of the

Mitarbeiter übermässig schwere Lasten trägt.³⁰³ Drohnen überwachen die Sicherheit von Geleisearbeitern der Bahn.³⁰⁴ Lastwagenfahrer tragen intelligente Mützen, die sie vor einem Sekundenschlaf warnen.³⁰⁵ Uber misst den Radeinschlag, um die Fahrfähigkeit und den Fahrstil seiner Taxichauffeure zu kontrollieren.³⁰⁶

Um die Compliance mit Antidiskriminierungs-Bestimmungen zu gewährleisten, prüft das System Themis, ob Softwares Vorurteile und Verzerrungen enthalten.³⁰⁷ Auch die Software von Paradigm aus San Francisco unterstützt Organisationen in ihrem Bestreben, vielfältiger und integrativer zu werden.³⁰⁸ Diese Software enthält Befangenheitstests, um Vorurteile, die jeder im Laufe seines Lebens entwickelt, aufzudecken.³⁰⁹

Die Datenanalysen dienen ferner als Grundlage, um die Interessen- und Werteangleichung zwischen Unternehmen und allen Mitarbeitenden voranzutreiben.³¹⁰

2.3.5 Arbeits- und Arbeitsplatzgestaltung

Zwischen Daumen und Zeigefinger implantierte Mikrochips vereinfachen die Arbeitsabläufe und erhöhen die Bequemlichkeit. Mit einer Handbewegung lassen sich Türen öffnen, Computer starten, Automotoren anwerfen oder Kantinenrech-

future workplace looks both helpful and intrusive, 05.10.2017, abrufbar unter <www.fastcompany.com> (besucht am 31.05.2020).

³⁰³ BERNAL *et al.*, 167.

³⁰⁴ COLLIER, 5.

³⁰⁵ EGGEN/STENGEL, N 8; ALLENSPACH, N 4.

³⁰⁶ KIULIAN ARTUR, Why your next boss will be a robot, 18.09.2017, abrufbar unter <www.linkedin.com> (besucht am 31.05.2020).

³⁰⁷ WILSON MARK, This breakthrough tool detects racism and sexism in software, 22.08.2017, abrufbar unter <www.fastcompany.com> (besucht am 31.05.2020).

³⁰⁸ KUCHLER HANNAH, Secrets, statistics and implicit bias, Financial Times vom 15.02.2018, abrufbar unter <www.ft.com> (besucht am 31.05.2020).

³⁰⁹ KUCHLER HANNAH, Secrets, statistics and implicit bias, Financial Times vom 15.02.2018, abrufbar unter <www.ft.com> (besucht am 31.05.2020).

³¹⁰ WEIBEL *et al.*, 24. Eine empirische Studie bei Grossunternehmen hat ergeben, dass das blossе Verteilen des Ethik-Kodex nicht genügt und viele Mitarbeiter die Werte und Vorschriften ihres Unternehmens nicht kennen: WEAVER *et al.*, 287.

nungen bezahlen.³¹¹ Rund hundert Angestellte der amerikanischen Technologieunternehmung Three Square Market liessen sich 2018 chippen.³¹²

Angestellte der Universität Luzern und der britischen Zeitung Daily Telegraph finden unter ihrem Arbeitstisch ein Infrarotkästchen, das die Auslastung der Arbeitsplätze misst. Dies dient der Gebäudeplanung.³¹³

Die Software zur Personal- und Rollmaterial-Einsatzplanung (Sopre) der Schweizerischen Bundesbahnen (SBB) bereitet täglich die Dienste von 20'000 Lokomotivführern, verteilt auf mehrere tausend Züge, vor.³¹⁴ Bei IBM stellt eine Software die Arbeitsteams zusammen, indem sie die für ein Projekt erforderlichen Qualifikationen mit den Lebensläufen der Arbeitnehmer abgleicht.³¹⁵ Kurzfristige Ausfälle erkennt die Arbeitgeberin frühzeitig, wenn sie interne Daten mit externen verknüpft; beispielsweise erweist sich aus den Bewegungsprofilen in den betrieblichen Mobilfunkgeräten, wer sich in besonders stark grippegefährdeten Gebieten bewegt.³¹⁶

Kollaborationssoftwares (z.B. Microsoft Teams und Kaizala von Microsoft, Whatsapp Business von Facebook oder SAP) führen alle Kommunikationsdienste

³¹¹ Solche Chips bieten z.B. das britische Unternehmen BioTeq und die schwedischen Konkurrenten Biohax und Mindshare an. Sie speichern auch medizinische Daten, aber nicht GPS-Daten: KOLLEWE JULIA, Alarm over talks to implant UK employees with microchips, *The Guardian* vom 11.11.2018, abrufbar unter <www.theguardian.com> (besucht am 31.05.2020).

³¹² COLLIER, 2–3; *The Economist* vom 05.01.2019, The spy who hired me, abrufbar unter <www.economist.com> (besucht am 31.05.2020). Bereits 2006 hat die amerikanische Überwachungsfirma CityWatcher.com zwei Angestellten solche Implantate in die Unterarme versetzt: COLLIER, 3.

³¹³ Zur Universität Luzern: DAVIS PLÜSS JESSICA / REUSSER KAI, Your employer might be watching you. Should you care?, 13.05.2019, abrufbar unter <www.swissinfo.ch> (besucht am 31.05.2020); zum schwarzen Kästchen OccupEye beim Daily Telegraph: AJUNWA/CRAWFORD/SCHULTZ, 737.

³¹⁴ ROTZINGER ULRICH, Pannen-Software kostete laut Insidern bereits über 70 Mio., *Blick* vom 08.01.2018, abrufbar unter <www.blick.ch> (besucht am 31.05.2020); SCHMID ANDREAS, Den SBB droht wegen fehlerhafter Software ein Notszenario, *NZZ* vom 23.12.2017, abrufbar unter <<https://nzzas.nzz.ch>> (besucht am 31.05.2020).

³¹⁵ DIETRICH *et al.*, 22.

³¹⁶ RUHLAND, 91–92. Auf ähnliche Weise wollte Google mit dem Projekt Flu Trends Grippefällen live vorhersagen: NEUBERGER, 159–160. Die Daten von Flu Trends sind jedoch nur noch eingeschränkt verfügbar, weil die Vorhersagen zu ungenau ausfielen. Vgl. auch BISSELS *et al.*, 3043.

zusammen (*unified communications*), was den Austausch von Information erleichtert.³¹⁷ Künftig soll die Kommunikation sogar direkt von Gehirn zu Gehirn laufen (*mind-to-mind communication*). Erforderlich sind hierfür ins Gehirn implantierte Speicherkarten (*brain chips*). Bei einem Tierversuch wurden zwei Ratten solche Gehirn-Chips eingebaut. Die eine Ratte musste über Wochen anspruchsvolle Aufgaben erlernen, um an ihr Futter zu gelangen. Dieser Lernprozess wurde auf der Speicherkarte abgelegt. Danach wurde die Speicherkarte dieser Ratte über das Internet mit derjenigen der zweiten Ratte, die sich in einer entfernten Stadt befand, verbunden. Die zweite Ratte fand den Weg zum Futter auf Anhieb.³¹⁸ Es ist somit technisch machbar, Lernprozesse und Wissen zwischen Arbeitnehmern auszutauschen. Die Literatur spricht diesbzgl. vom verbesserten «Robo Sapiens» (*enhanced robo sapiens*).³¹⁹ Dieser ist Ausdruck des besprochenen Internets der (Dinge und der) Menschen.³²⁰

Telepathie bestimmt auch die Interaktion zwischen Mensch und Roboter: Ein Arbeitnehmer kann über Handzeichen und Gehirnwellen den Industrieroboter Baxter des Massachusetts Institute of Technology (MIT) steuern und ihn beispielsweise veranlassen, eine Schraube anzuziehen.³²¹ Andere Roboter werden am Körper getragen: Ein (weicher) anziehbarer Roboter (*exosuit*) des Harvard Biodesign Lab entlastet die Hüfte, was die Stoffwechsel-Kosten im Körper um 17,4 Prozent reduziert.³²² Im Einsatz sind auch (harte) Exoskelette, mithilfe derer Arbeitnehmer auf Baustellen und in Werften schwere Gegenstände heben können.³²³

Arbeitnehmer können virtuelle Büroassistenten, die Sprache verarbeiten (z.B. Siri von Apple, Alexa von Amazon, der Intelligent Agent von Adobe oder interne

³¹⁷ HÄFNER-BEIL, 94; SIEGLE JOCHEN, Es muss nicht immer Whatsapp sein: Business-Chat mit Microsoft, NZZ vom 09.04.2019, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

³¹⁸ HOFFMAN STEVE, New brain computer interface technology, 29.08.2017, abrufbar unter <www.youtube.com> (besucht am 31.05.2020), 6min34sec–8min14sec; SCHI-NAGL, 507.

³¹⁹ VAN DEN HOVEN VAN GENDEREN, 12.

³²⁰ Siehe S. 28.

³²¹ ENGLAND RACHEL, MIT uses brain signals and hand gestures to control robots, 20.06.2018, abrufbar unter <www.engadget.com> (besucht am 31.05.2020).

³²² BURROWS LEAH, An exosuit tailored to fit, 28.02.2018, abrufbar unter <<https://news.harvard.edu>> (besucht am 31.05.2020).

³²³ WILDHABER/LOHMANN, 137; KLEBE/WEISS, 265.

Webseiten), mit Informations-Recherchen beauftragen.³²⁴ Arbeitnehmer in der Automobilproduktion tragen die intelligente Brille Google Glass, bei der sie über einen verbundenen Touchscreen Hilfe für bestimmte Aufgaben anfordern können.³²⁵ Fahrzeuge zeigen den Mitarbeitern auf einem Bildschirm an, welche Werkstoffe sie für Produktionszwecke aus dem Lager entnehmen sollen (*pick by light*, weil Lichtpunkte das zu holende Material auf dem Display markieren).³²⁶

2.3.6 Mitarbeiterbindung

Um Angestellte beruflich zu fördern, ermitteln intelligente Tutorsysteme, unter welchen Bedingungen sich die Talente (*high potentials*) bestmöglich entfalten.³²⁷ Google und McDonalds entwickeln gestützt auf die Analyse der Mitarbeiterbefragungen spezielle Trainingsprogramme für Vorgesetzte.³²⁸ Ein virtueller Karriereassistent (Virtual Career Assistant, Vicas) errechnet für jeden Mitarbeiter des Versicherungsunternehmens Axa das individuelle Risiko, dass ein Roboter seine Arbeit übernehmen könnte.³²⁹ Als Lösung zeigt der Vicas Möglichkeiten der internen Stellenmobilität und Weiterbildung an, damit die Betroffenen nicht auf ih-

³²⁴ Siri ist einst als virtueller Büroassistent für das amerikanische Militär entwickelt worden: SIMON FELIX, *Alexa, spiel mir das Lied vom wahren Lauschangriff*, NZZ vom 06.02.2018, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020). Alexa bahnt sich den umgekehrten Weg vom Privaten ins Büro: FRIED INA, *Exclusive: Alexa is coming to the office*, 12.03.2018, abrufbar unter <www.axios.com> (besucht am 31.05.2020). Zum Intelligent Agent: SIEGLE JOCHEN, *Ein intelligenter Agent ermöglicht es, mit Dokumenten zu sprechen*, NZZ vom 29.03.2019, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020). Interne Webseiten beantworten Fragen der Mitarbeiter bzgl. IT, Sozialleistungen und Personalpolitik: DAVENPORT/RONANKI, 112.

³²⁵ Vgl. KLEBE/WEISS, 265. Vgl. ALLENSPACH, N 1.

³²⁶ KLEBE/WEISS, 265.

³²⁷ BISSELS *et al.*, 3043; intelligente Verteilung von Arbeitsaufgaben zur systematischen Förderung von Menschen: BMAS 2017, 70.

³²⁸ Zur Oxygen-Studie von Google: REINDL/KRÜGL, 44–47; zu McDonalds: CLASSEN/GÄRTNER, 39.

³²⁹ KÜSTERLING SOPHIE, *People Analytics mit People-Analytix*, 21.02.2018, abrufbar unter <www.startupticker.ch> (besucht am 31.05.2020); SHOOK *et al.* *Die Axa arbeitet hierfür mit dem Zürcher Startup People Analytix zusammen (siehe FN 253). Die KI könnte rund 45 Prozent aller Aktivitäten erledigen, die heute Menschen erfüllen, so eine Studie des Beratungsunternehmens McKinsey: CHUI et al., 2.*

ren (gefährdeten) Positionen verharren.³³⁰ Ein Konkurrenzprodukt hierzu ist der Professional Reputation Score von Reputation.com, der den beruflichen Status bewertet und darauf den nächsten Karriereschritt vorschlägt.³³¹

Es lässt sich ein innerbetrieblicher sozialer Graph (*enterprise social graph*) errechnen, wenn man die Kommunikationsflüsse im Unternehmen nachzeichnet.³³² Microsoft und IBM testen auf diese Weise den Zusammenhalt auf Individual-, Team- und Unternehmensebene und definieren so beispielsweise, über wen am meisten Informationen laufen, wer andere beeinflusst und wer isoliert ist.³³³ Die Bank of America und Cubist Pharmaceuticals setzen auf die Mitarbeiterausweise von Humanyze, die mit Mikrofon, Infrarot-Empfänger, Schrittzähler und Bluetooth-Sender ausgestattet sind. Daraus erhellen die räumliche Position der Arbeitnehmer zueinander und ihre mündliche Kommunikation untereinander, ebenso der Tonfall der Dialoge oder wer wen unterbricht.³³⁴ Das Ziel ist es, den Einfluss einer Person als Wirkmoment zu nutzen, etwa für die Ausbreitung von Innovationen. Ursprünglich stammen solche Analysen aus dem viralen Marketing, das wissen will, welche Kunden so einflussreich sind, dass sie ihre Freunde vom Kauf eines Produkts überzeugen können.³³⁵

Der Tokioter Mischkonzern Hitachi nutzt für das Stressabbau- und Pausenmanagement das «Business Microscope» (auch «Happiness Meter»). Hierbei handelt es sich um einen Mitarbeiterausweis, der sich wie eine Halskette umlegen lässt.³³⁶ Das Business Microscope misst die Gehirnwellen auf Stress und Müdigkeit hin. Gestützt darauf passt Hitachi die Pausenpolitik an.³³⁷ So will der Konzern herausgefunden haben, dass sich die Produktivität verdreifache, wenn Gleichaltrige zusammen die Pausen verbringen.³³⁸ Derweil hat die Bank of America dank ihren

³³⁰ SHARP RACHEL, Virtual career assistants can solve coaching challenges, 13.04.2018, abrufbar unter <<http://hrmagazine.co.uk>> (besucht am 31.05.2020).

³³¹ World Economic Forum 2013, 29.

³³² HÖLLER/WEDDE 2018, 9.

³³³ Microsoft: HÖLLER/WEDDE 2018, 28; IBM: HÖLLER/WEDDE 2018, 33; DIETRICH *et al.*, 23.

³³⁴ REINDL/KRÜGL, 37–43; ROSENBLAT/WIKELIUS *et al.*, 3. Humanyze hiess vormals Sociometric Solutions.

³³⁵ HÖLLER/WEDDE 2018, 23; TRINDEL.

³³⁶ COLLIER, 5.

³³⁷ COLLIER, 6.

³³⁸ COLLIER, 5.

Ausweisen von Humanyze entdeckt, dass die Kündigungsrate sinkt, wenn Arbeitsteams gemeinsam Pause machen.³³⁹

IBM wertet im Projekt Enterprise Social Pulse die Gefühlslage im Unternehmen aus basierend auf frei zugänglichen Texten der Mitarbeiter auf internen und externen sozialen Netzwerken und Umfragen (*enterprise-oriented employee sentiment analysis*). Bezweckt wird, die kollektive Stimmung in einem weltweit tätigen Grossunternehmen in Echtzeit einzufangen und Sorgen aktiv anzusprechen.³⁴⁰

Zur Prognose der Personalfuktuation analysieren Arbeitgeberinnen die Daten aus- geschiedener Mitarbeiter. Aus diesen Erkenntnissen ergibt sich die Feststellung, welche Lebens- oder Beschäftigungssituation typischerweise zu einer Kündigung führt und dass sich der Grad der «inneren Kündigung» der bestehenden Belegschaft abschätzen lässt.³⁴¹ Um dem entgegenzuwirken, entwickeln Unternehmen wie SAS, Microsoft und Xerox für wertvolle Mitarbeiter Anreizprogramme.³⁴² Dabei sollen Weiterbildung und Teilhabe an der Unternehmensentwicklung den Mitarbeiter stärker an die Unternehmung binden.³⁴³ Conagra Foods setzt auf Anerkennung und nichtmonetäre Belohnungen.³⁴⁴

Um den Entscheid über eine Beförderung auf eine informierte Grundlage zu stellen, werden Stimm- und Gesprächsanalysen durchgeführt.³⁴⁵ Es gibt Smartphone-Applikationen, die eine 360°-Rückmeldung von Arbeitskollegen, Vorgesetzten und Kunden erlauben.³⁴⁶ Solche Feedback-Daten gibt es immer mehr, weil grosse Unternehmen wie General Electric, Schneider Electric, SAP, Adobe, Accenture

³³⁹ COLLIER, 5. Vgl. ROSENBLAT/WIKELIUS *et al.*, 3.

³⁴⁰ DIETRICH *et al.*, 26–27. Das Unternehmen kann auf diese Weise mit der Gewerkschaft eine alternative Lösung ausarbeiten, ohne Zeit mit dem Abschluss eines neuen Tarifvertrags zu verlieren: GAY/KAGAN. Innerbetriebliche soziale Netzwerke sind z.B. Yammer von Microsoft, IBM Connections oder Workplace von Facebook.

³⁴¹ GORICNIK/GRÜNANGER, N 1.11; McLoughlin Gavin, Irish business may use AI to spot staff at risk of leaving job, 11.09.2018, abrufbar unter <www.independent.ie> (besucht am 31.05.2020).

³⁴² SAS: WILSON *et al.*, 31; Microsoft und Xerox: NIKLAS/THURN, 1589; BISSELS *et al.*, 3043.

³⁴³ SPRAGUE 2015, 33.

³⁴⁴ NEUBERGER, 161.

³⁴⁵ DÄUBLER, N 429f.

³⁴⁶ Europarat 2016a, 29.

oder Deloitte Consulting von traditionellen Jahresgesprächen zu ständigen Feedbacks wechseln.³⁴⁷

Eine Software kann aber genauso gut die Beendigung des Arbeitsverhältnisses vorschlagen: Eine kritisch zu beurteilende Software sieht keine Zukunft für alle Mitarbeiter, die in den letzten fünf Jahren nicht befördert wurden.³⁴⁸ Bridgewater Associates, einer der weltweit grössten Hedgefonds mit Sitz in den USA, setzt auf das Verwaltungssystem Principles Operating System (PriOS), das für die automatisierte Einstellung und Entlassung von Mitarbeitern oder die Bewertung gegensätzlicher Perspektiven bei Meinungsverschiedenheiten im Team verantwortlich sein soll. Der Hedgefonds will auf diese Art jeden Einfluss von Emotionen und Stimmungen auf Investitionsentscheidungen vollständig ausschliessen.³⁴⁹

2.3.7 Zwischenfazit und Vorbehalte zur Klassifizierung der Verwendungszwecke

Eine Zusammenstellung der verschiedenen Verwendungszwecke und Anwendungsformen von People Analytics wie vorliegend hat es, soweit ersichtlich, bisher nicht gegeben.³⁵⁰ Dieser neue Beitrag zur Forschung ist aber erforderlich, um dem Leser die Dimension des Forschungsobjekts vor Augen zu führen: Es gibt eine unfassbare Variationsbreite von People Analytics-Angeboten, verteilt über alle Berufe. Produktlisten bleiben stets unvollständig, da sich der Markt laufend entwickelt.³⁵¹

Die vorgenommene heuristische Klassifizierung (Rekrutierung – Leistungssteuerung – Compliance-Management – Arbeits- und Arbeitsplatzgestaltung – Mitarbeiterbindung) dient der Praktikabilität und Abstrahierung, um mit dem begrenz-

³⁴⁷ ASTHEIMER SVEN, SAP-Personalchef: «Schulnoten für Mitarbeiter sind nicht zeitgemäss», FAZ vom 03.06.2017, abrufbar unter <www.faz.net> (besucht am 31.05.2020); GUENOLE *et al.*, 7–8; TechTarget, Making the shift to continuous performance management, 2017, abrufbar unter <<https://searchhrsoftware.techtarget.com>> (besucht am 31.05.2020).

³⁴⁸ DÄUBLER, N 429.

³⁴⁹ KIULIAN ARTUR, Why your next boss will be a robot, 18.09.2017, abrufbar unter <www.linkedin.com> (besucht am 31.05.2020).

³⁵⁰ Die vorliegende Zusammenstellung wurde aber erst möglich durch die Erkenntnisse aus der interdisziplinären Teamarbeit des NFP75-Projekts und ist im Wesentlichen bereits vorgezeichnet in: WILDHABER/KASPER, 759–765, und WEIBEL *et al.*, 26–27.

³⁵¹ WILDHABER/KASPER, 760.

ten Wissen Aussagen über das Phänomen der Personalanalysen als Ganzes zu formulieren. Andere Autoren nehmen eine andere Kategorisierung vor.³⁵²

Die gleichen Anwendungen lassen sich teilweise für mehrere Kategorien gleichzeitig einsetzen: Das (unter Leistungssteuerung erwähnte) Flugzeug-Flottenverwaltungs-System FES findet auch Verwendung, um die Einhaltung interner Richtlinien zu kontrollieren, beispielsweise ob die Piloten Anweisungen befolgen, den Benzinverbrauch beim Start ab 500 Meter Höhe zu reduzieren (Compliance).³⁵³ Die elektronische Standortübermittlung ausserhalb des Betriebsgeländes (Leistungssteuerung) ermöglicht die Verhinderung von Diebstählen und die Aufzeichnung der Fahrzeiten zum Arbeitnehmerschutz (Compliance).³⁵⁴ Der intelligente Teppich (Compliance) könnte für identifizierte Personen das Licht in einem Raum einschalten oder Türen automatisch öffnen (Arbeitsplatzgestaltung).³⁵⁵ Exoskelette dienen vermeintlich dem Gesundheitsschutz, indem sie die Rückenhaltung beim Heben von Lasten vorgeben (Compliance und Arbeitsplatzgestaltung); aber ebenso lässt sich genaustens überprüfen, wie viele Lasten der Arbeitnehmer täglich hochhebt (Leistungssteuerung).³⁵⁶ Schliesslich beinhalten Prognosen zur Personalfluktuations (Mitarbeiterbindung) auch einen Informationswert im Hinblick auf die künftige Personalplanung (Rekrutierung).

Nach der vorliegend vertretenen Einschätzung sind die meisten der beschriebenen People Analytics-Lösungen in der Schweiz wirtschaftlich umsetzbar. Einige davon mögen futuristisch klingen, so etwa die Gehirn-Chips zur direkten Kommunikation von Mensch zu Mensch.³⁵⁷ Die Technologie setzt den Verwendungszwecken aber grundsätzlich keine Grenzen. Daher ist zu untersuchen, wie es um die gegenwärtige und mögliche künftige Verbreitung von People Analytics steht (dazu sogleich).

³⁵² Analytik zum Zweck der Rekrutierung, Schulung sowie Entscheidung über Beförderung und Kündigung: GAY/KAGAN.

³⁵³ Siehe FN 273; General Electric and Business Insider Studios, How big data and the industrial internet can help southwest save \$100 million on fuel, 15.10.2015, abrufbar unter <www.businessinsider.com> (besucht am 31.05.2020).

³⁵⁴ WOLFER, N 432–443.

³⁵⁵ Vgl. CUKIER/MAYER-SCHÖNBERGER, 35.

³⁵⁶ Vgl. ALLENSPACH, N 15.

³⁵⁷ Siehe S. 54.

2.4 Verbreitung und praktische Relevanz

2.4.1 NFP75-Daten zur Verbreitung in der Schweiz

Im zweiten Modul des NFP75-Projekts wurde mit einer Online-Umfrage systematisch die gegenwärtige Verbreitung von People Analytics in der Schweiz erforscht.³⁵⁸ Die Online-Umfrage ergibt, dass knapp zwei Drittel der befragten Schweizer Unternehmen People Analytics verwenden (65 Prozent oder 102 von 158 Betrieben).

Bei grösseren Unternehmen ist People Analytics verbreiteter als bei kleineren (siehe Abb. 5).³⁵⁹ Es ist davon auszugehen, dass die Grenzkosten für People Analytics sinken und der Nutzen von Datenbearbeitungen steigt, je grösser das Unternehmen ist. Kleine und mittlere Unternehmen werden vielfach informelle Lösungen präferieren.

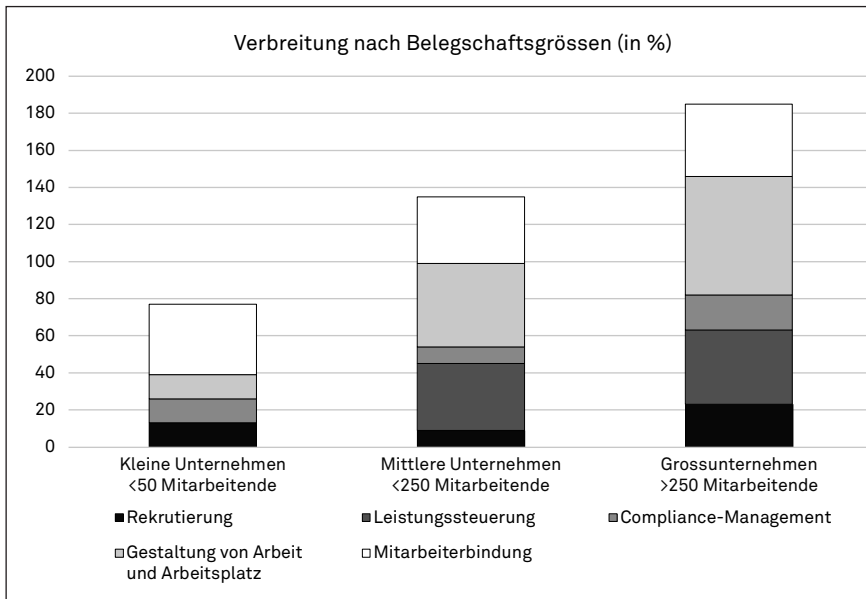


Abb. 5: Verbreitung von People Analytics in der Schweiz nach Belegschaftsgrössen

³⁵⁸ Siehe S. 14–16.

³⁵⁹ Vgl. auch WILDHABER/KASPER, 764.

People Analytics ist in allen Schweizer Wirtschaftszweigen verbreitet (siehe Abb. 6).³⁶⁰ Führend ist der Informations- und Kommunikationssektor, gefolgt vom Finanz- und Versicherungswesen.

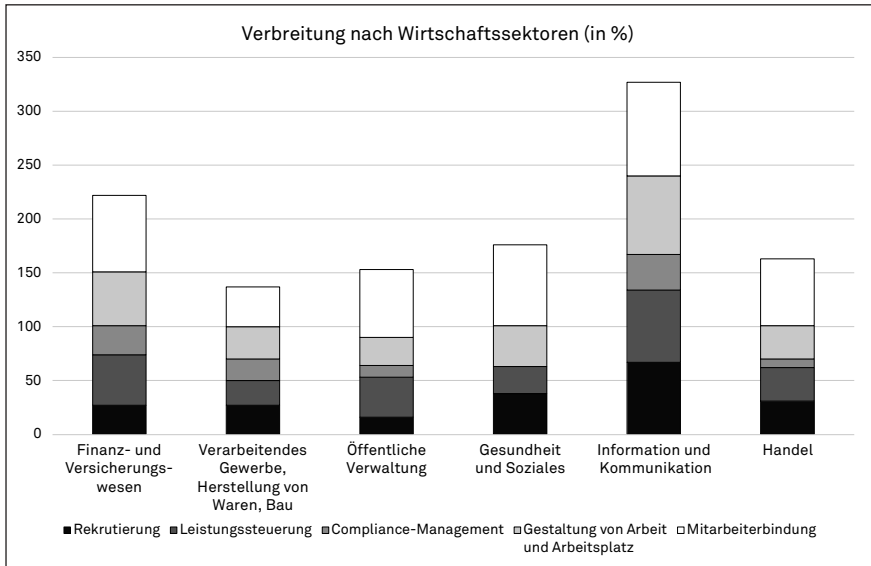


Abb. 6: Verbreitung von People Analytics in der Schweiz nach Wirtschaftssektoren

Die Umfrageergebnisse deuten darauf hin, dass sich People Analytics im Ausland bereits weiter als in der Schweiz entwickelt hat. Zwar wurden ausschliesslich Unternehmen mit Sitz in der Schweiz befragt, und von ihnen verwenden zwei Drittel People Analytics (66 Prozent). Jedoch hebt sich von diesem Durchschnitt eine kleine Gruppe von Unternehmen ab, die zu einem Konzern mit Hauptsitz im Raum USA und Kanada gehören: Alle von ihnen setzen People Analytics ein (100 Prozent).³⁶¹

Es resultiert folgende Verbreitung nach Verwendungszwecken von People Analytics (siehe Abb. 7).³⁶² Am häufigsten ist die Nutzung von People Analytics im Bereich der Mitarbeiterbindung (61 Prozent). Hier kommen Online-Befragungen zur Zufriedenheit der Arbeitnehmenden vor, um das Betriebsklima zu verbessern.

³⁶⁰ Vgl. auch WILDHABER/KASPER, 763.

³⁶¹ WILDHABER/KASPER, 767.

³⁶² Abb. 7 und entsprechende Zahlen bereits in: WEIBEL *et al.*, 26, und WILDHABER/KASPER, 765.

Auch gibt es zur Verbesserung der Feedback-Qualität Smartphone-Applikationen, die eine 360°-Rückmeldung von Arbeitskollegen, Vorgesetzten und Kunden ermöglichen. Bereits seit Längerem bekannt sind computerbasierte Austrittsbefragungen, um die Personalpolitik anzupassen. Zur Gestaltung der Arbeit und des Arbeitsplatzes (38 Prozent) sowie zur Leistungssteuerung (37 Prozent) findet People Analytics ungefähr gleich oft Anwendung. Im ersten Fall existieren zum Beispiel Video-Überwachungsanlagen zur Verbesserung der Arbeitsabläufe oder Softwares zur erleichterten Zusammenarbeit im Team, wie u.a. eine Software, die Stimmen erkennt und die Webcam in virtuellen Teamsitzungen steuert. Im letztgenannten Fall treten RFID-Ausweise zur Geolokalisierung und elektronische Zugangskontrollen auf. Ungefähr jedes fünfte Unternehmen, das People Analytics einsetzt, ist im Bereich der Rekrutierung aktiv (21 Prozent). Die Arbeitgeber nutzen vor allem Anwendungen, die automatische Suchprozesse und einen Abgleich (*matching*) von Fähigkeiten der Bewerber mit Stellenanforderungen ermöglichen. Ähnlich viele (18 Prozent) verwenden People Analytics für das Compliance-Management, etwa zur Auswertung von Telefonaten und E-Mails.

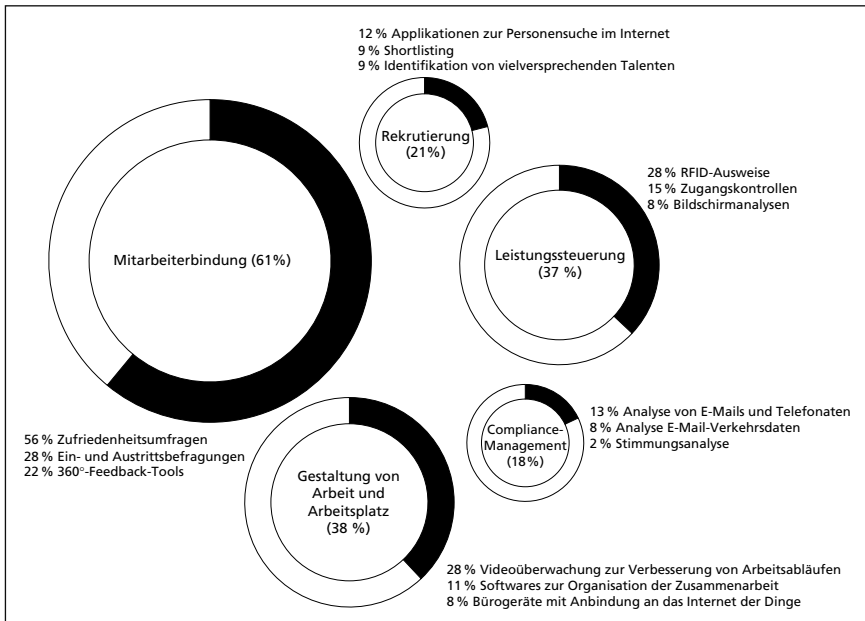


Abb. 7: Verbreitung von People Analytics in der Schweiz nach Verwendungszwecken einschliesslich der beliebtesten Technologien

Die beliebtesten Instrumente sind in dieser Reihenfolge: webbasierte Zufriedenheitsumfragen, Video-Überwachungsanlagen, Austrittsbefragungen, RFID-Ausweise und Feedbackinstrumente. Demgegenüber kaum genutzt werden derzeit Roboter zur Rekrutierung oder Stimmungsanalysen (siehe Abb. 8).³⁶³ Im Vergleich zu den Beispielen aus Literatur und Presse³⁶⁴ erweisen sich die beobachteten Datenanalysen als eher konservativ. Allerdings könnten die Daten zu neuen Zwecken wiederverwertet werden, wodurch der Grad an Einsicht in das Leben des Arbeitnehmers steigen würde.³⁶⁵ Beispielsweise verraten die elektronischen Ausweise Bewegungsmuster und Verhaltensprofile, wenn die Arbeitnehmer während der Arbeitszeit mehrfach ihren Aufenthaltsort wechseln und dabei immer wieder Zutrittsschranken passieren müssen.³⁶⁶

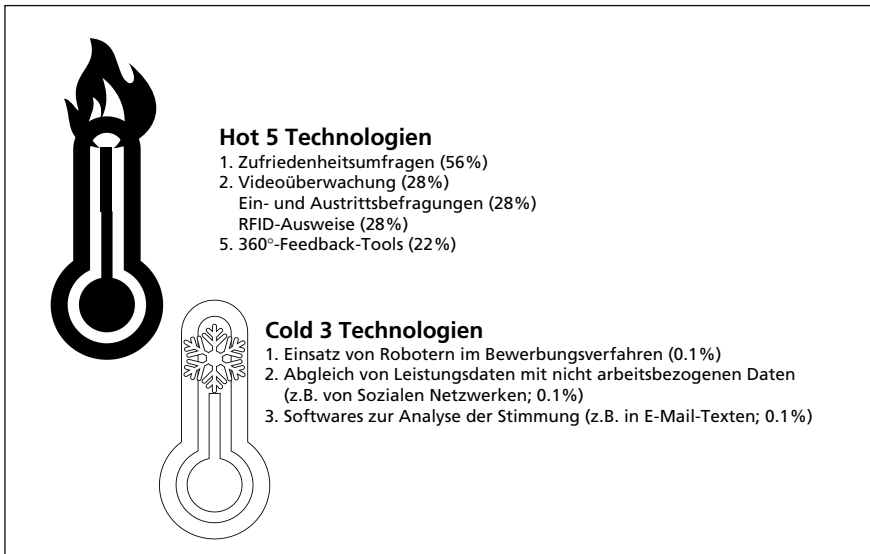


Abb. 8: Beliebteste und seltenste People Analytics-Technologien in der Schweiz

Die meisten Unternehmen begnügen sich nicht mit einer einzigen der erwähnten Techniken. Knapp die Hälfte (46 Prozent) aller befragten Unternehmen hat parallel mindestens drei verschiedene Anwendungsformen von People Analytics im

³⁶³ Vgl. auch WEIBEL *et al.*, 27, und WILDHABER/KASPER, 766.

³⁶⁴ Siehe S. 42–59.

³⁶⁵ Siehe S. 59.

³⁶⁶ WOLFER, N 393; DÄUBLER, N 324a.

Einsatz. Bei jedem vierten (27 Prozent) aller befragten Unternehmen sind es mindestens fünf. Vier befragte Unternehmen geben an, zehn oder mehr Tools gleichzeitig im Einsatz zu haben.³⁶⁷

2.4.2 Verbreitung in der Welt

Die Zahlen, die im NFP75-Projekt über People Analytics im schweizerischen Arbeitsmarkt erhoben wurden,³⁶⁸ bilden keine Ausnahme im Vergleich zu den Zahlen zur gegenwärtigen Verbreitung in der restlichen Welt, welche in der Literatur zu finden sind.³⁶⁹ Die technologiebasierte Überwachung und Kontrolle der Arbeitnehmenden wird sowohl auf der nördlichen als auch auf der südlichen Hemisphäre praktiziert.³⁷⁰ Im Jahr 2014 gab jedes vierte (26 Prozent) befragte deutsche Unternehmen in einer Umfrage an, People Analytics zu betreiben.³⁷¹ 2015 nutzte bereits fast jedes dritte (32 Prozent) der weltweit befragten Unternehmen Big Data zur Unterstützung des Personalbereichs.³⁷² People Analytics wird auch von öffentlich-rechtlichen Arbeitgebern betrieben.³⁷³

Vorliegend wurden entlang dem Mitarbeiter-Lebenszyklus fünf Zwecke von People Analytics identifiziert, nämlich Rekrutierung, Leistungssteuerung, Compliance-Management, Arbeits- und Arbeitsplatzgestaltung sowie Mitarbeiterbindung. Hinsichtlich der Bewerbungsphase ist bekannt, dass in den USA und Grossbritannien bis zu 70 Prozent der Bewerber automatisiert von algorithmischen Entscheidungssystemen bewertet und vorausgewählt werden, bevor ein Rekrutierer sich die verbliebenen Kandidaten ansieht.³⁷⁴ Erst jedoch jedes zwanzigste deut-

³⁶⁷ WILDHABER/KASPER, 766.

³⁶⁸ Siehe S. 60.

³⁶⁹ Siehe bereits die Zahlen zur globalen Verbreitung bei KASPER/WILDHABER, 192.

³⁷⁰ AKHTAR/MOORE, 102.

³⁷¹ BISSELS *et al.*, 3042.

³⁷² WILSON *et al.*, 8. A.M. KATZ MIRANDA, The creative ways your boss is spying on you, 08.12.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020): Sogar 94 Prozent der Unternehmen würden ihre Arbeitnehmer «auf irgendeine Art beobachten».

³⁷³ Die Bearbeitung von Personendaten zum Zweck der Personalverwaltung ist eine der hauptsächlichen Datenbearbeitungstätigkeiten von EU-Institutionen: EDSB 2019c.

³⁷⁴ DREYER/SCHULZ, 7. Fast zwei Drittel der Arbeitgeberinnen (63 Prozent) geben an, dass sie schon einmal Bewerbungen nur gestützt auf die Daten aus sozialen Online-Netzwerken abgewiesen haben: CareerBuilder.

sche Grossunternehmen (6 Prozent) benutzt vergleichbare Verfahren.³⁷⁵ Auch in der Schweiz kommt das sog. Hiring by Algorithm oder E-Recruiting vor.³⁷⁶

Im Bereich der Leistungssteuerung verfolgten 2012 knapp zwei Drittel (62 Prozent) der Firmen ihre Aussendienstmitarbeiter über GPS.³⁷⁷ In jedem fünften europäischen Unternehmen (18 Prozent) benutzten Arbeitnehmer 2015 Wearables zu Arbeitszwecken.³⁷⁸ Die Verbreitung von Wearables ist aber, gemessen an ihrem Potenzial, noch bescheiden.³⁷⁹ Wearables können in Gesundheitsprogrammen verwendet werden.³⁸⁰ Diese wiederum kommen in den USA in Grossunternehmen flächendeckend vor.³⁸¹

Zur Compliance-Überwachung kontrollierte schon 2002 jede fünfte Schweizer Arbeitgeberin (18 Prozent) die E-Mails ihrer Angestellten.³⁸² Zur gleichen Zeit überwachten bereits drei Mal so viele amerikanische Arbeitgeberinnen die Internetnutzung ihrer Arbeitnehmer.³⁸³ 2010 verfolgten drei von vier US-Arbeitgeberinnen

³⁷⁵ Die Tendenz ist jedoch steigend: 70 Prozent der deutschen Grossunternehmen glauben, dass algorithmische Vorselektionen Zukunft haben: FAZ vom 01.03.2018, Lieber Roboter als Personaler, abrufbar unter <www.faz.net> (besucht am 31.05.2020).

³⁷⁶ Z.B. bei der Fluggesellschaft Swiss, dem Warenhaus Manor, IBM oder der Berner Kantonsverwaltung: WILDHABER 2017, 214; ebenso bei den SBB sowie den Grossbanken Credit Suisse und UBS: BLATTNER MARCEL / NONNER TIM, Algorithmen gefährden die Demokratie, Tagesanzeiger vom 10.04.2018, abrufbar unter <www.tagesanzeiger.ch> (besucht am 31.05.2020).

³⁷⁷ 2008 waren es noch halb so viele (30 Prozent): COLLIER, 5.

³⁷⁸ AKHTAR/MOORE, 114.

³⁷⁹ EGGEN/STENGEL, N 2.

³⁸⁰ Bei jedem vierten Gesundheitsprogramm (25 Prozent) am Arbeitsplatz kommen Wearables vor. In 7 Prozent der Fälle wird aus den aufgezeichneten Daten der Gesundheitszustand der Arbeitnehmer gemessen: HAGGIN PATIENCE, Big issues in technology (a special report) – what's the best way for companies to handle data from employees' wearables?, The Wall Street Journal vom 23.05.2016, abrufbar unter <www.wsj.com> (besucht am 31.05.2020).

³⁸¹ Praktisch alle Unternehmen mit 200 oder mehr Mitarbeitern (99 Prozent) boten 2013 ein Gesundheitsprogramm an: AJUNWA 2017, m.w.H. AJUNWA/CRAWFORD/SCHULTZ, 764–765; The Kaiser Family Foundation/Health Research and Educational Trust, 196. Die starke Verbreitung ist auf amerikanische gesetzliche Bestimmungen zurückzuführen, die die Gesundheitsprogramme fördern und das gravierende Problem der Fettleibigkeit in den USA bekämpfen.

³⁸² RIESSELMANN-SAXER, 124.

³⁸³ Im Jahr 2001 verfolgten 62 Prozent die Internetnutzung: COLLIER, 9. 2001 «flächendeckende» Kontrollen: MEYER-MICHAELIS, 22. Von intensiverer Überwachung von Te-

(75 Prozent) die Kommunikation der Mitarbeiter und andere Arbeitstätigkeiten.³⁸⁴ Heute überwachen in den USA und in Grossbritannien praktisch alle (98 Prozent) Grossunternehmen digitale Aktivitäten der Angestellten.³⁸⁵ Auch bestimmen mittlerweile biometrische Fingerabdrücke, Gesichtserkennung und Iris-Scans in fast zwei von drei Unternehmen (62 Prozent), wer Zugang zu Gebäuden erhält.³⁸⁶

2.4.3 Steigende künftige Verbreitung

People Analytics ist eine relativ junge Disziplin, deren Anfänge auf die 2000er-Jahre zurückdatieren.³⁸⁷ Aufgrund der gestiegenen Zahlen der Vergangenheit ist anzunehmen, dass People Analytics auch künftig für die Unternehmensführung an Bedeutung zulegen wird.³⁸⁸ Gewichtige Anbieter wie SAP, IBM, HP, Oracle und weitere investieren grosszügig in die Entwicklung von Analytik-Produkten.³⁸⁹ Auf der Nachfrageseite entstehen neue Stellenprofile, wie beispielsweise der Data Scientist, Datenanalyst, People Analytics Leader oder Chief Operating Officer of

lefongesprächen, E-Mail, Internetnutzung und Computerdateien ausgehend, nämlich 73,5 Prozent im Jahr 2000, doppelt so viele wie 1997: WEST *et al.*, 286. Je nachdem, welcher Statistik man folgt, blieben die Zahlen bis 2007 stabil oder nahmen zu: Die Überwachung in den USA betraf 2007 die Internetnutzung (66 Prozent), den E-Mail-Verkehr (43 Prozent), Telefon-Randdaten wie Zeit und gewählte Nummern (45 Prozent) sowie Telefongespräche (16 Prozent) und Sprachnachrichten (9 Prozent): DETERMANN/SPRAGUE, 982. Vgl. auch COLLIER, 5.

³⁸⁴ AKHTAR/MOORE, 106.

³⁸⁵ Befragt wurden im Jahr 2018 Unternehmen mit mindestens 500 Mitarbeitern: COLLIER, 4.

³⁸⁶ Spiceworks, Data snapshot: biometrics in the workplace commonplace, but are they secure?, 12.03.2018, abrufbar unter <<https://community.spiceworks.com>> (besucht am 31.05.2020).

³⁸⁷ IBM betreibt People Analytics seit 2004 (DIETRICH *et al.*, 3, 22) und Google seit 2007 (REINDL/KRÜGL, 44). People Analytics ist seit 2009 in den USA und Grossbritannien verbreitet, später auch im deutschen Sprachraum: REINDL/KRÜGL, 15.

³⁸⁸ A.M. ANGRAVE *et al.*, 9–10: Es gebe gegenwärtig «wenig Hinweise», dass sich People Analytics zu einer strategischen Managementfunktion entwickle, weil zu grosse Verständigungsprobleme zwischen den Personalverantwortlichen und den Analytikabteilungen bestünden.

³⁸⁹ SAP und IBM: DIETRICH *et al.*, 1. HP, das US-amerikanische IT-Unternehmen EMC und Oracle: DAVENPORT, 13. Weitere namentlich bekannte Anbieter von Überwachungstechnologien sind Palantir, Vigilant Solutions, Cognitec, Amazon, Microsoft, Motorola und Axon: AI now institute, 8.

Culture.³⁹⁰ Prognosen gehen von einem Marktwachstum in Milliardenhöhe aus.³⁹¹ Die Beobachtungen in der Nische People Analytics stehen vor dem Hintergrund einer Reihe von Trends – sog. Megatrends –, die die Gesellschaft in grossem Stil tiefgreifend verändern. Es ist nun zu zeigen, wie einige dieser Megatrends People Analytics tragen.

Durch die Globalisierung entsteht ein erdumspannender Wettbewerb, in dem die Talente mobil sind. Sie sind besser informiert über die Vorteile anderer Arbeitgeber.³⁹² Der Aufwand steigt, um die Talente anzuziehen und zu behalten. Als Reaktion darauf schneiden die Unternehmen die Mitarbeiterführung mithilfe von Analytik auf den Einzelnen zu (*workforce of one*)³⁹³ durch Anbieten personalisierter Dienstleistungen wie gegenüber Kunden (*consumerisation of HR*).³⁹⁴

Eine jüngere Facette der Globalisierung zeigt sich in stärker wissensbasierten Prozessen, geschürt durch das Internet als Informationsmedium.³⁹⁵ In dieser Wissensgesellschaft erblüht der Dienstleistungssektor, der mittlerweile die Mehrheit der Bevölkerung beschäftigt.³⁹⁶ Routineaufgaben entfallen durch Automatisierung; komplexe Spezialistentätigkeiten erfordern ausgebildete Fachkräfte und mensch-

³⁹⁰ GUENOLE *et al.*, xv und 19; WESPI, 15; WEBER 2014, 24. Ein Chief Operating Officer of Culture pflegt die Unternehmenskultur mithilfe von Analytics: GUENOLE *et al.*, xvi.

³⁹¹ Marktvolumen von USD 11 Milliarden allein bei Analytik-Lösungen für das Leistungsmanagement: AJUNWA/CRAWFORD/SCHULTZ, 769; Wachstum um «Milliarden von Produkten und Millionen von Stellen»: REINSCH/GOLTZ, 37.

³⁹² Vgl. GUENOLE *et al.*, 1, 10–11.

³⁹³ Accenture, 2.

³⁹⁴ GUENOLE *et al.*, 7.

³⁹⁵ Vgl. BMAS 2017, 27. Die Globalisierung beschleunigte ab Mitte des 20. Jh. zunächst den Waren-, Dienstleistungs-, Kapital- und Personenverkehr: BMAS 2017, 25.

³⁹⁶ 73 Prozent der deutschen Erwerbstätigen im Dienstleistungssektor: BMAS 2015, 28; produzierende Berufe verschwindend: WOLTER *et al.*, 63. Arbeit besteht vermehrt aus Wissen, Technologie und Kommunikation als aus materieller Produktion: OTTO 2016, 1.

liche Kreativität.³⁹⁷ Für die Arbeitgeberin ist es wichtig, dass sie die individuellen Stärken ihrer Angestellten gründlich kennt.³⁹⁸

Wegen des demografischen Wandels, der eine Alterung und Schrumpfung der arbeitenden Bevölkerung mit sich bringt, wird sich der Fachkräftemangel zuspitzen.³⁹⁹ Dies erfordert eine effiziente Steuerung der knappen Arbeitskräfte. Denkbar ist, dass der Stress am Arbeitsplatz zunehmen wird, wenn weniger Personal die gleiche Arbeit erledigen muss. Damit könnten Stimmungsanalysen sowie das Stress- und Pausenmanagement an Bedeutung gewinnen.⁴⁰⁰

Ein kultureller Wertewandel hat eingesetzt, der sich durch eine neue Vielfalt der Lebensentwürfe und den Wunsch der Individuen nach einer Work-Life-Balance und Wertschätzung auszeichnet.⁴⁰¹ Wirtschafts- und Arbeitswelt sollen sich dem Menschen anpassen und nicht umgekehrt.⁴⁰² Um aber die individuellen Wünsche zu kennen, müssen Arbeitgeberinnen hierüber Daten erheben.

Schliesslich erlangen neue Arbeitsformen neben dem Standardarbeitsvertrag auf tiefem Niveau langsam an Bedeutung:⁴⁰³ Temporäre und Teilzeitarbeitnehmer,

³⁹⁷ BMAS 2015, 29; Zunahme der Spezialistentätigkeiten und Abnahme der Helfertätigkeiten bis 2035: WOLTER *et al.*, 59; Bedarf nach Kreativität: BRYNJOLFSSON/MCAFEE, 121. Das Bildungsniveau der Schweiz ist seit der Jahrtausendwende deutlich gestiegen: Beinahe Verdoppelung der schweizerischen Beschäftigten mit Tertiärabschluss von einem Fünftel (22 Prozent) im Jahr 1996 auf zwei Fünftel (39 Prozent) im Jahr 2015. Gleichzeitig sank der Anteil der Beschäftigten mit einem Bildungsabschluss mittlerer Qualifikationsstufe von 60 auf 48 Prozent: Schweizerischer Bundesrat 2017b, 31. Bildungsniveau in Deutschland steigend: BMAS 2017, 31. Unternehmen investieren immer mehr in die Ausbildung von Arbeitnehmern: WINICK, **A.M. KLEBE/WEISS**, 273; Arbeitnehmer, die Anweisungen über ein Pick-by-Light-System oder von einer intelligenten Brille erhielten (siehe S. 47), bräuchten weniger Qualifikationen.

³⁹⁸ Vgl. OTTO 2016, 107.

³⁹⁹ Demografischer Wandel in Deutschland: BMAS 2015, 26. Ende der 2020er Jahre wird fast ein Fünftel der deutschen Bevölkerung im erwerbsfähigen Alter zur Gruppe der 60- bis 66-Jährigen gehören: BMAS 2017, 29.

⁴⁰⁰ Siehe zur Stimmungsanalyse S. 57. Siehe zum Stress- und Pausenmanagement S. 56.

⁴⁰¹ BMAS/nextpractice GmbH, 21, 28 und 30. Vgl. mit Bezug auf die Erwartungen an den Staat: BMAS 2015, 36, m.w.H.

⁴⁰² BMAS 2017, 37.

⁴⁰³ Steigende Verbreitung der Telearbeit in der Schweiz: Schweizerischer Bundesrat 2016b, 15–16. Die aufgrund der Digitalisierung entstandenen neuen Arbeitsformen (z.B. sog. Gig-Work, Crowdwork und Work-on-Demand via Apps und Internet) stehen

freie Mitarbeiter sowie agiles Arbeiten unter Auflösung von Hierarchien erschweren die Kontrolle über ein Team. Auch gegenüber Arbeitnehmern im Homeoffice will die Vorgesetzte ihr Kontroll- und Weisungsrecht behalten.⁴⁰⁴ Dies beschwingt People Analytics insbesondere zum Zweck der Leistungskontrollen.

2.4.4 Zwischenfazit

Die Zahlen zur gegenwärtigen Verbreitung zeigen, dass People Analytics in einer Mehrheit der Schweizer Betriebe zur Realität gehört. Auch global gesehen wird People Analytics vermehrt zum festen Bestandteil der Geschäftsmodelle, wobei die Verbreitung von Land zu Land unterschiedlich weit fortgeschritten ist. Es ist jedoch davon auszugehen, dass die Verbreitung überall zunehmen wird.

Nach der hier vertretenen Einschätzung sind die Zahlen zur Verbreitung vorsichtig zu lesen. Die Ausbreitung verläuft je nach Betrieb verschieden schnell. Zudem hat People Analytics nicht für jeden Betrieb die gleiche Bedeutung. Die meisten Unternehmen existieren seit Langem und werden nur nach und nach einzelne Anwendungen in ihre bestehenden Geschäftsabläufe integrieren. People Analytics wird hier zu einer Modalität des Geschäftsmodells, gehört aber nicht zu dessen Kern. Dagegen operieren andere, vor allem jüngere Organisationen von Grund auf mit People Analytics-Daten. Zu denken ist etwa an das Taxi-Dienstleistungsunternehmen Uber, das ohne Daten über die Fahrer nicht funktionieren würde. Insgesamt resultiert aber selbst bei dieser zurückhaltenden Lesart der Statistiken eine fortgeschrittene gegenwärtige und steigende künftige Verbreitung.

2.5 Unterschiede zu älteren Überwachungsformen

2.5.1 Vorbemerkungen

Nachdem aufgrund der weiten Verbreitung von People Analytics die Relevanz des Themas in quantitativer Hinsicht erstellt ist, sind nun auch dessen qualitativ neue Aspekte herauszuarbeiten. Es ist etwas Abstand vom Phänomen zu nehmen, um

in der Schweiz jedoch noch am Anfang ihrer Entwicklung: Schweizerischer Bundesrat 2017b, 42. Bedeutungsverlust des Standard-Arbeitsvertrags in Europa: CARUSO, 95; ebenso in den USA: STONE, 75; Überblick zu den neuen Beschäftigungsformen: LINGEMANN/CHAKRABARTI. Vgl. auch ARNOLD/WINZER.

⁴⁰⁴ Vgl. Schweizerischer Bundesrat 2017b, 39. Vgl. BMAS 2017, 137.

es als Ganzes zu erkennen. Ein Vergleich mit älteren Überwachungsformen am Arbeitsplatz ist erforderlich (dazu sogleich). Danach sind die drei Kernelemente aufzuzeigen, durch die sich People Analytics von den früheren Formen der Überwachung am Arbeitsplatz abhebt: Es sind dies nach der hier vertretenen Auffassung die Ubiquität, die Interoperabilität und die steigende KI (dazu S. 71–75).

2.5.2 Geschichtliche Vorläufer der Mitarbeiterüberwachung

Die Überwachung, ob die Arbeitnehmenden die Arbeit pflichtgemäss erledigen, ist so alt wie der Arbeitsvertrag selbst. Zunächst war es die Arbeitgeberin persönlich oder ihre Stellvertreterin, die den Arbeitnehmern über die Schulter schaute. Vom britischen Philosophen und Sozialreformer Jeremy Bentham (1748–1832) stammt das «Panoptikum», ein Idealbauplan für Gefängnisse, aber auch Fabriken, welcher einer einzelnen Person erlaubt, viele Menschen aufs Mal zu überwachen. Im Mittelpunkt dieser Bauwerke steht ein Wachturm, von dem aus das gesamte Areal sichtbar ist. Weil der Beobachtungsposten des Wärters verdunkelt ist, die Arbeitsplätze aber sonnenbeschienen sind, wissen die Arbeitnehmer oder Gefängnisinsassen nie genau, ob sie gerade beobachtet werden.⁴⁰⁵ Überwachungspraktiken beschränkten sich aber nicht auf das Betriebsareal: Agenten der 1850 in Chicago gegründeten Detektei Pinkerton infiltrierten das Leben von Arbeitnehmern, die Arbeitgebende wegen ihrer Gewerkschaftszugehörigkeit als Bedrohung empfanden.⁴⁰⁶ Im Jahr 1914 gründete Henry Ford (1863–1947) eine firmeneigene soziologische Abteilung, deren Ermittler zu Hause bei den Arbeitnehmern inspizierten, ob diese den Ford-Verhaltenskodex einhielten, was Voraussetzung für den Anspruch auf gewisse Lohnbestandteile war.⁴⁰⁷

Arbeitgeber griffen schon früh zu technischen Hilfsmitteln, die die Kontrolle erleichterten: Ende des 19. Jh. kamen Stoppuhren auf, mit denen die Vorgesetzten verglichen, wer wie lange für einen Arbeitsschritt benötigte.⁴⁰⁸ Der amerikanische Ingenieur Frederick Winslow Taylor (1856–1915) nutzte die Stoppuhr zur Be-

⁴⁰⁵ ROSENBLAT/KNEESE/BOYD, 2–3. Die Idee des Panoptismus hat später Eingang in das Werk *Surveiller et punir* (1975) des französischen Philosophen Paul-Michel Foucault (1926–1984) gefunden.

⁴⁰⁶ COLLIER, 3.

⁴⁰⁷ SPRAGUE 2015, 8; COLLIER, 9.

⁴⁰⁸ Erste Stoppuhr vom amerikanischen Juwelier Willard Legrand Bundy (1845–1907) erfunden und im Jahr 1888 patentiert: COLLIER, 9.

gründung einer eigentlichen Arbeitswissenschaft.⁴⁰⁹ Um 1915 löste der flache *Modern Efficiency Desk*, der dem Vorgesetzten eine leichte Sicht auf die Arbeitsfläche verschaffte, den hohen Sekretär ab, hinter dem Arbeitnehmende zuvor einen gewissen Grad an Privatsphäre genossen hatten.⁴¹⁰

Bald wurde der Wert der Analyse von Datensätzen erkannt. Im Jahr 1922 konnte aufgezeigt werden, dass die systematische Auswertung des vergangenheitsbezogenen Verhaltens und des biografischen Hintergrunds dem Bauchgefühl bei der Prognose zukünftigen Verhaltens überlegen ist.⁴¹¹ In den 1990er- und frühen 2000er-Jahren setzte die amerikanische Baseballmannschaft Oakland Athletics bei der Suche nach Talenten auf objektive Statistiken statt auf Expertenmeinungen und feierte in der Folge mit von Experten als mittelmässig eingestuften Spielern sportliche Erfolge.⁴¹²

Spätestens seit der Verbreitung von persönlichen Computerterminals (PC) in den 1980er-Jahren setzte eine Automatisierung der Überwachung ein.⁴¹³ Jedenfalls die Phase der Datenerhebung wurde automatisiert; die Analyse der Aufzeichnungen dürfte anfangs noch weitgehend durch Menschen erfolgt sein.

2.5.3 Drei Kernelemente von People Analytics

a) Ubiquität

Die Datenbearbeitungen sind heute allgegenwärtig (lat. *ubique*: überall; vgl. engl. *ubiquitous computing*).⁴¹⁴ Erst einmal handelt es sich um eine örtliche Ubiquität: Ob der Schritt von den Grossrechnern zum PC, die Entwicklung der Smartphones und Tablets oder aber der Wechsel zur Cloud gemeint sind – sie alle bewirken eine Dezentralisierung der Datenbearbeitungen.⁴¹⁵ Die Miniaturisierung trägt das ih-

⁴⁰⁹ Bei der Arbeitswissenschaft nach Taylor überprüfen die Vorgesetzten mit der Stoppuhr, wie lange ein Arbeitnehmer für einen Arbeitsschritt benötigte, vgl.: SPRAGUE 2015, 29.

⁴¹⁰ ROSENBLAT/KNEESE/BOYD, 2.

⁴¹¹ CULIK, 65.

⁴¹² CULIK, 47.

⁴¹³ WESTIN, 439; COLLIER, 3.

⁴¹⁴ «*Ubiquitous data processing has become a reality of the modern workplace*»: CUSTERS/URSIC, 333.

⁴¹⁵ Dezentralisierung durch den PC: HÖLLER/WEDDE 2016, 298.

rige dazu bei, dass die Prozessoren überall mit von der Partie sind, etwa in Form von Wearables direkt am Körper.⁴¹⁶

Die Allgegenwart der Datenbearbeitungen ist auch von zeitlicher Dimension. Die elektronische Überwachung kann rund um die Uhr stattfinden.⁴¹⁷ Sie kann teilweise nicht gestoppt werden, weil die Geräte keine Ausschaltfunktion haben. Dies wird bei der RFID-Technologie augenscheinlich: Hier versorgt das Lesegerät (der Arbeitgeberin) den Transponder (des Arbeitnehmers) mit Energie, sodass dieser seine Position durchgibt.⁴¹⁸ Somit entscheidet primär die Arbeitgeberin, wann sie Aufzeichnungen vornehmen möchte.⁴¹⁹ Die Datenerhebung erfolgt in Echtzeit, nicht in Quartalsberichten und jährlichen Mitarbeitergesprächen. Langfristig erfassen die Analysen den gesamten Arbeitnehmer-Lebenszyklus von der Bewerbung bis zur Beendigung des Vertragsverhältnisses.⁴²⁰ Sind die Daten einmal aufgezeichnet, sind sie in der Regel verewigt.⁴²¹ Daten werden oft nicht gelöscht, sondern immer wieder aufs Neue aufbereitet und verwertet. Es entsteht ein digitales Gedächtnis oder eine temporale Version von Bentham's Panoptikum, sodass Betroffene nie sicher sein können, ob nicht gerade jemand Einsicht in lange vergessene Aufzeichnungen nimmt.⁴²² Menschen müssen lernen, mit ihrer aufgezeichneten Vergangenheit zu leben und müssen vorsichtiger sein, wenn sie etwas von sich preisgeben.⁴²³

⁴¹⁶ Miniaturisierung: POULLET 2013, 148 und 150; BOLLIGER *et al.*, 23–24. Vgl. EGGEN/STENGEL, N 4.

⁴¹⁷ RIEDY/WEN, 88; «immerwährende Kontrolle»: GORICNIK/GRÜNANGER, N 1.11.

⁴¹⁸ RFID-Systeme bestehen aus zwei Komponenten: Ein Lesegerät erzeugt ein hochfrequentes elektromagnetisches Wechselfeld; diesem ist ein Transponder (die zweite Komponente) ausgesetzt, der durch das Feld mit Energie versorgt wird und zum Antworten das Feld beeinflusst: DÄUBLER, N 324a; SPIEKERMANN, 330. Anders als beim Lesen eines Strichcodes wird bei der RFID-Technologie keine unmittelbare Nähe zwischen den beiden Komponenten verlangt – das Lesegerät kann z.B. so eingestellt werden, dass es die Transponder in 30 Meter Entfernung wahrnimmt: DÄUBLER, N 324a.

⁴¹⁹ Vgl. SPIEKERMANN, 324.

⁴²⁰ DIETRICH *et al.*, 21.

⁴²¹ «*Digital memory has become the default, and forgetting the exception*»: MAYER-SCHÖNBERGER, 196. «*Data, once created, is in many cases effectively permanent*»: White House, Executive Office of the President 2014, 9.

⁴²² MAYER-SCHÖNBERGER, 197. Siehe zum Panoptikum S. 70.

⁴²³ MAYER-SCHÖNBERGER, 109.

In personeller Hinsicht interessiert die Auswertung ganzer Teams und Belegschaften. Dies übersteigt die Überwachung in einzelnen begründeten Fällen (wie etwa bei konkretem Verdacht, dass ein Mitarbeiter gegen rechtliche Bestimmungen verstossen hat). Die Arbeitnehmenden sind nicht nur passive Betroffene, sondern speisen oft auch selbst Daten über sich in das System ein,⁴²⁴ beispielsweise indem sie sich mit dem Chatbot Mya von L'Oréal unterhalten.⁴²⁵ Die Daten stammen des Weiteren, wie der Big Data-Aspekt *variety*⁴²⁶ zeigt, von Dritten und aus dem Internet. Jedermann kann über das Internet Beobachtungen vornehmen, sodass sich der Betroffene nicht einem einzigen Big Brother, sondern «abertausenden Little Brothers» ausgesetzt sieht.⁴²⁷

Die Datenbearbeitungen durchdringen schliesslich auch inhaltlich alle Lebensbereiche (*pervasiveness*).⁴²⁸ Naturwissenschaftler nennen es die «Informatisierung des Alltags».⁴²⁹ Umfassende Datenbearbeitungen über das menschliche Treiben werden zur Routine im Sinne eines «passiven Monitorings», im Gegensatz zum «aktiven Tracking».⁴³⁰ Möglich wird dadurch die Erhebung von sog. kontextuellen, d.h. nicht aufgabenbezogenen Leistungsdaten, wie beispielsweise Mitarbeiterengagement, allgemeiner Gesundheitszustand oder Verhalten der Arbeitnehmer ausserhalb des Arbeitsplatzes.⁴³¹ Selbst wenn Dienstliches und Privates nie glasklar getrennt waren, so wirft das *ubiquitous computing* doch die Frage der Entgrenzung und der Trennung von Beruf und Privatleben in einer neuen Qualität

⁴²⁴ HÖLLER/WEDDE 2016, 304. Die Tatsache, dass Arbeitnehmer Daten in das System einspeisen, relativiert das sog. EVA-Prinzip, wonach die *Eingabe, Verarbeitung und Ausgabe* von Daten traditionell durch die gleiche Stelle erfolgte: HÖLLER/WEDDE 2016, 304.

⁴²⁵ Siehe zu Mya S. 44.

⁴²⁶ Siehe S. 38.

⁴²⁷ «*Nous ne sommes plus confrontés à un seul Big Brother, mais à des dizaines de milliers de Little Brothers*»: RAY, 29.

⁴²⁸ THOUVENIN/FRÜH/GEORGE, N 2.

⁴²⁹ So etwa der Computerwissenschaftler der Eidgenössischen Technischen Hochschule (ETH) Zürich: MATTERN FRIEDEMANN, *Die Informatisierung des Alltags*, Berlin/Heidelberg 2007.

⁴³⁰ Routinedatenerhebung als Nebenprodukt des digitalen Alltags: BAROCAS; passives Monitoring versus aktives Tracking: ROSENBLAT/KNEESE/BOYD, 7.

⁴³¹ LEICHT-DEOBALD *et al.* Kontextdaten im Medizinbereich berücksichtigt das Röntgengerät Illumeo von Philips. Neben den aufgezeichneten Röntgenbildern wertet es frühere Röntgenberichte aus und schlägt nach der Analyse der Bilder die Instrumente zur weiteren medizinischen Behandlung vor: WILSON/DAUGHERTY, 141–142.

auf.⁴³² Zu dieser Unschärfe tragen auch die Arbeitnehmer bei, wenn sie ihren Dienstcomputer nicht nur zu beruflichen Zwecken nutzen.⁴³³

b) Interoperabilität

Die Datenbearbeitungs-Systeme sind zunehmend imstande, im Sinne von Interoperabilität nahtlos miteinander zusammenzuarbeiten, sodass eine Kommunikation über die Grenzen einzelner Systeme hinweg möglich ist.⁴³⁴ Interoperabilität darf dabei nicht mit Gleichheit verwechselt werden: Sind mehrere Systeme zu 100 Prozent interoperabel, können sie nach wie vor verschiedenartig sein.⁴³⁵ People Analytics verknüpft Datenquellen, die in der Vergangenheit getrennt gehalten wurden.⁴³⁶ Die Datafizierung giesst die digitalen Daten in ein Standardformat, und das Internet fungiert als Medium für den Austausch von Information. Dadurch entfallen herkömmliche Schwierigkeiten beim Zusammenführen von Dateien aus mehreren Datenbanken.⁴³⁷ Die Interoperabilität zeigt sich beispielsweise darin, dass verschiedene Gerätetypen zusammenwachsen, weil die Software für den PC auch als App für das Tablet bereitsteht.⁴³⁸ Auch wächst die Interoperabilität an der Schnittstelle zwischen Hardware und Software: Sensoren zur Datenerhebung und Analyse-Algorithmen präsentieren sich als Ensemble, beispielsweise werden Videokameras mit integrierter Gesichtserkennungs-Software verkauft.⁴³⁹

Der Big Data-Teilaspekt *variety*⁴⁴⁰ steht sinnbildlich für die Interoperabilität. Aus der Verknüpfung von Datenquellen, die scheinbar nichts miteinander zu tun haben, beispielsweise Daten aus dem Personalbereich mit anderen Unternehmens-

⁴³² HÖLLER/WEDDE 2016, 305; LETOMBE, 27; inexistente Unterscheidung von Öffentlichkeits- und Privatsphäre: POULLET 2013, 156.

⁴³³ Vgl. RAY, 36.

⁴³⁴ Vgl. die Legaldefinition von «Interoperabilität»: Anbieterinnen von Diensten der Grundversorgung müssen die Kommunikationsfähigkeit zwischen allen Benutzerinnen und Benutzern dieser Dienste sicherstellen (Art. 21a Abs. 1 FMG). Sog. *global players* führen marktübergreifend Datensätze zusammen: HOEREN 2018, 190.

⁴³⁵ PALFREY/GASSER 2012, 10.

⁴³⁶ LEICHT-DEOBALD *et al.* Ein Referenzdatensatz kann als Zugriffsschlüssel dienen, um alle Daten zu einer Person in einer oder mehreren Datenbanken zu finden: POULLET 2013, 151.

⁴³⁷ CAVOUKIAN 2011, 6.

⁴³⁸ WEDDE 2016c, 5.

⁴³⁹ RAAB/WRIGHT, 372–373; CASCIO/MONTEALEGRE, 350.

⁴⁴⁰ Siehe S. 38.

daten oder externen Daten, entstehen Erkenntnisse von neuer Qualität.⁴⁴¹ «Rätselhaft» ist, dass auch intime Einsichten sich aus trivialen, teils generell verfügbaren Informationen speisen, etwa daraus, wie lange die Computermaus auf einem Inse-rat verharret, von welcher zu welcher Webseite jemand surft oder von wo bis wo jemand im öffentlichen Verkehr fährt.⁴⁴² Anonyme Daten bleiben nicht unbedingt namenlos, wenn sie mit anderen Daten kombiniert werden; gewählte Telefonnummern, besuchte Webseiten und E-Mail-Metadaten können genauso viele persönliche und private Informationen preisgeben wie die Inhalte der Kommunikation selbst.⁴⁴³

c) Steigende künstliche Intelligenz

Die Entwicklung von Quantencomputern und die Nutzung der Cloud-Technologie versprechen eine exponentiell wachsende Leistungsfähigkeit von Prozessoren und Verbesserungen der Speichertechnik⁴⁴⁴ – gleichzeitig sacken die Preise für die Infrastruktur in sich zusammen.⁴⁴⁵ Sogar die Zukunft wird greifbar, denn die prädik-tive Analytik konzipiert realistische Zukunftsszenarien, und präskriptive Algorithmen schlagen frühzeitig Massnahmen zur Erreichung von Unternehmenszielen vor.⁴⁴⁶ Die Arbeitgeberin kann somit die Zukunft antizipieren und ist dem Arbeit-nehmer stets einen Schritt voraus.

Die Arbeitgeberin kann sich immer mehr auf eine autonom agierende, intelligente Infrastruktur verlassen. Selbstlernende Algorithmen nehmen über Sensoren den Menschen wahr und können sich ihm anpassen.⁴⁴⁷ Roboter sind imstande, komplexe, nichtrepetitive Tätigkeiten selbständig oder in enger Zusammenarbeit mit

⁴⁴¹ DZIDA, 541.

⁴⁴² «*Privacy conundrum*»: SPRAGUE 2015, 14; POULLET 2013, 150.

⁴⁴³ SPRAGUE 2015, 35. Siehe zum Begriff der Metadaten: FN 213. Siehe zur Möglichkeit der Re-Identifizierung ausführlich später, S. 157–160.

⁴⁴⁴ VAN DEN HOVEN VAN GENDEREN, 3; Schweizerischer Bundesrat 2017b, 11; LEICHT-DEOBALD *et al.*

⁴⁴⁵ Für den gleichen Betrag erhält ein Käufer alle 18 Monate doppelt so viel Speicherkapazität und Rechenleistung: POULLET 2013, 147; billige Sensoren: ZUBOFF 2019, 17. Zur Verbilligung führt auch der Umstand, dass Mobiltelefone und Laptops, die die Arbeitnehmer ohnehin auf sich tragen, als Sensoren genutzt werden können: DAVENPORT, 51. Seit 2004 gibt es in den USA mehr Mobil- als Festnetztelefone: HALPERN, 5–2.

⁴⁴⁶ MAYER-SCHÖNBERGER/CUKIER, 195; CULIK, 58.

⁴⁴⁷ SEGARS, 4; Europarat 2016a, 7.

dem Menschen zu erledigen.⁴⁴⁸ Algorithmen übernehmen Denkarbeit und Führungsaufgaben, wie beispielsweise Risikoabschätzungen.⁴⁴⁹ Sie beaufsichtigen Arbeitnehmer, etwa ob diese ihre Schutzausrüstung tragen, und benachrichtigen gegebenenfalls den Vorgesetzten.⁴⁵⁰ Dadurch entsteht eine Umweltintelligenz (*ambient intelligence*), d.h., autonome intelligente Umgebungen treffen eine beispiellose Anzahl von Entscheidungen für das private und öffentliche Wohl.⁴⁵¹ Tastatur und Bildschirm werden als Schnittstellen zwischen Mensch und Maschine entfallen; stattdessen wird die Umwelt selbst, gespickt mit unsichtbaren Sensoren, zu ebendieser Schnittstelle.⁴⁵²

Algorithmen gelten als eine Quelle sozialer Ordnung.⁴⁵³ Damit ist gemeint, dass die KI das Zweipersonenverhältnis zwischen Arbeitgeberin und Arbeitnehmer beeinflusst. Das Dazwischenfunken einer dritten (wenn auch nicht rechtsfähigen) Person weckt Ängste: Selbstlernende Algorithmen, die sich verändern und ihrerseits wieder neue Algorithmen schreiben, entziehen einem die Kontrolle.⁴⁵⁴ Arbeitnehmende könnten durch verhaltenssteuernde Algorithmen «automatisiert» werden.⁴⁵⁵ Ohne zu beurteilen, wie begründet diese Sorgen sind: Recht ist eines von mehreren möglichen Mitteln zur Einwirkung auf diese Entwicklung.⁴⁵⁶

2.5.4 Zwischenfazit zu den drei Kernelementen

Während die Überwachung der Leistungserbringung schon immer zum Arbeitsverhältnis gehört hat, nimmt sie durch People Analytics eine neue Dimension an.

⁴⁴⁸ Schweizerischer Bundesrat 2017b, 11. AKHTAR/MOORE, 111. Indem KI adaptive Geschäftsabläufe ermöglicht, die nicht standardisiert und trotzdem effizient sind, stösst sie in eine Richtung, die konträr zu der durch Henry Ford (1863–1947) eingeleiteten Standardisierung von Betriebsprozessen und der Automatisierung durch die Informationstechnologie ab den 1970er-Jahren verläuft: WILSON/DAUGHERTY, 5–6.

⁴⁴⁹ PHAN *et al.*, 253; SAURWEIN, 49.

⁴⁵⁰ COLLIER, 3.

⁴⁵¹ HILDEBRANDT/KOOPS, 428.

⁴⁵² Konzept der Umweltintelligenz Ende der 1990er-Jahre von Philips eingeführt und von der Europäischen Kommission rezipiert: HILDEBRANDT/KOOPS, 430.

⁴⁵³ Mit Bezug auf die algorithmische Selektion: SAURWEIN, 49; HOFFMANN-RIEM, 51.

⁴⁵⁴ SMITH ANDREW, Franken-algorithms: the deadly consequences of unpredictable code, *The Guardian* vom 30.08.2018, abrufbar unter <www.theguardian.com> (besucht am 31.05.2020).

⁴⁵⁵ ZUBOFF 2019, 19.

⁴⁵⁶ Vgl. HOFFMANN-RIEM, 34.

Sie zeichnet sich durch Ubiquität, Interoperabilität und steigende KI aus. D.h., die Datenbearbeitungen sind allgegenwärtig; aus dem Zusammenführen von Datensätzen resultieren neue Erkenntnisse, die früher nicht möglich waren; und die KI der Algorithmen stärkt die Stellung der Arbeitgeberin im Arbeitsvertragsverhältnis. Diese drei Kernelemente hat der Autor vorliegend herausgearbeitet basierend auf der Detailanalyse der technischen Umgebung und der Verwendungszwecke von People Analytics sowie nach einem Blick zurück auf die geschichtlichen Vorläufer der Mitarbeiterüberwachung.

Nach der hier vertretenen Auffassung, zu welcher der Autor auch aufgrund seiner empirischen Forschungserfahrung gelangt ist, finden sich die drei Kernelemente von People Analytics in der Praxis aber nicht überall gleichmässig vor. Beispielsweise der virtuelle Karriereassistent⁴⁵⁷ führt zwar Daten zur Arbeitsmarktentwicklung mit Daten aus dem Lebenslauf und den Zeugnissen zusammen (Interoperabilität) und errechnet daraus selbständig das Risiko, dass die betreffende Stelle der Digitalisierung zum Opfer fallen wird (steigende KI). Doch ist diese Anwendung kaum allgegenwärtig (fehlende Ubiquität), weil der Karriereassistent nicht täglich, sondern vielleicht nur einige Male pro Jahr für die berufliche Weiterorientierung konsultiert wird. Der Umstand, dass die Datenbearbeitung nicht ubiquitär erfolgt, kann für die rechtliche Beurteilung entscheidend sein, weil in der Regel umso weniger Risiken für die Persönlichkeit entstehen, je weniger Daten bearbeitet werden. Hierauf ist später zurückzukommen.⁴⁵⁸

2.6 **Zwischenfazit: neuartiges, weit verbreitetes Phänomen**

In Kapitel 2 ist das Phänomen «People Analytics» beschrieben worden. Die Betrachtung des Daten-Lebenszyklus hat gezeigt, dass eine umfassende technische Apparatur hinter dem Forschungsgegenstand steckt.⁴⁵⁹ Es wurde festgestellt, dass entlang dem Arbeitnehmer-Lebenszyklus zahllose mannigfaltige Zwecke für die Verwendung von People Analytics existieren.⁴⁶⁰ Ausserdem hat das Phänomen bereits in weiten Teilen des Arbeitslebens Einzug gehalten und wird sich künftig

⁴⁵⁷ Siehe S. 55.

⁴⁵⁸ Siehe S. 147.

⁴⁵⁹ Siehe S. 19–41.

⁴⁶⁰ Siehe S. 42–59.

zunehmend verbreiten.⁴⁶¹ People Analytics ist ein neuartiges Phänomen, das sich im Unterschied zu seinen geschichtlichen Vorläufern durch Ubiquität, Interoperabilität und steigende KI auszeichnet.⁴⁶²

Insgesamt verbleibt von der vorliegenden Phänomenbeschreibung der Eindruck, dass sich People Analytics faktisch ungehindert ausbreitet und zu immer neuen Zwecken verwendet wird. Der technologische Fortschritt ermöglicht dies. Wenn aber die Technik keine Grenzen setzt, drängt sich die Frage auf, ob das Recht wirksame Schranken zum Schutz der Betroffenen bereithält. Dieser rechtlichen Seite des Phänomens sind die folgenden Kapitel gewidmet. Es ist zunächst zu prüfen, welche Rechtsprobleme durch die beliebige Entfaltung von People Analytics entstehen (dazu sogleich).

⁴⁶¹ Siehe S. 60–69.

⁴⁶² Siehe S. 69–77.

3 **Rechtsprobleme**

3.1 **Übersicht**

Nachdem in Kapitel 2 das Phänomen People Analytics beschrieben worden ist, wenden wir uns in den folgenden Kapiteln dessen rechtlicher Seite zu. Hierfür ist mit der Eruiierung der Rechtsprobleme zu beginnen. Das Grundproblem von People Analytics besteht darin, dass es zu einer Machtverschiebung von den Arbeitnehmern hin zur Arbeitgeberin kommt oder zumindest kommen kann (dazu sogleich, Unterkapitel 3.2, S. 79–82). Daraus folgen drei Rechtsprobleme, die nacheinander dargestellt werden: Persönlichkeitsverletzungen, Diskriminierungen und die Verletzung von Mitwirkungsrechten (Unterkapitel 3.3–3.5, S. 82–105).

3.2 **Machtverschiebung als Grundproblem**

Die drei dargestellten Charakteristika von People Analytics – Ubiquität, Interoperabilität und steigende künstliche Intelligenz⁴⁶³ – schaffen in ihrer Summe ein neues Problem, nämlich eine Informations- und Machtakkumulation bei der Arbeitgeberin in einem bisher nicht dagewesenen Ausmass.

Mit People Analytics hat die Arbeitgeberin die Möglichkeit, zu tiefen Grenzkosten wertschöpfende und entscheidungsrelevante Erkenntnisse zu erlangen.⁴⁶⁴ Wenn sie mit People Analytics ein Werkzeug zum Wissensgewinn in der Hand hält, der Arbeitnehmer dieses Werkzeug aber weder beeinflussen noch vollständig überschauen kann, führt dies zu einem Informationsgefälle.⁴⁶⁵ Dieses verstärkt sich

⁴⁶³ Siehe Unterkapitel 2.5.3a)–2.5.3c) bzw. zur Ubiquität S. 71–74, zur Interoperabilität S. 74–75 und zur steigenden KI S. 75–76.

⁴⁶⁴ GABATHULER resümiert nach einem Vergleich verschiedener Definitionsansätze, Big Data sei «die auf der Digitalisierung weiter Teile von Wirtschaft und Gesellschaft und des damit verbundenen schnellen Wachstums an verfügbaren Daten basierende Möglichkeit, durch Erheben, Speichern und Auswerten beliebiger Daten zu tiefen Grenzkosten wertschöpfende und entscheidungsrelevante Erkenntnisse zu erlangen und diese wenn möglich automatisiert und in Echtzeit anzuwenden»: GABATHULER SILVAN, 42. In der «Möglichkeit zum Erkenntnisgewinn» kommt das Verständnis von Information als Wertchance (und nicht als Wert) zum Ausdruck. Siehe dazu S. 21.

⁴⁶⁵ «Massive Informationsasymmetrien» entstehen auch zwischen den Entwicklern von Algorithmen einerseits und dem Gesetzgeber und Konsumenten andererseits: GASSER/ALMEIDA, 58. A.M. CULIK, 152 und 293; Die Arbeitgeberin sei einem Bewerber in informationeller Hinsicht strukturell unterlegen, weil sie wenig Informationen über

durch den Skaleneffekt in Plattformmärkten, welcher bewirkt, dass die Analysekosten pro Nutzer bei steigender Nutzerzahl sinken.⁴⁶⁶ Der Skaleneffekt dürfte am Arbeitsplatz zwar weniger stark zum Tragen kommen als etwa bei sozialen Netzwerken mit Millionen von Nutzern, weil die wenigsten Unternehmen so viele Beschäftigte haben. In grossen Unternehmen mit zehntausenden Angestellten mag er mehr ausmachen als in kleinen und mittleren Unternehmen. Doch darf nicht vergessen werden, dass auch kleine Unternehmen, die systematisch Daten ihrer Arbeitnehmer sammeln, sich einen umfangreichen Datenschatz aufbauen können. Das Datenvolumen, das im Arbeitsverhältnis entsteht, ist gross, weil die Arbeitnehmer regelmässig einen grossen Anteil der Gesamtzeit an der Arbeit verbringen.⁴⁶⁷ Kaum ein anderes Rechtsverhältnis gibt Anlass zur Erhebung und Bearbeitung personenbezogener Daten verschiedenster Art in solch grossem Umfang und während so langer Zeit wie das Arbeitsverhältnis.⁴⁶⁸

«Wissen ist Macht», ein Zitat des englischen Philosophen, Juristen und Staatsmannes BACON (1561–1626),⁴⁶⁹ bedeutet, dass aus dem Informationsungleichgewicht ein Machtgefälle folgt.⁴⁷⁰ Big Data vermittelt «Macht zur Vorhersage, Macht zur Gestaltung und Macht, Entscheidungen zu treffen, die das Leben der einfachen Menschen beeinflussen».⁴⁷¹ Zwischen kommerziellen Datensammlern und Betroffenen besteht ein strukturelles Ungleichgewicht.⁴⁷² Die Investitionen in die Entwicklung von Profilbildungstechnologie übersteigen diejenigen für die Entwicklung von Technologien, die die Privatsphäre schützen, um ein Vielfaches.⁴⁷³

seine Fähigkeiten und Motivation besitze, er sich aber durch allgemein zugängliche Quellen umfassend über sie informieren könne. Nach der vorliegend vertretenen Auffassung ist diese Ansicht zu relativieren: Die Bewerbungsunterlagen bieten einen recht detaillierten persönlichen Steckbrief des Bewerbers, und die Informationen, die ein Unternehmen über sich ins Internet stellt, sind einseitig positiv gefärbt und verlieren dadurch an Aussagekraft.

⁴⁶⁶ MARTINI, 1017.

⁴⁶⁷ Vgl. HOEREN 2018, 190: Durch eine Profilerstellung droht sich die Machtasymmetrie im Arbeitsverhältnis weiter zu verfestigen.

⁴⁶⁸ BBl 1988 II, 488.

⁴⁶⁹ «*Scientia potestas est*»: BACON, 39 (De Haeresibus).

⁴⁷⁰ AEBI-MÜLLER, N 705.

⁴⁷¹ RICHARDS/KING, 432.

⁴⁷² AEBI-MÜLLER, N 541; AB NR 1991, 967.

⁴⁷³ BAUMANN MAX-OTTO, 5. Vgl. die Ansicht, dass datenschutzfreundliche Technologien von den Marktkräften nicht akzeptiert werden: HILDEBRANDT/KOOPS, 460.

Die Regulierung von Informationsflüssen ist, wie aufgezeigt, eine Aufgabe des Informationsrechts.⁴⁷⁴ Die gerechte Zuweisung von Macht, wie sie etwa in der öffentlich-rechtlichen Gewaltenteilung zum Ausdruck kommt, ist ebenfalls eine Aufgabe des Rechts.⁴⁷⁵ Somit handelt es sich bei der beschriebenen Machtverschiebung zugunsten der Arbeitgeberin um ein Problem, das rechtlich gelöst werden kann.

Manche Autoren greifen zu einer Rhetorik, die geradezu einen neuen Gesellschaftsvertrag fordert.⁴⁷⁶ Sie stören sich am Umstand, dass einige Private durch die Informatisierung der Gesellschaft eine Machtposition erlangen, die mit der Macht staatlicher Träger vergleichbar ist, weil sie die Grundrechte anderer beeinträchtigen können.⁴⁷⁷ Das Datenschutzrecht, dessen Schwerpunkt ursprünglich auf der Abwehr staatlicher Eingriffe in Grundrechte lag, dient vermehrt auch dem Ausgleich zwischen privatwirtschaftlichen Interessen.⁴⁷⁸ Diese Argumente böten

⁴⁷⁴ Siehe S. 23.

⁴⁷⁵ Gewaltenteilung als «rechtskulturelle Errungenschaft»: TSCHENTSCHER, 636.

⁴⁷⁶ «Der Leviathan und globale Oligopole» gewinnen mit Big Data Instrumente zur Durchsetzung ihrer Interessen, weshalb demokratische Transparenz im Sinne einer «öffentlichen Diskussion über die Regeln für Big Data» wichtig sei: HORNUNG, 97. «Von John Locke (1632–1704) über Emile Durkheim (1858–1917)» bis heute könne man den zeitgenössischen Gesellschaftstyp als einen «vertraglichen» bezeichnen: ZUBOFF 2015, 81. Die moderne Überwachung von Arbeitnehmern sei «une véritable question de société»: RAY, 40. Privatsphäre sei eine Frage der Macht und die Macht des Rechtsstaats und der Gesellschaft müsse mobilisiert werden: O'ROURKE *et al.*, 166; RICHARDS/HARTZOG 2017, 1184.

⁴⁷⁷ HOFFMANN-RIEM, 26. Eine Machtkonzentration besteht besonders bei den sog. Big Five (Facebook, Google, Microsoft, Amazon, Apple): HOFFMANN-RIEM, 37. «Totalitäre Tendenzen des Silicon Valley»: BMAS 2017, 67, m.w.H.; «digitaler Imperialismus des Silicon Valley»: DSGVO-BDSG-K-MARTINI, Art. 35 DSGVO, N 77. «Überwachungs-Kapitalismus» («*surveillance capitalism*»): ZUBOFF 2015, 75. Code bzw. Software steuere in der digitalen Welt faktisch das Verhalten wie ein Gesetz: GANTNER, 1. «*Code writers are increasingly lawmakers*»: LESSIG, 79. «*Algorithmic decisionmakers are sovereign over important aspects of individual lives*»: KEATS CITRON/PASQUALE, 19. «*Design is power because people react to design in predictable ways*»: HARTZOG 2018, 34.

⁴⁷⁸ Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 8. Anscheinend mit der Forderung nach einer direkten Drittwirkung von Grundrechten: «*Le salarié reste un citoyen dans l'entreprise. Il a donc droit au respect de sa vie personnelle et de sa vie privée*»: LETOMBE, 25. Vgl. die Forderung nach Verfahrensgarantien (*procedural regularity*) beim Einsatz von prädiktiven Algorithmen: KEATS CITRON/PASQUALE, 18.

Stoff für eine rechtsphilosophische oder staatsrechtliche Abhandlung. Die vorliegenden Betrachtungen beschränken sich aber auf privatrechtliche Fragen.

Die grassierende Informations- und Machtdiskrepanz bildet gewissermassen eine Bodenströmung, die auf den ersten Blick unsichtbar bleibt. Bemerkbar wird sie an der Oberfläche, wenn den betroffenen Arbeitnehmern Rechtsgüter oder Ansprüche weggerissen werden. Namentlich drohen als rechtliche Folgeprobleme Verletzungen der Persönlichkeitsrechte, des Diskriminierungsschutzes und der Mitwirkungsrechte, wie sogleich darzulegen ist.

3.3 Persönlichkeitsverletzungen

3.3.1 Umfassender Persönlichkeitsschutz

Die Rechtsfragen, die People Analytics aufwerfen kann, drehen sich im Kern um den Persönlichkeitsschutz der Arbeitnehmer. Die Datenbearbeiter versuchen, Aussagen über Personen und ihr Verhalten zu gewinnen.⁴⁷⁹ Klagen der Arbeitnehmer wegen unrechtmässiger Bearbeitung von Personendaten durch die Arbeitgeberin richten sich nach dem zivilrechtlichen Schutz der Persönlichkeit (Art. 328 Abs. 1 Satz 1 OR i.V.m. Art. 328b Satz 2 OR i.V.m. Art. 15 Abs. 1 Satz 1 DSG i.V.m. Art. 28 f. ZGB; Art. 28 Abs. 2 Satz 1 E-DSG, Art. 32 Abs. 2 Satz 1 rev-DSG).

Das Gesetz enthält keine Legaldefinition des Begriffs «Persönlichkeit» (vgl. Art. 28 ZGB).⁴⁸⁰ Die Botschaft zu Art. 28 ZGB zählt «alle physischen, psychischen, moralischen und sozialen Werte, die einer Person kraft ihrer Existenz zukommen», zur Persönlichkeit.⁴⁸¹ Für das Bundesgericht besteht die Persönlichkeit aus all dem, «was zur Individualisierung einer Person dient und im Hinblick auf die Beziehungen zwischen den einzelnen Individuen und im Rahmen der guten Sitte als schutzwürdig erscheint».⁴⁸² Somit ist der Begriff der Persönlichkeit umfassend zu verstehen, unter Einbezug der physischen, psychischen, sozialen und seelischen Persönlichkeit.⁴⁸³

Persönlichkeitsrechte sind diejenigen Rechte, die den infrage stehenden Persönlichkeitsaspekt schützen. Mit der Verletzung der Persönlichkeit ist notwendiger-

⁴⁷⁹ Vgl. HOFFMANN-RIEM, 15.

⁴⁸⁰ WOLFER, N 84.

⁴⁸¹ BBl 1982 II, 658. Vgl. BBl 1988 II, 418.

⁴⁸² BGE 143 III 297 E. 6.4.1. Ständige Rechtsprechung, siehe bereits: BGE 45 II 623 E. 1.

⁴⁸³ AEBI-MÜLLER, N 376.

weise immer auch das betreffende Persönlichkeitsrecht verletzt.⁴⁸⁴ Das Gesetz spricht von einer Verletzung «der Persönlichkeit» (Art. 28 Abs. 1 ZGB) und nicht des Persönlichkeitsrechts. Vorliegend wird diese Begriffswahl fortgeführt, gemeint ist also immer auch die Missachtung des entsprechenden Rechts.⁴⁸⁵

3.3.2 Ausgewählte Aspekte der Persönlichkeit

a) Privatsphäre

People Analytics tangiert hauptsächlich die Persönlichkeitsaspekte der Privatsphäre und der psychischen Integrität.⁴⁸⁶ Die Privatsphäre bezeichnet einen Bereich, in dem die betreffende Person frei von Anpassungsdruck in der Authentizität ihres Verhaltens, in ihrer Spontaneität sowie freien Meinungs- und Willensbildung nicht gestört wird.⁴⁸⁷ In diesem Bereich darf die betreffende Person sich selbst sein, darf auch etwas eigentümlich sein (lat. *privatus*: persönlich, einer einzelnen Person gehörig, eigen, eigentümlich).

Permanente Überwachungen können zu einem Verlust von Authentizität und Kontrolle über die Selbstdarstellung sowie zu einer Störung von Beziehungsgestaltungen führen.⁴⁸⁸ Dies ist etwa denkbar bei der eingangs vorgestellten Software Intelligent Edge von Microsoft, die zur Überwachung der Einhaltung von Sicherheitsrichtlinien am Arbeitsplatz pro Sekunde 27 Millionen Aufzeichnungen liefert.⁴⁸⁹ Eine intensive elektronische Überwachung, deren sich die überwachte Person bewusst ist, ist geeignet, sie zu einer Anpassung ihres Verhaltens zu zwingen.⁴⁹⁰ Ein sozialwissenschaftliches Forschungsexperiment brachte hervor, dass Arbeitnehmer mehr Geld in die Kaffeekasse im Pausenraum steckten, wenn Augäpfel das Schild, das sie zur Zahlung anhielt, zierten, um ein Gefühl des Beobach-

⁴⁸⁴ WOLFER, N 88. Vgl.: «*un trouble aux biens de la personnalité d'autrui en violation des droits qui la protègent*»: BGE 120 II 369 E. 2.

⁴⁸⁵ So auch bei WOLFER, N 89.

⁴⁸⁶ WOLFER, N 87; zu den von People Analytics betroffenen Persönlichkeitsaspekten ausführlich: WOLFER, N 84–174.

⁴⁸⁷ Vgl. WOLFER, N 154.

⁴⁸⁸ WOLFER, N 325–331 und 623–625.

⁴⁸⁹ SULLIVAN MARK, At build, Microsoft's vision of the future workplace looks both helpful and intrusive, 05.10.2017, abrufbar unter <www.fastcompany.com> (besucht am 31.05.2020). Siehe zu Intelligent Edge: S. 51.

⁴⁹⁰ WOLFER, N 154.

tet-Werdens zu vermitteln.⁴⁹¹ Menschen beginnen, ihr Verhalten an den Analyse-Tools auszurichten, beispielsweise um zu möglichst guten Bewertungen zu kommen.⁴⁹² Ein authentisches Verhalten ist nur möglich, wenn man sich vor Einblicken durch andere schützen kann. Auf den Punkt gebracht: «Authentizität gedeiht nur in der Dunkelheit. Wie Sellerie.»⁴⁹³

Die grosse Herausforderung von People Analytics ist die Bewahrung von Autonomie als Aspekt der Privatsphäre:⁴⁹⁴ Je mehr Wissen die Arbeitgeberin über den Arbeitnehmer hat oder zumindest Hypothesen zu seinen Eigenschaften, seinem Verhalten und seinen Bedürfnissen, desto einfacher kann sie ihn beeinflussen,⁴⁹⁵ beispielsweise mit personalisierten Diensten.⁴⁹⁶ Der Arbeitnehmer wird dadurch manipulierbar.⁴⁹⁷ Dies zeigt sich am Beispiel von Uber: Für den Fahrdienstvermittler ist es überlebenswichtig, jederzeit genügend Autos im Angebot zu haben. Während der Zeiten, in denen die Nachfrage tief und weniger Geld zu verdienen ist, verzichten viele Fahrer auf das Anbieten ihrer Dienstleistung. Um dieser Tendenz entgegenzuwirken, sendet Uber den Chauffeuren Nachrichten, die sie an ihr Zieleinkommen erinnern und so zum Fahren stimulieren.⁴⁹⁸ Während der Eingriff in die Autonomie im Uber-Beispiel begrenzt erscheinen mag, steigt das Manipulationsrisiko je nach Technik, die bei People Analytics zur Anwendung gelangt. Beispielsweise bergen Anwendungen mit starker KI ein höheres Manipulations-

⁴⁹¹ RICHARDS, 106.

⁴⁹² Sog. Rückkoppelungseffekt: BMAS 2017, 65.

⁴⁹³ HARTZOG/STUTZMAN 2013, 47–48, m.w.H.

⁴⁹⁴ Bewahrung der Autonomie als Herausforderung für die digitale Transformation: HOFFMANN-RIEM, 30. Sowohl Art. 28 ZGB als auch das DSGVO haben letztlich den gleichen Zweck, nämlich die Autonomie und Entscheidungsfreiheit der betroffenen Personen zu schützen: BBl 1988 II, 458.

⁴⁹⁵ HÄNOLD, 131–132. Vgl. KASPER/WILDHABER, 215.

⁴⁹⁶ CROLL ALISTAIR, Big data is our generation's civil rights issue, and we don't know it, 31.07.2012, abrufbar unter <<http://solveforinteresting.com>> (besucht am 31.05.2020); KASPER/WILDHABER, 215.

⁴⁹⁷ Vgl. PRIEUR, 1645, BMAS 2017, 65, und LEWIS PAUL, Senator warns YouTube algorithm may be open to manipulation by «bad actors», The Guardian vom 05.02.2018, abrufbar unter <www.theguardian.com> (besucht am 31.05.2020). Direkte Beeinflussung von Personen durch Big Data: Art.-29-Datenschutzgruppe 2013, 35. Vgl. algo:aware [sic], 20. KASPER/WILDHABER, 215–216.

⁴⁹⁸ CUSTERS/URSIC, 329.

potenzial in sich als solche mit schwacher KI.⁴⁹⁹ Die prädiktive Analytik geht davon aus, dass sich Arbeitnehmer mit ähnlichen Attributen in vergleichbaren Situationen gleich verhalten.⁵⁰⁰ Wenn eine Arbeitgeberin einen Entscheid für alle mit einem bestimmten Profil fällt, ohne die Arbeitnehmer anzuhören, kann es sein, dass sie Entscheidungen vorwegnimmt, die der Arbeitnehmer fällen müsste.⁵⁰¹ Im Extremfall führt die Annahme, dass menschliches Verhalten berechenbar sei, zur Negierung des freien Willens.⁵⁰²

Dem Verständnis von Privatsphäre haftet etwas Subjektives an. Weltweit gesehen besteht kein Konsens bzgl. der Konkretisierung des Rechts auf Privatsphäre im digitalen Zeitalter.⁵⁰³ Pessimisten sehen das «Ende der Privatsphäre» kommen,⁵⁰⁴ wähen sich gar im «Post-Privacy-Zeitalter»,⁵⁰⁵ weil die Digitalisierung immer mehr familiäre und intime Aspekte des Lebens für Dritte zugänglich macht. Diese Angst mag bei einem rein räumlichen, eindimensionalen und mittlerweile antiquierten Verständnis von Privatsphäre, welches vom Schutz des (Grund-)Eigentums herkommt, begründet sein.⁵⁰⁶ Zu bedenken ist jedoch, dass sich das individuelle und gesellschaftliche Bedürfnis nach Privatsphäre über die Zeit geändert hat und ändern wird.⁵⁰⁷ Die neue Omnipräsenz der Datenbearbeitungen wird die

⁴⁹⁹ Zu den Begriffen der starken und schwachen KI: S. 31. Das grösste Risiko wird die gegenwärtig noch nicht existierende starke KI (*artificial general intelligence, AGI*) mit sich bringen: GUIHOT *et al.*, 453.

⁵⁰⁰ AKHTAR/MOORE, 112.

⁵⁰¹ POULLET 2013, 154–155. Um «Reduktionismus» handle es sich, wenn eine Person nur noch als Profil wahrgenommen werde: POULLET 2013, 156.

⁵⁰² DREYER, 139. Der durch Datenanalysen erlangte Wissensvorsprung ermögliche, die Entscheidungsautonomie des Betroffenen zu unterlaufen: BAUMANN MAX-OTTO, 3–4.

⁵⁰³ VON ARNAULD, 119. Für den angelsächsischen Raum sei Privatsphäre ein «amorphes und schwer fassbares Konzept»: HARTZOG 2018, 10. Rechtsvergleichend zwischen Europa, USA und Kanada resultiere «kein Konsens über die Definition des allgemein bekannten Rechts auf Privatsphäre»: OTTO 2016, 174.

⁵⁰⁴ SCHAAR 2007; «*death of privacy*»: RICHARDS/HARTZOG 2017, 1188.

⁵⁰⁵ HELLER. Vgl. eine 20-Jährige, die, angesprochen auf peinliche Fotos in sozialen Netzwerken, gegenüber der amerikanischen Computerzeitschrift Wired aussagt: «*the people who care will all retire and the world will be run by my generation, which doesn't give a shit*»: MATZNER, 96, m.w.H.

⁵⁰⁶ Räumliches Verständnis von Privatsphäre eng und antiquiert: RICHARDS/KING, 395. Noch dominiert die räumliche Auffassung von Privatsphäre; sie kommt von der Vorstellung von Grundeigentum: WALDMAN, 17–18. Vgl. DEBEER, 386.

⁵⁰⁷ TAMÒ-LARRIEUX, 251.

gesellschaftlichen Normen und Erwartungen an die Privatsphäre beeinflussen.⁵⁰⁸ Das moderne Verständnis von Privatsphäre ist subjektiver und betont stärker die Erwartungen, Wünsche und Vorstellungen des Einzelnen.⁵⁰⁹ Selbst zum gleichen Zeitpunkt innerhalb des gleichen Landes können die Erwartungen von Individuen bzgl. des Schutzes der Persönlichkeit stark auseinanderdriften.⁵¹⁰ Das Recht muss somit People Analytics nicht im Keim ersticken, sondern einen Weg finden, um die kontextuellen Normen zur Privatsphäre zu respektieren.⁵¹¹ Im Arbeitsverhältnis existieren unzählige solcher Kontextnormen, die je nach Arbeitsumgebungen, Beschäftigungsarten und Erwartungen der einzelnen Arbeitnehmer und Arbeitgeberinnen verschieden sind.⁵¹² Beispielsweise ist denkbar, dass die Mitarbeiter eines IT-Unternehmens, das People Analytics-Anwendungen entwickelt, eher gewillt sind, sich auswerten zu lassen, da sie auf diese Weise die selbst entwickelten Produkte testen können. Auch könnte die Bereitschaft zur Überwachung höher sein in Berufen, die ohnehin schon beaufsichtigt sind, etwa durch die Finanzmarktaufsicht. Von der Arbeitgeberin ist Fingerspitzengefühl gefordert, um die Erwartungshaltung ihrer Arbeitnehmer an die Privatsphäre einschätzen zu können.

b) Psychische Integrität

Zur psychischen Integrität gehört der seelisch-emotionale Lebensbereich einer Person, der von zahlreichen äusseren und inneren Einflüssen bestimmt wird.⁵¹³ Unterschieden werden die Teilgehalte des seelischen Wohlbefindens und der psychischen Gesundheit.⁵¹⁴ Ersteres bezeichnet einen Zustand der positiven Gefühle und Stimmungen,⁵¹⁵ Letztere eine Abwesenheit von besonders schweren psychischen Beanspruchungen, die psychiatrische Krankheitsfolgen nach sich ziehen können.⁵¹⁶ In vielen Berufen findet eine Verschiebung von vormals physischen zu

⁵⁰⁸ NISSIM/WOOD, 1.

⁵⁰⁹ OTTO 2016, 184.

⁵¹⁰ LE MÉTAYER, 327.

⁵¹¹ Vgl. NISSENBAUM 2004, 120. Vgl. OTTO 2016, 184. Z.B. im arbeitsrechtlichen Kontext sei die Erwartung einer Privatsphäre berechtigt: OTTO 2016, 197.

⁵¹² OTTO 2016, 184.

⁵¹³ WOLFER, N 90 und 107.

⁵¹⁴ WOLFER, N 618.

⁵¹⁵ WOLFER, N 92.

⁵¹⁶ WOLFER, N 105.

überwiegend psychischen Anforderungen statt.⁵¹⁷ People Analytics tangiert die psychische Integrität, wenn beispielsweise durch permanente Ortung des Arbeitnehmers ein erheblicher psychischer Überwachungsdruck, Stress und eine Einschränkung der Bewegungsfreiheit entstehen.⁵¹⁸ Stress ist die hauptsächlich negative Auswirkung von intensivierten technischen Überwachungen auf die Psyche des Arbeitnehmers.⁵¹⁹

c) Recht am eigenen Wort und Bild

Von People Analytics betroffen sein kann auch das Recht am eigenen Wort und an der eigenen Stimme, das den Schutz der verbalen Lebensäußerungen vor heimlicher Aufnahme, Manipulation und Weiterverbreitung an einen anderen als den zu erwarteten Personenkreis bezweckt.⁵²⁰ Ein weiterer Persönlichkeitsaspekt ist das Recht am eigenen Bild, welches zur Bestimmung über die Verwendung jeder Gestaltungsform und Darstellung, mit deren Hilfe ein Abbild geschaffen werden kann, berechtigt, also namentlich fotografische oder filmische Aufnahmen.⁵²¹ Das Recht am eigenen Wort und Bild wird beispielsweise tangiert, wenn Instrumente zur Stimmanalyse oder Videokameras bei People Analytics verwendet werden.

⁵¹⁷ BMAS 2017, 135.

⁵¹⁸ Zu den einzelnen Aspekten der psychischen Integrität: WOLFER, N 90–108. Permanente Überwachung kann auch am Ursprung von Mobbing stehen: AKHTAR/MOORE, 108.

⁵¹⁹ WOLFER, N 97, m.w.H. Stress, Burnout und Unfälle an der Schnittstelle Mensch–Maschine als Risiken der Digitalisierung: Schweizerischer Bundesrat 2017b, 105; Stress ist «ein Zustand, der mit physischen, psychischen oder sozialen Belastungen oder Beschwerden einhergeht und der darauf zurückzuführen ist, dass der Einzelne sich nicht in der Lage fühlt, die an ihn gestellten Erwartungen zu erfüllen»: ETUC *et al.*, Ziff. 3; BLANPAIN, 813–814. Beim taiwanesischen Elektronik-Unternehmen Foxconn, das mit elektronischen Mitteln die Leistungen der Arbeitnehmer auswertet, seien Stress, psychische Zusammenbrüche und physische Gesundheitsprobleme «Routine»: AKHTAR/MOORE, 109. Vgl. DAVIS PLÜSS JESSICA / REUSSER KAI, Your employer might be watching you. Should you care?, 13.05.2019, abrufbar unter <www.swissinfo.ch> (besucht am 31.05.2020).

⁵²⁰ WOLFER, N 172.

⁵²¹ WOLFER, N 168.

3.4 Diskriminierungen

3.4.1 Problembeschreibung

People Analytics bringt nicht immer die Objektivität in die Personalentscheidungen hinein, die verheissen wird.⁵²² Der Interpretation von Daten haftet immer etwas Subjektives an: Die Lichtstrahlen, die dem Datenempfänger das Abbild eines Wortes im Auge liefern, durchlaufen beim Lesenden einen komplexen inneren Prozess, der aus dem physikalischen Input (z.B. aus den Buchstaben «B-a-l-l») ein Bild (Ball) macht, wobei jeder Leser an etwas anderes denken kann (kugelförmiges Sportgerät oder festliche Tanzveranstaltung). Bei der Herstellung von «Verständnis» begegnet der eingehende Impuls einem Vorrat an früher erworbener Information, Zeichen- und Sprachkompetenz.⁵²³ Für die Frage der Objektivität ist somit entscheidend, wie bei People Analytics die Daten interpretiert und die Techniken angewendet werden.⁵²⁴

People Analytics birgt von Natur aus ein Risiko für Diskriminierungen in sich, weil gestützt auf Statistiken, scheinbar rational, zwischen Individuen «unterschieden» wird (lat. *discriminare*: (geistig) unterscheiden, trennen, absondern).⁵²⁵ Die Arbeitnehmer werden durch Profiling in Kategorien unterteilt, und Personalentscheidungen treffen jeweils Kategorien von Mitarbeitern mit vorbestimmten Profilen.⁵²⁶ Die algorithmischen Modelle unterscheiden stets zwischen Gewinnern und Verlierern: Suchresultate gibt der Algorithmus in einer Rangfolge bekannt, weil die Programmierung ihm befiehlt, die Informationen über Arbeitnehmer nach Relevanz zu sortieren.⁵²⁷ Wiederholt sind Vorurteile bzgl. Rassen- und Geschlechtszugehörigkeit in der Personalverwaltung nachgewiesen worden.⁵²⁸ Die

⁵²² Vgl. Europarat 2019, 10. Siehe zum Versprechen der Objektivität S. 2.

⁵²³ Vgl. DRUEY 1995, 15.

⁵²⁴ Vgl. TÜRK, 15.

⁵²⁵ WILDHABER *et al.*, 461–462. Vgl. BAROCAS/SELBST, 677. DREYER/SCHULZ, 7. Das Europäische Parlament appelliert zur Vorbeugung gegen algorithmische Diskriminierungen sowohl an die Behörden (Europäisches Parlament 2017, E. 20) als auch an Private (Europäisches Parlament 2017, E. 22). «*Social exclusion, marginalization and stigmatization*»: FAVARETTO *et al.*, 11. Vgl. ZARSKY, 1399.

⁵²⁶ Vgl. GOODMAN/FLAXMAN, 3. Vgl. HURLEY/ADEBAYO, 195: diskriminierendes Scoring, um gezielt verletzte Gruppen anzusprechen.

⁵²⁷ Vgl. Europarat 2016a, 27. Vgl. MRKONICH *et al.*, 22.

⁵²⁸ Europarat 2016a, 29, m.w.H.

erwähnten Versprechen betreffend mehr Objektivität durch Algorithmen⁵²⁹ werden daher entweder direkt bestritten⁵³⁰ oder zumindest in Zweifel gezogen.⁵³¹

3.4.2 Begriffserklärung

Der Begriff der Diskriminierung ist verfassungsrechtlich nicht legaldefiniert.⁵³² Hingegen findet sich eine Legaldefinition im internationalen Recht: Als Diskriminierung gilt jede Unterscheidung, Ausschliessung oder Bevorzugung aufgrund verpönter Gründe, welche dazu führt, die Gleichheit der Chancen oder der Behandlung in Beschäftigung oder Beruf aufzuheben oder zu beeinträchtigen. Verpönte Merkmale sind namentlich Rasse, Hautfarbe, Geschlecht, Glaubensbekenntnis, politische Meinung, nationale Abstammung und soziale Herkunft. Ist eine solche Unterscheidung in den Erfordernissen der Beschäftigung begründet, gilt sie nicht als Diskriminierung (vgl. Art. 1 Abs. 1–2 Übereinkommen 111).⁵³³

Es ist zwischen direkter und indirekter Diskriminierung zu differenzieren.⁵³⁴ Eine direkte Diskriminierung besteht, wenn eine Differenzierung zwischen Menschen ausdrücklich an ein verpöntes Merkmal anknüpft und nicht mit qualifizierten

⁵²⁹ Siehe S. 2.

⁵³⁰ Die Annahme der Objektivität sei ein Fehler: White House, Executive Office of the President 2016, 6. Der Algorithmus COMPAS, der gestützt auf 137 Persönlichkeitsmerkmale die Rückfälligkeit von Straftätern für US-Behörden und -Gerichte vorher-sagt, bringe keine genaueren oder gerechteren Ergebnisse hervor, als wenn eine Person ohne Erfahrung in der Strafrechtspflege die Prognose erstellen würde: DRESSER/FARID, 1. Vgl. ANGWIN JULIA / LARSON JEFF / MATTU SURYA / KIRCHNER LAUREN, Machine bias, 23.06.2016, abrufbar unter <www.propublica.org> (besucht am 31.05.2020).

⁵³¹ «*Appearance of scientific objectivity*»: AI now institute, 6; «*aura of truth, objectivity, and accuracy*»: AJUNWA 2014, 1233; «*belief [in] greater truth, objectivity, and accuracy*»: CRAWFORD/SCHULTZ, 96.

⁵³² PÄRLI 2009, N 30. Auf Gesetzesstufe des Bundesrechts finden sich nur Ansätze einer Begriffsdefinition für den spezifischen Bereich des jeweiligen Diskriminierungsverbots (z.B. Art. 3–4 GlG betreffend Gleichbehandlung der Geschlechter oder Art. 2 Abs. 2–4 BehiG betreffend die Benachteiligung von Behinderten).

⁵³³ PÄRLI 2009, N 1533.

⁵³⁴ PÄRLI 2009, N 33–34; WILDHABER *et al.*, 470. Auch das angloamerikanische Rechtssystem unterscheidet zwischen der direkten Diskriminierung (*disparate treatment*) und der indirekten Diskriminierung (*disparate impact*): algo:aware [sic], 16, und BAROCAS/SELBST, 694 und 701. Die indirekte Diskriminierung erklärt das US-Recht nur in bestimmten Fällen für unzulässig; hierzu gehört das Arbeitsverhältnis: ZARSKY, 1397.

Gründen gerechtfertigt werden kann.⁵³⁵ Eine indirekte Diskriminierung liegt vor, wenn eine nach dem Wortlaut neutrale Massnahme in ihren praktischen Auswirkungen eine Gruppe von Menschen mit einem verpönten Merkmal wesentlich stärker als alle anderen trifft, ohne dass dies sachlich begründet wäre.⁵³⁶ Während bei der direkten Diskriminierung die individuelle Dimension interessiert, stehen bei der indirekten Diskriminierung die Ergebnisse betreffend die Gruppe im Fokus.⁵³⁷

Im Kontext von People Analytics ist die indirekte die relevantere Form von Diskriminierung, da die Algorithmen tendenziell seltener explizit an verpönte Merkmale anknüpfen, sondern Arbeitnehmer nach neutralen Kriterien einteilen.⁵³⁸ Da die indirekte Diskriminierung nur widerrechtlich ist, wenn sie eine Gruppe wesentlich stärker trifft als eine andere, ist zu klären, wann diese Schwelle der Wesentlichkeit erreicht ist. Die schweizerische Rechtsprechung legt zur Feststellung, ob eine geschützte Gruppe wesentlich stärker benachteiligt wird, keine starren Grenzwerte fest; Kriterien zur Feststellung sind Werte aus Statistiken und die allgemeine Lebenserfahrung.⁵³⁹ Die europäische Rechtsprechung handhabt dies

⁵³⁵ Zur Diskriminierung von Arbeitnehmern: BGE 126 II 377 E. 6a.

⁵³⁶ BGE 126 II 377 E. 6c.

⁵³⁷ HACKER, 1152–1153.

⁵³⁸ WILDHABER *et al.*, 470. Indirekte Diskriminierung bei Machine Learning am relevantesten: HACKER, 1153. **A.M.** wohl ANGWIN JULIA / SCHEIBER NOAM / TOBIN ARIANA, Facebook job ads raise concerns about age discrimination, The New York Times vom 20.12.2017, abrufbar unter <www.nytimes.com> (besucht am 31.05.2020): Verizon, Amazon, Goldman Sachs, Target und Facebook platzierten online Stellenausschreibungen, die nur für bestimmte Altersgruppen sichtbar waren.

⁵³⁹ Vgl. BGE 141 II 411 E. 6.2. Vgl. BGE 143 II 366 E. 3.6. Kein starrer Grenzwert bzgl. der Gleichbehandlung der Geschlechter: PERRENOUD, 662.

gleich.⁵⁴⁰ Das amerikanische Common Law wiederum orientiert sich noch stärker an statistischen Grenzwerten,⁵⁴¹ was dort jedoch auf Kritik stösst.⁵⁴²

3.4.3 Ursachen der algorithmischen Diskriminierung

a) Diskriminierungen während des gesamten Daten-Lebenszyklus

Die Ursachen, die zu einer indirekten Diskriminierung führen können, sind entlang des gesamten Daten-Lebenszyklus, vor allem aber in der Phase der Datenanalyse zu verorten.⁵⁴³ Die Phase der Datenanalyse dient der eigentlichen Entscheidungsfindung mithilfe eines Algorithmus und ist weiter zu unterteilen in die Teilphasen «Eingabe» (*input*), «Modell zur Datenanalyse» und «Ausgabe» (*output*). In der Eingabephase werden die Daten aufbereitet. Der grösste Teil der personenbezogenen oder nichtpersonenbezogenen Eingabedaten dient dazu, den (Roh-)Algorithmus zu trainieren (sog. Trainingsdaten), während der kleinere verbleibende Datensatz erst später in den Algorithmus eingeführt wird, um zu testen, ob dieser richtig funktioniert (sog. Testdaten), bevor er in der Praxis zum Einsatz kommt. In der Modellphase werden die real zu untersuchenden Daten durch den Algorithmus bewertet und interpretiert. Die Ausgabephase beschreibt den Prozess, bei dem ge-

⁵⁴⁰ Vgl. Urteil EuGH vom 08.05.2019, Villar Láiz, C-161/18, EU:C:2019:382, N 39–40. Vgl. Urteil EuGH vom 28.02.2013, Kenny, C-427/11, EU:C:2013:122, N 42–43. ROMEI/RUGGIERI, 591.

⁵⁴¹ Mit Hinweisen auf die US-Rechtsprechung: WILDHABER *et al.*, 473. Die EEOC kennt die sog. Vier-Fünftel-Regel. Demnach begründet es den Anscheinsbeweis einer indirekten Diskriminierung, wenn die Selektionsrate bei geschützten Gruppen höchstens 80 Prozent der Selektionsrate von ungeschützten Gruppen beträgt: ROMEI/RUGGIERI, 591. Eine andere verbreitete Regel ist diejenige der statistischen Signifikanz. Sie besagt, dass die Zahl der Mitglieder der geschützten Gruppe im Verhältnis zur betreffenden Population nicht kleiner als drei Standardabweichungen von einer zufälligen Auswahl von Personen der betreffenden Population sein darf: ROMEI/RUGGIERI, 591.

⁵⁴² Die Vier-Fünftel-Regel sei reine Heuristik: VEALE/BINNS, 3. Weitere Hinweise zur Kritik an der Methode der statistischen Signifikanz: WILDHABER *et al.*, 473.

⁵⁴³ Siehe zum Daten-Lebenszyklus S. 19–20. Siehe zu den Ursachen der Diskriminierung durch Algorithmen: WILDHABER *et al.*, 464–469. Vgl. THELISSON *et al.*, 54. Diskriminierungen beim Festlegen des Ziels der Analyse (*target variable*), der Trainingsdaten und der Merkmale, die in die Analyse einfließen (*feature selection*), sowie bei der Berücksichtigung von Merkmalen, die stellvertretend für eine geschützte Gruppe von Personen stehen (*proxy variables*), und wenn die schürfende Person eine absichtliche Diskriminierung als zufällig verkleidet (*masking*): BAROCAS/SELBST, 675–676.

stützt auf die vom Modell errechneten Ergebnisse Entscheidungen getroffen oder Massnahmen angeordnet werden.⁵⁴⁴ Auf die drei Teilphasen und die damit einhergehenden Diskriminierungsrisiken ist nun näher einzugehen.

b) Diskriminierungen in der Eingabephase

Zunächst ist es möglich, dass die in der Eingabephase verwendeten Trainingsdaten an Mängeln leiden, etwa weil sie schlecht ausgewählt,⁵⁴⁵ unvollständig,⁵⁴⁶ doppelt,⁵⁴⁷ nichtrepräsentativ,⁵⁴⁸ subjektiv voreingenommen,⁵⁴⁹ veraltet oder falsch⁵⁵⁰ sind.⁵⁵¹ Dies will die vorliegende Arbeit anhand des Signalproblems und des Problems historischer Stereotypen illustrieren.

Den Trainingsdaten kann es wegen des sog. Signalproblems an Repräsentativität fehlen.⁵⁵² Die bei People Analytics verwendeten Daten lassen diejenigen Gruppen ausser Acht, die ihre Interessen nicht «signalisieren» (können).⁵⁵³ Mit People Analytics droht eine systematische soziale Ausgrenzung der Menschen, die aufgrund von Armut, Geographie oder Lebensstil weniger Daten über sich selbst produzieren als die durchschnittliche Bevölkerung.⁵⁵⁴ Prädiktive Algorithmen bevorzugen diejenigen Menschengruppen, die in den Trainingsdaten üppig repräsentiert sind,

⁵⁴⁴ Beschreibung der drei Teilphasen «Input», «Modell» und «Output»: WILDHABER *et al.*, 465–466; algo:aware [sic], ii–iii.

⁵⁴⁵ Zum Problem der geeigneten Trainingsmenge: ZWEIG/KRAFFT, 113.

⁵⁴⁶ Sog. Verzerrung aufgrund weggelassener Variablen (*omitted variable bias*): ŽLIOBAITĖ/CUSTERS, 191.

⁵⁴⁷ HOEREN 2017, 108.

⁵⁴⁸ THELISSON *et al.*, 54; REINSCH/GOLTZ, 50. Ein bei Entwicklern weit verbreiteter Trainings-Datensatz ist zu 74 Prozent männlich und 83 Prozent weiss: SHELLNBARGER SUE, A crucial step for averting AI disasters, The Wall Street Journal vom 13.02.2019, abrufbar unter <www.wsj.com> (besucht am 31.05.2020).

⁵⁴⁹ CRAWFORD; KIM 2017, 876.

⁵⁵⁰ REINSCH/GOLTZ, 41; zu den gezielten Vergiftungsattacken auf algorithmische Entscheidungssysteme mittels Einspeisen falscher Daten (*poisoning attacks*), die zu einem Lernen in gegnerischem Interesse (*adversarial machine learning*) führen: ZWEIG/KRAFFT, 114–115.

⁵⁵¹ Vgl. WILDHABER *et al.*, 466.

⁵⁵² WILDHABER *et al.*, 467.

⁵⁵³ KIM 2017, 877.

⁵⁵⁴ WILDHABER *et al.*, 467, m.w.H.; LERMAN, 57. Personengruppen werden in den Hintergrund gedrängt (*sidelining*), sodass ihnen die Möglichkeit verwehrt bleibt, sich dem System anzuschliessen (*antisubordination*): LERMAN, 56–57.

da mit diesen Vorhersagen weniger Unsicherheit verbunden ist.⁵⁵⁵ Beispielsweise sah sich die Swisscom mit dem Problem auseinandergesetzt, dass die Hälfte ihrer Belegschaft ihre Teilnahme an einem Smart Data-Pilotprojekt verweigert hat, mit dem das Unternehmen herausfinden wollte, welche Art von Zusammenarbeit Stress verursacht.⁵⁵⁶ Auch mangelnder Zugang zu Internet, Computer und Smartphones kann zu Ungleichheiten und Diskriminierungen führen.⁵⁵⁷ Arbeitgeberinnen müssen erforschen, wie sich solch verschiedene Zugangsmöglichkeiten auf die Trainingsdaten auswirken.⁵⁵⁸ D.h., es genügt nicht, bloss die vorhandenen Daten zu kennen. Stattdessen muss die Arbeitgeberin auch ermitteln, welche Daten ihr fehlen und ob sie gewisse Gruppen vergisst, die keine Datensignale von sich geben. Angesichts des auf europäischer Ebene neu eingeführten Rechts auf Vergessenwerden (Art. 17 DSGVO) mag dies paradox klingen: Aber das Diskriminierungsrecht pocht auf das «Recht, *nicht* vergessen zu werden».⁵⁵⁹

Selbst in einem repräsentativen Datensatz können sich Diskriminierungen einschleichen: Historische Stereotypen der Gesellschaft können sich in den Trainings-Datensätzen fortsetzen und gar verschärfen, weil die Algorithmen die in vergangenen Daten enthaltenen Vorbilder nachahmen.⁵⁶⁰ Dies zeigt sich etwa bei Programmen zur Stimmerkennung und Sprachanalyse: Die Wörter «weiblich» und «Frau» werden mehr mit Geisteswissenschaften verbunden; «männlich» und «Mann» dagegen mehr mit Mathematik und Ingenieurberufen.⁵⁶¹ Euro-amerikanische Namen sind in Sprachmustern eher mit angenehmen, afro-amerikanische mit unangenehmen Begriffen verbunden.⁵⁶² Der Algorithmus schlägt infolgedessen

⁵⁵⁵ GOODMAN/FLAXMAN, 4.

⁵⁵⁶ DAVIS PLÜSS JESSICA / REUSSER KAI, Your employer might be watching you. Should you care?, 13.05.2019, abrufbar unter <www.swissinfo.ch> (besucht am 31.05.2020).

⁵⁵⁷ FAVARETTO *et al.*, 15, m.w.H.

⁵⁵⁸ CRAWFORD/CALO, 313.

⁵⁵⁹ LERMAN, 63.

⁵⁶⁰ WILDHABER *et al.*, 467; HÄNOLD, 129; algo:aware [sic], 17; DAEDELLOW 2018, N 10; TRINDEL. Vgl. VEALE/BINNS, 2. Vertiefung von Vorurteilen auch in der Modellphase: THELISSON *et al.*, 54.

⁵⁶¹ DEVLIN HANNAH, AI programs exhibit racial and gender biases, research reveals, The Guardian vom 13.04.2017, abrufbar unter <www.theguardian.com> (besucht am 31.05.2020).

⁵⁶² DEVLIN HANNAH, AI programs exhibit racial and gender biases, research reveals, The Guardian vom 13.04.2017, abrufbar unter <www.theguardian.com> (besucht am 31.05.2020).

bei identischen Lebensläufen mit 50 Prozent höherer Wahrscheinlichkeit die Einladung zu einem Bewerbungsgespräch vor, wenn der Name des Bewerbers euro-amerikanisch ist.⁵⁶³ Die medizinische Fakultät St. George's der University of London nutzte bereits in den 1980er-Jahren einen Algorithmus zur Bewerbungsselektion, um aufgrund früherer Bewerbungen vorherzusagen, wem eine erfolgreiche Arztkarriere beschieden sei. Das System neigte dazu, Frauen und Bewerber mit nichteuropäisch klingenden Namen ungeachtet ihrer akademischen Leistungen abzulehnen.⁵⁶⁴ Der Algorithmus von Amazon hat sich beigebracht, dass männliche Kandidaten vorzuziehen sind, und wertete Bewerbungen ab, in welchen Begriffe wie «Frauen-Schachclub» oder Namen von Frauen-Colleges vorkamen.⁵⁶⁵ Und auch Google zeigt Inserate für gut bezahlte Stellen Männern überproportional häufiger an als Frauen.⁵⁶⁶

c) Diskriminierendes Modell

Das mathematische Modell ist der Schritt zwischen Eingabe- und Ausgabephase, bei welchem die eingegebenen Daten mit einer Wertung versehen, analysiert und in einen Entscheidungsvorschlag umformuliert werden. Zunächst fließen das Weltbild und die Überzeugungen der betreffenden Programmierer in die Modellierung ein.⁵⁶⁷ Somit können Algorithmen die Vorurteile der Programmierer widerspiegeln und an Fehlern leiden.⁵⁶⁸ Nehmen die Programmierer gewisse Begriffe nicht in das Modell auf, droht der Algorithmus, Bewerbungen fälschlicherweise wegen fehlender Schlüsselwörter auszusortieren, obwohl sie zum Stellenprofil passen

⁵⁶³ DEVLIN HANNAH, AI programs exhibit racial and gender biases, research reveals, *The Guardian* vom 13.04.2017, abrufbar unter <www.theguardian.com> (besucht am 31.05.2020).

⁵⁶⁴ BLATTNER MARCEL / NONNER TIM, Algorithmen gefährden die Demokratie, *Tagesanzeiger* vom 10.04.2018, abrufbar unter <www.tagesanzeiger.ch> (besucht am 31.05.2020); THELISSON *et al.*, 54.

⁵⁶⁵ DASTIN JEFFREY, Amazon scraps secret AI recruiting tool that showed bias against women, abrufbar unter <<https://mobile.reuters.com>> (besucht am 31.05.2020). A.M. ARYANI, 1057: Die Verwendung biografischer Daten im Bewerbungsprozess führe zu einer Bevorzugung von Frauen, Minderheiten und älteren Bewerbern.

⁵⁶⁶ THELISSON *et al.*, 53; CRAWFORD KATE, Artificial intelligence's white guy problem, *The New York Times* vom 25.06.2016, abrufbar unter <www.nytimes.com> (besucht am 31.05.2020).

⁵⁶⁷ ZWEIG/KRAFFT, 113; VEALE/BINNS, 2. Vgl. THELISSON *et al.*, 54.

⁵⁶⁸ AI now institute, 1; DREYER/SCHULZ, 14.

würden.⁵⁶⁹ Die Sicht des Algorithmus ist stets auf diejenige des Programmierers beschränkt. Der Algorithmus kann sich nicht in die Situation des Betroffenen versetzen und ignoriert beispielsweise, dass die Mutter eines Arbeitnehmers gerade im Spital liegt und dieser Umstand auf die Stimmung und Leistung des Arbeitnehmers drückt.⁵⁷⁰

Ein Diskriminierungsrisiko besteht, selbst wenn auf diskriminierungsrelevante Attribute verzichtet wird. Der Verzicht schliesst zwar eine direkte Diskriminierung aus; die Gefahr einer indirekten Diskriminierung besteht aber weiter.⁵⁷¹ Denn die verbleibenden Attribute können Stellvertreter geschützter Merkmale sein (sog. stellvertretende oder «Proxy-Variable», daher auch «Proxy-Diskriminierung».⁵⁷² Bereits relativ triviale Informationen können eng mit geschützten Charakteristika korrelieren. Beispielsweise korrelieren Facebook-Likes mit Geschlecht und politischer Gesinnung oder verwendeter Wortschatz mit Rasse.⁵⁷³ Eine weitere Ausprägung der indirekten Diskriminierung am Arbeitsplatz ist die Geokodierung (auch *weblining*, abgeleitet von *redlining*, dem Ziehen von roten Linien auf Landkarten im Zusammenhang mit der Vergabe von Finanzkrediten).⁵⁷⁴ Hier kann die Arbeitgeberin aus dem neutralen Kriterium der Wohnadresse des Betroffenen auf dessen ethnische Zugehörigkeit schliessen, wenn in gewissen Quartieren vorwiegend Personen der gleichen Ethnie wohnen.⁵⁷⁵ Wie schon angesprochen⁵⁷⁶ stellte das Software-Unternehmen Evolv fest, dass Mitarbeiter, die 0–5 Meilen von ihrem Arbeitsplatz entfernt wohnen, um 20 Prozent länger ihrer Stelle treu bleiben als diejenigen, die weiter weg wohnen. Die Arbeitgeberin kann auf diesem Weg die

⁵⁶⁹ WILDHABER 2017, 215.

⁵⁷⁰ O'CONNOR SARAH, Algorithms at work signal a shift to management by numbers, 06.02.2018, abrufbar unter <www.ft.com> (besucht am 31.05.2020), 1.

⁵⁷¹ ŽLIOBAITĖ/CUSTERS, 185.

⁵⁷² WILDHABER *et al.*, 467; WILSON *et al.*, 33; SNYDER, 257.

⁵⁷³ Korrelation von Likes mit Geschlecht und politischer Gesinnung: KIM/HANSON, 19; HERMSTRÜWER, 108; KASPER/WILDHABER, 210; WILDHABER *et al.*, 468, m.w.H.

⁵⁷⁴ WILDHABER *et al.*, 468.

⁵⁷⁵ MRKONICH *et al.*, 37; EDWARDS/VEALE, 29; algo:aware [sic], 15.

⁵⁷⁶ Siehe S. 43–44. Evolv schloss die Distanz zwischen Wohn- und Arbeitsort wegen Bedenken bzgl. der Korrelation mit Ethnie und niedrigerem Einkommen von seinen Selektionsalgorithmen wieder aus: ROSENBLAT/WIKELIUS *et al.*, 2. BAROCAS. Stattdessen betont Evolv, dass der zentrale Standort des Arbeitgebers und die Nähe zu Parks, Restaurants und Geschäften entscheidend sind, um Mitarbeiter zu binden: ROSENBLAT/WIKELIUS *et al.*, 3.

Demografie ihres Bewerberpools beeinflussen, indem sie etwa Stelleninserate nur für Personen mit einer bestimmten IP-Adresse freischaltet.⁵⁷⁷

Diskriminierungen können sich ferner aus einem unzureichenden Stand der Technik ergeben: So erteilte eine Software zur Sprachanalyse in einem Call-Center Nichtmuttersprachlern und Arbeitnehmern mit starkem Sprachakzent oder einer Sprachbehinderung eine tiefere Bewertung, weil der Algorithmus die Sprechgewohnheiten nicht einordnen konnte.⁵⁷⁸ Oder das US-amerikanische behördliche System E-Verify verweigert fälschlicherweise Arbeitsbewilligungen, weil es mit Namen von Ausländern und Frauen, die nach der Heirat den Namen wechseln oder mehrere Nachnamen tragen, nicht zurechtkommt.⁵⁷⁹ Des Weiteren können Homonyme, also gleichlautende Wörter, die für verschiedene Begriffe stehen, zu Verwechselungen führen: Als ein Forschungsteam 2011 die Arbeitslosenquote der USA ermittelte, indem es in sozialen Netzwerken nach Begriffen wie *«jobs»* suchte, verzerrte die zeitgleiche Flut von Beiträgen zum Tod von Apple-Gründer Steve Jobs die Forschungsergebnisse.⁵⁸⁰ Ein Algorithmus kann zudem nur Größen berücksichtigen, die nach dem Stand der Technik messbar sind. Hierzu zählen beispielsweise Verkaufszahlen, Produktionszeit und Dienstalster.⁵⁸¹ Schwieriger ist etwa die Messung, wie gut ein Lehrer seine Klasse motivieren kann. Weil eine Evaluation an amerikanischen Schulen dies übersah und die Lehrpersonen weitgehend aufgrund der Prüfungsergebnisse der Schüler einstuftete, kam es zu zahlreichen ungerechtfertigten Entlassungen.⁵⁸²

Schliesslich können Diskriminierungen aus Übersetzungsschwierigkeiten zwischen der Rechts- und der Computerwissenschaft hervorgehen. In der Literatur fehlt eine einheitliche formelhafte Definition von Diskriminierung für Program-

⁵⁷⁷ Vgl. MRKONICH *et al.*, 37.

⁵⁷⁸ O'CONNOR SARAH, Algorithms at work signal a shift to management by numbers, 06.02.2018, abrufbar unter <www.ft.com> (besucht am 31.05.2020), 1; DZIDA/GROH, 1918–1919.

⁵⁷⁹ White House, Executive Office of the President 2014, 52. Vgl. auch ein System der amerikanischen Behörden, das elektronische Anträge auf Sozialhilfe zu oft ablehnt, weil es Eingabefehler als Betrugsversuche bewertet: EUBANKS VIRGINIA, Algorithms designed to fight poverty can actually make it worse, 01.11.2018, abrufbar unter <www.scientificamerican.com> (besucht am 31.05.2020).

⁵⁸⁰ SNYDER, 255.

⁵⁸¹ KIM 2017, 876. Schwierig ist es dagegen, vorauszusehen, wie viel Betreuung ein Bewerber benötigen wird: GAY/KAGAN.

⁵⁸² CUSTERS/URSIC, 328.

mierer und Computerwissenschaftler.⁵⁸³ Diese Berufsgattungen haben verschiedene mathematische Definitionen von Gerechtigkeit vorgeschlagen.⁵⁸⁴ Die verschiedenen Perspektiven bei der Einschätzung, welches Kriterium das richtige sein soll, schliessen sich teilweise gegenseitig aus, sodass Kompromisse unumgänglich sind, wie anhand der folgenden drei Problemfelder aufzuzeigen ist.⁵⁸⁵

Erstens besteht ein Konflikt zwischen der Gerechtigkeit für die Gruppe und für Einzelpersonen. Es ist angeblich statistisch erwiesen, dass die besten Informatiker diejenigen mit einer Vorliebe für Manga-Comics sind.⁵⁸⁶ Daher erscheint es aus Gruppenperspektive gerecht, die Gruppe der Manga-Liebhaber gegenüber dem Rest bei der Bewerbung oder bei Beförderungen zu bevorzugen. Auf Individual-ebene kann es jedoch ungerecht sein, einem talentierten Informatiker, der keine Manga liest, sein Talent abzusprechen. Der Algorithmus muss sich entscheiden, ob er einen Entscheid fällt, der für die Gruppe oder für die Einzelpersonen gerecht ist. Auch eine Mischrechnung ist denkbar, sodass etwa die maximal vorstellbare Gerechtigkeit für die Gruppe zu 60 Prozent und diejenige für den Einzelnen zu 40 Prozent erfüllt werden.⁵⁸⁷

Zweitens ist die Gerechtigkeit zwischen verschiedenen Gruppen zu verteilen, was insbesondere in Fällen der Proxy-Diskriminierung Mühe bereiten kann:⁵⁸⁸ Ein Algorithmus mag beispielshalber errechnen, dass ein Arbeitnehmer, dem die negative Eigenschaft X fehlt, bessere Leistungen als andere Angestellte erbringt. Daraufhin stellt sich jedoch heraus, dass die Bevorzugung aller, denen die Eigenschaft X fehlt, gleichzeitig eine Benachteiligung aller Arbeitnehmer mit einem

⁵⁸³ FAVARETTO *et al.*, 21.

⁵⁸⁴ Arten von Gerechtigkeit sind z.B. gleich genaue Resultate für alle Gruppen (*accuracy equity*), Chancengleichheit für die Mitglieder jeder Gruppe (*equality of opportunity*) oder der Ausgleich von unterschiedlichen Fehlerquoten bei den Gruppen (*disparate mistreatment*): algo:aware [sic], 18.

⁵⁸⁵ HACKER, 1182; algo:aware [sic], 21.

⁵⁸⁶ PECK DON, They're watching you at work, The Atlantic vom 12.2013, abrufbar unter <www.theatlantic.com> (besucht am 31.05.2020); HUSMANN NELE, Wenn künstliche Intelligenz über die Bewerbung richtet, Handelszeitung vom 25.10.2017, abrufbar unter <www.handelszeitung.ch> (besucht am 31.05.2020); WILDHABER *et al.*, 462.

⁵⁸⁷ HACKER, 1183; Gerechtigkeit sei «mathematisch nur begrenzt» erreichbar: CORBETT-DAVIES SAM / PIERSON EMMA / FELLER AVI / GOEL SHARAD, A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear, The Washington Post vom 17.10.2016, abrufbar unter <www.washingtonpost.com> (besucht am 31.05.2020).

⁵⁸⁸ Zur Proxy-Diskriminierung: S. 95.

verpönten Merkmal Y bedeutet (Proxy-Diskriminierung). Dies könnte zutreffen, wenn X bedeutet, dass jemand immer etwas früher als die Kollegen die Arbeit verlässt, und Y bedeutet, dass die Angestellte eine Frau ist; alle im Betrieb angestellten Frauen sind zudem alleinerziehende Mütter, die früher gehen, weil sie am Abend ihre Kinder rechtzeitig von der Krippe abholen müssen. Hier muss dem Algorithmus beigebracht werden, ob er sich gegenüber der Gruppe derjenigen, denen die negative Eigenschaft X fehlt, oder gegenüber derjenigen mit dem verpönten Merkmal Y gerecht verhalten soll.⁵⁸⁹ Angezeigt ist in diesem Beispiel nicht eine Umprogrammierung des Algorithmus, sondern eine Flexibilisierung der Arbeitszeiten.⁵⁹⁰

Drittens zeigt auch das sog. Simpson-Paradoxon, das einen scheinbaren Widerspruch zwischen der Gesamtpopulation und den Subpopulationen beschreibt,⁵⁹¹ dass die Frage der Gleichbehandlung davon abhängt, wie man die Daten gruppiert. Nicht alles, was ungerecht aussieht, ist eine Diskriminierung: Facebook sah sich dem Vorwurf ausgesetzt, die Codes seiner Programmiererinnen zu 35 Prozent

⁵⁸⁹ Vgl. das Dilemma rund um den Algorithmus COMPAS des Software-Herstellers Equivant (vormals Northpointe), der für US-Behörden die Rückfälligkeit eines Straftäters errechnet. Die Berechnung der Rückfall-Wahrscheinlichkeit stützt sich auf die Anzahl früherer Straftaten (negative Eigenschaft X). Bereits früher straffällig Gewordene weisen eine statistisch höhere Rückfälligkeit auf. Deshalb erteilt COMPAS allen wiederholten Straftätern eine höhere Rückfälligkeitsprognose. Die Eigenschaft der wiederholten Straftäterschaft korreliert mit dem Merkmal der Rasse (verpöntes Merkmal Y). Alle mit dunkler Hautfarbe erhalten eine höhere Rückfälligkeitsprognose, auch wenn COMPAS das Merkmal der Hautfarbe nicht für seine Berechnungen verwendet (Proxy-Diskriminierung). Dies kritisieren Investigativjournalisten von ProPublica. Doch Equivant verteidigt sich damit, dass es ungerecht wäre, denjenigen Hellhäutigen ohne Vorstrafen künstlich eine höhere Rückfälligkeitsprognose auszustellen, nur damit die Prognose für Schwarze und Weiße gleich ausfällt: CORBETT-DAVIES SAM / PIERSON EMMA / FELLER AVI / GOEL SHARAD, A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear, The Washington Post vom 17.10.2016, abrufbar unter <www.washingtonpost.com> (besucht am 31.05.2020).

⁵⁹⁰ Lange Arbeitszeiten benachteiligen Frauen, die sich um Kinder kümmern; hier sei aber nicht ein Algorithmus zu ändern, sondern die gesellschaftlichen Strukturen, die die Chancen verschiedener Personen unterschiedlich beeinflussen: KIM 2017, 871.

⁵⁹¹ Das Simpson-Paradoxon wurde erstmals 1899 von Karl Pearson entdeckt und 1951 durch Edward Hugh Simpson eingehend beschrieben: PEARL, 128. Eingang in die Rechtsprechung fand das Simpson-Paradoxon anlässlich einer (abgewiesenen) Diskriminierungsklage gegen die Berkeley University of California: PEARL, 174.

häufiger zurückzuweisen als diejenigen der männlichen Angestellten.⁵⁹² Facebook entgegnete, dass mehrheitlich junge Frauen, die noch lernen und daher Kritik erhalten, bei Facebook arbeiten, während Frauen auf der Stufe Senior Engineering untervertreten sind.⁵⁹³ Nähme man statt der gesamten Belegschaft nur die Subpopulation der Jungen als Massstab, wäre das Risiko, kritisiert zu werden, für Frauen geringer als dasjenige für Männer.

d) Diskriminierungen in der Ausgabephase

Diskriminierend ist die falsche Folgerung von der Gruppenwahrscheinlichkeit auf den Einzelnen, weil sie eine Gleichbehandlung von Ungleichem bedeutet.⁵⁹⁴ Beispielsweise wäre es falsch, jemandem, der online nach einer Fritteuse sucht, ungesunde Essensgewohnheiten zu attestieren, da die Fritteuse möglicherweise als Geschenk für Dritte gedacht ist. Die Arbeitgeberin, die gesunde Angestellte rekrutieren will, würde übereilt und diskriminierend handeln, wenn sie solche Bewerbungen aussortieren würde.⁵⁹⁵

3.5 Verletzung von Mitwirkungsrechten

3.5.1 Zweck und zwingende Geltung der Mitwirkungsrechte

In allen Fragen des Gesundheitsschutzes am Arbeitsplatz sind die Mitwirkungsrechte zu berücksichtigen (Art. 48 Abs. 1 lit. a ArG). Zum Gesundheitsschutz zählt der für People Analytics typische Einsatz von Überwachungs- und Kontrollsystemen, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen (vgl.

⁵⁹² DEEPA SEETHARAMAN, Facebook's female engineers claim gender bias, The Wall Street Journal vom 02.05.2017, abrufbar unter <www.wsj.com> (besucht am 31.05.2020); WOLFANGEL EVA, Künstliche Intelligenz voller Vorurteile, NZZ vom 02.09.2017, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

⁵⁹³ DEEPA SEETHARAMAN, Facebook's female engineers claim gender bias, The Wall Street Journal vom 02.05.2017, abrufbar unter <www.wsj.com> (besucht am 31.05.2020).

⁵⁹⁴ Vgl. Lorenz Hilty, Professor für Informatik und Nachhaltigkeit an der Universität Zürich, in: GENOVA MICHAEL, Mit Robotern gegen Hochstapler: Firmen jagen unehrliche Mitarbeiter, Tagblatt vom 22.07.2018, abrufbar unter <www.tagblatt.ch> (besucht am 31.05.2020).

⁵⁹⁵ LOHR STEVE, Sizing up big data, broadening beyond the internet, The New York Times vom 19.07.2013, abrufbar unter <https://bits.blogs.nytimes.com> (besucht am 31.05.2020); WILDHABER *et al.*, 468–469.

Art. 26 ArGV 3).⁵⁹⁶ Die Mitwirkung der Arbeitnehmer auf betrieblicher Ebene wird gesetzlich einerseits durch das MitwG, andererseits durch Art. 37–39 ArG (sowie Art. 67–68 ArGV 1) betreffend Betriebsordnung geregelt.⁵⁹⁷

Die Mitwirkung bezweckt die Information und Mitsprache der Arbeitnehmer in den Betrieben (vgl. Titel des MitwG). Sie bringt den Arbeitnehmern Teilhabe, Kontrolle und informationelle Mitbestimmung beim Einsatz von People Analytics.⁵⁹⁸ Umgekehrt kann die Arbeitgeberin in einem frühen Stadium die Akzeptanz geplanter People Analytics-Massnahmen abschätzen. Denn die Auffassungen zur Privatsphäre variieren sowohl zwischen den Betrieben als auch innerhalb desselben Betriebs.⁵⁹⁹ Zudem erhöht ein aktiver Dialog die Produktivität des Unternehmens.⁶⁰⁰

Das MitwG ist als Rahmengesetz konzipiert, das im Wesentlichen die institutionellen Voraussetzungen der betrieblichen Mitwirkung normiert. In welchen Bereichen und in welchem Umfang Mitwirkungsrechte bestehen, steht in den entsprechenden Spezialgesetzen (OR, ArG).⁶⁰¹ Wichtig ist, zu sehen, dass die betriebsverfassungsrechtlichen Rechte des MitwG relativ zwingendes Gesetzesrecht darstellen.⁶⁰² Von den Mitwirkungsrechten (Art. 9–10 MitwG) darf nicht zuungunsten der Arbeitnehmer abgewichen werden, auch nicht durch Gesamtarbeitsvertrag (vgl. Art. 2 Satz 2 MitwG). Eine Abweichung zugunsten der Arbeitnehmer ist jedoch zulässig (Art. 2 Satz 1 MitwG, sog. Günstigkeitsprinzip).⁶⁰³ Die relativ zwingende und kollektive Natur der Mitwirkungsrechte bedeutet, dass nicht durch individuelle Einwilligungen auf sie wirksam verzichtet werden kann.⁶⁰⁴

⁵⁹⁶ Siehe zu Art. 26 ArGV 3 ausführlich später, S. 149–154.

⁵⁹⁷ WILDHABER 2011, 367.

⁵⁹⁸ Vgl. zur Bedeutung von Kontrolle: HÄNOLD, 151; DRUEY 1995, 73.

⁵⁹⁹ Siehe S. 85–86. Vgl. GILBERT, 280. «*Information societies*», die verschieden weit entwickelt sind, seien zu unterscheiden: FLORIDI, 1.

⁶⁰⁰ FURER 2009a, 153; Dr. phil. II Kathrin Amacker, Leiterin Unternehmenskommunikation bei Swisscom von 2010 bis 2013 und Leiterin Kommunikation bei den SBB von 2013 bis 2020, im Interview: FURER 2009b, 179.

⁶⁰¹ WILDHABER 2011, 368; GABATHULER THOMAS, N 6.

⁶⁰² FRITZ/SCHULER, 28. Verworfen hat der Gesetzgeber eine flexiblere Formulierung, die auf relativ zwingende Bestimmungen verzichtet und Abweichungen bei einer insgesamt gleichwertigen Mitwirkungsvereinbarung zugelassen hätte: FRITZ/SCHULER, 29.

⁶⁰³ Somit stellt das MitwG eine «Minimalordnung» dar: WILDHABER 2011, 368.

⁶⁰⁴ Vgl. zum deutschen Recht: WEDDE 2016c, 15–16.

Eine Verwirkung dieser Rechte fällt ausser Betracht.⁶⁰⁵ Auch erlöschen die datenschutzbezogenen Mitwirkungsrechte nicht, wenn die Arbeitgeberin einen Datenschutzverantwortlichen bezeichnet, der unabhängig (ebenfalls) die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht (vgl. Art. 11a Abs. 5 lit. e DSG; vgl. Art. 9 E-DSG, Art. 10 rev-DSG).⁶⁰⁶

3.5.2 Informationsrecht

Die Mitwirkungsrechte können stufenweise in Informations-, Mitsprache- und Mitentscheidungsrechte unterteilt werden.⁶⁰⁷ Die schwächste Form der Mitwirkung stellt das Informationsrecht dar.⁶⁰⁸ Es besteht ein Anspruch auf rechtzeitige und umfassende Information über alle Angelegenheiten, deren Kenntnis Voraussetzung für eine ordnungsgemässe Erfüllung der Aufgaben der Arbeitnehmervertretung ist (Art. 9 Abs. 1 MitwG). Die Aufgaben der Arbeitnehmervertretung bestehen darin, gegenüber der Arbeitgeberin die gemeinsamen Interessen der Arbeitnehmer wahrzunehmen und Letztere regelmässig über ihre Tätigkeit zu informieren (Art. 8 MitwG). People Analytics betrifft in der Regel den gesamten Betrieb oder ganze Abteilungen, weshalb gemeinsame Arbeitnehmerinteressen angesprochen sind und ein Informationsrecht besteht. Abzugrenzen ist das Informationsrecht des Arbeitnehmerkollektivs von der Information und der Anleitung der individuellen Arbeitnehmer (Art. 5 ArGV 3), auf welche vorliegend nicht näher eingegangen wird.

Das Informationsrecht beschränkt sich auf die Mitteilung; ein Mitberaten ist ausgeschlossen.⁶⁰⁹ Die Bedeutung des Informationsrechts liegt darin, dass es die Voraussetzung für alle weitergehenden Formen der Mitwirkung ist.⁶¹⁰ Die «umfassende» Information (Art. 9 Abs. 1 MitwG) muss somit zumindest hinreichend für die weitere Aufgabenerfüllung sein,⁶¹¹ die bei People Analytics in der Mit-

⁶⁰⁵ Vgl. zum deutschen Recht: RUHLAND, 94–95.

⁶⁰⁶ Nach deutschem Recht erlischt die Überwachungspflicht des Betriebsrats nicht dadurch, dass ein betrieblicher Datenschutz-Beauftragter bestellt ist: RUHLAND, 98.

⁶⁰⁷ WILDHABER 2011, 372; MÜLLER, 225. Gesamtarbeitsverträge können zudem Selbstverwaltungsrechte vorsehen, die einzelne Aufgaben der Arbeitnehmervertretung zur selbständigen Erledigung übertragen: ILG, 62–63.

⁶⁰⁸ MÜLLER, 226.

⁶⁰⁹ MÜLLER, 227.

⁶¹⁰ MÜLLER, 226. Vgl. mit Bezug auf die weitergehenden Rechte bei einem Betriebsübergang: WILDHABER 2011, 376.

⁶¹¹ BB1 1992, 648.

sprache besteht, wie noch gezeigt werden wird.⁶¹² Tendenziell dürfte eine stichwortartige Schilderung des People Analytics-Systems genügen, während etwa der Quellcode eines verwendeten Algorithmus von den legitimen Geheimhaltungsinteressen der Arbeitgeberin gedeckt bleibt, solange dessen Kenntnis für die Mitsprache beim Gesundheitsschutz nicht erforderlich ist.⁶¹³ Jedenfalls besteht eine Verschwiegenheitspflicht hinsichtlich der betrieblichen Angelegenheiten, die jemand in der Eigenschaft als Arbeitnehmervertreter erfährt (Art. 14 MitwG). Die Information umfasst auch die Arbeitnehmerrechte im Zusammenhang mit der Bearbeitung von Personendaten. Hinzuweisen ist etwa auf Art. 328b OR, auf das Auskunftsrecht (Art. 8 DSG, Art. 23 E-DSG, Art. 25 rev-DSG) und auf behördliche Anordnungen zum Gesundheitsschutz (Art. 6 Abs. 2 Satz 2 ArGV 3).⁶¹⁴

Die Information muss rechtzeitig erfolgen (Art. 9 Abs. 1 MitwG). Rechtzeitig bedeutet frühzeitig.⁶¹⁵ Angemessen erscheint ein Zeitpunkt, der die Arbeitnehmervertretung in die Lage versetzt, die weitergehenden Mitwirkungsrechte auszuüben, etwa durch Entwicklung eigener Vorschläge und Bedenken, die bei der Planung berücksichtigt werden können.⁶¹⁶ Als allgemeiner Richtwert für eine angemessene Frist werden zwei Wochen erwähnt.⁶¹⁷ Doch ist ein abstrakter zeitlicher Richtwert nach der vorliegend vertretenen Auffassung nicht tauglich. Vielmehr beurteilt sich nach Treu und Glauben (vgl. Art. 11 Abs. 1 MitwG) und den Umständen des Einzelfalls (z.B. Komplexität und Dringlichkeit der Fragen sowie konkrete Aufgabe der Arbeitnehmervertretung), ob eine Information rechtzeitig erfolgt.⁶¹⁸ Das Bundesgericht hält eine Konsultationsfrist von 24 Stunden im Hinblick auf eine Massenentlassung für zu kurz.⁶¹⁹ Bei People Analytics erscheint eine frühe Information als zumutbar, weil die Arbeitgeberin entsprechende Projekte in der Regel planmässig einführt. In der Praxis kommt es vor, dass die neuen Geräte und Softwares zunächst als Pilotprojekt mit einer Gruppe von freiwilligen Arbeitnehmern getestet werden. Erst wenn diese Testphase erfolgreich verlaufen ist, entscheidet

⁶¹² Siehe S. 103–105.

⁶¹³ Auch bei Betriebsübergängen genügen stichwortartige Informationen: WILDHABER 2011, 378. Auch nach Art. 9 Abs. 2 MitwG genügt eine Information über den Geschäftsgang «in groben Zügen»: FRITZ/SCHULER, 40.

⁶¹⁴ SECO 2018, 326–3; EDÖB 2014b, 6.

⁶¹⁵ ILG, 51.

⁶¹⁶ MÜLLER, 260. Vgl. BGE 123 III 176 E. 4a.

⁶¹⁷ FRITZ/SCHULER, 22.

⁶¹⁸ Vgl. bzgl. des Anhörungsrechts: BGE 130 III 102 E. 4.3 und BGE 123 III 176 E. 4b.

⁶¹⁹ BGE 123 III 176 E. 4c.

die Geschäftsleitung, ob und in welcher Form sie die People Analytics-Anwendung im gesamten Unternehmen auf obligatorischer Basis einführen wird. Idealerweise wird die Arbeitnehmervertretung ins Pilotprojekt eingebunden. So ist ein genügend früher Zeitpunkt für den Beginn der Mitwirkung sichergestellt. Spätestens aber bevor entschieden wird, dass und in welcher Form das Projekt unternehmensweit lanciert werden soll, muss die Arbeitnehmervertretung informiert und ihr eine angemessene Zeit zum Einbringen von Vorschlägen gewährt werden.⁶²⁰

Über die Form der Information äussern sich weder das ArG noch die ArGV 3. Möglich sind die mündliche Information an einer Sitzung der Arbeitnehmervertretung oder an einer Betriebsversammlung, ein internes Schreiben oder eine E-Mail an die Arbeitnehmervertretung bzw. die Belegschaft, der Aushang eines Informationsschreibens ans schwarze Brett oder die Publikation in der Firmenzeitung.⁶²¹ Aus Beweisgründen ist es vorzuziehen, die Information schriftlich zu dokumentieren.⁶²²

3.5.3 Mitspracherecht

Ein umfassendes Mitspracherecht existiert bzgl. aller Fragen des Arbeitnehmer-Gesundheitsschutzes (Art. 10 lit. a MitwG i.V.m. Art. 48 Abs. 1 lit. a ArG; vgl. Art. 6 Abs. 3 Satz 1 ArG; Art. 6 ArGV 3). Diese Fragen schliessen People Analytics ein, weil die Überwachung der Arbeitnehmer eine Frage des Gesundheitsschutzes ist (vgl. Art. 26 ArGV 3). Wenn diesbzgl. Betriebsbesuche der Vollzugsbehörde stattfinden, gilt ebenfalls das Mitspracherecht.⁶²³

⁶²⁰ Vgl. zum deutschen Betriebsrat: RUHLAND, 94.

⁶²¹ WILDHABER 2011, 382.

⁶²² WILDHABER 2011, 382.

⁶²³ Die Arbeitgeberin muss vorgängig über Besuche der Vollzugsbehörde informieren (Art. 71 Abs. 1 Satz 1 Teilsatz 1 ArGV 1). Sie muss die Arbeitnehmer in geeigneter Form zu Abklärungen und Betriebsbesuchen der Vollzugsbehörde beiziehen (Art. 6 Abs. 2 Satz 1 ArGV 3), sofern sie dies wünschen (Art. 71 Abs. 1 Satz 1 Teilsatz 2 ArGV 1). Bei unangemeldeten Betriebsbesuchen sind die Arbeitnehmer ebenfalls beizuziehen (Art. 71 Abs. 1 Satz 2 ArGV 1). Die Arbeitgeberin muss den Arbeitnehmern oder deren Vertretung im Betrieb von Anordnungen der Vollzugsbehörde Kenntnis geben (Art. 6 Abs. 2 Satz 2 ArGV 3, Art. 71 Abs. 2 ArGV 1). Die gesetzessystematische Einordnung dieser Bestimmungen (Art. 6 ArGV 3, Art. 71 ArGV 1) als Anhörungsrecht (Art. 6 ArGV 3) und Mitwirkungs- bzw. Mitspracherecht (Art. 48 und Art. 6 ArG i.V.m. Art. 71 ArGV 1) bedeutet, dass es sich dabei um ein Mitsprache- und nicht um ein blosses Informationsrecht handelt.

Das Mitspracherecht geht eine Stufe weiter als das Informationsrecht. Es umfasst den Anspruch auf Anhörung und Beratung (Art. 48 Abs. 2 ArG). Anhören bedeutet, dass die Arbeitnehmer das Recht haben, (einseitig) Vorschläge zu unterbreiten (Art. 6 Abs. 1 Satz 2 ArGV 3).⁶²⁴ Der Begriff des Beratens bedeutet «gemeinsam überlegen und besprechen».⁶²⁵ Die Arbeitgeberin muss sich im (wechselseitigen) Dialog mit den Vorschlägen der Arbeitnehmerseite auseinandersetzen, ehe sie entscheidet.⁶²⁶ Es genügt nicht, dass die Arbeitgeberin die Anliegen der Arbeitnehmerseite bloss zur Kenntnis nimmt.⁶²⁷ Die Arbeitgeberin ist jedoch nicht verpflichtet, den Vorschlägen der Arbeitnehmer zu folgen. Dies ergibt sich aus dem Anspruch auf Begründung des Entscheids, wenn dieser den Einwänden der Arbeitnehmerseite nicht oder nur teilweise Rechnung trägt (Art. 48 Abs. 2 Teilsatz 2 ArG).

Heikel ist die Frage, wer innerhalb des Unternehmens die Arbeitnehmer anhört (und wer nicht).⁶²⁸ Dies ist im Einzelfall festzustellen und dürfte von Unternehmen zu Unternehmen verschieden sein.⁶²⁹ Idealerweise tritt diejenige Person ins Gespräch mit der Arbeitnehmerseite, welche befugt ist, den infrage stehenden Entscheid auszuführen.

Über die Form der Anhörung äussert sich das Gesetz nicht. Die Arbeitnehmer können ihre Anliegen und Vorschläge mündlich oder schriftlich einbringen.⁶³⁰ Für die Beratung erscheint der mündliche Weg naheliegend. Aufgrund der Beweisbarkeit empfiehlt es sich aber, den Ablauf des Konsultationsverfahrens und das Ergebnis der Konsultation schriftlich genau zu dokumentieren.⁶³¹

Zeitlich muss die Anhörung erfolgen, bevor die Arbeitgeberin den Entscheid trifft (Art. 48 Abs. 2 ArG). Für den unbestimmten Rechtsbegriff der «frühzeitigen» Anhörung (Art. 6 Abs. 1 ArGV 3) kann an die Ausführungen zur rechtzeitigen Information erinnert werden.⁶³²

⁶²⁴ MÜLLER, 229.

⁶²⁵ FRITZ/SCHULER, 48.

⁶²⁶ MÜLLER, 229; WYLER/HEINZER, 1204.

⁶²⁷ FRITZ/SCHULER, 48.

⁶²⁸ GEISER 2009, 19.

⁶²⁹ Vgl. FURER 2009a, 157.

⁶³⁰ WILDHABER 2011, 386; FRITZ/SCHULER, 48.

⁶³¹ WILDHABER 2011, 386.

⁶³² Siehe S. 102; vgl. die lapidare Feststellung, dass die Anhörung zu spät kommt, wenn Überwachungsskandale in der Presse erscheinen: COLLIER, 7.

Zu ergänzen ist, dass die aktive Rolle in der Mitsprache die Verpflichtung der Arbeitnehmer mit sich bringt, die Arbeitgeberin in der Durchführung der Vorschriften über den Gesundheitsschutz zu unterstützen (Art. 6 Abs. 3 Satz 2 ArG i.V.m. Art. 10 ArGV 3). Dies umfasst insbesondere eine Meldepflicht, wenn der Arbeitnehmer Mängel feststellt, welche den Gesundheitsschutz beeinträchtigen (Art. 10 Abs. 2 Satz 2 ArGV 3).

3.5.4 Fehlendes Mitentscheidungsrecht

Die stärkste Form der Mitwirkung ist das Mitentscheidungsrecht. Hier haben die Arbeitnehmer bzw. deren Vertretung das Recht, sich unmittelbar am Entscheidungsprozess zu beteiligen, wobei das Ausmass der Mitentscheidung variieren kann.⁶³³ Mitentscheidungsrechte haben Arbeitnehmer namentlich in Bezug auf die Arbeits- und Ruhezeit (z.B. Art. 10 Abs. 2 Satz 1 ArG) und den Sonderschutz für schwangere Frauen und stillende Mütter (z.B. Art. 35a Abs. 1 und 3 ArG).⁶³⁴ Im Zusammenhang mit der Überwachung am Arbeitsplatz sieht das Gesetz jedoch kein Mitentscheidungsrecht vor (vgl. Art. 6 Abs. 3, Art. 48 ArG). Diese Rechtslage entspricht den Anforderungen des Europarats⁶³⁵ und der IAO⁶³⁶ an die Mitwirkung bei der automatisierten Bearbeitung von Daten über Arbeitnehmer. Durch das Ausbleiben von Mitentscheidungsrechten bei People Analytics unterscheidet sich die Rechtslage in der Schweiz aber von derjenigen in Deutschland⁶³⁷ und Österreich.⁶³⁸

⁶³³ Denkbar sind ein Zustimmungsrecht oder ein Vetorecht: FRITZ/SCHULER, 23.

⁶³⁴ Liste der Gesetzesbestimmungen mit Mitentscheidungsrechten: FRITZ/SCHULER, 23.

⁶³⁵ Der Europarat empfiehlt lediglich, vor der Einführung von People Analytics-Projekten die Zustimmung der Arbeitnehmervertretung einzuholen, sofern das innerstaatliche Recht keine anderen geeigneten Rechtsgarantien vorsieht: Europarat 2015, N 20.2. Vgl. Europarat 2015, N 21.c. Vgl. Europarat 2016b, 44.

⁶³⁶ *«Informed and consulted»*: ILO, Ziff. 12.2.

⁶³⁷ Der Betriebsrat hat ein zwingendes Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen (§ 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz vom 15.01.1972, zuletzt geändert 18.12.2018). Dieses deckt bedingt durch die umfassendere Nutzung von IT in der digitalen Arbeitswelt mittlerweile praktisch einen grossen Teil des Einsatzes von Hard- und Software ab: BMAS 2017, 149. BENECKE, N 280.

⁶³⁸ Zu ihrer Rechtswirksamkeit bedürfen der Zustimmung des Betriebsrats Personalfragebögen, Kontrollmassnahmen und technische Systeme zur Kontrolle der Arbeitnehmer (§ 96 Abs. 1 Ziff. 2 und 3 Arbeitsverfassungsgesetz vom 14.12.1973, zuletzt geändert

3.6 Zwischenfazit: Rechtsprobleme vom Kontext abhängig

People Analytics forciert das Machtungleichgewicht in Arbeitsverhältnissen. Dies kann zu rechtlich problematischen Folgeerscheinungen wie Persönlichkeitsverletzungen, Diskriminierungen oder Verletzungen der Mitwirkungsrechte führen. Diese Probleme betreffen sowohl Individuen (bei Persönlichkeitsverletzungen und direkten Diskriminierungen) als auch Gesellschaftsgruppen (bei indirekten Diskriminierungen und Verletzungen von Mitwirkungsrechten).

Doch nach der vorliegend vertretenen Meinung sind nicht immer Rechtsprobleme mit People Analytics verbunden. Beispielsweise hängen die subjektiven Erwartungen an den Schutz der Privatsphäre vom Kontext ab, sodass die identische Anwendung in einem Betrieb zu Privatsphäreverletzungen führen kann, im andern jedoch nicht.⁶³⁹ Ferner kann etwa eine Anwendung aus der Sicht einer Einzelperson diskriminierend sein, während sie für gesamte Gruppen von Betroffenen gerechte Resultate hervorbringt.⁶⁴⁰ Daher ist eine differenzierte Sicht auf People Analytics erforderlich. Es kann nicht das Ziel sein, People Analytics von Grund auf zu verbieten. Stattdessen sind rechtliche Optionen gesucht, die der sich versteifenden Machtasymmetrie entgegenwirken und die nötige Flexibilität in die Arbeitsbeziehungen zurückbringen. Zur Prüfung dieser Optionen ist im Folgenden zunächst zu fragen, welche rechtlichen Erlasse überhaupt für People Analytics relevant sind (dazu sogleich).

19.11.2019). Es handelt sich um notwendige erzwingbare Betriebsvereinbarungen: KNAPP/HAAS, 82.

⁶³⁹ Siehe S. 85–86.

⁶⁴⁰ Siehe S. 97.

4 Relevante Rechtsbestimmungen

4.1 Übersicht

Um den in Kapitel 3 beschriebenen Rechtsproblemen zu begegnen, ist zu prüfen, welche Erlasse auf die entsprechenden Sachverhalte anwendbar sind. Vor dem Risiko der Persönlichkeitsverletzungen schützen der arbeitsrechtliche und der datenschutzrechtliche Persönlichkeitsschutz sowie der öffentlich-rechtliche Arbeitnehmer-Gesundheitsschutz (dazu sogleich, Unterkapitel 4.2–4.4, S. 107–115). Zum Schutz vor Diskriminierungen bestehen spezifische Diskriminierungsverbote und ein allgemeines arbeitsrechtliches Diskriminierungsverbot (Unterkapitel 4.5, S. 115–126). Das Mitwirkungsrecht ist zu betrachten (Unterkapitel 4.6, S. 126–127). Ferner sind das Strafrecht, die EMRK und die verfassungsrechtlichen Grundrechte sowie weitere völkerrechtliche Erlasse zu berücksichtigen (Unterkapitel 4.7–4.9, S. 127–131).

4.2 Arbeitsrechtlicher Persönlichkeitsschutz

Schutz vor unrechtmässigen Persönlichkeitsverletzungen durch People Analytics bietet der allgemeine zivilrechtliche Persönlichkeitsschutz gemäss Art. 27 und 28 ff. ZGB. Zudem sind die arbeitsvertraglichen Bestimmungen einzuhalten (Art. 319 ff. OR). Die Fürsorgepflicht auferlegt der Arbeitgeberin, die Persönlichkeit des Arbeitnehmers im Arbeitsverhältnis zu achten und zu schützen, auf dessen Gesundheit gebührend Rücksicht zu nehmen und für die Wahrung der Sittlichkeit zu sorgen (Art. 328 Abs. 1 Satz 1 OR).

Zu beachten sind gegebenenfalls spezifische arbeitsrechtliche Bestimmungen, die in einzelnen Betrieben relevant sind. Zu denken ist an zwingende (normative) Mindestarbeitsbedingungen gemäss Gesamtarbeitsverträgen (vgl. Art. 357 OR), an Betriebsordnungen (Art. 37–39 ArG), an Personalreglemente und an Vereinbarungen im Einzelarbeitsvertrag.⁶⁴¹

⁶⁴¹ Zur Rangordnung der Normen im Arbeitsrecht: FRITZ/SCHULER, 28.

4.3 Datenschutzrechtlicher Persönlichkeitsschutz

4.3.1 Schweizerisches Datenschutzrecht

Im Informationszeitalter erlangt das Datenschutzrecht im arbeitsrechtlichen Kontext eine wichtige Stellung, weil es den Persönlichkeitsschutz im Bereich von Datenbearbeitungen konkretisiert.⁶⁴² Trotz dieser zunehmenden Bedeutung existiert nur eine generalklauselartige privatrechtliche Bestimmung zum Datenschutz im Arbeitsverhältnis.⁶⁴³ Als Ausfluss der Fürsorgepflicht⁶⁴⁴ ist der Arbeitgeberin die Bearbeitung von Daten über den Arbeitnehmer, welche nicht seine Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind, verboten (Art. 328b Satz 1 OR). Die Schweiz kennt keinen spezifischen Erlass über den Arbeitnehmer-Datenschutz. Diese Rechtslage trifft auch auf Deutschland, das einen Entwurf für ein Gesetz zum Beschäftigtendatenschutz diskutiert und verworfen hat,⁶⁴⁵ und auf Österreich⁶⁴⁶ zu. EU-Vorarbeiten zu einer Arbeitnehmer-Datenschutz-Richtlinie kommen desgleichen nicht voran.⁶⁴⁷

Im Arbeitsverhältnis gelten im Übrigen die (allgemeinen) Bestimmungen des DSG (Art. 328b Satz 2 OR). Sie ergänzen den allgemeinen zivilrechtlichen Persönlichkeitsschutz und lassen dieses System (Art. 28 ff. ZGB) dem Grundsatz nach unverändert.⁶⁴⁸ Für die vorliegend zu untersuchenden privatrechtlichen Arbeitsverhältnisse sind die bundesrechtlichen Bestimmungen massgeblich; die kantonalen Datenschutzerlasse treten in den Hintergrund, einerseits weil das Bun-

⁶⁴² MEIER PHILIPPE, N 332. Vgl. WOLFER, N 612. Datenschutzrecht als Teilgebiet des rechtlichen Autonomieschutzes besonders bedeutsam: HOFFMANN-RIEM, 39.

⁶⁴³ WOLFER, N 641.

⁶⁴⁴ Vor In-Kraft-Treten des Art. 328b OR (01.07.1993) floss die Pflicht der Arbeitgeberin, die Daten des Arbeitnehmers zu schützen, aus Art. 328 OR: RIESSELMANN-SAXER, 5.

⁶⁴⁵ § 26 BDSG als einzige gesetzliche Regelung, in der es spezifisch um den Umgang mit Daten aus einem Beschäftigungsverhältnis geht: HÄRTING, N 343; ergebnislose Gespräche zum Entwurf eines Gesetzes zum Beschäftigtendatenschutz am 25.08.2010: WYBITUL/SCHULTZE-MELLING, N 14; endgültige Zurückstellung des Gesetzesentwurfs am 26.02.2013: OWSCHIMIKOW, 47.

⁶⁴⁶ Der Begriff «Arbeitnehmerdatenschutz» ist der österreichischen Rechtsordnung fremd und ein eigenes Arbeitnehmer-Datenschutzrecht ist nicht vorgesehen: GORICNIK/GRÜNANGER, N 1.2; KNAPP/HAAAS, 79.

⁶⁴⁷ SCHAAR 2007, 208.

⁶⁴⁸ AEBI-MÜLLER, N 580.

desrecht entgegenstehendem kantonalem Recht vorgeht (Art. 49 Abs. 1 BV), andererseits weil die kantonalen Datenschutzerlasse nur für die Bearbeitung von Personendaten durch kantonale öffentliche Organe gelten (vgl. etwa Art. 2 Abs. 1 DSG SG).

4.3.2 Europäisches Datenschutzrecht

a) Datenschutz-Grundverordnung der Europäischen Union

Die DSGVO verändert die digitale Welt spürbar, indem sie Betroffene verstärkt schützt und die Anforderungen an die Verantwortlichen der Datenbearbeitung erhöht.⁶⁴⁹ Die DSGVO hat als Verordnung allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat der Europäischen Union (Art. 288 Abs. 2 AEUV). Aus Sicht der Schweiz ist der im Vergleich zur DSRL substanziell erweiterte räumliche Anwendungsbereich der DSGVO (Art. 3 DSGVO) folgenreich.⁶⁵⁰ Die Fälle, in denen die DSGVO auf Sachverhalte mit Schweiz-Bezug anwendbar ist, sind nachfolgend darzulegen.

Das Marktortprinzip⁶⁵¹ hat zur Folge, dass ausserhalb der EU domizilierte Unternehmen von der DSGVO erfasst werden können.⁶⁵² Die aus Sicht einer in der Schweiz operierenden Arbeitgeberin wichtige Bestimmung zur territorialen Geltung ist Art. 3 Abs. 2 lit. b DSGVO: Die EU-Verordnung findet Anwendung auf die Bearbeitung personenbezogener Daten von betroffenen Personen, die sich in der EU befinden, durch einen nicht in der EU niedergelassenen Verantwortlichen oder Auftragsbearbeiter, wenn die Datenbearbeitung im Zusammenhang damit

⁶⁴⁹ BURRI/SCHÄR, 105.

⁶⁵⁰ BURRI/SCHÄR, 107. Zu konkretisieren ist jedoch, dass die Erweiterung im Einklang mit der Rechtsprechung des EuGH zur extraterritorialen Anwendung der DSRL steht. Die DSRL erfasste spätestens seit dem Entscheid gegen Google Spain im Jahr 2014 Datenbearbeitungstätigkeiten, die auf die Einwohner von EU-Staaten ausgerichtet waren. Insofern darf der weite Geltungsbereich der DSGVO nicht überraschen: Urteil EuGH vom 13.05.2014, Google Spain, C-131/12, EU:C:2014:317, 60. Die DSGVO ist für die Schweiz als Nicht-EU-Mitgliedstaat nicht direkt anwendbar, entfaltet aber aufgrund des Anwendungsbereichs in gewissen Fällen extraterritoriale Wirkung: Datenschutzbeauftragter des Kantons Zürich, 1.

⁶⁵¹ FRANZEN, 320; auch «Kriterium der Zielgruppe»: EDÖB 2018b, 3.

⁶⁵² Das DSG gilt umgekehrt nicht für Unternehmen mit Sitz ausserhalb der Schweiz, die Datenbearbeitungen mit Auswirkungen in der Schweiz vornehmen. Eine entsprechende Forderung aus der Vernehmlassung wurde in der Botschaft nicht berücksichtigt: BBl 2017, 6982.

steht, das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt. Der Aufenthaltsort der betroffenen Person, nicht etwa ihre Staatsangehörigkeit oder ihr Wohnsitz, entscheidet somit über die Anwendbarkeit der DSGVO.⁶⁵³ Die DSGVO entfaltet extraterritoriale Wirkung für eine Schweizer Arbeitgeberin, die dienstlich zur Verfügung gestellte Mobiltelefone ihrer im EU-Ausland tätigen oder auf Dienstreise befindlichen Arbeitnehmenden überwacht.⁶⁵⁴ Unter die DSGVO fallen auch (Online-)Bewerbungsverfahren von Schweizer Arbeitgeberinnen, wenn Verhaltensdaten von Bewerbenden im EU-Raum bearbeitet werden.⁶⁵⁵ Dies dürfte beispielsweise zutreffen, wenn schweizerische Unternehmen Softwares verwenden, die ermitteln, ob jemand kreativ ist (z.B. die Software von Evolv), wie sich ein Internetnutzer aktuell verhält (z.B. die Lösungen von Talentwunder oder Joberate), oder wenn ein Chatbot Gespräche mit Bewerbern aus dem EU-Raum führt (z.B. Mya von L'Oréal).⁶⁵⁶

Die DSGVO sieht drei weitere Fälle der extraterritorialen Wirkung vor: Ebenfalls eine Ausprägung des Markortprinzips ist die Erfassung von Datenbearbeitungen bei Waren- oder Dienstleistungsangeboten in der EU (Art. 3 Abs. 2 lit. a DSGVO), worunter jedoch nicht die Datenbearbeitungen im Zusammenhang mit Arbeitsverträgen subsumiert werden können.⁶⁵⁷ Darüber hinaus gilt die DSGVO bei Tätigkeiten einer Niederlassung in der EU (Sitzprinzip, Art. 3 Abs. 1 DSGVO)⁶⁵⁸ und bei Verantwortlichen, die aufgrund des Völkerrechts dem Recht

⁶⁵³ EDÖB 2018b, 4; MÉTILLE/ARASTEH, 142.

⁶⁵⁴ DAEDELLOW 2017, 37.

⁶⁵⁵ Vgl. DAEDELLOW 2017, 37.

⁶⁵⁶ Siehe S. 43–44.

⁶⁵⁷ Die DSGVO enthält keine genaue Definition des Begriffs «Waren- und Dienstleistungsangebot»: EDÖB 2018b, 6. Gemäss dem Europäischen Datenschutzausschuss qualifiziert die Bearbeitung von Mitarbeiterdaten durch ein Unternehmen aus einem Nicht-EU-Staat zum Zweck der Gehaltszahlung weder als Dienstleistungsangebot noch als Verhaltensüberwachung: EDSA 2018, 16–17. In diesem Sinne dürfte die DSGVO auch keine Wirkung entfalten, wenn schweizerische Arbeitgeber Stellenausschreibungen an den EU-Raum richten.

⁶⁵⁸ Sitzprinzip: FRANZEN, 320. Somit gilt die DSGVO für Schweizer Handelsgesellschaften, die im EU-Raum personenbezogene Daten ihrer Arbeitnehmer bearbeiten, unmittelbar und verbindlich: DAEDELLOW 2017, 34. Auch unterliegt es der DSGVO, wenn der EU-Hauptsitz Daten der Mitarbeiter einer Schweizer Zweigniederlassung bearbeitet: DAEDELLOW 2017, 37. Die vorliegende Arbeit konzentriert sich auf Arbeitsverhältnisse, bei denen die Arbeitgeberin Sitz in der Schweiz hat und der Arbeitnehmer seine Arbeit in einer Schweizer Betriebsstätte verrichtet. Konstellationen mit Konzerngesell-

eines EU-Mitgliedstaats unterliegen (Art. 3 Abs. 3 DSGVO). Diese Tatbestände sind nicht Gegenstand der vorliegenden Untersuchung.

Der sachliche Anwendungsbereich der DSGVO erstreckt sich auf die ganz oder teilweise automatisierte Bearbeitung personenbezogener Daten sowie auf die nichtautomatisierte Bearbeitung personenbezogener Daten, die in einem Dateisystem gespeichert werden (Art. 2 Abs. 1 DSGVO). Persönlich erfasst werden insbesondere natürliche und juristische Personen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Bearbeitung von personenbezogenen Daten entscheiden (sog. Verantwortliche, Art. 4 Nr. 7 DSGVO). In zeitlicher Hinsicht gilt die DSGVO seit dem 25.05.2018 (Art. 99 Abs. 2, vgl. Art. 94 Abs. 1 DSGVO). Somit ist bei People Analytics-Projekten, die (extra-)territorial von der DSGVO erfasst werden, auch der sachliche, persönliche und zeitliche Geltungsbereich der DSGVO eröffnet.

Nicht nur bei People Analytics-Projekten zur Beobachtung des Verhaltens von Personen im EU-Raum entfaltet die DSGVO extraterritoriale Wirkung. Für viele andere Schweizer Arbeitgeber entfaltet die DSGVO eine starke mittelbare Wirkung in dem Sinne, dass sie ihre People Analytics-Praktiken – ob mehr oder weniger freiwillig – am Schutzniveau der DSGVO ausrichten. Hierfür gibt es eine Reihe von Gründen: Erstens, das Übereinkommen 108 des Europarats ist für die Schweiz bindend und gibt ein ähnliches Schutzniveau wie dasjenige der DSGVO vor.⁶⁵⁹ Die Schweiz hat vor, auch das überarbeitete Übereinkommen 108 zu ratifizieren,⁶⁶⁰ welches am 18.05.2018 verabschiedet worden ist.⁶⁶¹ Die DSGVO stellt eine Staatenpraxis dar, die im Rahmen der völkerrechtlichen Auslegung des Übereinkommens 108 berücksichtigt werden muss, weil die Mehrheit der Vertragsstaaten des Übereinkommens 108, nämlich alle EU- und EWR-⁶⁶² Staaten, sie anwendet.⁶⁶³ Zweitens, wenn die Kommission beschliesst, dass ein betreffendes Drittland ein angemessenes Schutzniveau bietet, ist unter der DSGVO eine Übermittlung personenbezogener Daten an dieses Drittland ohne besondere Genehmigung zulässig (Art. 45 Abs. 1 DSGVO). Um diesen Wettbewerbsvorteil zu erlan-

schaften oder Zweigniederlassungen in der EU sind nicht Teil des vorliegenden Forschungsgegenstands.

⁶⁵⁹ FREI, N 26. Siehe zum Übereinkommen 108 S. 129–130.

⁶⁶⁰ EDÖB 2018a, 12. Siehe auch S. 129–130.

⁶⁶¹ Europarat 2018b.

⁶⁶² Vgl. Überschrift zur DSGVO: «Text für den EWR».

⁶⁶³ FREI, N 26.

gen, strebt die Schweiz eine Erneuerung des Angemessenheitsbeschlusses und somit ein gleichwertiges Datenschutzniveau wie in der EU an.⁶⁶⁴ Drittens, die Schweiz muss die der DSGVO sehr ähnliche Richtlinie 2016/680, die zum Schengen-Besitzstand gehört, im Bereich der Strafverfolgung umsetzen.⁶⁶⁵

b) Nationale Bestimmungen der Mitgliedstaaten der Europäischen Union betreffend Beschäftigtendaten

Für den Bereich des Datenschutzes am Arbeitsplatz lässt die DSGVO Raum für konkretisierende nationale Bestimmungen (sog. Öffnungsklausel).⁶⁶⁶ Die EU-Mitgliedstaaten «können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Bearbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschliesslich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen» (Art. 88 Abs. 1 DSGVO). Diese konkretisierenden nationalen Bestimmungen der EU-Mitgliedstaaten müssen Schweizer Arbeitgebende zusätzlich einhalten, sofern sie Beschäftigtendaten aus dem jeweiligen

⁶⁶⁴ Schweizerischer Bundesrat 2018; FREI, N 26. Schweizer Unternehmen sähen sich bei ausbleibender Erneuerung des Angemessenheitsbeschlusses mit einem deutlichen administrativen Mehraufwand konfrontiert: HUSI-STÄMPFLI, N 22. Der Angemessenheitsbeschluss ist ein Wettbewerbsvorteil für den betreffenden Drittstaat: GILBERT, 256. A.M. BENZ NICOLA, Die neue Datenschutzverordnung der EU aus Sicht der Schweiz, NZZ vom 18.06.2018, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020): Ein Entzug des Angemessenheitsstatus hätte nur geringfügige Konsequenzen, da es andere Möglichkeiten für die Übermittlung von Daten in Länder ohne adäquates Schutzniveau gebe. – Es wird bezweifelt, ob die Schweiz die Angemessenheit unter dem rev-DSG fortführen kann, weil der EDÖB weniger Kompetenzen haben wird als seine europäischen Amtskollegen (für Sanktionen sind in der Schweiz ausschliesslich die Strafverfolgungsbehörden zuständig); zudem sind die Sanktionen aufgrund der geringeren Bussgeldbeträge und der reduzierten strafbaren Tatbestände milder als in der EU: FREI, N 67.

⁶⁶⁵ FREI, N 26.

⁶⁶⁶ DAEDELLOW 2017, 35.

EU-Land bearbeiten und dieses Land von seiner Ermächtigung Gebrauch gemacht hat.⁶⁶⁷

Es ist umstritten, ob die konkretisierenden mitgliedstaatlichen Bestimmungen strenger ausfallen dürfen als die DSGVO. Solange der EuGH über diese Frage nicht entschieden hat, verbleibt eine gewisse Rechtsunsicherheit. Gewichtige Gründe sprechen für die Zulässigkeit strengerer nationaler Bestimmungen.⁶⁶⁸ Diesen Schluss legt das historische Auslegungselement nahe, das bei jungen Erlassen stärker als bei alten zu betonen ist.⁶⁶⁹ Der Vorschlag der Kommission, mit Art. 88 DSGVO lediglich Regelungen «in den Grenzen dieser Verordnung» zuzulassen, wurde im Gesetzgebungsverfahren verworfen.⁶⁷⁰ Auch aus systematischen Überlegungen kann die DSGVO für den Bereich des Arbeitnehmer-Datenschutzes nur Mindest-, nicht Höchststandard sein, weil die EU diesbzgl. eine Kompetenz zum Erlass von «Mindestvorschriften» hat (Art. 153 Abs. 1 lit. b AEUV).⁶⁷¹ Der Umstand, dass die DSGVO von Öffnungsklauseln durchzogen ist,⁶⁷² dämpft die Erwartung, der Wechsel von Richtlinie (95/46/EG) zu Verordnung (DSGVO) bedeute eine Vollharmonisierung.⁶⁷³ Ferner wird vertreten, die Kompetenz zum Erlass «spezifischerer Vorschriften» (Art. 88 DSGVO) belasse den Mitgliedstaaten mehr Raum als nur ein «näheres Bestimmen» (wie unmittelbar vorangehend vorgesehen in Art. 87 DSGVO).⁶⁷⁴ Schliesslich wird meistens die nationale Aufsichtsbehörde zuständig sein (vgl. Art. 55–56 DSGVO), womit der Arbeitnehmer-

⁶⁶⁷ DAEDELLOW 2017, 37.

⁶⁶⁸ Restriktivere nationale Regulierung in engen Grenzen zulässig: DREYER/SCHULZ, 43; strengere nationale Arbeitnehmerdatenschutzvorschriften zulässig, wobei der EuGH das letzte Wort hierzu sprechen wird: GRAF/KRIŽANAC, 92. Vgl. OTTO 2015, 362.

⁶⁶⁹ Vgl. die schweizerische Rechtsprechung: BGE 126 V 103 E. 3b.

⁶⁷⁰ Siehe die Streichung des Zusatzes «*within the limits of this regulation*»: Europäisches Parlament 2014, Art. 82 Abs. 1, und Europäisches Parlament 2014, E. 124. Der Zusatz «in den Grenzen dieser Verordnung» fehlt nun in E. 155 und Art. 88 DSGVO. CULIK, 102, m.w.H.

⁶⁷¹ CULIK, 103.

⁶⁷² FEILER.

⁶⁷³ Vgl. CULIK, 102. Nationale Regelungen müssen über den Standard der DSGVO hinausgehen, da reine Wiederholungen des EU-Rechts durch nationale Normen unzulässig und damit unwirksam sind: GOLA 2019, N 205.

⁶⁷⁴ FEILER *et al.*, Art. 88 DSGVO N 2. «Näher bestimmen» bedeutet, dass die Bestimmungen der DSGVO nicht widersprechen dürfen: FEILER *et al.*, Art. 87 DSGVO N 1.

Datenschutz verfahrenstechnisch eine weitgehend nationale Angelegenheit bleiben wird.⁶⁷⁵

Die gegenteilige Auffassung versteht den Wortlaut («spezifischere Vorschriften», Art. 88 Abs. 1 DSGVO) als Ermächtigung zu reinen Präzisierungen. Es sei den Mitgliedstaaten verwehrt, durch nationale Regelungen das Schutzniveau der DSGVO zu erhöhen oder abzusenken.⁶⁷⁶ Dies entspreche dem Harmonisierungsgedanken der DSGVO (E. 9–10 DSGVO).⁶⁷⁷

Nach der hier vertretenen Auffassung bildet die DSGVO einen Mindeststandard, der durch strengere nationale Bestimmungen verstärkt werden kann. Das materielle Ziel der DSGVO, die natürlichen Personen bei der Bearbeitung personenbezogener Daten zu schützen, muss dem formellen Ziel der unionsweiten Harmonisierung des Datenschutzrechts vorgehen. Es ist somit denkbar, dass EU-Mitgliedstaaten solche Vorschriften mit extraterritorialer Wirkung erlassen. Beispielsweise könnte ein Mitgliedstaat die Einwilligung als Rechtfertigungsmöglichkeit für Datenbearbeitungen im Arbeitskontext ausschliessen.⁶⁷⁸ Existieren solche spezifischeren Vorschriften, sind sie kumulativ zur DSGVO auf die vorliegend interessierenden Sachverhalte anwendbar. Schweizerische Arbeitgeber sollten daher das nationale Recht der EU-Mitgliedstaaten, zu denen sie in Kontakt stehen, kennen und einhalten.

4.4 Öffentlich-rechtlicher Arbeitnehmer-Gesundheitsschutz

Im Kontext von People Analytics gilt das Verbot von Überwachungs- und Kontrollsystemen zur Verhaltensüberwachung am Arbeitsplatz (Art. 26 ArGV 3), welches die Rechtsprechung jedoch gelockert hat.⁶⁷⁹ Arbeitnehmer haben einen zivil-

⁶⁷⁵ GRAF/KRIŽANAC, 105.

⁶⁷⁶ KAINER/WEBER, 2740; DAEDELLOW 2017, 35.

⁶⁷⁷ Aber: Trotz EU-weit vereinheitlichtem Datenschutzniveau könnten die Mitgliedstaaten andere Bereiche, die den Datenschutz tangieren, heterogen regeln. Unternehmen, die Zugang zum EU-Markt wollen, müssen sich z.B. in den Bereichen Meinungsausserungsfreiheit, Gesundheitswesen oder Arbeitsbedingungen mit unterschiedlichen Regulierungen befassen: BURRI/SCHÄR, 110–111.

⁶⁷⁸ EPINEY/KERN, 53.

⁶⁷⁹ Siehe später, S. 150–154, die Diskussion betreffend Urteil BGer 6B_536/2009 vom 12.11.2009.

rechtlichen Anspruch auf Erfüllung öffentlich-rechtlicher Verpflichtungen der Arbeitgeberin über die Arbeit, wenn die Verpflichtung Inhalt des Einzelarbeitsvertrages sein könnte (Art. 342 Abs. 2 OR). Das erwähnte Überwachungsverbot konkretisiert die Pflicht der Arbeitgeberin zum Schutz der Gesundheit der Arbeitnehmer (Art. 6 Abs. 1 Satz 1, Art. 6 Abs. 4 ArG) und ist eine öffentlich-rechtliche Norm.⁶⁸⁰ Somit können Arbeitnehmer die Einhaltung des Überwachungsverbots auch zivilrechtlich einfordern. Die Parteien können nicht durch privatrechtliche Abrede vom Überwachungsverbot abweichen (vgl. Art. 19–20 OR).⁶⁸¹ Das Überwachungsverbot gilt – als Teil der Vorschriften über den Gesundheitsschutz – grundsätzlich für alle privatrechtlichen Arbeitsverhältnisse, einschliesslich gegenüber Arbeitnehmern, die eine höhere leitende Tätigkeit oder eine wissenschaftliche oder selbstständige künstlerische Tätigkeit ausüben (Art. 3a lit. b ArG), ebenso gegenüber Lehrern an Privatschulen (Art. 3a lit. c ArG).⁶⁸² Dadurch ist sein Anwendungsbereich wesentlich breiter als derjenige der übrigen Bestimmungen des ArG (vgl. Art. 1 Abs. 1 i.V.m. Art. 3 lit. d–e ArG).

4.5 Diskriminierungsschutz

4.5.1 Beschränkter Geltungsbereich der Diskriminierungsverbote

Die Analytik diskriminiert begriffsnotwendig zwischen Individuen, die statistisch ähnlich erscheinen, und solchen, die statistisch verschieden sind.⁶⁸³ In der Schweiz fehlt ein umfassender Spezial-Erlass zum arbeitsrechtlichen Verbot von Diskriminierungen, wie er etwa in Deutschland mit dem Allgemeinen Gleichbehandlungsgesetz (AGG) existiert.⁶⁸⁴ Stattdessen gilt der Grundsatz der privatrechtlichen Ver-

⁶⁸⁰ Vgl. die verfassungsrechtlichen Grundlagen gemäss der Präambel des ArG und die SR-Nummer 822.11 (Einteilung in der Abteilung 8, «Gesundheit – Arbeit – Soziale Sicherheit»).

⁶⁸¹ Vgl. STREIFF/VON KAENEL/RUDOLPH, Art. 341 OR N 2.

⁶⁸² MÜLLER, 252. Auch die öffentlich-rechtlichen Arbeitsverhältnisse von Verwaltungen des Bundes, der Kantone und Gemeinden sowie von Lehrern, Fürsorgern, Erziehern und Aufsehern in Anstalten werden erfasst (Art. 3a lit. a und c ArG).

⁶⁸³ Siehe S. 88.

⁶⁸⁴ In Deutschland existiert mit dem Allgemeinen Gleichbehandlungsgesetz (AGG) ein umfassendes arbeitsrechtliches Diskriminierungsverbot: WILDHABER *et al.*, 470. Der Bundesrat hat den Erlass eines allgemeinen Antidiskriminierungsgesetzes bis anhin stets abgelehnt: WILDHABER *et al.*, 470. Indirekter Diskriminierungsschutz in der

tragsfreiheit (Art. 19 Abs. 1 OR), die Teil der verfassungsrechtlich geschützten Wirtschaftsfreiheit ist (Art. 27 BV).⁶⁸⁵ Im Privatrecht geht die Vertragsfreiheit grundsätzlich dem Gleichbehandlungsgebot vor.⁶⁸⁶

Besondere gesetzliche Diskriminierungsverbote schränken jedoch die Vertragsfreiheit ein.⁶⁸⁷ Spezialgesetze schützen insbesondere die Persönlichkeitsmerkmale Geschlecht (Art. 3 GlG),⁶⁸⁸ Erbgut bzw. genetische Abstammung (Art. 4 GUMG)⁶⁸⁹ und Heimarbeit (Paritätslohn gemäss Art. 4 Abs. 1 HArG).⁶⁹⁰ Auch das Merkmal der Staatsangehörigkeit geniesst Rechtsschutz, wodurch sich der schweizerische und der europäische Diskriminierungsschutz vom Arbeitsvölkerrecht abheben, welches die Staatsangehörigkeit nicht unter den Diskriminierungskriterien auführt oder sogar ausdrücklich davon ausnimmt:⁶⁹¹ Der Status des Wanderarbeitnehmers steht in grenzüberschreitenden Sachverhalten unter Diskriminierungsschutz (Art. 2, Art. 7 lit. a FZA sowie Anhang I Art. 9 Abs. 1 und 4 FZA).⁶⁹² Des Weiteren ist die Erteilung einer Bewilligung für die Beschäftigung ausländischer Arbeitskräfte an die Voraussetzung geknüpft, dass Arbeitgeberinnen den ausländischen Arbeitnehmenden bei gleicher Arbeit die gleichen Lohn- und Arbeitsbedingungen gewähren wie den schweizerischen Arbeitnehmenden (Art. 22 AIG).⁶⁹³

Der verfassungsrechtliche Schutz der Rechtsgleichheit statuiert in einer nicht abschliessenden («namentlichen») Liste den Schutz von neun die Identität des Menschen prägenden Merkmalen (Art. 8 Abs. 2 BV). Diese sind die Herkunft und Rasse, das Geschlecht und Alter, die Sprache und soziale Stellung, die Lebens-

Schweiz nur ansatzweise vorhanden: WILDHABER 2017, 215; zum AGG: DZIDA, 543. Zu beachten ist auch, dass die DSGVO, anders als das DSG, explizit auf das Risiko der Diskriminierung hinweist (vgl. E. 71 Abs. 2, E. 75, E. 85 Satz 1 DSGVO).

⁶⁸⁵ PÄRLI 2009, N 1547.

⁶⁸⁶ Mit Bezug auf den Vertragsinhalt seien grundsätzlich «beliebige Differenzierungen zwischen den einzelnen Vertragspartnern erlaubt»: CHK OR AT-KUT, Art. 19–20 OR, N 5.

⁶⁸⁷ WILDHABER *et al.*, 471–472.

⁶⁸⁸ Gestützt auf das GlG sind auch Fragen zur Eignungsabklärung nach bevorstehenden Militärdienstplichten unzulässig: PÄRLI 2018, N 17.40.

⁶⁸⁹ WILDHABER *et al.*, 471–472.

⁶⁹⁰ PÄRLI 2009, N 8.

⁶⁹¹ PÄRLI 2009, N 1555.

⁶⁹² WILDHABER *et al.*, 472; PÄRLI 2009, N 8; unmittelbare Drittwirkung des FZA: PÄRLI 2019, N 30.

⁶⁹³ PÄRLI 2009, N 8.

form, (religiöse, weltanschauliche oder politische) Überzeugung und eine allfällige (körperliche, geistige oder psychische) Behinderung. Die Rechtsgleichheit entfaltet auf privatrechtliche Arbeitsverträge bloss indirekt Drittwirkung (vgl. Art. 35 Abs. 3 BV), abgesehen von der direkten Drittwirkung des Gebots des gleichen Lohns für gleichwertige Arbeit von Mann und Frau (Art. 8 Abs. 3 Satz 3 BV). Das grundsätzliche Fehlen einer direkten Verpflichtung Privater durch die Rechtsgleichheit erhellt etwa aus dem Umstand, dass das Merkmal einer körperlichen, geistigen oder psychischen Beeinträchtigung ausdrücklich nur in öffentlich-rechtlichen Arbeitsverhältnissen des Bundes geschützt wird (vgl. Art. 3 lit. g, Art. 13 BehiG).⁶⁹⁴

Insgesamt stellt sich der schweizerische arbeitsrechtliche Diskriminierungsschutz als Flickenteppich heraus, weil grundsätzlich die privatrechtliche Vertragsfreiheit vorherrscht und nur punktuelle Diskriminierungsverbote existieren.⁶⁹⁵ Persönlichkeitsmerkmale bleiben schutzlos, wenn sie nicht explizit auf Verfassungs- oder Gesetzesstufe als diskriminierungssensibel deklariert werden.

Der eingeschränkte Geltungsbereich des Diskriminierungsschutzrechts macht sich bei People Analytics bemerkbar, wenn die Belegschaft *ad hoc* in beliebige Gruppen eingeteilt wird, die sich nicht durch ein anerkanntes diskriminierungssensibles Merkmal auszeichnen.⁶⁹⁶ Für diese Form der Unterscheidung nach Persönlichkeitsmerkmalen, die nicht durch ein Spezialgesetz oder Art. 8 Abs. 2–4 BV geschützt sind, wird vorliegend die Bezeichnung «Lifestyle-Diskriminierung» verwendet.⁶⁹⁷ Besonders aus den USA sind Fälle der Lifestyle-Diskriminierung bekannt. In der Bewerbungsphase lehnen verschiedene Arbeitgeberinnen verteilt über alle US-Gliedstaaten Raucher generell ab.⁶⁹⁸ Ein texanisches Spital hat eine Richtlinie gegen die Einstellung von schwer übergewichtigen Personen erlassen.⁶⁹⁹ Für gewisse Arbeitgeberinnen ist massgebend, mit welchem Browser ein

⁶⁹⁴ Vgl. WILDHABER *et al.*, 471. Auch in den USA stellt dies in der Regel keine verbotene Diskriminierung dar: CHK OR BT 2-EMMEL, Art. 328 OR, N 6. In Deutschland aber wäre ein Algorithmus, der Bewerbungen aussortiert, weil er eine Schwerbehinderung des Bewerbers erkennt und negativ bewertet, unzulässig: DZIDA, 543.

⁶⁹⁵ Siehe S. 115–117. Vgl. WILDHABER *et al.*, 471.

⁶⁹⁶ Vgl. WILDHABER *et al.*, 474, MITTELSTADT, 475–476, und FAVARETTO *et al.*, 11.

⁶⁹⁷ So auch: PARISI, 320.

⁶⁹⁸ ROBERTS, 573.

⁶⁹⁹ Keine Einstellung ab einem Body-Mass-Index von 35 im Citizens Medical Center: ROBERTS, 574; Diskriminierung wegen Übergewichts und Rauchens: AJUNWA/CRAWFORD/SCHULTZ, 767.

Bewerber seine Unterlagen hochlädt.⁷⁰⁰ Erhöhter Blutdruck und positive Nikotin-Testresultate haben zu Kündigungen geführt.⁷⁰¹ Die Arbeitgeberin kann ihren Entscheidungen auch weitere Kriterien zugrunde legen: Bewegungsgewohnheiten von Arbeitnehmern können über deren Impulsivität und Ungeduld sowie über Alkohol- und Drogenmissbrauch, Essstörungen und Rauchgewohnheit Aufschluss geben.⁷⁰² Verzeichnet ein Wearable⁷⁰³ einen unruhigen Schlaf, kann dies auf psychologische Probleme, verminderte kognitive Leistung, Wut, Depressionen oder Gesundheitsprobleme hinweisen.⁷⁰⁴ Für Arbeitgeberinnen, die den innerbetrieblichen sozialen Graphen messen, ist relevant, wo und wann Arbeitnehmer zu Mittag essen⁷⁰⁵ und welche Sympathien und Antipathien sowie welche Dynamiken zwischen Personen bestehen.⁷⁰⁶ Aus den Aufzeichnungen resultieren individuelle Risikoprognosen, gegebenenfalls in Kombination mit weiteren Kontextdaten wie der Kreditwürdigkeit oder der Tatsache, ob jemand allein lebt.⁷⁰⁷

Den erwähnten Lifestyle-Kriterien ist gemeinsam, dass sie nicht durch die Rechtsordnung als diskriminierungssensibel eingestuft werden.⁷⁰⁸ Dies könnte darauf zurückzuführen sein, dass die Lifestyle-Kriterien tendenziell an ein Verhalten der betroffenen Person anknüpfen und nicht an ein Persönlichkeitsmerkmal.⁷⁰⁹ Der rechtliche Schutz lässt sich beispielhaft am Kriterium des Übergewichts nachzeichnen: Gemäss dem EuGH besteht im EU-Recht «kein allgemeines Verbot der Diskriminierung wegen Adipositas als solcher in Beschäftigung und Beruf».⁷¹⁰

⁷⁰⁰ DAEDELLOW 2018, N 38.

⁷⁰¹ PARISI, 320.

⁷⁰² PARISI, 332.

⁷⁰³ Siehe zum Begriff «Wearable» S. 25–26.

⁷⁰⁴ PARISI, 332.

⁷⁰⁵ Vgl. BURDON/HARPUR, 680. Siehe zum innerbetrieblichen sozialen Graphen S. 56.

⁷⁰⁶ STRAHILEVITZ 2013, 2024.

⁷⁰⁷ ROWLAND CHRISTOPHER, With fitness trackers in the workplace, bosses can monitor your every step – and possibly more, The Washington Post vom 16.02.2019, abrufbar unter <www.washingtonpost.com> (besucht am 31.05.2020).

⁷⁰⁸ Adipositas und Raucherstatus auch in den USA nicht diskriminierungsrechtlich geschützt: AJUNWA/CRAWFORD/FORD, 478.

⁷⁰⁹ ROBERTS, 571. Die USA schützen Arbeitnehmer auf Bundesstaatsebene nur vor merkmalsbezogener Diskriminierung: ROBERTS, 634. Die Gliedstaaten schützen Arbeitnehmer zu unterschiedlichen Graden auch vor verhaltensbezogener Diskriminierung: ROBERTS, 634.

⁷¹⁰ Urteil EuGH vom 18.12.2014, Kaltoft, C-354/13, EU:C:2014:2463, N 40.

Eine Ausnahme besteht aber dann, wenn die Unterscheidung nach einem Lifestyle-Kriterium mit der Diskriminierung aufgrund eines verpönten Diskriminierungsmerkmals gleichzusetzen ist: Der EuGH behandelt die Adipositas eines Arbeitnehmers als eine «Behinderung» im Sinne der Richtlinie 2000/78/EG betreffend die Gleichbehandlung in Beschäftigung und Beruf, wenn das Übergewicht eine Einschränkung mit sich bringt, die unter anderem auf physische, geistige oder psychische Beeinträchtigungen von Dauer zurückzuführen ist. Zudem ist vorausgesetzt, dass diese Beeinträchtigungen den Arbeitnehmer in Wechselwirkung mit verschiedenen Barrieren an der vollen und wirksamen Teilhabe am Berufsleben, gleichberechtigt mit den anderen Arbeitnehmern, hindern können.⁷¹¹ Die sozialversicherungsrechtliche Rechtsprechung des Bundesgerichts zielt in eine ähnliche Richtung: Adipositas begründet für sich allein keine (teilweise) Arbeitsunfähigkeit.⁷¹² Adipositas kann jedoch eine Invalidität bewirken, die zum Bezug von Rentenleistungen berechtigt, wenn sie körperliche oder geistige Schäden verursacht oder die Folge von solchen Schäden ist.⁷¹³ Eine vergleichbare Rechtslage besteht in den USA.⁷¹⁴

Der mangelnde Schutz von Lifestyle-Kriterien kann sich als diskriminierungsrechtliches Problem erweisen. Dies ist am Beispiel der Browseranalyse zu schildern: Es wurde ermittelt, dass Arbeitnehmer, die selbst einen Browser auf dem Computer einrichten (z.B. Chrome auf einem Applegerät), leistungsfähiger sind und ihrer Stelle länger treu bleiben als solche, die den vorinstallierten Browser verwenden (z.B. Safari auf einem Applegerät).⁷¹⁵ Dies kann eine Arbeitgeberin dazu veranlassen, Arbeitnehmer und Bewerber systematisch zu benachteiligen, die einen vorinstallierten Browser verwenden. Die betroffene Person kann spürbare Nachteile erfahren (z.B. Nichtbeförderung, Abweisung der Bewerbung), weil die Gesamtheit der Vergleichsgruppe, in die sie einsortiert wird (Personen mit vorin-

⁷¹¹ Urteil EuGH vom 18.12.2014, Kaltoft, C-354/13, EU:C:2014:2463, N 64.

⁷¹² Urteil BGer I 623/2006 vom 28.02.2007 E. 4.2.

⁷¹³ Urteil BGer 8C_663/2017 vom 12.12.2017 E. 3.2. Zudem muss Adipositas selbst in Abwesenheit von körperlichen oder geistigen Schäden unter Berücksichtigung der besonderen Gegebenheiten des Einzelfalles als invalidisierend betrachtet werden, wenn sie weder durch geeignete Behandlung noch durch zumutbare Gewichtsabnahme auf ein Mass reduziert werden kann, bei welchem das Übergewicht in Verbindung mit allfälligen Folgeschäden keine voraussichtlich bleibende oder längere Zeit dauernde Beeinträchtigung der Erwerbsfähigkeit bzw. der Betätigung im bisherigen Aufgabenbereich zur Folge hat: Urteil BGer 8C_663/2017 vom 12.12.2017 E. 3.2.

⁷¹⁴ WILDHABER *et al.*, 474–475.

⁷¹⁵ Siehe S. 44.

stalliertem Browser), sich mit einer gewissen Wahrscheinlichkeit in bestimmter Weise verhält (schwächere Arbeitsleistung und früherer Stellenwechsel).⁷¹⁶ Dem Betroffenen wird somit kein individueller Vorwurf gemacht.⁷¹⁷ Möglicherweise handelt es sich aber um eine sachlich nicht gerechtfertigte Gleichbehandlung von Ungleichem, wenn eine leistungsfähige Person, die ebenfalls den Standardbrowser verwendet, die gleichen Nachteile erleidet wie die leistungsschwächeren Personen, die den Standardbrowser nutzen. Die Lifestyle-Diskriminierung wird zum Problem, wenn die Transparenz fehlt, d.h., wenn die betroffene Person in einem Persönlichkeitsprofil «eingeschlossen» wird, wobei sie weder das Profil kennt noch den Algorithmus hinterfragen kann, der im Verborgenen die Einteilung vornimmt.⁷¹⁸

Das bestehende Antidiskriminierungsrecht ist nur begrenzt fähig, den Lifestyle-Diskriminierungen zu begegnen.⁷¹⁹ Aufgrund der Gemeinsamkeiten mit den verpönten Merkmalen und weil Andersbehandlungen aufgrund von Lifestyle-Kriterien genauso wie gesetzlich verpönte Diskriminierungen zu ungerechten Behandlungen führen können,⁷²⁰ fragt sich, ob die partiellen Diskriminierungsverbote um weitere Tatbestände, die Lifestyle-Diskriminierungen einschliessen, ergänzt werden sollten.⁷²¹ Es ist eine Wertungsentscheidung des Gesetzgebers, welche Persönlichkeitsmerkmale als verpönte Diskriminierungsmerkmale festgelegt werden und welche legitimen Arbeitgeberinteressen als Rechtfertigungsgründe anerkannt werden.⁷²² Letztlich geht es um die Frage, welche Anpassung den Individuen zugemutet werden soll.⁷²³ Nach der vorliegend vertretenen Ansicht ist zunächst zu untersuchen, ob ein Lifestyle-Diskriminierungsschutz mithilfe des bestehenden Arbeits- und Datenschutzrechts erreicht werden kann (dazu sogleich), bevor die spezialgesetzlichen Diskriminierungstatbestände erweitert werden.

⁷¹⁶ HORNUNG, 93.

⁷¹⁷ Vgl. HORNUNG, 94.

⁷¹⁸ Europarat 2016c, 37. Vgl. White House, Executive Office of the President 2016, 8–9. Sog. «info-strukturelle Diskriminierung»: BURDON/HARPUR, 681; Diskriminierung selbst dann nicht erkennbar, wenn Informationen zur Funktionsweise des Systems und Begründung von Entscheiden vorliegen: HÄNOLD, 150.

⁷¹⁹ Vgl. HÄNOLD, 150. Vgl. WILDHABER *et al.*, 475.

⁷²⁰ HÄNOLD, 150.

⁷²¹ Für die Ausdehnung des Diskriminierungsschutzes über die bekannten «Offline-Kategorien» hinaus: MITTELSTADT, 476.

⁷²² PÄRLI 2009, N 37.

⁷²³ PÄRLI 2009, N 1571.

4.5.2 Arbeitsrechtlicher Diskriminierungsschutz

Gegen Ungleichbehandlungen am Arbeitsplatz kann grundsätzlich der allgemeine arbeitsrechtliche Persönlichkeitsschutz angerufen werden (Art. 328 und 328b OR sowie Art. 336 OR; vgl. auch Art. 2 und 28 ZGB). Aus diesem entspringt ein allgemeines arbeitsrechtliches Diskriminierungsverbot, das Angestellte während des ganzen Arbeitnehmer-Lebenszyklus vor direkter und indirekter⁷²⁴ Diskriminierung schützt.⁷²⁵ Gemäss WILDHABER müssen Algorithmen, die im Bewerbungsverfahren zum Einsatz kommen, so programmiert sein, dass sie Schutz vor direkter und indirekter Anstellungsdiskriminierung bieten.⁷²⁶ Konsequenterweise darf die Programmierung auch in laufenden Arbeitsverhältnissen nicht diskriminieren.⁷²⁷ Das arbeitsrechtliche Diskriminierungsverbot ist allgemeiner Natur, weil es an den Begriff der Persönlichkeit anknüpft, die jedem Menschen eigen ist, und somit nicht (nur) eine bestimmte gesellschaftliche Gruppe vor Diskriminierung schützt.⁷²⁸ Im Rahmen des allgemeinen arbeitsrechtlichen Diskriminierungsverbots gelten insbesondere Vorstrafen, Charaktereigenschaften, das Alter und der Raucherstatus als diskriminierungssensibel.⁷²⁹ Das allgemeine arbeitsrechtliche Diskriminierungsverbot kann somit vor Lifestyle-Diskriminierungen schützen, die die Persönlichkeit verletzen. Tendenziell unzulässig wäre eine nachteilige Behandlung gestützt auf Wearable-Daten, die auf einen unruhigen Schlaf und mögliche Gesundheitsprobleme hinweisen, solange sich dies nicht in der Arbeitsleistung niederschlägt. Nach hier vertretener Ansicht kann das allgemeine arbeits-

⁷²⁴ WILDHABER 2017, 215; PÄRLI 2009, N 1386.

⁷²⁵ PÄRLI 2009, N 1566 und 1594. Auch aus den internationalen Abkommen lässt sich eine Verpflichtung zu umfassendem Diskriminierungsschutz in allen Phasen des privatrechtlichen Arbeitsverhältnisses ableiten: PÄRLI 2009, N 1535. WOLFER, N 173.

⁷²⁶ WILDHABER 2017, 214.

⁷²⁷ WILDHABER *et al.*, 470; KASPER/WILDHABER, 210.

⁷²⁸ PÄRLI 2009, N 1566; WILDHABER *et al.*, 470.

⁷²⁹ Vorstrafen und Charaktereigenschaften: PÄRLI 2009, N 1571; Alter: CHK OR BT 2-EMMEL, Art. 328 OR, N 6. In der Schweiz kommen Diskriminierungen aufgrund des Alters häufiger vor als in Deutschland, Italien, Frankreich und dem europäischen Durchschnitt: PÄRLI 2009, N 84. Raucherstatus: PÄRLI 2009, N 1373. Vgl. zur missbräuchlichen Kündigung wegen einer Krankheit des Arbeitnehmers: CHK OR BT 2-EMMEL, Art. 336 OR, N 3. Weitere, über die Missbrauchstatbestände (Art. 336 OR) hinausgehende Kündigungsmotive, die wegen Verstosses gegen Treu und Glauben (Art. 2 ZGB) missbräuchlich sind: PÄRLI 2009, N 1567. Hingegen toleriert das amerikanische privatrechtliche Arbeitsrecht Diskriminierungen wegen Vorstrafen: AJUNWA/ONWUACHI-WILLIG, 1392, 1394 und 1397.

rechtliche Diskriminierungsverbot jedoch keinen Schutz bieten, wenn sich eine nachteilige Behandlung auf die Browserwahl stützt; dies deshalb, weil der Browser keine Eigenschaft ist, die dem Arbeitnehmer kraft seiner Persönlichkeit zusteht.

Das allgemeine arbeitsrechtliche Diskriminierungsverbot ist vom arbeitsrechtlichen Gleichbehandlungsgrundsatz abzugrenzen.⁷³⁰ Dieser verbietet willkürliche Entscheidungen der Arbeitgeberin, in denen eine den Arbeitnehmer verletzende Geringschätzung seiner Persönlichkeit zum Ausdruck kommt.⁷³¹ Gemäss WOLFER kann es etwa unzulässig sein, einen Arbeitnehmer als Einzigen oder Teil einer Minderheit willkürlich zu überwachen und dadurch schlechter als andere Arbeitnehmer zu stellen.⁷³² Die Geringschätzung kann jedoch nur bestehen, wenn ein Arbeitnehmer gegenüber einer Vielzahl von anderen Arbeitnehmern deutlich ungünstiger gestellt wird, ohne dass hierfür sachliche Gründe vorliegen. Keine solche Geringschätzung ist gegeben, wenn die Arbeitgeberin bloss einzelne Arbeitnehmer willkürlich besserstellt.⁷³³ Der Gleichbehandlungsgrundsatz kommt nur restriktiv und nur bei freiwilligen Leistungen der Arbeitgeberin zur Anwendung.⁷³⁴

4.5.3 Datenschutzinstrumente gegen Diskriminierungen

Es hat sich gezeigt, dass der Geltungsbereich der spezialgesetzlichen Diskriminierungsverbote begrenzt ist⁷³⁵ und dass auch das allgemeine arbeitsrechtliche Diskriminierungsverbot nicht vor allen Lifestyle-Diskriminierungen schützen kann.⁷³⁶ Somit ist es ratsam, über den Tellerrand des Antidiskriminierungsrechts hinauszuschauen und zu fragen, ob der im Arbeitsrecht geltende Datenschutz helfen

⁷³⁰ PÄRLI 2009, N 1572; unklar: «der allgemeine Gleichbehandlungsgrundsatz [...] als individuelles Diskriminierungsverbot»: CHK OR BT 2-EMMEL, Art. 328 OR, N 6.

⁷³¹ BGE 129 III 276 E. 3.1; KASPER/WILDHABER, 210.

⁷³² Vgl. WOLFER, N 174. Wenn die Arbeitgeberin wisse, dass alle ihre Arbeitnehmer während der Arbeit Facebook besuchten, aber nicht interveniere, sei es unangemessen, einen einzelnen Beschäftigten dafür zu bestrafen: RIEDY/WEN, 98.

⁷³³ BGE 129 III 276 E. 3.1; KASPER/WILDHABER, 210.

⁷³⁴ PÄRLI 2009, N 1572. «Einen allgemeinen Gleichbehandlungsgrundsatz kennt das schweizerische Arbeitsrecht nicht, so die wohl herrschende Lehre»: PÄRLI 2009, N 7.

⁷³⁵ Siehe S. 115–120.

⁷³⁶ Siehe S. 121–122.

könnte, die L cher im por sen Diskriminierungsschutz zu stopfen.⁷³⁷ Aus der Kombination von Daten- und Diskriminierungsschutz k nnte ein h herer Schutzstandard resultieren.⁷³⁸

Es ist aus der Warte des Diskriminierungsschutzes positiv, dass das DSG vor Pers nlichkeitsverletzungen im Allgemeinen sch tzt (Art. 1 DSG, Art. 1 E-DSG, Art. 1 rev-DSG) und nicht nur vor Ungleichbehandlungen wegen spezialgesetzlich bestimmter Merkmale. Das DSG findet auf alle Personendaten Anwendung (Art. 3 lit. a DSG, Art. 4 lit. a E-DSG, Art. 5 lit. a rev-DSG). D.h., das DSG reguliert beispielsweise auch die Bearbeitung von personenbezogenen Browserdaten, w hrend die spezialgesetzlichen Diskriminierungsverbote und das allgemeine arbeitsrechtliche Diskriminierungsverbot hier mangelhaft sch tzen.⁷³⁹

F r den Diskriminierungsschutz ist es auch f rderlich, dass die Arbeitgeberin nur Daten  ber den Arbeitnehmer bearbeiten darf, welche einen sachlichen Bezug zur Arbeit aufweisen (Art. 328b Satz 1 OR). Diese Beschr nkung verbietet der Arbeitgeberin, nach Daten  ber den Lifestyle zu fragen, wenn dieser die Arbeit nicht beeinflusst. Auf dieses sog. Frageverbot wird zu einem sp teren Zeitpunkt n her eingegangen.⁷⁴⁰

Zu den datenschutzrechtlichen Instrumenten, die sich f r den Diskriminierungsschutz urbar machen lassen, z hlt weiter das Prinzip von Treu und Glauben (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG). Es verbietet eine algorithmische Diskriminierung, die sich nicht sachlich begr nden l sst.⁷⁴¹ Sodann steht der Grundsatz der Datenrichtigkeit (Art. 5 DSG, Art. 5 Abs. 5 E-DSG, Art. 6 Abs. 5 rev-DSG) der Verwendung von Daten entgegen, die mit falschen Vorurteilen behaftet sind.⁷⁴²

Dem Diskriminierungsschutz kommen auch datenschutzrechtliche Bestimmungen zugute, die auf den fr hzeitigen Pers nlichkeitsschutz (*ex ante*) zielen; sie sind im europ ischen Recht bereits umgesetzt und werden auch in der Schweiz eingef hrt

⁷³⁷ WILDHABER *et al.*, 479.

⁷³⁸ Vorschlag einer «*integrated vision of anti-discrimination and data protection law*»: HACKER, 1143. Siehe auch HACKER, 1171 und 1184, und DAEDELLOW 2018, N 6.

⁷³⁹ Siehe S. 119 und 122.

⁷⁴⁰ Siehe S. 197–199.

⁷⁴¹ Bzgl. Art. 5 Abs. 1 lit. a DSGVO: HACKER, 1172.

⁷⁴² Bzgl. Art. 5 Abs. 1 lit. d DSGVO: HACKER, 1172.

werden.⁷⁴³ Hierzu zählen die Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO; Art. 20 E-DSG, Art. 22 rev-DSG)⁷⁴⁴ und die Pflicht, den Datenschutz von Anfang an in die Technik zu integrieren und die Voreinstellungen datenschutzfreundlich vorzunehmen (Art. 25 DSGVO; Art. 6 E-DSG, Art. 7 rev-DSG). Eine Erweiterung dieser Pflicht zum Datenschutz durch Technikgestaltung (*data protection by design*) könnte einen Diskriminierungsschutz durch Technikgestaltung (*equal treatment by design*) einschliessen.⁷⁴⁵

Die genannten datenschutzrechtlichen Instrumente wirken *de facto* auf den Diskriminierungsschutz hin.⁷⁴⁶ Fraglich ist, ob auch *de jure* ein Diskriminierungsschutz beabsichtigt wird bzw. ob der Gesetzgeber den Diskriminierungsschutz als Zielnorm ins DSG aufnehmen wollte. Es fällt auf, dass das DSG bei der Bearbeitung von Daten zu diskriminierungsrelevanten Tatbeständen einen erhöhten Schutz bietet,⁷⁴⁷ der auch als «informationelles Diskriminierungsverbot» bezeichnet wird:⁷⁴⁸ Bei besonders schützenswerten Personendaten (Art. 3 lit. c DSG, Art. 4 lit. c E-DSG, Art. 5 lit. c rev-DSG) gelten im privatrechtlichen Arbeitsverhältnis die Erfordernisse einer ausdrücklichen Einwilligung (Art. 4 Abs. 5 Satz 2 DSG, Art. 5 Abs. 6 Satz 2 E-DSG, Art. 6 Abs. 7 lit. a rev-DSG), einer Anmeldepflicht (Art. 11a Abs. 3 lit. a DSG), einer Rechtfertigung vor der Bekanntgabe an Dritte (Art. 12 Abs. 2 lit. c DSG, Art. 26 Abs. 2 lit. c E-DSG, Art. 30 Abs. 2 lit. c rev-DSG), einer Informationspflicht (Art. 14 Abs. 1 DSG) und einer ausdrücklichen Strafbewehrung (Art. 35 DSG). Für Persönlichkeitsprofile (Art. 3 lit. d DSG) gelten die gleichen erhöhten Schutzbedingungen.⁷⁴⁹ Nach der hier vertretenen Ansicht sprechen diese Normen dafür, dass das DSG zu einem gewissen Grad auch den Diskriminierungsschutz bezweckt. Im Arbeitskontext muss dies umso mehr gelten, weil zusätzlich (Art. 328b Satz 2 OR) das allgemeine arbeitsrechtliche Dis-

⁷⁴³ Siehe zu den geplanten Änderungen des schweizerischen DSG S. 319–332.

⁷⁴⁴ HACKER, 1171 und 1179.

⁷⁴⁵ Siehe dazu später, S. 320. Vgl. WILDHABER *et al.*, 484.

⁷⁴⁶ WILDHABER *et al.*, 477. «Datenschutz bewirkt Diskriminierungsschutz»: PÄRLI 2009, N 1365. LOCHER, 49; zum deutschen Recht: DORNDORF, 76.

⁷⁴⁷ WILDHABER *et al.*, 479.

⁷⁴⁸ Vgl. zum europäischen Recht (Art. 9 Abs. 1 DSGVO, auch E. 71 Abs. 2, E. 75, E. 85 Satz 1 DSGVO), das Bestimmungen enthält, die im Grundsatz ähnlich sind wie die schweizerischen betreffend besonders schützenswerte Personendaten: DAEDELLOW 2018, N 6. Vgl. ŽLIOBAITE/CUSTERS, 188.

⁷⁴⁹ Hingegen gelten nicht alle der genannten Pflichten für das Profiling (Art. 4 lit. f E-DSG, Art. 5 lit. f–g rev-DSG).

kriminierungsverbot gilt. Somit müsste beispielsweise für die Beurteilung, ob eine Datenbearbeitung verhältnismässig ist (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG), mitberücksichtigt werden, ob daraus diskriminierende Wirkungen für einzelne Arbeitnehmer resultieren.

Trotz der vielversprechenden Ansätze kann das Datenschutzrecht aber nicht überall dort zu Hilfe eilen, wo der Geltungsbereich des Diskriminierungsschutzrechts aufhört.⁷⁵⁰ Ein ausdrückliches generelles Diskriminierungsverbot enthält das DSG nicht. Das Datenschutzrecht orientiert sich mehr an den Bearbeitungsprozessen statt an den (diskriminierenden) Auswirkungen auf die Persönlichkeit der Betroffenen.⁷⁵¹ Diskriminierungsrisiken können auch von anonymisierten Daten ausgehen, die nicht in den Anwendungsbereich des DSG fallen.⁷⁵² Lifestyle-Merkmale gelten nicht als besonders schützenswert – das DSG beschränkt den besonderen Schutz auf Personendaten, die im Wesentlichen die verfassungsrechtlichen Diskriminierungsmerkmale betreffen (Art. 3 lit. c Ziff. 1–4 DSG, Art. 4 lit. c Ziff. 1–6 E-DSG, Art. 5 lit. c Ziff. 1–6 rev-DSG; vgl. Art. 8 Abs. 2 BV). Nicht höchstrichterlich geklärt ist die Anwendbarkeit des DSG, wenn nicht bestimmte Einzelpersonen (vgl. Art. 3 lit. a DSG, Art. 4 lit. a E-DSG, Art. 5 lit. a rev-DSG), sondern Gruppen betroffen sind;⁷⁵³ und gerade um den Schutz von Gruppen geht es bei Diskriminierungen.⁷⁵⁴ Ein potenzieller Kläger bräuchte Informationen zu den Ergebnissen der algorithmischen Auswertung verschiedener Gruppen, um einen Anschein einer Diskriminierung zu etablieren.⁷⁵⁵ Das datenschutzrechtliche Auskunftsrecht ist aber auf die betroffene Person selbst reduziert («Daten über sie», Art. 8 Abs. 1 DSG, Art. 23 Abs. 1 E-DSG, Art. 25 Abs. 1 rev-DSG). Es vermittelt keinen Anspruch auf Bekanntgabe von personenbezogenen Daten über

⁷⁵⁰ KIM 2017, 905.

⁷⁵¹ WILDHABER *et al.*, 487. Siehe dazu auch später ausführlich auf S. 136–140.

⁷⁵² Vgl. KASPER/WILDHABER, 216. Siehe auch S. 88–99.

⁷⁵³ Vgl. zum Phänomen der Typisierungen, bei dem eine Person aufgrund ihrer Gruppenzugehörigkeit auf eine bestimmte Weise behandelt wird: S. 160. Für einen Schutz der Privatsphäre von Gruppen bei Big Data Analytics: MITTELSTADT, 475. **A.M.**, kaum Potenzial für gruppen- und gesellschaftsbezogene Ziele wie Nichtdiskriminierung und Teilhabe in der DSGVO: DREYER/SCHULZ, 9, 10, 40 und 43; Datenschutz-Folgenabschätzung der DSGVO nicht auf Gemeinwohlbelange ausgerichtet: HOFFMANN-RIEM, 64–65; «*individual-oriented understanding of privacy*» in den USA: BAMBERGER/MULLIGAN 2015, 22.

⁷⁵⁴ CUSTERS/URSIC, 338; HORNUNG, 94. Siehe zum Begriff der Diskriminierung S. 89–91.

⁷⁵⁵ WILDHABER *et al.*, 480.

Dritte.⁷⁵⁶ Immerhin aber sollte nach der vorliegend vertretenen Auffassung der Betroffene aggregierte Informationen zur Berechnung von Gruppenwahrscheinlichkeiten, die ihn betreffen, verlangen können.⁷⁵⁷

Insgesamt kann das DSG nicht alle Lücken schliessen, die das Diskriminierungsschutzrecht offen lässt. Jedoch enthält das DSG gewisse Elemente, die zum Schutz vor Diskriminierungen beitragen können. Durch eine Kombination der drei Rechtsgebiete – Diskriminierungsverbote, Arbeitsrecht und Datenschutzrecht – kann der Diskriminierungsschutz weitgehend sichergestellt werden.

4.5.4 Zwischenfazit zum Geltungsbereich des Diskriminierungsschutzrechts

Zusammenfassend dominiert im privatrechtlichen Arbeitsrecht der Grundsatz der Vertragsfreiheit, während das Diskriminierungsschutzrecht ein Schattendasein fristet. Die punktuellen Diskriminierungsverbote bzgl. bestimmter, sog. verpönter Persönlichkeitsmerkmale schützen nicht vor Lifestyle-Diskriminierungen, etwa Diskriminierungen wegen des verwendeten Browsers. Unterstützend können das allgemeine arbeitsrechtliche Diskriminierungsverbot und gewisse Instrumente des Datenschutzrechts einige Lücken des Antidiskriminierungsrechts schliessen. Diskriminierungen können aber nicht gänzlich verhindert werden. Man muss lernen, mit den Diskriminierungsrisiken der Algorithmen am Arbeitsplatz umzugehen. Von der Arbeitgeberin ist ein Bewusstsein zu fordern, dass eine Verletzlichkeit der Arbeitnehmer-Persönlichkeit auch bei Lifestyle-Diskriminierungen bestehen kann.

4.6 Mitwirkungsrecht

Ein besonderes Merkmal des Arbeitsvertrags besteht darin, dass neben individuellen auch Interessen der Belegschaft als Kollektiv auf dem Spiel stehen.⁷⁵⁸ Das MitwG verleiht der Arbeitnehmervertretung ein Informations- und Mitsprache-

⁷⁵⁶ BBl 1988 II, 453; WILDHABER *et al.*, 480. Es besteht grundsätzlich auch kein Anspruch auf Auskunft über Personendaten von Gruppen: WILDHABER *et al.*, 487.

⁷⁵⁷ So auch bzgl. Art. 15 Abs. 1 lit. h DSGVO: HACKER, 1173–1174. Recht auf Auskunft in Form einer Begründung des Scoringergebnisses in einfachen Worten: DAEDELLOW 2018, N 32. Vgl. S. 166.

⁷⁵⁸ Europarat 2016b, 24.

recht in Fragen des Arbeitnehmerschutzes.⁷⁵⁹ Der persönliche Geltungsbereich des MitwG erstreckt sich auf alle privaten Betriebe, die ständig Arbeitnehmer in der Schweiz beschäftigen (Art. 1 MitwG). In sachlicher Hinsicht erfasst das MitwG die gemeinsamen Interessen der Arbeitnehmer (vgl. Art. 8 MitwG). Damit ist bereits gesagt, dass die im MitwG niedergeschriebenen Rechte allgemeiner, kollektiver und nicht individueller Natur sind.⁷⁶⁰ Für (Informations- bzw. Auskunfts-) Ansprüche zum konkreten Arbeitsverhältnis muss sich der Arbeitnehmer auf den Einzelarbeitsvertrag stützen.⁷⁶¹

4.7 Strafrecht

Wenn People Analytics den Geheim- oder Privatbereich im strafrechtlichen Sinn betrifft, sind die entsprechenden Straftatbestände (Art. 179 ff. StGB) zu prüfen. Eine Strafbarkeit wegen Ungehorsams gegen amtliche Verfügungen ist zudem denkbar, wenn die Arbeitgeberin einer Verfügung des Arbeitsinspektorats (Art. 292 StGB i.V.m. Art. 51 Abs. 2 ArG) nicht Folge leistet.

Zu beachten sind auch die Tatbestände des Nebenstrafrechts (vgl. Art. 333 Abs. 1 StGB). Im Datenschutzrecht sind die Verletzung der Auskunfts-, Melde- und Mitwirkungspflichten (Art. 34 DSG, Art. 54 E-DSG, Art. 60 rev-DSG) und die Verletzung der beruflichen Schweigepflicht (Art. 35 DSG, Art. 56 E-DSG, Art. 62 rev-DSG) unter Strafe gestellt. Die Arbeitgeberin ist strafbar, wenn sie den Vorschriften über den Gesundheitsschutz, beispielsweise dem Verbot der Verhaltensüberwachung (Art. 26 ArGV 3), vorsätzlich oder fahrlässig zuwiderhandelt (Art. 59 Abs. 1 lit. a ArG). Denkbar ist auch eine strafrechtliche Verantwortlichkeit des Arbeitnehmers, der ein People Analytics-System bedient (Art. 60 ArG). Sind genetische Daten Gegenstand von People Analytics, erlangen die Straftatbestände sowohl der genetischen Untersuchung ohne Zustimmung (Art. 36 GUMG) oder ohne Bewilligung (Art. 37 GUMG) als auch der Missbräuche im Arbeitsbereich (Art. 39 i.V.m. Art. 21 GUMG) Bedeutung. Dagegen scheidet eine strafbare unlautere Wettbewerbshandlung aus.⁷⁶²

⁷⁵⁹ Siehe S. 101–105.

⁷⁶⁰ Bzgl. des Informationsrechts: FRITZ/SCHULER, 38–39; bzgl. des Mitspracherechts: FRITZ/SCHULER, 48. Vgl. MÜLLER, 358.

⁷⁶¹ FRITZ/SCHULER, 39.

⁷⁶² Wettbewerbsrechtlich nicht strafbar ist die Nichteinhaltung von Arbeitsbedingungen (Art. 7 UWG i.V.m. Art. 23 Abs. 1 UWG *e contrario*). Die Personalabwerbung, etwa

4.8 Europäische Menschenrechtskonvention und Verfassungsrecht

Das Völkerrecht ist (neben den Bundesgesetzen) für das Bundesgericht und die anderen rechtsanwendenden Behörden massgebend (Art. 190 BV, vgl. Art. 5 Abs. 4 BV). Die EMRK statuiert ein Menschenrecht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK). Nach der Rechtsprechung des EGMR kann der Begriff «Privatleben» auch berufliche Tätigkeiten umfassen.⁷⁶³ Als Vertragspartei der EMRK ist die Schweiz verpflichtet, das Recht auf Achtung des Privatlebens auch im Verhältnis zwischen Arbeitnehmer und privater Arbeitgeberin zu schützen.⁷⁶⁴

Auf Stufe der verfassungsrechtlichen Grundrechte gilt es, erstens, den Anspruch auf Schutz vor Missbrauch der persönlichen Daten umzusetzen (Art. 13 Abs. 2 BV). Nach verbreiteter Auffassung geht dieses Recht über die alleinige Abwehr von Missbräuchen hinaus und vermittelt einen umfassenden Anspruch auf Datenschutz bis hin zu einem Recht auf informationelle Selbstbestimmung.⁷⁶⁵ Diese verbreitete Meinung wird vorliegend später noch hinterfragt werden.⁷⁶⁶ Zweitens existiert der Anspruch auf Achtung des Privat- und Familienlebens, der Wohnung sowie des Brief-, Post- und Fernmeldeverkehrs (Art. 13 Abs. 1 BV). Die beiden Ansprüche werden unter der Bezeichnung «Schutz der Privatsphäre» zusammen-

mittels Active Sourcing (dazu S. 44), fällt unter die Grundsatzbestimmung (Art. 2 UWG), nicht unter den Tatbestand der Verleitung zum Vertragsbruch (Art. 4 lit. a UWG), und ist somit nicht strafbar (Art. 23 Abs. 1 UWG *e contrario*): BSK UWG-FRICK, Art. 4 lit. a–c UWG, N 33.

⁷⁶³ Urteil EGMR vom 05.09.2017, *Bărbulescu vs. Romania*, Nr. 61496/08, E. 71.

⁷⁶⁴ Indirekte Horizontalwirkung der EMRK: SGK-SCHWEIZER, Art. 35 BV, N 62; KÄLIN/KÜNZLI, N 12.59. Vgl. Schutzpflichten aus Völkerrecht: PÄRLI 2005, 228. Vgl. GRABENWARTER, Art. 8 EMRK N 82. Vgl. GRABENWARTER/PABEL, N 56. Bei der Erfüllung der positiven Verpflichtungen aus Art. 8 EMRK stehe den Staaten ein Ermessensspielraum zu: MOWBRAY, 588–589.

⁷⁶⁵ SGK-SCHWEIZER, Art. 13 Abs. 2 BV, N 72, m.w.H.; BSK DSG-MAURER-LAMBROU/KUNZ, Art. 1 DSG, N 5; MEIER PHILIPPE, N 17; GERSCHWILER *et al.*, N 3.10; BELSER 2011a, § 6 N 61 und 88. Der europäische Art. 8 GrCh umschreibe den Gehalt des schweizerischen Art. 13 Abs. 2 BV treffend: RUDIN 2010, 130–131. Vgl. RUDIN 2008, 7. Die Botschaft zur Bundesverfassung spricht nicht von einer Abwehr von Missbräuchen, sondern von einem «Anspruch auf Datenschutz»: BBl 1997 I, 153. – A.M. GÄCHTER/EGLI: Art. 13 Abs. 2 BV sei restriktiv auszulegen und ver helfe bloss zu einem Recht, «allein gelassen zu werden».

⁷⁶⁶ Siehe S. 137–138 und S. 263–273.

gefasst (Marginalie zu Art. 13 BV).⁷⁶⁷ Der verfassungsrechtliche Schutz der Privatsphäre entspricht inhaltlich Art. 8 Abs. 1 EMRK in bewusster Übereinstimmung, auch im Hinblick auf die Einschränkung des Grundrechts (Art. 8 Abs. 2 EMRK; Art. 13 i.V.m. Art. 36 BV).⁷⁶⁸ Parallel zum Grundrecht auf Schutz der Privatsphäre ist dasjenige auf persönliche Freiheit zu prüfen (Art. 10 Abs. 2 BV).⁷⁶⁹ Auch eine Prüfung der Grundrechte auf Rechtsgleichheit (Art. 8 BV, etwa bei Diskriminierungen) und Menschenwürde (Art. 7 BV) ist unumgänglich. Die Grundrechte müssen in der ganzen Rechtsordnung zur Geltung kommen (Art. 35 Abs. 1 BV), so auch im vorliegend interessierenden Bereich des Privatrechts. Die Behörden sorgen dafür, dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden (Art. 35 Abs. 3 BV). Die Horizontalwirkung der Grundrechte entfaltet sich namentlich, wenn unter Privaten ein erhebliches Machtgefälle besteht.⁷⁷⁰ Dies trifft auf People Analytics zu.⁷⁷¹ Somit sind die vorstehend genannten Rechtsquellen, insbesondere die offen formulierten Normen wie die Fürsorgepflicht (Art. 328 OR), im Sinne der verfassungsrechtlichen Grundrechte auszulegen und anzuwenden.⁷⁷²

4.9 Weiteres Völkerrecht

Die Schweiz hat das Übereinkommen 108 des Europarats ratifiziert. Das Übereinkommen 108 ist der erste verbindliche, aber nicht unmittelbar anwendbare völker-

⁷⁶⁷ Aber eingehend zur Unterscheidung von Abs. 1 und Abs. 2 von Art. 13 BV: S. 136–138.

⁷⁶⁸ SGK-BREITENMOSER, Art. 13 Abs. 1 BV, N 2–3.

⁷⁶⁹ SGK-BREITENMOSER, Art. 13 Abs. 1 BV, N 4; GÄCHTER, 188; Art. 13 Abs. 2, Art. 13 Abs. 1 und Art. 10 Abs. 2 BV seien getrennt zu prüfen: BELSER 2011a, § 6 N 164.

⁷⁷⁰ SGK-SCHWEIZER, Art. 35 BV, N 48.

⁷⁷¹ Siehe S. 79. Eine Gefahr für die informationelle Selbstbestimmung geht zunehmend von datenbearbeitenden Arbeitgebern aus: BELSER 2011a, § 6 N 110. Diese Autorin geht so weit, aus Art. 13 Abs. 2 BV eine unmittelbare Horizontalwirkung abzuleiten, die staatliche und private Akteure gleichermassen verpflichte, «ähnlich wie Art. 8 Abs. 2 Satz 3 BV»: BELSER 2011a, § 6 N 171.

⁷⁷² WOLFER, N 20; BELSER 2011a, § 6 N 112; arbeitsvertraglicher Persönlichkeitsschutz als «legitimes Einfallstor» für die Grundrechte im Arbeitsverhältnis: PÄRLI 2005, 227; SGK-SCHWEIZER, Art. 35 BV, N 56. Vgl. SGK-SCHWEIZER, Art. 13 Abs. 2 BV, N 84. Schliessung von Gesetzeslücken: SGK-SCHWEIZER, Art. 35 BV, N 60.

rechtliche Vertrag zum Datenschutz.⁷⁷³ Die Vertragsparteien verpflichten sich, das Übereinkommen auf automatisierte Dateien und Datensammlungen sowie automatische Bearbeitungen von personenbezogenen Daten im öffentlichen und im privaten Bereich anzuwenden (Art. 3 Abs. 1 Übereinkommen 108). Das Übereinkommen 108 ist am 18.05.2018 modernisiert worden (CM/Inf(2018)15-final). Zur Ratifikation des modernisierten Übereinkommens 108 sind ein entsprechender Bundesbeschluss und die Revision des DSG erforderlich.⁷⁷⁴ Die Ratifikation ist ein wichtiges Signal an die EU im Hinblick auf den Entscheid über den Angemessenheitsbeschluss (vgl. Art. 45 DSGVO).⁷⁷⁵

Gemäss dem Internationalen Pakt über bürgerliche und politische Rechte vom 16.12.1966 (SR 0.103.2), dem die Schweiz beigetreten ist, darf niemand willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden (Art. 17 Abs. 1 IPBPR). Bemerkenswert ist, dass eine Begrenzungsklausel (wie Art. 36 BV und Art. 8 Abs. 2 EMRK) fehlt.⁷⁷⁶ Zudem erwähnt der IPBPR ausdrücklich eine positive Verpflichtung des Staats zum Schutz der datenschutzrechtlichen Positionen zwischen Privaten (in Art. 17 Abs. 2 IPBPR).⁷⁷⁷ Die Verbindlichkeit des IPBPR ist insoweit gewährleistet, als der UNO-Menschenrechtsausschuss über seine Einhaltung wacht (vgl. Art. 28 ff., Art. 40 ff. IPBPR). Individualbeschwerden gegen einen Vertragsstaat sind nach dem ersten Fakultativprotokoll zum IPBPR möglich; die Schweiz hat dieses jedoch nicht unterzeichnet.

Ferner ist auf die Dokumente der OECD und der IAO zu verweisen. Die OECD-Leitlinien 1980 zum Schutz der Privatsphäre und zum grenzüberschreitenden Datenverkehr sind völkerrechtlich nicht verbindlich.⁷⁷⁸ Sie gründen primär auf einem

⁷⁷³ SCHIEDERMAIR, 316 und 325. Vgl. Art. 4 Abs. 1 Übereinkommen 108. «Völkerrechtlich verbindlich»: Europarat, Vertragsbüro, Details zum Vertrag-Nr. 108, abrufbar unter <www.coe.int> (besucht am 18.05.2018); «*not self-executing*»: TAMÒ-LARRIEUX, 76, m.w.H.

⁷⁷⁴ Der Nationalrat hat als Erstrat in der Frühjahrssession 2020 den entsprechenden Bundesbeschluss angenommen: AB NR 2020, 279. Die Abstimmung im Ständerat ist noch ausstehend (Stand 31.05.2020).

⁷⁷⁵ AB NR 2020, 279.

⁷⁷⁶ GRABENWARTER, 2.

⁷⁷⁷ GRABENWARTER, 2; KÄLIN/KÜNZLI, N 12.59.

⁷⁷⁸ NEUNHOEFFER, 46; SCHIEDERMAIR, 150; blosser Empfehlungscharakter: BBl 2017, 6968.

wirtschaftlichen Ansatz, während das Übereinkommen 108 und der IPBPR menschenrechtlich motiviert sind.⁷⁷⁹ Sie sind durch die OECD-Leitlinien 2013 revidiert worden. Die IAO hat das Übereinkommen 111 über die Diskriminierung in Beschäftigung und Beruf verabschiedet, welches die Schweiz ratifiziert hat. Es ist davon auszugehen, dass das Übereinkommen 111 keine unmittelbar anwendbaren Bestimmungen enthält, auf die sich Einzelpersonen berufen könnten.⁷⁸⁰ Zudem hat die IAO einen Verhaltenskodex zum Schutz der personenbezogenen Daten der Arbeitnehmer (*Code of practice on the protection of workers' personal data*, Genf, 1997).

4.10 Zwischenfazit: Querschnittsmaterie People Analytics

In diesem Kapitel wurden nur die wichtigsten Erlasse, die bei People Analytics zu berücksichtigen sind, aufgezählt. Zusammenfassend sind auf People Analytics nationale und internationale, privat- und öffentlich-rechtliche Bestimmungen sowie Individual- und Kollektivrechte kumulativ anwendbar. Die erwähnten Erlasse können nicht isoliert voneinander betrachtet werden; erst durch ihre Wechselwirkung entsteht ein echter Schutz der arbeitnehmerseitigen Interessen.⁷⁸¹ Beispielsweise werden bei internationalen Sachverhalten datenschutzfreie Bereiche verhindert, indem neben dem DSG auch die DSGVO und nationale Bestimmungen der Mitgliedstaaten der EU betreffend Beschäftigtendaten für anwendbar erklärt werden.⁷⁸² Des Weiteren garantieren die gesetzlichen Diskriminierungsverbote allein noch keinen effektiven Schutz vor algorithmischen Diskriminierungen; aber in Kombination mit dem Arbeitsrecht und dem Datenschutzrecht können die Schutzlücken weitgehend geschlossen werden.⁷⁸³ Somit handelt es sich bei People Analytics um eine komplexe Querschnittsmaterie, deren Bewältigung ein hohes Mass

⁷⁷⁹ SCHIEDERMAIR, 317.

⁷⁸⁰ Das Bundesgericht hat die unmittelbare Anwendbarkeit der durch die Schweiz ratifizierten anderen IAO-Übereinkommen Nr. 87, 98 und 154 verneint: BGE 144 I 50 E. 5.1; BGE 132 III 122 E. 3.2.2.1. A.M. PÄRLI 2009, N 230: Es sei «nicht abschliessend deutlich», ob das Übereinkommen 111 direkt anwendbar sei oder ob es nur den Staat zu einer völkerrechtsfreundlichen Auslegung der Grundrechte verpflichte.

⁷⁸¹ Art.-29-Datenschutzgruppe 2001, 4. Vgl. DANKERT, 161: Big Data ist «keinesfalls nur ein Datenschutzproblem».

⁷⁸² Siehe S. 108–114.

⁷⁸³ Siehe S. 115–126.

an Fachwissen voraussetzt. Nur wer sich mit allen genannten Bestimmungen auskennt, kann People Analytics (als Arbeitgeberin) rechtskonform anwenden oder sich (als Arbeitnehmer) wirksam gegen unzulässige Praktiken wehren. Im Folgenden sind diese Bestimmungen näher zu betrachten. Zuerst werden die datenschutzrechtlichen Rahmenbedingungen geprüft, welche die Arbeitgeberin einhalten muss (dazu sogleich, Kapitel 5, S. 133–250), bevor auf die Möglichkeiten der Arbeitnehmer zur Rechtsdurchsetzung eingegangen wird (dazu später, Kapitel 6, S. 251–293).

5 **Datenschutzrechtliche Rahmenbedingungen**

5.1 **Übersicht**

Ausgehend von den verschiedenen für People Analytics relevanten Rechtsnormen, die in Kapitel 4 dargelegt worden sind, ist nun auf das Datenschutzrecht (DSG, aber auch Art. 328b OR und Art. 26 ArGV 3) näher einzugehen, weil es den Persönlichkeitsschutz (Art. 28 ZGB, Art. 328 OR) in Bezug auf Datenbearbeitungen konkretisiert. Hierbei sind zunächst einige übergeordnete Überlegungen zum Aufbau und Zweck des DSG anzustellen (dazu sogleich, Unterkapitel 5.2–5.3, S. 133–154). Diese Ausgangsdiskussion wird helfen, die übrigen Rechtsbestimmungen im Kontext von People Analytics richtig und angemessen zu verstehen und auszulegen.

Danach ist der Geltungsbereich des DSG abzustecken (Unterkapitel 5.4, S. 154–173), und auf die wichtigsten Bearbeitungsregeln ist einzugehen (Unterkapitel 5.5–5.9, S. 173–212). Big Data fordert insbesondere die Gebote der Zweckbindung, Erkennbarkeit und Richtigkeit sowie die aus dem Verhältnismässigkeitsprinzip fließenden Pflichten der Datenminimierung, Speicherbegrenzung und Datenlöschung heraus,⁷⁸⁴ die in dieser Reihenfolge vorliegend besprochen werden. Falls die Bearbeitungsregeln verletzt werden, ist zu klären, welche Rechtfertigungsmöglichkeiten hierfür bestehen (Unterkapitel 5.10, S. 212–242). Schliesslich ist zu fragen, ob sich die Betriebspraxis bei der Anwendung von People Analytics tatsächlich an die datenschutzrechtlichen Rahmenbedingungen hält (Unterkapitel 5.11, S. 242–247).

5.2 **Aufbau des Datenschutzgesetzes**

Das DSG nimmt eine Sonderstellung unter den Bundeserlassen ein, weil es ein Einheitsgesetz aus öffentlichem und privatem Recht ist.⁷⁸⁵ Im vorliegend interessierenden privaten Bereich zielt es primär auf den Schutz der Persönlichkeit beim Informationsaustausch unter Privaten, während im öffentlich-rechtlichen Bereich der Schutz der Grundrechte bei Handlungen staatlicher Behörden im Vordergrund

⁷⁸⁴ Vgl. Europarat 2017, 1.

⁷⁸⁵ BSK DSG-MAURER-LAMBROU/KUNZ, Art. 1 DSG, N 4.

steht (vgl. Art. 1 DSG, Art. 1 E-DSG, Art. 1 rev-DSG).⁷⁸⁶ Das DSG enthält zunächst Bestimmungen, die generell gelten (Art. 1–11a DSG, Art. 1–25 E-DSG, Art. 1–13 und Art. 16–29 rev-DSG), und anschliessend solche, die nur für das Bearbeiten von Personendaten entweder durch private Personen (Art. 12–15 DSG, Art. 26–28 E-DSG, Art. 30–32 rev-DSG) oder durch Bundesorgane gelten (Art. 16–25^{bis} DSG, Art. 29–38 E-DSG, Art. 33–42 rev-DSG).⁷⁸⁷ Schliesslich folgen sowohl die Bestimmungen über die Aufsicht als auch die Strafbestimmungen (Art. 26–35 DSG, Art. 39–60 E-DSG, Art. 43–66 rev-DSG).

In dem generell geltenden Teil werden zuerst der Zweck des DSG, der Geltungsbereich und die wichtigsten Begriffe erklärt (Art. 1–3 DSG, Art. 1–4 E-DSG, Art. 1–5 rev-DSG). Sodann statuiert das DSG allgemeine Rechtsgrundsätze und spezifische Datenbearbeitungsregeln. Zu den allgemeinen Rechtsgrundsätzen zählen die Rechtmässigkeit (Art. 4 Abs. 1 DSG, Art. 5 Abs. 1 E-DSG, Art. 6 Abs. 1 rev-DSG), das Handeln nach Treu und Glauben und die Verhältnismässigkeit (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG). Die spezifischen Datenbearbeitungsregeln umfassen die Zweckbindung (Art. 4 Abs. 3 DSG, Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG), die Erkennbarkeit (Art. 4 Abs. 4 DSG, Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG) und die Voraussetzungen für eine gültige Einwilligung (Art. 4 Abs. 5 DSG, Art. 5 Abs. 6 E-DSG, Art. 6 Abs. 6–7 rev-DSG).⁷⁸⁸ Zusätzlich gelten die Grundsätze der Richtigkeit (Art. 5 DSG, Art. 5 Abs. 5 E-DSG, Art. 6 Abs. 5 rev-DSG) und Datensicherheit (Art. 7 DSG, Art. 7 E-DSG, Art. 8 rev-DSG) und die Bestimmungen zum Auskunftsrecht (Art. 8–10 DSG, Art. 23–25 E-DSG, Art. 25–27 rev-DSG), ebenso die Vorschriften zu Zertifizierungsverfahren (Art. 11 DSG, Art. 12 E-DSG, Art. 13 rev-DSG) und zum Register der Datensammlungen (Art. 11a DSG, vgl. Art. 11 E-DSG, vgl. Art. 12 rev-DSG).

Für das vorliegend zu untersuchende Bearbeiten durch private Personen spezifiziert das DSG, wann von einer Persönlichkeitsverletzung auszugehen ist (Art. 12 DSG, Art. 26 E-DSG, Art. 30 rev-DSG) und wann eine solche gerechtfertigt wer-

⁷⁸⁶ BSK DSG-MAURER-LAMBROU/KUNZ, Art. 1 DSG, N 6.

⁷⁸⁷ Auch bei den aufsichtsrechtlichen und strafrechtlichen Bestimmungen (Art. 26–35 DSG, Art. 39–60 E-DSG, Art. 43–66 rev-DSG) ist diese Zweiteilung erkennbar (für Bundesorgane: Art. 27 DSG; für Private: Art. 28–29, Art. 34 DSG. – Vgl. im Wortlaut des totalrevidierten DSG: Art. 3, Art. 43, Art. 52, Art. 54 E-DSG bzw. Art. 4, Art. 49, Art. 58, Art. 60 rev-DSG).

⁷⁸⁸ Zur Unterscheidung zwischen den allgemeinen Rechtsgrundsätzen und den spezifischen Datenbearbeitungsregeln: SHK DSG-BAERISWYL, Art. 4 DSG, N 1.

den kann (Art. 13 DSG, Art. 27 E-DSG, Art. 31 rev-DSG). Zudem gelten bestimmte Informationspflichten für Private Datenbearbeiter (Art. 14 DSG, vgl. Art. 17 E-DSG, vgl. Art. 19 rev-DSG), und die Rechtsansprüche richten sich nach dem Persönlichkeitsschutz des ZGB (Art. 15 DSG, Art. 28 E-DSG, Art. 32 rev-DSG).

5.3 Zweck des Datenschutzgesetzes

5.3.1 Zwei Aspekte des Zweckartikels des Datenschutzgesetzes

a) Schutz vor Persönlichkeitsrisiken

Der Datenschutz bezweckt in privatrechtlichen Rechtsverhältnissen den Schutz der Persönlichkeit (Art. 1 DSG, Art. 1 E-DSG, Art. 1 rev-DSG). Der Datenschutz will somit nicht die Daten schützen, sondern die betroffenen Personen.⁷⁸⁹ So verstanden verhält es sich wie beim Regenschutz, der den Träger und nicht den Regen schützt. Die Ausrichtung auf den Schutz der betroffenen Personen bedeutet, dass das DSG die Risiken und allfälligen negativen Auswirkungen von Datenbearbeitungen auf den Menschen minimieren will. Das DSG enthält deshalb einige risikoorientierte Normen.

Die Orientierung am Risiko zeigt sich insbesondere bei den übergeordneten allgemeinen Rechtsgrundsätzen des DSG.⁷⁹⁰ Zum einen beinhaltet der Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG) das Gebot der schonenden Rechtsausübung.⁷⁹¹ Danach muss ein Berechtigter für den Fall, dass er von seinem Recht ohne Nachteil auf verschiedene Arten Gebrauch machen kann, diejenige Art der Rechtsausübung wählen, die für den Verpflichteten am wenigsten schädlich ist.⁷⁹² Entscheidend für die Einhaltung von Treu und Glauben ist somit eine möglichst geringe negative Aussenwirkung. Zum andern verlangt das Verhältnismässigkeitsprinzip (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG), dass eine Datenbearbeitung geeignet, er-

⁷⁸⁹ BSK DSG-MAURER-LAMBROU/KUNZ, Art. 1 DSG, N 3; MEIER PHILIPPE, N 326.

⁷⁹⁰ Zum Verhältnis zwischen den allgemeinen Rechtsgrundsätzen und den spezifischen Datenbearbeitungsregeln siehe S. 134.

⁷⁹¹ BSK ZGB I-HONSELL, Art. 2 ZGB, N 22. Wohl **a.M.**, das Verhältnismässigkeitsprinzip konkretisiere den allgemeinen Rechtsgrundsatz der schonenden Rechtsausübung: WOLFER, N 204.

⁷⁹² Vgl. BGE 131 III 459 E. 5.3.

forderlich und für den Betroffenen zumutbar sein muss. Bei der Prüfung der Zumutbarkeit (Verhältnismässigkeit im engeren Sinne) sind die Interessen der Arbeitgeberin und des Arbeitnehmers abzuwägen.⁷⁹³ Mit anderen Worten ist der Eingriffszweck der Eingriffswirkung gegenüberzustellen. Daraus ergibt sich, dass die Verhältnismässigkeitsprüfung wirkungs- und risikoorientiert ist.

Die Risikoorientierung wird unter dem rev-DSG beibehalten werden und zunehmen. Beispielsweise wird eine Datenschutz-Folgenabschätzung erforderlich sein, wenn voraussichtlich «ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person» von der Datenbearbeitung ausgeht (Art. 20 Abs. 1 Satz 1 E-DSG, Art. 22 Abs. 1 Satz 1 rev-DSG; vgl. auch Art. 35 Abs. 1 Satz 1 DSGVO). Im ausländischen Schrifttum zeichnen sich weitere Bestrebungen hin zur Risikoorientierung ab.⁷⁹⁴

Die Risikoorientierung des DSG ist nicht unumstritten. Zumindest hinsichtlich des öffentlich-rechtlichen Bereichs des DSG wird kritisiert, dass die Normen teilweise «konturlos» seien.⁷⁹⁵ Insbesondere ist der Wunsch nach einer Konkretisierung des datenschutzrechtlichen Verhältnismässigkeitsprinzips an den Gesetzgeber geäussert worden.⁷⁹⁶ Auch mit Blick auf das privatrechtliche Datenschutzrecht bleiben die Grundsätze von Treu und Glauben und der Verhältnismässigkeit recht abstrakt. Der zweite Aspekt des DSG-Zweckartikels kann dieser Kritik begegnen, wie so gleich aufgezeigt wird.

b) Regelung der Datenbearbeitungsprozesse

Die Feststellung, dass das DSG den Schutz vor Risiken für die Persönlichkeit bezweckt, kann nicht vollends befriedigen. Wenn allein der Persönlichkeitsschutz

⁷⁹³ Vgl. HOFFMANN-RIEM, 57–58.

⁷⁹⁴ In Europa wird für «hochriskante» Ableitungen aus Analysen (*high-risk inferential analytics*) ein Recht auf angemessene Schlussfolgerungen (*right to reasonable inferences*) gefordert: WACHTER/MITTELSTADT, 617–618. In den USA erkennen PALFREY und GASSER das Risiko, das in der Interoperabilität liegt, und entwerfen eine Theorie, die hilft, das optimale Mass der Vernetzung von Datenquellen zu finden und zu verwirklichen: PALFREY/GASSER 2012, 3. Siehe zum Begriff der Interoperabilität S. 74–75.

⁷⁹⁵ RUDIN 2010, 137. Vgl. RUDIN 2004b, 433.

⁷⁹⁶ RUDIN 2010, 138; SCHWEIZER, N 1.66.

erstrebt würde, der privatrechtlich bereits durch Art. 28 ZGB und Art. 328 OR abgesichert ist, käme die Frage auf: Könnte man nicht auf das DSG verzichten?⁷⁹⁷

Das DSG hat aber seine Daseinsberechtigung. Diese ist auf einen weiteren Begriff mit eigenständiger Bedeutung im Zweckartikel zurückzuführen: denjenigen der Datenbearbeitung (vgl. Art. 1 DSG, Art. 1 E-DSG, Art. 1 rev-DSG).⁷⁹⁸ Dieser Terminus bezieht sich nicht (direkt) auf die Persönlichkeit des Betroffenen, sondern auf die «Daten» selbst (vgl. Art. 3 lit. a DSG, Art. 4 lit. a E-DSG, Art. 5 lit. a rev-DSG) und auf die «Bearbeitungs»-Prozesse, die bei der Datenanalyse ablaufen (vgl. Art. 3 lit. e DSG, Art. 4 lit. d E-DSG, Art. 5 lit. d rev-DSG). Der Mehrwert des Datenschutzrechts besteht somit auch darin, dass es die Bedeutung des Persönlichkeitsschutzes im Zusammenhang mit der Informationsbearbeitung genauer umschreibt bzw. konkretisiert, welche Arten der Datenbearbeitung die Persönlichkeit gefährden können.⁷⁹⁹ Dies bedeutet eine Erweiterung des allgemeinen Persönlichkeitsschutzes (Art. 28 ZGB).⁸⁰⁰

Die Interpretation, dass Art. 1 DSG (bzw. Art. 1 E-DSG bzw. Art. 1 rev-DSG) zwei Aspekte der Zwecksetzung enthält (Schutz vor Persönlichkeitsrisiken einerseits, Regelung der Bearbeitungsprozesse andererseits), kann verfassungsrechtlich hergeleitet werden. Das Bundesgericht betrachtet zwar den verfassungsrechtlichen Datenschutz (Art. 13 Abs. 2 BV) als Teilgehalt des Schutzes der Privatsphäre (Art. 13 Abs. 1 BV), so wie dies auch die Marginalie des Art. 13 BV suggeriert.⁸⁰¹ Es hat sich aber, soweit ersichtlich, noch nicht vertieft mit dem Verhältnis der beiden Absätze von Art. 13 BV zueinander befasst.⁸⁰² GÄCHTER und EGLI sowie BELSER grenzen das Recht auf Schutz vor Missbrauch persönlicher Daten (Art. 13 Abs. 2 BV) vom Recht auf Schutz der Privatsphäre (Art. 13 Abs. 1 BV) und vom Schutz der persönlichen Freiheit (Art. 10 Abs. 2 BV) ab.⁸⁰³ Die beiden letztge-

⁷⁹⁷ Der Autor dankt Herrn Dr. iur. David Vasella, Rechtsanwalt, für das Aufwerfen dieser Frage und die inspirierende Diskussion darüber.

⁷⁹⁸ Vgl. BSK DSG-MAURER-LAMBROU/KUNZ, Art. 1 DSG, N 3.

⁷⁹⁹ BBl 1988 II, 438; HK-ROSENTHAL/JÖHRI, Art. 1 DSG, N 2.

⁸⁰⁰ BELSER 2011c, § 2 N 43.

⁸⁰¹ BGE 128 II 259 E. 3.2; so auch die Botschaft zur BV: BBl 1997 I, 153; ebenso BSK DSG-MAURER-LAMBROU/KUNZ, Art. 1 DSG, N 5. Siehe zu den anwendbaren Grundrechten: S. 128.

⁸⁰² Gleicher Meinung: GÄCHTER, 186.

⁸⁰³ GÄCHTER/EGLI, N 64 und 78; BELSER 2011a, § 6 N 57, 121, 168 und 174. Die Autoren beziehen sich zwar auf das öffentlich-rechtliche Datenschutzrecht. Doch müssen ihre verfassungsrechtlichen Überlegungen aufgrund der indirekten Drittwirkung der

nannten Grundrechte schützen ein (vorliegend auf Informationen bezogenes) Verhalten und erfordern Interessenabwägungen im Einzelfall, woraus Unsicherheit und Unberechenbarkeit bzgl. des Gehalts der Grundrechte resultieren können.⁸⁰⁴ Das erstgenannte Grundrecht reguliert dagegen die Daten, verkörpert eine «strukturelle Garantie» und ist nicht ein Element materieller Interessenabwägung.⁸⁰⁵ Es ist «prozedural angelegt» und stellt ähnlich wie die Verfahrensgarantien (Art. 29 BV) Anforderungen an das formelle (Verfahrens- und Organisations-)Recht.⁸⁰⁶ Das verfassungsrechtliche Datenschutzrecht ist in diesem Sinn ein «Datenverkehrsrecht», das dem Persönlichkeitsschutz dient.⁸⁰⁷ So wie die Verfassungsrechtler zwischen Abs. 1 und 2 von Art. 13 BV unterscheiden, werden vorliegend auf Gesetzesstufe zwei verschiedene Aspekte in der Zwecksetzung in Art. 1 DSG (bzw. Art. 1 E-DSG bzw. Art. 1 rev-DSG) gelesen.

In Erfüllung des Auftrags, die Bearbeitungsprozesse zu regulieren, statuiert das DSG überwiegend prozessorientierte Normen. Die Bestimmungen des DSG drehen sich um die Daten und das Verfahren der Beschaffung, Analyse und Löschung von Daten:⁸⁰⁸ Auf diese Weise werden etwa Kategorien von Daten definiert (Art. 3 lit. a und c DSG, Art. 4 lit. a und c E-DSG, Art. 5 lit. a und c rev-DSG) und Grundsätze der Bearbeitung statuiert (Art. 4 ff. DSG, Art. 5 ff. E-DSG, Art. 6 ff. rev-DSG). Von einer Persönlichkeitsverletzung geht das DSG aus, wenn formelle Verhaltensrichtlinien übertreten werden, etwa durch den Verstoss gegen die genannten Bearbeitungsgrundsätze, durch eine Bearbeitung gegen den ausdrücklichen Willen des Betroffenen oder durch Bekanntgabe besonders schützenswerter Personendaten oder Persönlichkeitsprofile (Art. 12 Abs. 2 lit. a–c DSG, Art. 26 Abs. 2 lit. a–c E-DSG, Art. 30 Abs. 2 lit. a–c rev-DSG).

Die gleiche Feststellung, dass sich das Datenschutzrecht mehrheitlich mit den Bearbeitungsprozessen beschäftigt, gilt auch im internationalen Umfeld hinsichtlich

Grundrechte (Art. 35 Abs. 1 und 3 BV) auch für das privatrechtliche Datenschutzrecht massgebend sein (vgl. S. 129).

⁸⁰⁴ GÄCHTER/EGLI, N 299.

⁸⁰⁵ GÄCHTER/EGLI, N 299. Vgl. BELSER 2011a, § 6 N 120.

⁸⁰⁶ GÄCHTER, 185; BELSER 2011a, § 6 N 120.

⁸⁰⁷ GÄCHTER/EGLI, N 26; GÄCHTER, 185. Vgl. die Forderung, dass der Datenschutz den Informationsfluss als solchen regeln müsse: WILDHABER *et al.*, 483–484. Relevant sei die «Datenverarbeitung als Prozess»: ALBERS, 607.

⁸⁰⁸ Vgl. WILDHABER *et al.*, 485. Vgl. MEIER PHILIPPE, N 334: «*C'est plus le processus de la communication [...] qui se trouve au centre de la protection des données.*»

der DSGVO,⁸⁰⁹ der OECD-Leitlinien 1980⁸¹⁰ und der US-amerikanischen *Fair Information Practice Principles* (FIPP).⁸¹¹

Auch die prozessorientierten Normen des DSG sehen sich der Kritik ausgesetzt. Naheliegend ist der Vorwurf, dass Bestimmungen, die primär die Daten und Bearbeitungsverfahren regeln, höchstens indirekt und ungenügend die Persönlichkeit schützen.⁸¹² Sie können nicht alle Faktoren umfassend berücksichtigen, welche das für die Persönlichkeit relevante Ergebnis beeinflussen. Die Wirkung einer Datenbearbeitung ergibt sich nicht allein aus der Bearbeitungshandlung; auch andere, davon unabhängige oder nachgelagerte Faktoren spielen eine Rolle.⁸¹³ So kommt es zur paradoxen Situation, dass gewisse Unternehmen das Datenschutzrecht vollkommen einhalten mögen, die Betroffenen aber dennoch Persönlichkeitsverletzungen erfahren.⁸¹⁴ Der Gesetzgeber sollte beobachten, ob die von ihm geschaffenen Bestimmungen ihre Wirkung erzielen.⁸¹⁵ Ein weiterer Kritikpunkt dreht sich um die Prinzipien der Verhältnismässigkeit (Art. 5 Abs. 2 BV) und Subsidiarität (Art. 5a BV). Es wird beanstandet, dass bereits die vorgelagerten Gefährdungshandlungen verboten werden statt wie üblich erst die tatsächliche Beeinträchtigung der Persönlichkeit (Erfolg).⁸¹⁶ Das DSG bleibt manchmal eine Präzisierung

⁸⁰⁹ DSGVO-Fokus auf Erhebung und Speicherung der Daten: GOODMAN/FLAXMAN, 1.

⁸¹⁰ Schwergewicht der OECD-Leitlinien 1980 auf der verfahrensrechtlichen statt der materiellen Gerechtigkeit: CUSTERS/URSIC, 331.

⁸¹¹ Die FIPP konzentrieren sich auf die Verwaltung und Bearbeitung von Daten und betonen die Wahlrechte, Einwilligungsbedingungen und die informationelle Selbstbestimmung: HARTZOG 2017, 966.

⁸¹² Für den EU-Raum spricht HORNING, 82: «Die datenschutzrechtlichen Herausforderungen von Big Data werden durch die DSGVO weder verändert noch gelöst.»

⁸¹³ Vgl. FORD, 1105–1106.

⁸¹⁴ Sog. *privacy paradox*: CUSTERS/URSIC, 338; Zweifel, ob die Offenlegung des Innern eines Scoringprozesses eine Persönlichkeitsverletzung verhindern kann: ZARSKY, 1408. Selbst wenn ein Unternehmen, das ein soziales Netzwerk betreibt, vollkommen FIPP-konform wäre, würden die Mitglieder immer noch falsche Profile erstellen, sich gegenseitig ausspionieren und Privatsphärengrenzen überschreiten: HARTZOG 2017, 967.

⁸¹⁵ RUDIN 2004b, 433–434. Vgl. auch KIM 2017, 195.

⁸¹⁶ WOLFER, N 216; Prof. Dr. Florent Thouvenin, Lehrstuhl für Informations- und Kommunikationsrecht der Universität Zürich, im Interview: FAKI SERMIN / WURM ANJA, Daten-Professor Florent Thouvenin verteidigt Facebook, Google und Co.: «Die beißen doch nicht!», Blick vom 30.05.2018, abrufbar unter <www.blick.ch> (besucht am 31.05.2020).

schuldig, inwiefern die Missachtung der Bearbeitungsformalien die Persönlichkeit (immer) verletzt. Schliesslich taucht der Einwand auf, dass Bestimmungen zu den Mitteln des Datenschutzes angesichts des technischen Fortschritts rasch an Aktualität einbüßen, während ergebnisorientierte Normen beständiger sind.⁸¹⁷

5.3.2 Risikoorientierte Auslegung der prozessorientierten Regeln

a) Allgemeines

Die Kritik an den risiko- und prozessorientierten Datenschutzbestimmungen zeigt, dass weder ein rein risiko- noch ein rein prozessorientiertes Verständnis des Datenschutzes genügen können. Es braucht verfahrensbezogene Normen, um den Persönlichkeitsschutz im Datenkontext zu konkretisieren. Doch müssen diese Prozessnormen nach der hier vertretenen Auffassung risikoorientiert ausgelegt werden. Der im Zweckartikel festgehaltene Bezug zum Persönlichkeitsschutz und zu den Grundrechten muss die Leitlinie für die Auslegung der einzelnen Datenschutzbestimmungen sein.⁸¹⁸ Auch das bundesrätliche Verordnungsrecht verlangt diese Risikoorientierung. Beispielsweise beurteilt es nach den möglichen Risiken der Datenbearbeitung für die betroffenen Personen, welche Massnahmen der Datensicherheit ergriffen werden müssen (Art. 8 Abs. 2 lit. c VDSG).

Der Schritt zur risikoorientierten Auslegung erlaubt es, die sonst relativ starr formulierten prozessorientierten Normen flexibel anzuwenden.⁸¹⁹ Doch der richtige Umgang mit dieser Flexibilität kann schwierig sein. Das DSG verlangt von der privatrechtlichen Rechtsanwenderin, zahlreiche Wertentscheide zu treffen. Dies ist im Bereich der öffentlich-rechtlichen Datenbearbeitung anders, da die Behörden für jede Datenbearbeitung eine gesetzliche Grundlage benötigen und sich damit auf vorweg vom Gesetzgeber getroffene Wertungen abstützen können.⁸²⁰

Um das Finden eines angemessenen Wertentscheids zu erleichtern, wird der Autor der vorliegenden Arbeit nun einige allgemeine Parameter erarbeiten, wobei die Aufzählung nicht abschliessend ist. Die Parameter werden illustrieren, wie eine

⁸¹⁷ GASSER 2016, 68.

⁸¹⁸ BBl 1988 II, 438.

⁸¹⁹ Vgl. World Economic Forum 2013, 12: Ein verantwortungsvoller Umgang mit den Risiken innerhalb bestimmter Grenzen ist nötig, nicht aber ein Schutz der Individuen vor allen möglichen Risiken.

⁸²⁰ ROSENTHAL 2012, 70.

risikoorientierte Auslegung von Prozessnormen in der Praxis funktionieren könnte (dazu sogleich). Weitere, spezifischere Kriterien für eine risikoorientierte Auslegung werden anschliessend bei der Besprechung der jeweiligen DSG-Bestimmungen erörtert.⁸²¹

b) Parameter für die risikoorientierte Auslegung

aa) Unterscheidung von Wissensgewinnung und -anwendung

Mit Bezug auf den Daten-Lebenszyklus sind die Phasen der Datenbeschaffung, -analyse und -wiederaufbereitung, die der Wissensgewinnung dienen, gedanklich zu trennen von der Phase der Datennutzung, in dem die Erkenntnisse angewendet werden.⁸²² Bei der Nutzung entstehen die Auswirkungen auf die Umwelt und die beschriebenen Rechtsprobleme.⁸²³ In dieser Phase ist eine restriktive Handhabung des Datenschutzrechts geboten. Das Datenschutzrecht sollte sich nach verbreiteter Meinung stärker an den Konsequenzen der Datenbearbeitung bzw. der Auswirkung auf die Persönlichkeit des Betroffenen ausrichten statt am Verhalten der Bearbeiter.⁸²⁴ Dagegen sollte die Wissensgewinnung in den Phasen der Beschaffung, Analyse und gegebenenfalls der Wiederaufbereitung von Daten relativ freizügig gewährt werden.⁸²⁵

Die Unterscheidung von Wissensgewinnung und -anwendung liegt in der Gedankenfreiheit begründet. Beim Prozess der Datenbearbeitung handelt es sich im

⁸²¹ Siehe z.B. zur risikoorientierten Auslegung des Geltungsbereichs des DSG S. 167–172.

⁸²² Vgl. World Economic Forum 2013, 20. Siehe zum Daten-Lebenszyklus S. 19–20.

⁸²³ Siehe zu den Rechtsproblemen Kapitel 3, S. 79–106.

⁸²⁴ WILDHABER *et al.*, 483. «Das wirkliche Problem sind die Folgen der Datenerfassung»: BAUMANN MAX-OTTO, 3. Orientierung an der Auswirkung (*impact*): MAYER-SCHÖNBERGER/CUKIER, 173; Orientierung am Ergebnis (*outcome*): BAMBERGER/MULLIGAN 2011, 311; Orientierung am Zweck (*goal*): GASSER 2016, 68; unterscheidend zwischen folgenorientierten (*consequentialist*) und verhaltensorientierten (*behaviourist*) Datenschutzregulierungen: FORD, 1104; Prof. Dr. Florent Thouvenin, Lehrstuhl für Informations- und Kommunikationsrecht der Universität Zürich, im Interview: FAKI SERMÍN / WURM ANJA, Daten-Professor Florent Thouvenin verteidigt Facebook, Google und Co.: «Die beissen doch nicht!», Blick vom 30.05.2018, abrufbar unter <www.blick.ch> (besucht am 31.05.2020). Orientierung an der Datennutzung (*use of data*): World Economic Forum 2013, 3. Vgl. SPRAGUE 2015, 44, DE MAURO *et al.*, 127, und RICHARDS/KING, 394. «*What really matters about big data is what it does*»: White House, Executive Office of the President 2014, 3.

⁸²⁵ World Economic Forum 2013, 12; Forderung nach einer «*permissionless innovation*»: GUIHOT *et al.*, 419.

Grunde genommen um ein Gedankenexperiment, solange die Erkenntnisse nicht auf die Umwelt angewendet werden. An dieser Stelle ist daran zu erinnern, dass der Begriff der Daten nicht auf Angaben in digitaler Form beschränkt ist.⁸²⁶ Die Prozesse, die ein menschliches Gehirn mit Daten ausführt, sind vergleichbar mit dem, was eine Maschine aus den digitalen Daten macht. Theoretisch könnte das DSG – anders als das Übereinkommen 108 und die DSGVO – Geltung beanspruchen, wenn ein Mensch Informationen über einen andern in seinem Gehirn sammelt.⁸²⁷ Es handelt sich hier um ein von den angewandten Mitteln und Verfahren unabhängiges Bearbeiten (Art. 3 lit. e DSG, Art. 4 lit. d E-DSG, Art. 5 lit. d rev-DSG) von Angaben (Art. 3 lit. a DSG, Art. 4 lit. a E-DSG, Art. 5 lit. a rev-DSG) über eine bestimmte betroffene Person (Art. 3 lit. b DSG, Art. 4 lit. b E-DSG, Art. 5 lit. b rev-DSG) durch eine private Person (Art. 2 Abs. 1 lit. a DSG, Art. 2 Abs. 1 lit. a E-DSG, Art. 2 Abs. 1 lit. a rev-DSG).

Trotz der Parallelen zu maschinellen Datenbearbeitungen reguliert das DSG die Vorgänge im Gehirn nicht: Es statuiert eine Ausnahme für Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt (Art. 2 Abs. 2 lit. a DSG, vgl. Art. 2 Abs. 2 lit. a E-DSG, vgl. Art. 2 Abs. 2 lit. a rev-DSG). Es wäre schlicht unmöglich, in jemandes Kopf hineinzusehen, wie bereits eines der politischsten deutschen Volkslieder weismacht: «Die Gedanken sind frei. Wer kann sie erraten?»⁸²⁸ Ausserrechtliche Normen lenken das Spiel der Gewährung und Verweigerung von Information

⁸²⁶ Siehe S. 23.

⁸²⁷ Das DSG lässt offen, ob die erfassten Datenbearbeitungen durch eine Maschine oder einen Menschen erfolgen. Nur bei bestimmten Datenbearbeitungen durch Bundesorgane kommt zum Ausdruck, dass es sich um automatisierte Bearbeitungen handelt (Art. 17a, Art. 19 Abs. 3^{bis} DSG; Art. 31, Art. 32 Abs. 5, ebenso aber Art. 4 lit. f, Art. 15, Art. 19 E-DSG; Art. 35, Art. 36 Abs. 5, ebenso aber Art. 5 lit. f–g, Art. 18, Art. 21, Art. 28 Abs. 1 lit. a rev-DSG). Gleichermassen offen bleiben die OECD-Leitlinien: SCHIEDERMAIR, 145–146. Demgegenüber beschränkt sich das Übereinkommen 108 des Europarats explizit auf «automatische Bearbeitungen» (Art. 1 Übereinkommen 108). Auch die DSGVO gilt für «ganz oder teilweise automatisierte» Bearbeitungen sowie für nichtautomatisierte Bearbeitungen, wenn Daten «in einem Dateisystem gespeichert werden» (Art. 2 Abs. 1 DSGVO).

⁸²⁸ Die Geschichte dieses Freiheitslieds reicht zurück bis in die Antike. Es erklang seit Ende des 18. Jh. bei verschiedenen Freiheitsbewegungen. Das Lied und seine Geschichte sind nachzuhören in der folgenden Radiosendung: SWR 2, MARQUART ALFRED, Die Gedanken sind frei, 26.11.2010, abrufbar unter <www.swr.de> (besucht am 31.05.2020).

auf Ausgangs- wie Empfängerseite.⁸²⁹ Die Gedankenfreiheit ist somit (zumindest teilweise) von Natur gegeben und existiert unabhängig vom Willen des Gesetzgebers. Das Recht zahlt hier einen Preis dafür, dass es eben Recht und nicht Gewalt ist: Es kann Informationsflüsse nicht umfassend regeln, weil es selber Information ist.⁸³⁰

Aufgrund der beschränkten Möglichkeiten hält sich das Recht bei der Informationsregulierung zurück. Es gelten die Glaubens- und Gewissensfreiheit sowie die Meinungs- und Informationsfreiheit (Art. 15 und 16 BV). Das DSG basiert auf dem Ansatz, dass Datenbearbeitungen unter Privaten wegen der Privatautonomie grundsätzlich zulässig sind.⁸³¹ Auch gibt es – unter Ausnahme des *numerus clausus* der Immaterialgüterrechte – keine informationsrechtlichen (Rechts-)Positionsgarantien.⁸³² Das Recht gewährt Informationsansprüche nur, wenn es hierfür einen besonderen Rechtfertigungsgrund gibt.⁸³³ Von Motiven der Gleichbehandlung und Transparenz motiviert sind beispielsweise die Informationspflicht der Erben (Art. 610 Abs. 2 ZGB) und die *Ad-hoc*-Publizitätspflichten für börsennotierte Gesellschaften (Art. 53 und 54 KR SIX). Die Mitwirkungspflicht im Prozess (Art. 160 ZPO) dient der Wahrheitsfindung.

Die Gedankenfreiheit ist aber nicht nur naturgegeben, sondern leitet sich auch vom (Natur-)Recht ab und muss vom Souverän gewährleistet werden.⁸³⁴ Hierfür machten sich schon der englische Staatstheoretiker, Philosoph und Mathematiker HOBES (1588–1679)⁸³⁵ und der französische Staatstheoretiker und Philosoph MON-

⁸²⁹ DRUEY 1995, 86.

⁸³⁰ DRUEY 1995, 83.

⁸³¹ GLASS, 103; SCHMIDT, 79, m.w.H. Öffentliche Organe bedürfen hingegen einer gesetzlichen Erlaubnis für die Bearbeitung von Personendaten (Art. 17 Abs. 1 DSG, Art. 30 Abs. 1 E-DSG, Art. 34 Abs. 1 rev-DSG).

⁸³² DRUEY 1995, 438.

⁸³³ DRUEY 1995, 106.

⁸³⁴ Zu den Prinzipien des Naturrechts gehören namentlich die Freiheit des Gewissens, die Freiheit der Religionsausübung und das Recht der freien Meinungsäußerung: MESSNER, 436–441. Vgl. mit Bezug auf die Religionsfreiheit und die Naturrechtslehre: KRAUSE, 4. Vgl. SCHRÖDER, 199.

⁸³⁵ HOBES stellt in seinem Monumentalwerk «Leviathan» fest: «[It is an error] to extend the power of the law, which is the rule of actions onely [sic], to the very thoughts, and consciences of men [...] notwithstanding the conformity of their speech and actions»: HOBES, 471.

TESQUIEU (1689–1755)⁸³⁶ stark. Auf den Punkt bringt es aber Roderich, Marquis von Posa, in SCHILLERS «Don Carlos», als er im Geiste des aufgeklärten Absolutismus vom spanischen König Philipp II. fordert: «Geben Sie Gedankenfreiheit.»⁸³⁷ Die Rechtsordnung muss somit die Rahmenbedingungen für die freien Gedanken und Informationsflüsse schaffen. Die Meinungsfreiheit setzt einen (realen oder virtuellen) geschützten Vorhof voraus, in dem die Meinung frei gebildet werden kann, bevor sie für die Meinungsäußerung reif ist.⁸³⁸

Insgesamt ist von der Analogie über Vorgänge im menschlichen Gehirn und von den Ausführungen zur Gedankenfreiheit mitzunehmen, dass die Innen- und die Aussenwelt unterschieden werden müssen. Die Persönlichkeit kann erst Schaden leiden, wenn Informationen vermittelt, also wahrnehmbar gemacht werden.⁸³⁹ Eine risikoorientierte Auslegung von Datenschutzbestimmungen setzt voraus, sich zu vergegenwärtigen, ob man sich in der Phase der Wissensgewinnung oder der -anwendung befindet. Beispielsweise könnte eine risikoorientierte Auslegung des Zweckbindungsgebots (Art. 4 Abs. 3 DSG, Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG) Folgendes bedeuten:⁸⁴⁰ Es genügt, den Zweck der Datenbearbeitung relativ grob zu umschreiben, solange es nur um die Analyse von Daten geht. Demzufolge wäre auch ein überwiegend exploratives Untersuchen von Datensätzen erlaubt. Doch wenn das aufgedeckte Wissen auf Personen angewendet werden soll,

⁸³⁶ MONTESQUIEU greift zur folgenden Anekdote: «Einem Marsyas träumte, er schnitte Dionys die Gurgel durch. Dieser liess ihn hinrichten und gab an, wenn Marsyas nicht tags daran gedacht hätte, würde er nachts nicht davon geträumt haben. Das war ausgesprochene Tyrannei: selbst wenn er daran gedacht hätte, so hatte er doch keinen Versuch gewagt. Die Gesetze haben nur die Aufgabe, äussere Handlungen zu ahnden»: MONTESQUIEU, 256 (12. Buch, 11. Kapitel). Es handelt sich dabei um Dionysios I., den gefürchteten Tyrannen von Syrakus (430–367 v. Chr.), und Marsyas, einen seiner Offiziere. Mit Dionysios I. ist sinnbildlich der Staat und mit Marsyas der Bürger gemeint. Die vollständige Anekdote ist in der Parallelbiografie Dion/Brutus des antiken griechischen Schriftstellers PLUTARCH nachlesbar: PLUTARCH, 15, Ziff. 9.

⁸³⁷ SCHILLER, dritter Akt, zehnter Auftritt.

⁸³⁸ Den geschützten Vorhof zur Meinungsbildung als «*intellectual privacy*» bezeichnend: RICHARDS, 95. Dieser Vorhof zeichnet sich durch mindestens drei Dimensionen aus – die Gedankenfreiheit, das Recht auf Informationsbeschaffung und die Vertraulichkeit von Kommunikation: RICHARDS, 108.

⁸³⁹ Art und Form der Information sind dagegen unerheblich, vgl.: SCHEFZIG, 105.

⁸⁴⁰ Siehe zum Zweckbindungsgebot ausführlich später, S. 173–199.

müssen der Zweck und die Konsequenzen für die Betroffenen klar und eng umschrieben sein.⁸⁴¹

bb) Intensität der Wissens- und Machtasymmetrie

Die Intensität der Wissens- und Machtasymmetrie zwischen Arbeitgeberin und Arbeitnehmern ist ein weiteres Mass zur Bestimmung des Risikos, das einer Datenbearbeitung innewohnt.⁸⁴² Die Manipulationsgefahr, die mit People Analytics verbunden ist,⁸⁴³ reduziert sich, wenn die Arbeitnehmer über die Datenbearbeitungen informiert sind und der Arbeitgeberin bzgl. Wissensstand auf Augenhöhe begegnen können. Deshalb sollte bei der Auslegung der DSG-Pflichten gewichtet werden, ob in einem Betrieb das Informations- und das Mitspracherecht aktiv gelebt werden.⁸⁴⁴ Eine mögliche Auslegung des Datenminimierungsgebots wäre beispielsweise, Datenerhebungen ziemlich grosszügig zu tolerieren, sofern durch die Mitwirkung die Wissensasymmetrie zwischen Arbeitgeberin und Arbeitnehmer reduziert wird.⁸⁴⁵

cc) Datenherkunft, Nutzung von Interoperabilität

Eine risikoorientierte Auslegung des Geltungsbereichs des DSG bedeutet auch, die Herkunft der Daten einzubeziehen. Es ist zwischen direkt hergegebenen, beobachteten und abgeleiteten Daten zu unterscheiden. Direkt hergegebene Daten werden vom Arbeitnehmer selbst anderen Personen überlassen, sei es freiwillig oder wegen einer gesetzlichen oder vertraglichen Pflicht. Beobachtete Daten werden nicht vom Betroffenen jemand anderem überlassen, sondern eben von Dritten beobachtet. Abgeleitete Daten werden aus der Analyse anderer Daten oder aus der Kombination verschiedener Daten gewonnen.⁸⁴⁶ Die Kombination ist möglich wegen der Interoperabilität, die vorliegend als eines der Kernelemente von People Analytics herausgearbeitet wurde.⁸⁴⁷

⁸⁴¹ Vgl. HERMSTRÜWER, 115–116.

⁸⁴² Siehe zur Wissens- und Machtasymmetrie S. 79. Die DSGVO geht von einem erhöhten Risiko aus, wenn der Betroffene aufgrund eines Machtungleichgewichts zwischen den Parteien schutzbedürftig ist, was auf Arbeitnehmer zutreffe: Art.-29-Datenschutzgruppe 2017a, 12.

⁸⁴³ Siehe S. 84.

⁸⁴⁴ Siehe zu den Mitwirkungsrechten S. 99–105.

⁸⁴⁵ GUTWIRTH/HILDEBRANDT, 38.

⁸⁴⁶ World Economic Forum 2014, 16; THOUVENIN/WEBER/FRÜH, 7–8.

⁸⁴⁷ Siehe S. 74–75.

Bei Nutzung der Interoperabilität von Datensätzen können besonders schützenswerte Erkenntnisse aus der Zusammenführung verschiedener, für sich allein genommen harmloser Daten abgeleitet werden.⁸⁴⁸ Wie bei Mosaiksteinen, deren Bedeutung erst erkennbar wird, wenn sie zu einem Bild zusammengesetzt werden, sagen die einzelnen Datenpunkte als Gesamtwerk mehr aus als die Summe ihrer Teile.⁸⁴⁹ Die Akkumulation (das Mosaikbild) macht die Sensibilität der Daten aus, nicht die einzelnen Datenpunkte (Mosaiksteine).⁸⁵⁰ Auch können heute anonyme Daten morgen durch das Zusammenführen einen Personenbezug erhalten.⁸⁵¹ Die Existenz abgeleiteter Daten ist den betroffenen Individuen oft nicht bewusst, weshalb sie deren Entstehung und Nutzung kaum kontrollieren können.⁸⁵² Abgeleitete Daten sollten daher ein eigenständiges Datenschutzanliegen sein.⁸⁵³ Dies bedeutet nach vorliegender Meinung, dass das DSG restriktiver ausgelegt werden sollte, wenn es um abgeleitete Daten geht. Weniger strenge Regeln sollten hingegen bei direkt hergegebenen Daten gelten, da der Betroffene hier eher den Überblick und die Kontrolle behält. Für beobachtete Daten ist ein Mittelweg der Auslegung zu finden.

In diesem Zusammenhang ist auch zu erwähnen, dass die Kombination verschiedener interoperabler Technologien für die Interpretation des DSG eine Rolle spielt. Es besteht etwa ein höheres Schutzbedürfnis, wenn Überwachungssysteme kombiniert mit Identifikationssystemen im Einsatz sind, als wenn ein Überwachungssystem allein vorhanden ist.⁸⁵⁴ Diesem Bedenken tragen die Datenschutzgesetze des Bundes und der Kantone nach der hier vertretenen Auffassung nicht gebührend Rechnung, weil sie weitgehend technikneutral formuliert sind.⁸⁵⁵ Die technikneutral verfassten Bestimmungen sollten einzelfallweise verschieden ausgelegt werden, d.h. restriktiver, wenn mehrere interoperable Technologien gleich-

⁸⁴⁸ Ableitungen durch Profiling: Art.-29-Datenschutzgruppe 2017c, 15.

⁸⁴⁹ «*Mosaic theory*»: SPRAGUE 2015, 21.

⁸⁵⁰ POULLET 2013, 150. Vgl. KASPER/WILDHABER, 215.

⁸⁵¹ Europarat 2016c, 21.

⁸⁵² THOUVENIN/WEBER/FRÜH, 8. Die Rede ist von einer «unsichtbaren Sichtbarkeit» (*invisible visibility*) des Arbeitnehmers, weil dieser sich nicht bewusst ist, was die Arbeitgeberin alles über ihn weiss: HÄNOLD, 131–132.

⁸⁵³ Vgl. SOLOVE, 117–121, WALDMAN, 65, CRAWFORD/SCHULTZ, 101, und HÄRTING, N 321, m.w.H.

⁸⁵⁴ RUDIN 2004b, 433.

⁸⁵⁵ SCHWEIZER, N 1.26.

zeitig angewendet werden, oder aber freizügiger, wenn bloss eine einzelne Technologie aufs Mal im Einsatz ist.

dd) Umfang der Datenbearbeitung

In der Regel dürfte das Risiko für die Persönlichkeit tiefer ausfallen, je weniger Daten bearbeitet werden. Der Umfang der Datenbearbeitung ist etwa mitentscheidend für die Beurteilung, ob die technischen und organisatorischen Massnahmen der Datensicherheit genügend sind (vgl. Art. 8 Abs. 2 lit. b VDSG). Des Weiteren sieht das künftige Recht eine De-Minimis-Regel bzgl. der Pflicht zur Erstellung eines Verzeichnisses der Bearbeitungstätigkeiten vor (Art. 11 Abs. 5 E-DSG, Art. 12 Abs. 5 rev-DSG). Diese Erleichterung wird in Abhängigkeit der Anzahl Beschäftigter zugestanden. Diese quantitative Referenzgrösse ist zwar praktikabel, doch würden die Anzahl der Daten pro Betroffenen,⁸⁵⁶ die Zahl der Bearbeitungsschritte, die Dauer oder die Komplexität mehr über das Risikopotenzial aussagen.⁸⁵⁷ So wie der Gesetzgeber eine De-Minimis-Regelung vorsieht, sollten auch die rechtsanwendenden Behörden bei der Auslegung des DSG vorgehen: Sind die quantitativen Elemente der Datenbearbeitung gering, sollte dies berücksichtigt werden.⁸⁵⁸ Weniger Daten fallen beispielsweise an, wenn eine Datenbearbeitung nicht ubiquitär erfolgt. Das Merkmal der Ubiquität ist etwa beim besprochenen virtuellen Karriereassistenten nur schwach ausgebildet,⁸⁵⁹ weshalb von dieser Anwendung geringere Risiken für die Persönlichkeit der Arbeitnehmer ausgehen.

⁸⁵⁶ Im Entstehungsprozess zur europäischen Bestimmung betreffend die Datenschutz-Folgenabschätzung wurde zur Definition einer «umfangreichen» Bearbeitung (Art. 35 Abs. 3 lit. b DSGVO) der absolute Schwellenwert von 5'000 Datensätzen von verschiedenen betroffenen Personen innerhalb von zwölf Monaten diskutiert. Diesen Wert überschreiten Unternehmen aber schnell, zumal viele Aufbewahrungsfristen eine Löschung nach Ablauf eines Jahres nicht zulassen: DOCHOW, 54.

⁸⁵⁷ Der Nationalrat beschreibt das Dilemma zwischen Praktikabilität und Aussagekraft leicht hilflos wie folgt: «[...] eigentlich spielt die Grössenordnung der Unternehmen [...] überhaupt keine Rolle. Man müsste so etwas wie die Risikotiefe der Bearbeitung [...] definieren – aber wie man das formulieren würde, haben wir zumindest in der Kommission noch nicht herausgefunden. Also müssen wir uns auf die Grössenordnung der Unternehmen berufen [...]»: AB NR 2019, 1798. Vgl. DOCHOW, 54.

⁸⁵⁸ Vgl. die Forderung nach Härtefallklauseln für die Protokollierungspflicht nach Art. 5 Abs. 2 DSGVO: MARTINI, 1022.

⁸⁵⁹ Siehe S. 77.

ee) Gezielter Personenbezug

Für die risikoorientierte Auslegung kann auch der Zweck der Datenbearbeitung ausschlaggebend sein. Beispielsweise bildet der Zweck der Datenbearbeitung ein Kriterium für die Beurteilung, ob die ergriffenen technischen und organisatorischen Massnahmen der Datensicherheit angemessen sind (Art. 8 Abs. 2 lit. a VDSG). ROSSNAGEL sieht tiefere Risiken bei Datenbearbeitungen «ohne gezielten Personenbezug», d.h. zur Erbringung einer rein technischen Funktion.⁸⁶⁰ Für solche Datenbearbeitungen schlägt er eine spezielle Auslegung des Datenschutzrechts vor: Einerseits könnte eine Lockerung erlauben, auf eine vorherige Information der betroffenen Personen zu verzichten, und der Anspruch auf Auskunft über einzelne Daten würde nicht bestehen, um kontraproduktive Protokollverfahren zu vermeiden.⁸⁶¹ Andererseits müssten ein strenges Datenminimierungs-Gebot und Zweckentfremdungs-Verbot sowie eine Löschpflicht sofort nach der Bearbeitung greifen.⁸⁶² Ähnlich differenziert die DSGVO: Sie sieht Erleichterungen vor, wenn für die Zwecke der Bearbeitung eine Identifizierung der betroffenen Person nicht erforderlich ist (vgl. E. 57 und Art. 11 DSGVO). Umgekehrt liegt gemäss der Art.-29-Datenschutzgruppe ein Indiz für ein hohes Risiko vor, wenn ein Unternehmen «systematisch» die Tätigkeiten seiner Angestellten überwache, wie beispielsweise ihre Internetnutzung.⁸⁶³

In der Schweiz aber differenzieren soweit ersichtlich weder das DSG noch das rev-DSG danach, ob eine Datenbearbeitung gezielt personenbezogen erfolgt oder nicht, was bedauerlich ist. Das Arbeitnehmerschutzrecht versucht, sich des Anliegens, den gezielten Personenbezug zu berücksichtigen, anzunehmen. Es gilt das Verbot für Systeme, die das Verhalten der Arbeitnehmer überwachen (vgl. Art. 26 ArGV 3). Dieses Verbot ist aber zu starr formuliert und entbehrt einer genügenden Rechtsgrundlage, wie sogleich dargelegt wird. Daher besteht im schweizerischen Rechtsraum noch Potenzial für Konkretisierungen durch den Gesetzgeber, welche generellen Erleichterungen gelten sollen, wenn ein gezielter Personenbezug fehlt.

⁸⁶⁰ ROSSNAGEL, 280. Beispielsweise besteht offensichtlich kein hohes Risiko, wenn ein Textbearbeitungsprogramm die Rechtschreibung überprüft, auch wenn es sich hierbei um eine automatisierte Bearbeitung von Arbeitnehmerdaten handelt: REISMAN *et al.*, 12.

⁸⁶¹ ROSSNAGEL, 281.

⁸⁶² ROSSNAGEL, 281.

⁸⁶³ Art.-29-Datenschutzgruppe 2017a, 13.

5.3.3 Risikoorientierung am praktischen Beispiel der Verhaltensüberwachung

a) Verordnung und frühere Rechtsprechung

Die vorstehend vorgeschlagene Lösung, die prozessbezogenen Bestimmungen des Datenschutzrechts risikoorientiert auszulegen und anzuwenden, soll am Beispiel der Verhaltensüberwachung dargestellt werden. Im Fall der Verhaltensüberwachung am Arbeitsplatz existiert eine prozessorientierte Verordnungsbestimmung (Art. 26 ArGV 3). Die diesbezügliche Rechtsprechung hat sich aber von einer prozessorientierten weg und hin zu einer risikoorientierten Anwendung des Datenschutzrechts bewegt, wie sogleich aufzuzeigen ist.⁸⁶⁴

Gemäss der bundesrätlichen Verordnung dürfen Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden (Art. 26 Abs. 1 ArGV 3). Mit einem «System» ist eine Datenbearbeitungs-Anlage als Einheit gemeint, bestehend aus Rechner, Programm und gegebenenfalls weiteren Modulen.⁸⁶⁵ Ein System, das «überwachen soll», liegt vor, wenn es objektiv dazu geeignet ist.⁸⁶⁶ Unzulässig sind Überwachungssysteme, wenn sie ausschliesslich oder vorwiegend die Kontrolle des Verhaltens der Arbeitnehmer bezwecken.⁸⁶⁷ Nur ausnahmsweise sind die beschriebenen Überwachungs- und Kontrollsysteme zulässig, nämlich wenn sie aus andern Gründen erforderlich sind; dann sind sie insbesondere so zu gestalten und anzuordnen, dass die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer nicht beeinträchtigt werden (Art. 26 Abs. 2 ArGV 3). Der «andere Grund» muss gegenüber dem Überwachungsmotiv klar überwiegen.⁸⁶⁸

⁸⁶⁴ Vgl. die Darstellung der früheren und aktuellen Rechtsprechung bei KASPER/WILDHABER, 221–224.

⁸⁶⁵ Zum Begriff der «technischen Systeme» gemäss deutschem Recht: RUHLAND, 96.

⁸⁶⁶ Zum Begriff «zur Verhaltensüberwachung bestimmt» gemäss deutschem Recht: RUHLAND, 97.

⁸⁶⁷ BGE 130 II 425 E. 4.4; CHK OR BT 2-EMMEL, Art. 328 OR, N 4; BSK OR I-PORTMANN/RUDOLPH, Art. 328b OR, N 49; REHBINDER/STÖCKLI, Art. 328b OR N 29. Ein gleiches Verbot von Systemen «*for the direct and principal purpose of monitoring employees' activity and behaviour*» sieht auch der Europarat vor: Europarat 2015, N 15.1. Vgl. KASPER/WILDHABER, 221.

⁸⁶⁸ SECO 2018, 326–2; KUKO OR-PIETRUSZAK, Art. 328 OR, N 19a. Vgl. KASPER/WILDHABER, 221.

Gestützt auf die Verordnungsbestimmung (Art. 26 ArGV 3) erachtete das Bundesgericht 2004 ein GPS-System von damals als verhältnismässiges Mittel zur Überwachung einer Fahrzeugflotte. Die Arbeitgeberin hatte es zum Zweck des Diebstahlschutzes, der Arbeitsorganisation und der Überprüfung der Arbeitsverrichtung in ihren Fahrzeugen installiert. Das System zeichnete die geografische Position des Fahrzeugs und die Parkdauer bei einem Kunden auf. Es liess jedoch keine Schlüsse zu, ob oder wie ein Arbeitnehmer seine Arbeit verrichtete, weshalb die Gefahr einer Verhaltensüberwachung limitiert war.⁸⁶⁹

Im selben, rechtskräftigen⁸⁷⁰ Entscheid bestätigte die zweite öffentlich-rechtliche Abteilung des Bundesgerichts die Verordnungsbestimmung des Bundesrats: Entscheidend für die Beurteilung, ob ein Überwachungssystem zulässig ist oder nicht, seien die Beweggründe (*«motifs»*), die für ihre Einführung massgebend gewesen seien, und die Zwecke (*«buts»*), welche ihr Einsatz verfolge, aber weniger die Art (*«type»*) der Überwachung und deren Auswirkungen (*«effets»*).⁸⁷¹ Die Verordnung und die damalige Rechtsprechung sind prozessorientiert, weil sie sich am Zweck der Datenbearbeitung ausrichten, welcher in der Phase der Wissensgewinnung festgelegt wird. Hingegen sollte gemäss Verordnung und früherer Rechtsprechung der Effekt der Datenbearbeitung, welcher in der Phase der Wissensanwendung eintritt, belanglos sein. Das Bundesgericht bestätigte ausdrücklich die Gesetzmässigkeit von Art. 26 ArGV 3.⁸⁷²

b) Aktuelle Rechtsprechung

Heutzutage sind GPS-basierte Gesamtüberwachungssysteme verfügbar, die das Verhalten wesentlich detaillierter aufzeichnen als frühere GPS-Systeme.⁸⁷³ Das

⁸⁶⁹ BGE 130 II 425 E. 5.3–5.5. A.M. PÄRLI 2018, N 17.59: Nicht zulässig sei der GPS-Einsatz als Mittel der Diebstahlbekämpfung und zur Optimierung der Arbeitsorganisation. Darstellung der früheren Rechtsprechung bei KASPER/WILDHABER, 221–224.

⁸⁷⁰ Das Bundesgericht hat die Sache zwar zur neuen Beurteilung an die Vorinstanz zurückgewiesen (BGE 130 II 425 Dispositivziffer 1). Darauf wurde jedoch die Beschwerde zurückgezogen und das Verfahren abgeschrieben: *Décision Tribunal administratif du Canton de Genève A/1745/2004-EP* vom 15.03.2006 2.

⁸⁷¹ BGE 130 II 425 E. 4.1.

⁸⁷² «[Art. 26 ArGV 3] *s'insère parfaitement dans le cadre de la délégation de compétence prévue à [Art. 6 Abs. 4 i.V.m. Art. 40 Abs. 1 lit. a ArG]*» und «[Art. 26 ArGV 3] *est donc conforme au principe de la légalité*»: BGE 130 II 425 E. 3.3. Darstellung der früheren Rechtsprechung bei KASPER/WILDHABER, 221.

⁸⁷³ Siehe zur Beschreibung heutiger GPS-Systeme auch KASPER/WILDHABER, 222.

vorgestellte System ORION von UPS lokalisiert die Fahrzeuge, verwertet geographische Daten (z.B. Adressen, Landkarten) und erhebt Daten über die Pakete (z.B. Absende- und Zustellungszeitpunkt).⁸⁷⁴ Gestützt darauf errechnet ein Algorithmus die kürzeste Fahrstrecke für die zu verteilenden Pakete. Dadurch sinken Treibstoffverbrauch und Fahrerbedarf und steigt die Anzahl zugestellter Pakete.⁸⁷⁵ Sensoren melden im Voraus, wann Fahrzeugteile ersetzt werden müssen.⁸⁷⁶ Sie zeichnen auch auf, wann der Fahrer die Tür öffnet, das Fahrzeug sichert, wann sein Fuss das Bremspedal berührt, wann der Motor leertläuft und wann der Fahrer die Sicherheitsgurte anschnallt.⁸⁷⁷

Es stellt sich die Frage, ob ORION und andere heutige GPS-basierte Gesamtüberwachungssysteme zu einem wesentlichen Teil das Verhalten aufzeichnen und nach Art. 26 ArGV 3 zu verbieten sind. Für die Beantwortung dieser Frage ist ein jüngeres Urteil aus dem Jahr 2009 heranzuziehen. Die strafrechtliche Abteilung des Bundesgerichts hat entschieden, dass es an einer genügenden Delegationsnorm in einem Gesetz im formellen Sinn fehlt, welche den Bundesrat zum Erlass einer Verordnungsnorm betreffend die Überwachung der Arbeitnehmer am Arbeitsplatz ermächtigen würde (vgl. Art. 182 Abs. 1 BV).⁸⁷⁸

Aufgrund der fehlenden Gesetzmässigkeit ist Art. 26 Abs. 1 ArGV 3 «einschränkend auszulegen»: Nur «soweit sie geeignet sind, die Gesundheit oder das Wohlbefinden der Arbeitnehmer zu beeinträchtigen», dürfen Überwachungs- und Kontrollsysteme, die das Verhalten der Angestellten am Arbeitsplatz überwachen

⁸⁷⁴ Siehe S. 48. KASPER/WILDHABER, 222.

⁸⁷⁵ KASPER/WILDHABER, 222; KONRAD ALEX, Meet Orion, software that will save UPS millions by improving drivers' routes, Forbes vom 01.11.2013, abrufbar unter <www.forbes.com> (besucht am 31.05.2020); AJUNWA/CRAWFORD/SCHULTZ, 743–744.

⁸⁷⁶ Sog. *preventative maintenance*: KASPER/WILDHABER, 222; ZAX DAVID, Brown down: UPS drivers vs. the UPS algorithm, 01.03.2013, abrufbar unter <www.fastcompany.com> (besucht am 31.05.2020).

⁸⁷⁷ KASPER/WILDHABER, 222; BRUDER JESSICA, These workers have a new demand: stop watching us, 27.05.2015, abrufbar unter <www.thenation.com> (besucht am 31.05.2020).

⁸⁷⁸ Urteil BGer 6B_536/2009 vom 12.11.2009 E. 3.3.2; Darstellung der aktuellen Rechtsprechung bei KASPER/WILDHABER, 222–223. Bereits im Jahr 2002 hat RIESSELMANN-SAXER erkannt, dass Art. 26 Abs. 1 ArGV 3 als Verordnungsbestimmung gegenüber der höherrangigen Gesetzesbestimmung von Art. 328b OR ungültig ist: RIESSELMANN-SAXER, 112. STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 8, m.w.H.

sollen, nicht eingesetzt werden.⁸⁷⁹ Diese Änderung der Rechtsprechung bedeutet eine Neuorientierung, weg vom Prozess, hin zum Ergebnis: Entscheidend ist, ob es zu einer Gesundheitsbeeinträchtigung kommt.⁸⁸⁰ Diese ist nicht *eo ipso* gegeben, wenn ein Überwachungssystem (hauptsächlich) der Überwachung dient.⁸⁸¹

Anstatt allein auf das K.-o.-Kriterium des Bearbeitungszwecks abzustellen, beurteilt das Bundesgericht das Risiko für die Gesundheit anhand mannigfaltiger Massstäbe: Neben dem Zweck sind insbesondere die Häufigkeit und die Dauer der Überwachung massgebend sowie die Art der vom System erfassten Tätigkeiten.⁸⁸² Weitere Kriterien sind die eingesetzte Technik, die verwendete Datenmenge, die Zugänglichkeit der Informationen und die Relevanz, welche die Daten hinsichtlich des Persönlichkeitsrechts des Betroffenen aufweisen (Sensibilität der Informationen, Anzahl betroffener Persönlichkeitsaspekte).⁸⁸³ Daher kann ein Überwachungssystem, das den Arbeitnehmer nur sporadisch und kurzzeitig bei bestimmten Gelegenheiten erfasst, erlaubt sein, selbst wenn es (hauptsächlich) der gezielten Überwachung des Verhaltens der Arbeitnehmer am Arbeitsplatz dient.⁸⁸⁴ Die Überwachung muss im Vergleich zum beabsichtigten Zweck ein verhältnismässiges Mittel (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG) darstellen.⁸⁸⁵ Verboten ist die ständige generelle Verhaltensüberwachung.⁸⁸⁶

Bei heutigen GPS-Ausrüstungen von Flotten ist somit zu prüfen, ob aus ihnen eine überwachende Wirkung und damit eine Gesundheitsbeeinträchtigung für die Ar-

⁸⁷⁹ Urteil BGer 6B_536/2009 vom 12.11.2009 E. 3.6.1; MORSCHER, 189–190; BSK OR I-PORTMANN/RUDOLPH, Art. 328b OR, N 50a; Darstellung der aktuellen Rechtsprechung bei KASPER/WILDHABER, 222–223.

⁸⁸⁰ Urteil BGer 6B_536/2009 vom 12.11.2009 E. 3.6.2; KASPER/WILDHABER, 223.

⁸⁸¹ Urteil BGer 6B_536/2009 vom 12.11.2009 E. 3.6.2; KASPER/WILDHABER, 223.

⁸⁸² Urteil BGer 6B_536/2009 vom 12.11.2009 E. 3.4.1; Darstellung der aktuellen Rechtsprechung bei KASPER/WILDHABER, 223.

⁸⁸³ WILDHABER 2017, 219. Vgl. WOLFER, N 182–197; KASPER/WILDHABER, 223.

⁸⁸⁴ Urteil BGer 6B_536/2009 vom 12.11.2009 E. 3.6.2; BSK OR I-PORTMANN/RUDOLPH, Art. 328b OR, N 50a; KUKO OR-PIETRUSZAK, Art. 328 OR, N 19a; KASPER/WILDHABER, 223.

⁸⁸⁵ BSK OR I-PORTMANN/RUDOLPH, Art. 328b OR, N 49. Es geht beim Verbot der Verhaltensüberwachung letztlich um die Verhältnismässigkeit im engeren Sinn, d.h. um eine Abwägung zwischen Zweck und Wirkung, so auch: DONAUER/MÖRI, 1057; KASPER/WILDHABER, 223.

⁸⁸⁶ STUTZ/VALLONI, N 5.45; Unzulässigkeit ständiger Beobachtung: WOLFER, N 615. Regelungsdruck ergibt sich, wenn das Leistungs- und Arbeitsverhalten von Beschäftigten lückenlos dokumentiert wird: BMAS 2017, 144–145; KASPER/WILDHABER, 223.

beitnehmer resultiert. Unerheblich ist dagegen, ob eine überwachende Wirkung in der Absicht der Arbeitgeberin liegt und dem Sinn der technischen Einrichtung entspricht.⁸⁸⁷ Bei einem System wie ORION, das den Fahrer anweist, die Sicherheitsgurte anzuschallen, *bevor* er den Motor anlässt, um Benzin zu sparen, und welches für eine geringe Abweichung von der algorithmisch optimalen Route eine Rechtfertigung verlangt, erscheint eine überwachende Wirkung gegeben.⁸⁸⁸ Berichten zufolge erleben die Fahrer Stress, Angst und Erschöpfung in Form von kalten Schweissausbrüchen, Atemproblemen und Panikattacken.⁸⁸⁹ Problematisch erscheinen auch Geolokalisierungs-Sensoren, die der Arbeitnehmer direkt auf sich trägt, so beispielsweise die Paketscanner der Lagerhallenarbeiter von FedEx und Amazon, welche die Arbeitsgeschwindigkeit vorschreiben und bei Pausen ausserhalb der regulären Zeiten Alarm schlagen.⁸⁹⁰ Ein Kriterium für die Einstufung der überwachenden Wirkung muss auch der Datenzugriff sein: Kann sich der Arbeitnehmer selbst mit seiner Leistung in der Vergangenheit vergleichen, wie etwa bei MyAnalytics von Microsoft,⁸⁹¹ ist People Analytics eine Hilfe zum Selbstmanagement. Können dagegen auch Vorgesetzte und Arbeitskollegen die Resultate einsehen, kann Stress entstehen.⁸⁹² Auch der gut gemeinte Ansatz, Arbeit zu einem Wettbewerb gleich einem Spiel auszugestalten, bei dem alle im Unternehmen permanent gegenseitig ihren Punktestand sehen (sog. *gamification*⁸⁹³), kann eine überwachende Wirkung entfalten.⁸⁹⁴

Zusammenfassend hat sich nach der Einschätzung des Autors die Rechtslage betreffend die Systeme zur Überwachung und Kontrolle des Verhaltens der Arbeitnehmer am Arbeitsplatz gewandelt: Während zunächst mit dem Bearbeitungszweck eine Prozessmodalität im Fokus stand, gibt heute mit der Gesundheitsbeeinträchtigung das Ergebnis den Ausschlag über die Zulässigkeit eines

⁸⁸⁷ WILDHABER 2017, 219; KASPER/WILDHABER, 223.

⁸⁸⁸ KASPER/WILDHABER, 223–224.

⁸⁸⁹ BRUDER JESSICA, These workers have a new demand: stop watching us, 27.05.2015, abrufbar unter <www.thenation.com> (besucht am 31.05.2020); KONRAD ALEX, Meet Orion, software that will save UPS millions by improving drivers' routes, Forbes vom 01.11.2013, abrufbar unter <www.forbes.com> (besucht am 31.05.2020).

⁸⁹⁰ Siehe S. 46; FedEx: FN 260; WILDHABER 2017, 219; Amazon: AJUNWA/CRAWFORD/SCHULTZ, 744; HOLTHAUS *et al.*, 676; KASPER/WILDHABER, 224.

⁸⁹¹ Siehe S. 50.

⁸⁹² KASPER/WILDHABER, 224.

⁸⁹³ AJUNWA/CRAWFORD/SCHULTZ, 770; BODIE *et al.*, 974–975.

⁸⁹⁴ KASPER/WILDHABER, 224.

Überwachungssysteme. Früher, als einzig der Bearbeitungszweck (Überwachung und Kontrolle) über die Zulässigkeit entschieden hat, konnte ein System bereits unzulässig sein, wenn die Gefahr für die Gesundheit der Arbeitnehmer rein abstrakter Natur war. Seit der Änderung der Rechtsprechung von 2009 entscheidet hingegen die konkrete Auswirkung der Verhaltensüberwachung auf die Gesundheit über die Zulässigkeit des erwähnten Systems. Das Bundesgericht legt Art. 26 ArGV 3 somit risikoorientiert aus.

5.3.4 Zwischenfazit zum Zweck des Datenschutzgesetzes

Das DSG bezweckt im privatrechtlichen Bereich den Schutz vor Persönlichkeitsverletzungen bei der Bearbeitung von Personendaten. Diese Zwecksetzung erfordert nach den vorliegend gewonnenen Erkenntnissen einerseits den Erlass risikoorientierter Bestimmungen, die den Persönlichkeitsschutz statuieren. Andererseits sind prozessorientierte Normen nötig, welche die zulässigen Datenbearbeitungsverfahren konkretisieren; dadurch erhält das DSG eine eigenständige Bedeutung neben dem allgemeinen Persönlichkeitsschutz (Art. 27–28 ZGB). Die gegenwärtigen Normen des DSG setzen sich mehrheitlich mit der Beschaffenheit der Daten und dem Prozess ihrer Bearbeitung auseinander. Diese prozessbezogene Regulierungsart kann dazu führen, dass Datenbearbeitungen DSG-konform erscheinen, obwohl sie eine Wirkung entfalten, die die Persönlichkeit des Betroffenen verletzt. Umgekehrt können strenge Bearbeitungsregeln Anwendungen von People Analytics behindern, denen ein geringes Verletzungspotenzial innewohnt.

Um die Probleme der prozessorientierten DSG-Bestimmungen zu entschärfen, wird vorliegend eine risikoorientierte Auslegung der entsprechenden Normen vorgeschlagen. Gemäss der aktuellen Rechtsprechung bzgl. des Verhaltensüberwachungsverbots (Art. 26 ArGV 3) entscheidet die persönlichkeitsbeeinträchtigende Wirkung einer Datenbearbeitung über deren Zulässigkeit und nicht mehr allein der Bearbeitungszweck. Dies bedeutet einen Wandel von einer prozess- zu einer risikoorientierten Interpretation des Datenschutzrechts. Diese risikoorientierte Lesart wird im Folgenden die Besprechung der weiteren DSG-Bestimmungen prägen.

5.4 Geltungsbereich des Datenschutzgesetzes

5.4.1 Überblick

Die sachliche Anwendbarkeit des Datenschutzrechts ist auf das Vorliegen einer besonderen Kategorie von Daten, nämlich Personendaten, beschränkt, während

anonyme Daten nicht dem DSG unterstehen (dazu sogleich). Diese Denkweise nach Datenkategorien kann zu Schwierigkeiten führen bei der Frage, ob Typisierungen datenschutzrechtlich erfasst sein sollen (dazu S. 160–166). Nach der vorliegend vertretenen Meinung werden die Typisierungen, die ein hohes Persönlichkeitsschutzrechtliches Gefährdungspotenzial aufweisen, durch das DSG erfasst (dazu S. 167–172).

5.4.2 Unterscheidung zwischen Personendaten und Sachdaten

Das DSG ist sachlich anwendbar auf die Bearbeitung von Personendaten (Art. 2 Abs. 1 DSG, Art. 2 Abs. 1 E-DSG, Art. 2 Abs. 1 rev-DSG). Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (Art. 3 lit. a DSG, Art. 4 lit. a E-DSG, Art. 5 lit. a rev-DSG). Eine Person ist bestimmt, wenn sich direkt aus der Information selbst ergibt, dass es sich genau um diese Person handelt.⁸⁹⁵ Dies ist beispielsweise bei einem Personalausweis der Fall.⁸⁹⁶ Bestimmbar ist eine Person, wenn sich ihre Identität indirekt anhand der Kombination verschiedener Informationen ermitteln lässt (z.B. aufgrund von Sachen, die einem Angestellten gehören).⁸⁹⁷ Bei zahlreichen People Analytics-Anwendungen besteht der Zweck darin, Informationen über bestimmte Arbeitnehmer zu gewinnen, weil besonders Daten über Gehalt, Leistung, berufliche Entwicklung, Anstellungsdauer, Geschäftskosten-Rückgewinnung und Compliance interessieren.⁸⁹⁸ Somit liegen bei People Analytics oft Personendaten vor.

Sachdaten sind demgegenüber kein Schutzobjekt des DSG, d.h., sie werden nicht durch das DSG reguliert.⁸⁹⁹ Sie weisen keinen Personenbezug auf, und dieser lässt sich auch nicht herstellen.⁹⁰⁰ Zu den Sachdaten zählen anonymisierte Personenda-

⁸⁹⁵ BSK OR I-PORTMANN/RUDOLPH, Art. 328b OR, N 3; REHBINDER/STÖCKLI, Art. 328b OR N 2; BAERISWYL 2014, 49; KASPER/WILDHABER, 211.

⁸⁹⁶ BBl 1988 II, 444; KASPER/WILDHABER, 211.

⁸⁹⁷ BAERISWYL 2014, 49; REHBINDER/STÖCKLI, Art. 328b OR N 2; KASPER/WILDHABER, 211.

⁸⁹⁸ MRKONICH *et al.*, 13. Vgl. zu Big Data-Anwendungen THOUVENIN 2014, 80.

⁸⁹⁹ KASPER/WILDHABER, 212.

⁹⁰⁰ WEBER/OERTLY, N 5. Vgl. TAMÒ-LARRIEUX, 77: Datenschutz nur anwendbar, wenn es um Personendaten geht. KASPER/WILDHABER, 212. Siehe aber zur Möglichkeit der Re-Identifizierung durch Verknüpfung von Datensätzen sogleich, S. 157–160.

ten, sofern die Anonymisierung irreversibel ist, und statistische Erkenntnisse.⁹⁰¹ Der Begriff der «Sachdaten» kommt im DSG zwar nicht vor, und «anonymisierte Daten» finden nur am Rande Erwähnung (Art. 21 Abs. 2 lit. a, Art. 22 Abs. 1 lit. a DSG; Art. 34 Abs. 2 lit. a, Art. 35 Abs. 1 lit. a E-DSG; Art. 38 Abs. 2 lit. a, Art. 39 Abs. 1 lit. a rev-DSG). Die Existenz dieser Datenkategorien ergibt sich aber *e contrario* aus dem DSG (vgl. Art. 2 Abs. 1 i.V.m. Art. 3 lit. a DSG, Art. 2 Abs. 1 i.V.m. Art. 4 lit. a E-DSG, Art. 2 Abs. 1 i.V.m. Art. 5 lit. a rev-DSG) und ist in der Rechtsprechung und vom EDÖB anerkannt.⁹⁰²

Die Kategorisierung in Personen- und Sachdaten bietet in vielen Fällen eine trennscharfe Handhabe, um Sachverhalte entweder dem DSG zu unterstellen oder von ihm zu befreien. Ist eine Anonymisierung beabsichtigt, so ist der Umgang mit dem Ergebnis der Anonymisierung – den anonymisierten Daten – datenschutzrechtlich irrelevant.⁹⁰³ Der durch People Analytics gewonnene, aggregierte Erfahrungssatz als solcher ist somit kein personenbezogenes Datum.⁹⁰⁴ Hingegen sind die Grundsätze des DSG auf den Prozess der Datenerhebung und Anonymisierung anzuwenden. Gleiches gilt für Zufallsfunde, etwa wenn eine Analyse mit an sich nicht personenbezogener Zwecksetzung wider Erwarten personenbezogene Ergebnisse hervorbringt.⁹⁰⁵

Mit der binären Unterscheidung zwischen personenbezogenen und anonymisierten Daten steht das DSG nicht alleine da: Die EU (E. 26 Sätze 5–6 DSGVO),⁹⁰⁶

⁹⁰¹ FLUECKIGER 2017, 7; WEBER/OERTLY, N 9. Statistische Erkenntnisse stellen keine Personendaten dar, soweit sie mit den jeweiligen Personen nicht mehr verbunden sind: SCHEFZIG, 116. Anonymisierungstechniken befreien von den Datenschutzpflichten: WACHTER/MITTELSTADT, 616; KASPER/WILDHABER, 212.

⁹⁰² «Sachdaten»: EDÖB, Erläuterung zu Big Data, abrufbar unter <www.edoeb.admin.ch> (besucht am 31.05.2020); «anonymisierte Personendaten»: Urteil BGer 1C_394/2016 vom 27.09.2017 E. 4.10.

⁹⁰³ WEBER/OERTLY, N 10.

⁹⁰⁴ Mit Bezug auf Big Data-Erfahrungssätze unter der DSGVO und dem deutschen Recht: DAUBLER, N 429a.

⁹⁰⁵ BAERISWYL 2014, 53.

⁹⁰⁶ Nur absolut anonyme Daten sind dem Anwendungsbereich der DSGVO entzogen, weshalb die Unterscheidung nach deutschem Recht zwischen absoluter und faktischer Anonymität (KARG, 524) unter der DSGVO nicht mehr gelten kann: HÄRTING, N 22.

die USA⁹⁰⁷ und die meisten anderen Rechtssysteme⁹⁰⁸ operieren im Wesentlichen mit dem gleichen Begriffspaar.

5.4.3 Re-identifizierbare Daten

Im Zeitalter von People Analytics wird es immer schwieriger, Personen- und Sachdaten auseinanderzuhalten.⁹⁰⁹ Wegen der Möglichkeit zur Re-Identifizierung können immer mehr Daten (wieder) einen Personenbezug erhalten.⁹¹⁰ Mit den bestehenden Anonymisierungstechniken⁹¹¹ ist es nicht immer leicht, eine irreversible Anonymisierung zu bewerkstelligen.⁹¹² (Vermeintlich) anonymisierte Daten können wieder einen Personenbezug erhalten, wenn verschiedene Quellen miteinander korreliert werden.⁹¹³ So konnte beispielsweise SWEENEY im Jahr 2000 87 Prozent der US-Bürger eindeutig re-identifizieren, indem sie nur die Postleitzahl, das Geschlecht und das Geburtsstagsdatum miteinander kombinierte.⁹¹⁴ Überholt ist auch die Einschätzung, dass die Bestimmbarkeit fehle, wenn für die Identifizierung einer Person die «komplizierte Analyse einer Statistik» erforderlich wäre.⁹¹⁵ Mit den zur Verfügung stehenden technischen Mitteln verursacht eine Re-Identifizierung immer weniger Aufwand und eine Person wird immer leichter «be-

⁹⁰⁷ Die US-Gesetze schützen sog. *personally identifiable information* (PII), die mit der Identität oder den Eigenschaften einer Person verknüpft werden können: WOOD *et al.*, 215. Die Definition von PII in den USA ist enger gefasst als der Begriff der personenbezogenen Daten in der EU: NISSIM *et al.*, 710. Vgl. MRKONICH *et al.*, 17.

⁹⁰⁸ World Economic Forum 2013, 12.

⁹⁰⁹ WEBER/OERTLY, N 34; KASPER/WILDHABER, 212.

⁹¹⁰ SGK-SCHWEIZER, Art. 13 Abs. 2 BV, N 75.

⁹¹¹ Technische Lösungen sind z.B.: k-Anonymität, l-Diversität, *t-Closeness*, Randomisierung, Datenverteilung, Kryptografiertechniken und multidimensionale sensitivitätsbasierte Anonymisierung (MDSBA). Zur Erklärung dieser Begriffe: RAM MOHAN RAO *et al.*, 3. Vgl. die Leitlinien der Art.-29-Datenschutzgruppe zu den Anonymisierungsmassnahmen: Art.-29-Datenschutzgruppe 2014, 12–23. WEBER/OERTLY, N 12. Vgl. ISO/IEC 29100:2011 und ISO/IEC 15408-2:2008.

⁹¹² WEBER 2018, 102; TAMÖ-LARRIEUX, 230, m.w.H.; Fortschritt der Re-Identifizierungs- und Scheitern der Anonymisierungstechnologien: PURTOVA 2018, 78.

⁹¹³ Europäisches Parlament 2017, 8; BAERISWYL 2014, 53; DUISBERG, N 22. Siehe S. 38 und 74.

⁹¹⁴ SWEENEY, 2.

⁹¹⁵ So die Botschaft zum DSG im Jahr 1988: BBl 1988 II, 444–445; KASPER/WILDHABER, 212.

stimmbar» (im Sinne von Art. 3 lit. a DSGVO, Art. 4 lit. a E-DSG bzw. Art. 5 lit. a rev-DSG).⁹¹⁶

Es stellt sich somit die Frage, ob (künftig) alle People Analytics-Anwendungen in den Geltungsbereich des DSGVO fallen. Die bundesgerichtliche Rechtsprechung schränkt jedoch ein: Sie fordert für die Annahme der Bestimmbarkeit, dass die Datenbearbeiterin ein Interesse daran hat, den für eine (Re-)Identifizierung nötigen Aufwand zu betreiben (sog. relativer Charakter des Personendatums).⁹¹⁷ Das Interesse an der Re-Identifizierung ist gegeben, wenn aus Sicht der jeweiligen Inhaberin der Information⁹¹⁸ vernünftigerweise damit gerechnet werden muss, dass die Identifizierung erfolgt.⁹¹⁹

Ob die Verantwortliche ein Interesse an einer Re-Identifizierung verfolgt, ist abhängig vom konkreten Fall.⁹²⁰ Zu den Kriterien zur Bestimmung, ob ein Interesse besteht, gehört der objektiv erforderliche Aufwand (z.B. Kosten, Zeitaufwand), um eine bestimmte Information einer Person zuordnen zu können. Für die Identifizierbarkeit spricht eine geringe Anzahl analysierter Personen: Erhebt die Arbeitgeberin anonymisierte Profile von wenigen (den interessanten Schlüssel-)Mitarbeitern, wird es häufig ohne unverhältnismässigen Aufwand möglich sein, auf einen konkreten Arbeitnehmer zurückzuschliessen.⁹²¹ Auch die technischen Möglichkeiten sind in die Erwägung einzubeziehen. Algorithmen reduzieren den Aufwand und die Kosten für eine Re-Identifizierung.⁹²² Datenbearbeitungen, bei denen die KI mitmischet, werden eher vom Datenschutzrecht erfasst als eine Datenbearbeitung ohne KI.⁹²³

Es genügt nicht jede theoretische Möglichkeit der Identifizierung; ist der Aufwand derart gross, dass nach der allgemeinen Lebenserfahrung nicht damit gerechnet

⁹¹⁶ KASPER/WILDHABER, 212, m.w.H. Vgl. auch zur Rechtslage unter dem Übereinkommen 108: Europarat 2010, 21.

⁹¹⁷ BGE 136 II 508 E. 3.2. Vgl. Urteil BVGer A-3144/2008 vom 27.05.2009 E. 2.2.1. ROSENTHAL 2017a, 202; ROSENTHAL 2017b, N 14; BSK OR I-PORTMANN/RUDOLPH, Art. 328b OR, N 3; MORSCHER, 175–177; KASPER/WILDHABER, 212–213.

⁹¹⁸ BGE 136 II 508 E. 3.4; KASPER/WILDHABER, 213.

⁹¹⁹ WEBER/OERTLY, N 6; KASPER/WILDHABER, 213. Gleich verhält es sich unter dem Übereinkommen 108: Europarat 2018c, N 17.

⁹²⁰ KASPER/WILDHABER, 213.

⁹²¹ DZIDA, 542; KASPER/WILDHABER, 195.

⁹²² Vgl. WRIGLEY, 190. KASPER/WILDHABER, 195.

⁹²³ WRIGLEY, 190.

werden muss, dass ihn ein Interessent auf sich nehmen wird, liegt keine Bestimmbarkeit vor.⁹²⁴ Ein Argument gegen die Identifizierbarkeit liegt vor, wenn die Arbeitgeberin Daten von vielen (allenfalls nicht mehr nur Schlüssel-)Mitarbeitern auswertet, sodass eine Identifizierung konkreter Personen nicht oder nur mit unverhältnismässigem Aufwand möglich ist bzw. die Daten anonymisiert bleiben.⁹²⁵ Auch aufgrund technischer Grenzen kann das Interesse an der Re-Identifizierung nachlassen: Ein Algorithmus, der Milliarden von Daten auf bestimmte Werte hin filtert, kostet Zeit und Energie; ein Unternehmen wird ihn nur dort einsetzen, wo er erforderlich ist.⁹²⁶ Oft weiss die Arbeitgeberin nicht, welche Daten einen guten Arbeitnehmer auszeichnen, was eine Re-Identifizierung weniger wahrscheinlich macht.⁹²⁷ Zudem unterliegen Personendaten teilweise einer Halbwertszeit: Sie verlieren über die Zeit an Wert, wenn kein Zugang zu zusätzlichen neuen Informationen gegeben ist.⁹²⁸ Damit sinkt das Interesse an einer personenbezogenen Nutzung und Re-Identifizierung.⁹²⁹ Allerdings können Personendaten im Verlauf der Zeit auch wesentlich an Wert gewinnen, wenn sie mit anderen Datensätzen kombiniert werden können. Auf diese Möglichkeit der Wertsteigerung ist später zurückzukommen.⁹³⁰

Die von der Rechtsprechung vorgenommene Auslegung des Begriffs der Personendaten und der Bestimmbarkeit scheint für das Bundesgericht im Einklang mit der Rechtslage in der EU zu stehen.⁹³¹ Dieser Einschätzung kann jedoch nicht vorbehaltlos zugestimmt werden. Zwar ist für einen Teil der europäischen Lehre entscheidend, inwiefern es gerade der speichernden Stelle mit den ihr zur Verfügung stehenden Kenntnissen, Mitteln und Möglichkeiten mit verhältnismässigem Aufwand möglich ist, aggregierte Angaben einer Person zuzuordnen (sog. subjektive

⁹²⁴ BSK OR I-PORTMANN/RUDOLPH, Art. 328b OR, N 3. Vgl. E. 26 DSGVO. KASPER/WILDHABER, 211–212.

⁹²⁵ DZIDA, 543; KASPER/WILDHABER, 200.

⁹²⁶ Vgl. KENYON MILES, How Wechat filters images for one billion users, 14.08.2018, abrufbar unter <<https://citizenlab.ca>> (besucht am 31.05.2020); Unverhältnismässigkeit, wenn die Rechenkapazitäten zu gering sind, um den Personenbezug in akzeptablem Zeitraum herzustellen: KARG, 526; KASPER/WILDHABER, 213.

⁹²⁷ FAZ vom 01.03.2018, Lieber Roboter als Personaler, abrufbar unter <www.faz.net> (besucht am 31.05.2020); KASPER/WILDHABER, 213.

⁹²⁸ EGGIMANN, 9.

⁹²⁹ ROSENTHAL 2017a, 201; KASPER/WILDHABER, 213.

⁹³⁰ Siehe S. 177.

⁹³¹ BGE 136 II 508 E. 3.6. Vgl. KASPER/WILDHABER, 215.

Perspektive).⁹³² Auch versichert die Art.-29-Datenschutzgruppe, dass die rein hypothetische, abstrakte Möglichkeit zur Bestimmung einer Person nicht ausreicht, um die Person als bestimmbar anzusehen.⁹³³ Aber die DSGVO verlangt, dass «alle objektiven Faktoren» berücksichtigt werden müssen, die dafür sprechen, dass eine «Verantwortliche oder eine andere Person» die Re-Identifizierung vornimmt (E. 26 Sätze 2–3 DSGVO).⁹³⁴ Die nicht ganz eindeutige Rechtslage steht am Ursprung des Lehrstreits betreffend Typisierungen (dazu sogleich).

5.4.4 Typisierungen

a) Zum Begriff der Typisierung

Aufgrund der beschriebenen Rechtsprechung zum Interesse an der Re-Identifizierung will eine Lehrmeinung einen bedeutenden Teil der People Analytics-Anwendungen vom Geltungsbereich des DSG ausnehmen. Dies betrifft die Fälle der reinen Typisierung von Arbeitnehmern (auch «Aussondern», entsprechend dem Wortlaut von E. 26 DSGVO, oder «Singularisierung»⁹³⁵ in wortschöpferischer Anlehnung an den englischen Wortlaut «*singling out*»⁹³⁶). Das Individuum wird hier zwar «eindeutig individualisiert» in dem Sinne, dass es allein von der Restgruppe ausgesondert wird.⁹³⁷ Aber die Arbeitgeberin will gar nicht wissen, wer die reale Person ist. Es interessiert sie nur beispielsweise, was die Führungsstärke eines bestimmten Typs von Arbeitnehmern auszeichnet.⁹³⁸ Das Individuum interessiert nur insoweit, als es mit anderen korreliert werden kann, beispielsweise ob

⁹³² Die subjektive Perspektive entspreche der h.M., so: SCHEFZIG, 106. Es wird kritisiert, dass bei Annahme einer objektiven Perspektive selbst Vorgänge erfasst werden könnten, bei denen sich der Verantwortliche nicht bewusst ist, dass die Information personenbezogen sein könnte, und er Personen informieren müsste, die er nicht kennt bzw. mit unverhältnismässigem Aufwand identifizieren müsste: WRIGLEY, 191.

⁹³³ Art.-29-Datenschutzgruppe 2007, 17. Vielmehr entscheide der Kontext der jeweiligen Situation über das Vorliegen von Bestimmbarkeit: Art.-29-Datenschutzgruppe 2007, 15.

⁹³⁴ Sog. «*objective approach*»: FEILER *et al.*, Art. 4 DSGVO N 3; auch sog. «absoluter Ansatz», von dem die Europäische Kommission schon im Entwurf vom 25.02.2012 zur DSGVO ausging: LIEDKE, 144.

⁹³⁵ ROSENTHAL 2017a, 198; «singularisiert»: Art.-29-Datenschutzgruppe 2007, 16.

⁹³⁶ KASPER/WILDHABER, 213.

⁹³⁷ «Singularisierung» bedeute eine «eindeutige Individualisierung»: ROSENTHAL 2017a, 200.

⁹³⁸ Vgl. KASPER/WILDHABER, 213, m.w.H.

aufgrund einer Korrelation zwischen einem Mitarbeiter und der Vergleichsgruppe auf besondere Risiken oder Verhaltensweisen bei ihm geschlossen werden kann.⁹³⁹ Schaltet die Arbeitgeberin ein Inserat für eine Führungsposition, muss es einen bestimmten Zielmarkt erreichen, jedoch nicht bestimmte Personen.⁹⁴⁰ Um den Zielmarkt effektiv anzusprechen, müssen die potenziellen Bewerber nicht identifiziert, sondern lediglich «klassifiziert» werden.⁹⁴¹

b) Argumentation gegen den Datenschutz bei Typisierungen

Namentlich ROSENTHAL vertritt die Meinung, dass Typisierungen bloss als Indiz der Bestimmbarkeit gewertet werden, allerdings nicht alleine zur Anwendbarkeit des DSG genügen könnten.⁹⁴² Weil die betroffenen Arbeitnehmer nach traditionellem Verständnis anonym blieben, könne die Datenbearbeitung nicht direkt auf sie wirken und sie in ihrer Persönlichkeit verletzen.⁹⁴³ Eine solchermaßen restriktive Auslegung des DSG-Geltungsbereichs versucht zunächst, Situationen gerecht zu werden, in denen die Bearbeitung von Personendaten die Persönlichkeit kaum zu beeinträchtigen droht und es unverhältnismässig wäre, die strikte Einhaltung sämtlicher Datenschutzpflichten des DSG zu verlangen.

Beispielsweise müssten beim Fehlen des erforderlichen Re-Identifizierungs-Interesses das Scannen zum Viren- oder Betrugsschutz oder eine nicht personalisierte Protokollierung des Internet- und E-Mail-Verkehrs ausserhalb des DSG verbleiben.⁹⁴⁴ Ebenso wenig existieren Personendaten im Sinne des DSG, wenn die Arbeitgeberin die Auslastung der Infrastruktur misst, ohne die persönliche Anwesenheit einzelner Arbeitnehmer zu kontrollieren (z.B. Sensor zur Lüftungsregulierung, der die Anzahl Anwesender und den CO₂-Gehalt im Sitzungszimmer misst).⁹⁴⁵ Auch ist eine Anwendbarkeit des DSG weniger wahrscheinlich bei rein produktbezogenen Überwachungen als bei der Überwachung eines Vorgangs, an dem Personen beteiligt sind (z.B. die Bedienung einer Maschine).⁹⁴⁶

⁹³⁹ MITTELSTADT, 478.

⁹⁴⁰ Vgl. bzgl. Werbetreibender und Werbe-Zielmärkte: MITTELSTADT, 478.

⁹⁴¹ MITTELSTADT, 478.

⁹⁴² ROSENTHAL 2017a, 198. Vgl. KASPER/WILDHABER, 213–214, m.w.H.

⁹⁴³ ROSENTHAL 2017a, 200.

⁹⁴⁴ STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 18. Vgl. KASPER/WILDHABER, 214, m.w.H. RUDIN 2001, 8.

⁹⁴⁵ Vgl. KASPER/WILDHABER, 214, m.w.H.

⁹⁴⁶ KASPER/WILDHABER, 214.

Anscheinend sollten aber auch Typisierungen mit grösserem Potenzial zur Einwirkung auf die Persönlichkeit vom DSG befreit sein: HORNUNG findet, dass die «Bändigung der durch Big Data-Wissen generierten Macht» überwiegend ausserhalb des Datenschutzrechts erfolgen müsse.⁹⁴⁷ Datenschutz sei gemäss anderen Vertretern der deutschen Lehre kein umfassendes Autonomieschutzrecht und nicht auf den Umgang mit nichtpersonenbezogenen Daten und daraus eventuell resultierenden Eingriffen ausgerichtet.⁹⁴⁸

In der Konsequenz fallen genetische Daten und IP-Adressen nicht als Personen-daten unter das DSG, wenn der Arbeitgeberin aggregierte Daten genügen.⁹⁴⁹ Grundsätzlich kein Interesse der Arbeitgeberin an einer Re-Identifizierung ist erkennbar, wenn sie aus aggregierten Datenbeständen der Belegschaft generische Muster und Prinzipien für künftige Personalentscheidungen ablesen will.⁹⁵⁰ So erforscht beispielsweise McDonald's bewährte Vorgehensweisen (*best practices*) zu Führungsstilen;⁹⁵¹ Google entwickelte in seiner Oxygen-Studie Anforderungsprofile für Führungskräfte;⁹⁵² und der People Analytics-Dienstleister Humanyze, der über Mitarbeiterausweise die Stimm-lage und Sprechlänge bei Konversationen auswertet, nicht aber den Gesprächsinhalt, liefert seinen Kunden ein ganzheitliches Trendbarometer, jedoch keine Berichte über einzelne Arbeitnehmer.⁹⁵³

c) Argumentation für den Datenschutz bei Typisierungen

aa) Hinterfragung der Rechtsprechung und Lehre

Nach der vorliegend vertretenen Auffassung sind sowohl die Rechtsprechung zum notwendigen Interesse an der Re-Identifizierung als auch die Lehrmeinung, Typi-

⁹⁴⁷ HORNUNG, 93; Rechtsgüterschutz durch Wettbewerbsrecht und sonstiges Regulierungsrecht: HOFFMANN-RIEM, 39.

⁹⁴⁸ HOFFMANN-RIEM, 53. Welche Konsequenzen sich aus der Zuordnung einer Prognosewahrscheinlichkeit zu einem Arbeitnehmer für Letzteren ergeben, sei für die Einordnung als personenbezogene Daten belanglos: CULIK, 125–126; SCHEFZIG, 116.

⁹⁴⁹ Vgl. ROSENTHAL 2017a, 198. Aggregierte Daten sind Daten, die zu analytischen, statistischen oder Forschungszwecken zusammengefasst wurden: GILBERT, 269. Vgl. KASPER/WILDHABER, 214.

⁹⁵⁰ Vgl. KASPER/WILDHABER, 214.

⁹⁵¹ Siehe S. 55.

⁹⁵² NIKLAS/THURN, 1589.

⁹⁵³ KATZ MIRANDA, The creative ways your boss is spying on you, 08.12.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020); COLLIER, 6.

sierungen lägen ausserhalb des DSG, infrage zu stellen.⁹⁵⁴ Hierfür ist zunächst der Begriff der Identität zu klären (dazu sogleich), bevor auf die Argumente eingegangen werden kann, die für die Anwendbarkeit des DSG auf Typisierungen sprechen (dazu später, S. 165–172).

bb) Begriff der Identität

Die Beurteilung, ob Typisierungen unter das DSG fallen sollen, bedingt eine Auseinandersetzung mit den Begriffen der Bestimmtheit und Bestimmbarkeit, weil bei Typisierungen unklar ist, ob die Betroffenen hinreichend bestimmt sind für die Anwendbarkeit des DSG (vgl. Art. 3 lit. a DSG, Art. 4 lit. a E-DSG, Art. 5 lit. a rev-DSG). «Bestimmt» und «bestimmbar» werden oft gleichgesetzt mit «identifiziert» und «identifizierbar».⁹⁵⁵ Die Begriffe der Identifizierung oder Identität treten aber im DSG und E-DSG nur am Rande in Erscheinung.⁹⁵⁶ Deshalb muss anderswo nach Antworten gesucht werden auf die Frage, was Identität bedeutet.

Auch ein Blick auf das EU-Recht lohnt sich, um den Sinn der Identität zu ergründen, nicht zuletzt deshalb, weil jene Normen das schweizerische Recht beeinflussen.⁹⁵⁷ Um den Begriff der Identität zu verstehen, kann es helfen, mit der gegen teiligen «Anonymität» zu beginnen. Sie bedeutet wörtlich «Namenlosigkeit».⁹⁵⁸ Doch geht es beim Datenschutzrecht nicht allein um den Namen, sondern um das Nichtoffenlegen der Identität.⁹⁵⁹ Auf einer «Identitätsachse» sind Anonymität und Identität die Gegenpole, das (idealtypische) «Nichts-Wissen» das Gegenstück zum (idealtypischen) «Alles-über-eine-Person-Wissen».⁹⁶⁰

Die DSGVO führt die Begriffe der Identität und Identifizierung wesentlich häufiger und prominenter auf als das DSG.⁹⁶¹ Der Begriff der Identität ist unter der

⁹⁵⁴ So auch KASPER/WILDHABER, 215, und PURTOVA 2018, 75.

⁹⁵⁵ Statt vieler Autoren hier BSK DSG-BLECHTA, Art. 3 DSG, N 10: «Bestimmbar ist eine Person», wenn «die Möglichkeit besteht, ihre Identität festzustellen».

⁹⁵⁶ «Identifikation», Art. 36 Abs. 4 lit. c DSG; «identifizieren», Art. 4 lit. c Ziff. 4 E-DSG bzw. Art. 5 lit. c Ziff. 4 rev-DSG. Das rev-DSG spricht zudem an einigen Stellen von der «Identität des Verantwortlichen» (z.B. Art. 11 Abs. 2 lit. a E-DSG, Art. 12 Abs. 2 lit. a rev-DSG).

⁹⁵⁷ Siehe S. 109–114.

⁹⁵⁸ Von altgr. *án-* «an-» (ohne), und *ónoma* «ónoma» (Name).

⁹⁵⁹ RUDIN 2008, 6.

⁹⁶⁰ RUDIN 2004a, 5. Zwischen «personenbezogen» und «anonym» gebe es «kein rechtliches Zwischenstadium»: KARG, 520.

⁹⁶¹ Siehe insbesondere E. 26 und 57 sowie Art. 4 Ziff. 1, 5 und 14 und Art. 11 DSGVO.

DSGVO breit zu verstehen. Sowohl die physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle als auch die soziale Identität werden geschützt (Art. 4 Nr. 1 Teilsatz 2 DSGVO). Die DSGVO sieht eine natürliche Person bereits als identifizierbar an, wenn diese beispielsweise mittels Zuordnung zu einer Online-Kennung identifiziert werden kann (Art. 4 Nr. 1 Teilsatz 2 DSGVO). Es ist somit nicht erforderlich, einen Arbeitnehmer mit Namen und Adresse zu kennen, damit er als identifiziert gilt und der Schutz der DSGVO greift.⁹⁶²

Wie viel Interpretationsspielraum im Begriff der Identität steckt, zeigt auch die Philosophie. Der deutsche Philosoph HÖFFE weist darauf hin, dass ein identisches Wesen zu verschiedenen Zeiten unterschiedliche, sogar entgegengesetzte Eigenschaften haben kann (ein Baum erst klein, dann gross, erst jung, dann alt).⁹⁶³ Beim Menschen gibt es zudem eine doppelte Perspektive auf die Identität, je nachdem, ob ein beobachtender Dritter über das Subjekt spricht (Aussenperspektive, Fremdbild) oder die Person über sich selbst (Innenperspektive, Selbstbild).⁹⁶⁴ Ein weiterer deutscher Philosoph, MITTELSTADT, differenziert zwischen der «Offline-Identität» und «Profiling-Identität». Erstere setzt sich aus direkten Identifikatoren einer Person wie Name und Adresse zusammen, Letztere aus Variablen, die sich erst durch die Korrelation mit einer Vergleichsgruppe als relevant erweisen, etwa das Verhalten und demografische Merkmale. Die Profiling-Identität kann bestenfalls eine unvollkommene Spiegelung der Persönlichkeit sein, da sie auf die Attribute der Vergleichsgruppe reduziert ist.⁹⁶⁵

Gestützt auf die vorstehenden Ausführungen erweist sich der datenschutzrechtliche Begriff der Identität als breit und vielfältig. Schon ab einer relativ tiefen Schwelle kann eine Person als identifiziert gelten, etwa wenn ihre IP-Adresse bekannt ist. Das Vorliegen von Identität kann nur dann eindeutig verneint werden, wenn nichts über eine Person bekannt ist bzw. wenn sie anonym ist. Die mit dem Begriff der Identität im Wesentlichen gleichbedeutende, im DSG massgebliche «Bestimmtheit» kann daher ebenfalls schon bei Vorliegen von verhältnismässig wenigen Informationen bejaht werden.

⁹⁶² «Ein Name ist zur Identifizierung einer Person keineswegs immer notwendig»: Art.-29-Datenschutzgruppe 2007, 16.

⁹⁶³ HÖFFE, 98.

⁹⁶⁴ HÖFFE, 98.

⁹⁶⁵ MITTELSTADT, 478. Ähnlich spricht der Europarat von «*digital identity*»: Europarat 2018c, N 18.

cc) Generelle rechtliche Erfassung von Typisierungen

Zufolge des offenen Begriffs der Identität tendiert das europäische Ausland dazu, Typisierungen generell dem Datenschutzrecht zu unterwerfen. Die EU sieht in einer Typisierung ein Indiz für das Vorliegen von Personendaten und somit für die Anwendbarkeit der DSGVO (vgl. E. 26 Satz 3 DSGVO zum «Aussondern»). Die EU stellt sich damit auf den Standpunkt, dass ein Schutzbedürfnis auch bestehen kann, selbst wenn ein Betroffener nicht im traditionellen Sinn «bestimmt» ist. Als Exkurs sei an dieser Stelle auf die EuGH-Rechtsprechung zum Erfordernis einer Einwilligung für den Einsatz von Cookies unter der Richtlinie 2002/58/EG («E-Privacy») erinnert. Das Einwilligungserfordernis gilt selbst dann, wenn mit dem Cookie keine Personendaten bearbeitet werden und daher die DSGVO nicht zur Anwendung kommt.⁹⁶⁶ Der EuGH begründet dies damit, dass alle in Endgeräten gespeicherten Informationen, unabhängig davon, ob es sich um personenbezogene Daten handelt, Teil der mit der Richtlinie 2002/58/EG zu schützenden Privatsphäre der Nutzer sind.⁹⁶⁷

Gemäss dem Europarat genügt für die Anwendbarkeit des Übereinkommens 108 eine «Individualisierung», die es ermöglicht, jemanden anders als den Rest zu behandeln.⁹⁶⁸ Es braucht nicht notwendigerweise eine «Identifizierung».⁹⁶⁹ Um eine Individualisierung handelt es sich auch, wenn man sich auf ein spezifisches Gerät (z.B. Computer oder Mobiltelefon) beziehen kann basierend auf einer Identifikationsnummer, einem Pseudonym, biometrischen oder genetischen Daten, Ortungsdaten oder einer IP-Adresse.⁹⁷⁰

⁹⁶⁶ Urteil EuGH vom 01.10.2019, Planet49, C-673/17, EU:C:2019:801, N 71. Der Entscheid ist umso erstaunlicher, als der Titel der Richtlinie 2002/58/EG sich auf «personenbezogene Daten» bezieht. Kritisch zur EuGH-Rechtsprechung und mit dem Hinweis, dass in der Schweiz über Cookies nur informiert werden muss, wenn sie personenbezogen sind: ROSENTHAL DAVID, Cookies: comment la CJUE lutte-t-elle contre la mentalité du «cliquer et fermer sans regarder», abrufbar unter <www.lawinside.ch> (besucht am 31.05.2020).

⁹⁶⁷ Urteil EuGH vom 01.10.2019, Planet49, C-673/17, EU:C:2019:801, N 70–71. Der Bezug eines Cookies zu einem Endgerät genüge für die Anwendbarkeit der Richtlinie 2002/58/EG, unabhängig davon, ob der Benutzer des Geräts identifiziert werden könne: Europarat 2010, 23.

⁹⁶⁸ «*The notion of <identifiable> refers not only to the individual's civil or legal identity as such, but also to what may allow to <individualise> or single out (and thus allow to treat differently) one person from others*»: Europarat 2018c, N 18.

⁹⁶⁹ Europarat 2010, 22.

⁹⁷⁰ Europarat 2018c, N 18.

Verschiedene deutsche Rechtswissenschaftler wollen Typisierungen datenschutzrechtlich regulieren: Der Nutzen einer Datenanalyse besteht darin, eine Aussage über die Wahrscheinlichkeit des Vorliegens des jeweiligen Merkmals bei dem Betroffenen zu machen.⁹⁷¹ Beschreibt beispielsweise der aus People Analytics gewonnene Erfahrungssatz abstrakt die Kriterien, unter welchen eine Vergleichsgruppe von Arbeitnehmern Zukunftsaussichten oder eben keine hat, will die Arbeitgeberin dieses Wissen konkret auf ihre Belegschaft oder die Bewerber ummünzen. Durch diesen Bezug des generellen Erfahrungssatzes auf eine konkrete Person wird die Gruppenwahrscheinlichkeit den persönlichen Verhältnissen des Betroffenen zugeschrieben.⁹⁷² Ab diesem Moment der Bezugnahme sind die Aussagen zur Vergleichsgruppe als personenbezogene Daten zu werten.⁹⁷³ Es handelt sich um eine «indirekte Identifizierung».⁹⁷⁴ Dies gilt auch, wenn der Erfahrungssatz auf eine Person angewendet wird, über die gar keine Daten erhoben worden sind.⁹⁷⁵

Wenn den Typisierungen aber generell ein Personenbezug attestiert wird, führt dies zum Problem, dass das strenge, nicht skalierbare Regime des Datenschutzrechts ausgefahren wird, selbst wenn die Bearbeitung von Personendaten die Persönlichkeit kaum beeinträchtigt. Dies kann zu einer «Systemüberlastung» führen in dem Sinne, dass das Datenschutzrecht nicht eingehalten wird.⁹⁷⁶ Eine generelle

⁹⁷¹ SCHEFZIG, 116.

⁹⁷² SCHEFZIG, 115; HOFFMANN-RIEM, 54.

⁹⁷³ Die betroffene Person muss somit über die Existenz dieser Einordnung und über die Kriterien aufgeklärt werden, die zu dieser Beurteilung geführt haben (Art. 14, Art. 1 lit. a DSGVO). DÄUBLER, N 429a; SCHEFZIG, 116; sog. «mittelbarer Personenbezug»: HOFFMANN-RIEM, 45.

⁹⁷⁴ Nach dem Konzept der DSGVO spiele es keine Rolle, ob sich die Person, auf die sich Daten bezögen, namentlich identifizieren lasse. Die Zuordnung zu einer Person, die von anderen Personen unterscheidbar sei, genüge. Die E-Mail-Adresse «hase69@gmy.de» erfülle diese Voraussetzungen kraft ihrer Funktion als Adresse eines bestimmten Individuums: HÄRTING, N 120. Typisierung sei eine «indirekte Identifikation», die dem Anwendungsbereich des europäischen Datenschutzrechts unterstehe, wobei die Wahrscheinlichkeit einer Nutzung von Mitteln zur Identifikation einschliesslich Kosten und Zeitaufwand zu berücksichtigen seien: HERMSTRÜWER, 105.

⁹⁷⁵ Beeinträchtigung der Persönlichkeit bei Personen, die nur indirekt oder gar nicht in die Datenbearbeitung involviert sind: MATZNER, 97–98. Die prädiktive Analytik berechnet die Aussagen zu einer Person in erster Linie gestützt auf die Daten anderer Personen bzw. Dritte seien die «Haupterzeuger» der Daten für die Prognosemodelle: DREYER, 138.

⁹⁷⁶ PURTOVA 2018, 75.

datenschutzrechtliche Erfassung von Typisierungen vermag somit nicht zu überzeugen.

**dd) Einzelfallweise rechtliche Erfassung von Typisierungen
in Abhängigkeit von ihrem Risikopotenzial**

i. Übersicht

Nach der hier vertretenen Meinung sollte im Einzelfall beurteilt werden, ob Typisierungen durch das DSG erfasst werden. Dabei sollte die Anwendbarkeit des DSG nicht mehr nur vom formalen Kriterium des Vorliegens von Daten mit personenbezogenem Inhalt abhängen, da dieser Anknüpfungspunkt stets Probleme und Unklarheiten mit sich bringt (dazu sogleich). Stattdessen sollte (auch) das von einer Typisierung ausgehende persönlichkeitschutzrechtliche Risiko über die Geltung des DSG (mit-)entscheiden. Es sind Beispielfälle aufzuzeigen, in denen Typisierungen ein hohes Risiko verkörpern und somit datenschutzrechtlich reguliert werden sollten (dazu später, S. 170–172).

ii. Verschwimmende Grenzen zwischen den Datenkategorien

Das DSG versucht, theoretisch trennscharfe Linien zwischen den Datenkategorien der Sachdaten, Personendaten und besonders schützenswerten Personendaten zu ziehen. Aber möglicherweise braucht es etwas Distanz zu dem gegenwärtigen Datenschutzsystem. Zu beachten ist etwa, dass die Kategorie der besonders schützenswerten Daten (Art. 3 lit. c DSG, Art. 4 lit. c E-DSG, Art. 5 lit. c rev-DSG) von der Bundesverfassung nicht zwingend vorgegeben ist.⁹⁷⁷

GASSER postuliert, das Datenschutzrecht solle sich grundlegend neu ausrichten und sich von Begriffen wie «Personendaten» und «Anonymisierung» verabschieden.⁹⁷⁸ PURTOVA⁹⁷⁹ sowie RICHARDS und KING⁹⁸⁰ liegen auf der gleichen Linie. NISSIM und WOOD doppelten nach und fordern eine Abkehr von den Dichotomien

⁹⁷⁷ Die Bundesverfassung unterscheidet im Gegensatz zum DSG nicht zwischen besonders schützenswerten und anderen Personendaten (vgl. Art. 13 Abs. 2 BV): BELSER 2011a, § 6 N 91 und 120. Einschränkungen im Bereich sensibler Personendaten und Persönlichkeitsprofile sind aber besonders rechtfertigungsbedürftig (nach Art. 36 BV): SGK-SCHWEIZER, Art. 13 Abs. 2 BV, N 77.

⁹⁷⁸ GASSER 2016, 68. Es ergibt immer weniger Sinn, formale Datenkategorien auseinanderzuhalten: BERANEK ZANON, 113.

⁹⁷⁹ «*Abandon the concept of personal data as a cornerstone of data protection altogether*»: PURTOVA 2018, 79.

⁹⁸⁰ Simplistisch sei die Vorstellung, dass Privatsphäre ein binärer «*On-or-off*»-Zustand sei: RICHARDS/KING, 396.

«private/allgemein zugänglich gemachte» und «gewöhnliche/besonders schützenswerte» Personendaten.⁹⁸¹

Die theoretische, starre Kategorisierung von Daten durch das DSG in Abhängigkeit von ihrem Inhalt (anonym, personenbezogen oder besonders schützenswert) steht im Gegensatz zur heutigen und künftigen «hypervernetzten» Welt.⁹⁸² In der Realität ist der Status eines Datums, beispielsweise «personenbezogen», dynamisch und kann sich im Verlauf des Daten-Lebenszyklus ändern.⁹⁸³ Die Definition personenbezogener Daten ist abhängig vom Kontext und von sozialen Normen.⁹⁸⁴ Bereits die Rechtsprechung, wonach es für die Qualifikation als Personendaten auf die Wahrscheinlichkeit der Re-Identifizierung ankommt, rückt den Kontext (das momentane Interesse der jeweiligen Datenbearbeiterin an der Re-Identifizierung) ins Zentrum.⁹⁸⁵ Die Veränderbarkeit des Datenstatus führt zu einer Verwischung der Grenzen zwischen den Datenkategorien. Die Vorstellung von datenschutzrechtlich «belanglosen Daten» taugt nicht mehr angesichts der möglichen Verwendungszwecke, die plötzlich zu einem Personenbezug führen können.⁹⁸⁶ Es kann beispielsweise nicht abstrakt gesagt werden, ob die IP-Adresse eines Computers ein Personendatum ist.⁹⁸⁷ Es wird zum Normalzustand, dass «alle Daten einen Personenbezug aufweisen» können,⁹⁸⁸ etwa durch Verknüpfung mit andern Datensät-

⁹⁸¹ Vgl. NISSIM/WOOD, 6.

⁹⁸² Vgl. die Forderung nach einer Aktualisierung der OECD-Leitlinien 1980, welche der heutigen Datenschutzgesetzgebung zugrunde liegen: World Economic Forum 2013, 16.

⁹⁸³ Zum Daten-Lebenszyklus: S. 19–20.

⁹⁸⁴ «On ne peut se limiter au seul contenu des informations: il faut également tenir compte du contexte [...] du traitement»: MEIER PHILIPPE, N 334. World Economic Forum 2013, 7. Für die Kategorie besonders schützenswerter Personendaten gelte, dass die Sensibilität von Daten niemals abstrakt anhand einzelner Daten definiert werden könne, sondern immer nur konkret mithilfe des spezifischen Bearbeitungszusammenhangs: HAAS, N 7–8. BOLLIGER *et al.*, 227.

⁹⁸⁵ Siehe S. 157. Zur europäischen Rechtsprechung: PURTOVA 2018, 47.

⁹⁸⁶ Urteil Bundesverfassungsgericht [Deutschland] 1 BvR 209/83 vom 15.12.1983 N 150; WACHTER/MITTELSTADT, 615.

⁹⁸⁷ SCHWEIZER/RECHSTEINER, N 2.8.

⁹⁸⁸ «All data is personal»: PURTOVA 2018, 42.

zen.⁹⁸⁹ Deshalb ist es nur eine Frage der Zeit, bis der Mangel an Rechten an nicht personenbezogenen Daten zu einem Problem werden wird.⁹⁹⁰

Die Denkweise, dass (nur) die Identifizierung die Persönlichkeit beeinträchtigen und somit den Datenschutz berufen könne, ist teilweise verfehlt: In der Identifizierung liegt nicht das grösste Datenschutzproblem.⁹⁹¹ Im Gegenteil, ironischerweise wäre bisweilen eine genaue Identifizierung sogar erwünscht: Es wird beklagt, People Analytics behandle Personen nicht mehr als eigenständige Individuen, sondern nur noch als Mitglied einer Gruppe bzw. als Profiling-Identitäten.⁹⁹² Das Problem dabei ist, dass Gruppenprofile nur für die Gruppe und die Mitglieder der Gruppe zutreffen, nicht aber für die Einzelpersonen als solche.⁹⁹³ Die Bedeutung, die einer bestimmten Gruppe gegeben und damit dem Einzelnen auferlegt wird, spiegelt nicht unbedingt sein Selbstverständnis wider.⁹⁹⁴

Die rigide Ausrichtung an der Identifizierbarkeit zieht realwirtschaftliche Folgen nach sich: Wenn die Geltung des Gesetzes davon abhängt, ob eine Information anonym oder personenbezogen ist, erstaunt es nicht, dass die meisten technischen Lösungen zum Persönlichkeitsschutz auf Anonymisierung abzielen.⁹⁹⁵ Wie dargelegt ist aber oft eine Re-Identifizierung möglich.⁹⁹⁶ Der Persönlichkeitsschutz ist somit nicht gewahrt und durch die Anonymisierung geht wertvolles Wissen verloren. Eine Umorientierung des DSG könnte den Weg für neuere technische Konzepte zum Schutz der Persönlichkeit ebnen, welche beispielsweise das ursprüng-

⁹⁸⁹ Selbst Wetterdaten seien als Personendaten zu qualifizieren, wenn sie in Kombination mit andern Datensätzen dazu verwendet würden, das Verhalten bestimmter Personen zu beeinflussen: PURTOVA 2018, 58.

⁹⁹⁰ Zur schweizerischen DSG-Revision BOLLIGER *et al.*, 227. Vgl. EDWARDS/VEALE, 82, und Europäische Kommission, Synopsis report of the public consultation on building a European data economy, 07.09.2017, abrufbar unter <<https://ec.europa.eu>> (besucht am 31.05.2020). Von anonymisierten Daten kann ein – zumindest latentes – Risiko der Persönlichkeitsbeeinträchtigung ausgehen: WACHTER/MITTELSTADT, 617; PURTOVA 2018, 80.

⁹⁹¹ MATZNER, 98.

⁹⁹² Vgl. HÄNOLD, 130. Siehe zur Profiling-Identität S. 164.

⁹⁹³ HÄNOLD, 130.

⁹⁹⁴ MITTELSTADT, 479–480.

⁹⁹⁵ RAM MOHAN RAO *et al.*, 3.

⁹⁹⁶ Siehe S. 157.

liche Format und die Vielfalt der Daten beibehalten, aber die sensiblen Attribute vom Rest der Daten trennen.⁹⁹⁷

Insgesamt ist festzustellen, dass die Grenzen zwischen den Datenkategorien verschwimmen. Dies verursacht Unklarheiten bei der Beantwortung der Frage, ob bei einer Typisierung Personendaten vorliegen. Es erscheint nicht sachgerecht, allein den (personenbezogenen oder anonymen) Inhalt der Daten und damit ein formales Kriterium über die Anwendbarkeit des DSG entscheiden zu lassen. Nach dem hier vertretenen Standpunkt ist der Geltungsbereich des DSG risikoorientiert auszulegen, weshalb als Nächstes zu ermitteln ist, in welchen Fällen ein hohes persönlichkeitschutzrechtliches Risiko mit der Typisierung einhergeht.

iii. *Typisierungen mit hohem persönlichkeitschutzrechtlichem Risiko*

Für die in der besprochenen Literatur⁹⁹⁸ verlangte Neuausrichtung des Datenschutzrechts ist nach der hier vertretenen Meinung beim Risiko anzusetzen.⁹⁹⁹ Auch nach Ansicht der amerikanischen Behörde FTC sollten Daten umfassend auf ihre Auswirkungen auf die Privatsphäre hin untersucht werden, während die Unterscheidung zwischen Daten mit und ohne Personenbezug verschwommen sei.¹⁰⁰⁰ Eine Orientierung am potenziellen Risiko, das von der Datenbearbeitung für die Persönlichkeit der Betroffenen ausgeht, würde es ermöglichen, sich von der binären Betrachtungsweise (Personendaten/anonymisierte Daten) zu lösen und die Natur der Daten eher graduell zu betrachten. Gleichzeitig rückt damit die Wirkung der Datenbearbeitung auf die Menschen in den Fokus und das Datum selbst in den Hintergrund.

Beispielsweise sollten nach Ansicht des Autors Typisierungen in den folgenden drei Fällen der datenschutzrechtlichen Regulierung unterstehen, in denen eine hohe Gefahr für die Persönlichkeit droht. Erstens kann eine solche Gefahr etwa bestehen, wenn ein Mensch auf ein Profil reduziert wird, das als Grundlage für

⁹⁹⁷ Eine solche neue technische Lösung ist das sog. *Data-Lake-Konzept*: RAM MOHAN RAO *et al.*, 9–10. Vgl. NISSIM *et al.*, 690.

⁹⁹⁸ Siehe S. 167.

⁹⁹⁹ Siehe auch S. 140. Vgl. GUIHOT *et al.*, 452: «*The high costs of, and challenges to, effective regulatory intervention require that the attention of regulators should be carefully focused on the areas posing the greatest risk.*» Ähnlich verlangt PURTOVA eine Ausrichtung des Datenschutzrechts an den «*information-induced harms*», womit sie alle negativen Konsequenzen der Datenbearbeitung für Einzelpersonen oder die Gesellschaft meint: PURTOVA 2018, 80.

¹⁰⁰⁰ Bzgl. PII und non-PII: FTC 2012, 19; NISSIM *et al.*, 709.

einschneidende Entscheidungen über ihn dient, obwohl es seiner Identität nicht entspricht.¹⁰⁰¹ Dies ist etwa der Fall bei der erwähnten People Analytics-Anwendung,¹⁰⁰² die in Bezug auf sämtliche Mitarbeiter, die in den vergangenen fünf Jahren nicht befördert wurden, die Beendigung des Arbeitsverhältnisses vorschlägt. Es ist möglich, dass jemand mit seiner seit Jahren unveränderten Stellung im Unternehmen zufrieden ist, auf Beförderungen verzichtet und trotzdem motiviert und zuverlässig arbeitet. Eine Kündigung allein basierend auf dem Vorschlag des Algorithmus wäre daher unangemessen. Hier erscheint es vertretbar, den Anwendungsbereich des DSG zu eröffnen. Dies würde die Überprüfung erlauben, ob das Richtigkeitsgebot (Art. 5 DSG, Art. 5 Abs. 5 E-DSG, Art. 6 Abs. 5 rev-DSG) eingehalten wurde bzw. ob das Profil («seit fünf Jahren nicht befördert») die Identität des Arbeitnehmers («nicht motiviert und unzuverlässig») korrekt beschreibt. Die beiden hier eigenständig formulierten Kriterien der einschneidenden Entscheidung und der Diskrepanz zwischen Profil und Identität schaffen Klarheit, wann ein hohes Risiko besteht.¹⁰⁰³ Im selben Zug wird klargestellt, dass nicht jede Reduktion auf ein Profil zu einer Persönlichkeitsverletzung führt.¹⁰⁰⁴ Der Gesetzgeber hat bisher für das Bearbeiten von «Persönlichkeitsprofilen» (Art. 3 lit. d DSG) einheitliche Regeln aufgestellt, ohne auf das mit dem Profil verbundene Risiko Rücksicht zu nehmen. Es ist zu begrüßen, dass sich das Parlament dazu entschlossen hat, im totalrevidierten DSG zwischen einem Profiling¹⁰⁰⁵ mit hohem Risiko (Art. 4 lit. f^{bis} E-DSG, Art. 5 lit. g rev-DSG) und dem übrigen Profiling (Art. 4 lit. f E-DSG, Art. 5 lit. f rev-DSG) zu unterscheiden. Bei einem Profiling mit hohem Risiko durch eine private Person muss eine Einwilligung – sofern eine sol-

¹⁰⁰¹ Europarat 2008, 6.

¹⁰⁰² Siehe S. 58.

¹⁰⁰³ Es handelt sich im Grunde genommen um doppelrelevante Tatsachen: Einerseits entscheiden die zwei Kriterien mit über die Anwendbarkeit des DSG auf Typisierungen, andererseits sind sie bei der materiellen Beurteilung der Einhaltung des DSG zu berücksichtigen. Denn die «einschneidende Entscheidung» wird bei der Betrachtung des Verhältnismässigkeitsprinzips (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG) und die «Diskrepanz zwischen Profil und Identität» bei der Betrachtung des Richtigkeitsgebots (Art. 5 DSG, Art. 5 Abs. 5 E-DSG, Art. 6 Abs. 5 rev-DSG) relevant.

¹⁰⁰⁴ Gleicher Meinung: ROSENTHAL 2017b, N 27.

¹⁰⁰⁵ Zur Unterscheidung zwischen den Begriffen «Persönlichkeitsprofil» (Art. 3 lit. d DSG) und «Profiling» (Art. 4 lit. f E-DSG, Art. 5 lit. f–g rev-DSG): ROSENTHAL 2017b, N 27. Vgl. Art.-29-Datenschutzgruppe 2017c, 6–7.

che verlangt ist – ausdrücklich erfolgen (Art. 5 Abs. 7 E-DSG, Art. 6 Abs. 7 lit. b rev-DSG).

Zweitens kann eine andere Gefahr bestehen, wenn die Arbeitgeberin über eine Typisierung Informationen erlangt, für die ein arbeitsrechtliches Frageverbot gilt. Beispielsweise deckte der amerikanische Detailhandelsriese Target gestützt auf die Daten zum Einkaufsverhalten auf, ob eine Kundin schwanger war.¹⁰⁰⁶ Für Target war es nicht erforderlich, die Frau zu identifizieren, sondern nur, sie als Schwangere zu typisieren. Die Betroffene wusste zwar, dass Daten über ihr Kaufverhalten zum Zweck eines verbesserten Kundenerlebnisses erhoben wurden, jedoch nicht, dass gestützt darauf ihre Schwangerschaft abgeleitet werden konnte.¹⁰⁰⁷ Analog kann eine Arbeitgeberin ermitteln, ob die Arbeitnehmerin eine Schwangerschaft beabsichtigt. Mit der Gesundheits-App für die Mitarbeiterinnen von Walmart geschieht dies bereits.¹⁰⁰⁸

Drittens ist auch in der Bearbeitung genetischer Daten ein Persönlichkeitsrisiko zu verorten. Eine generelle Befreiung der Typisierungen von der Last des Datenschutzes würde bedeuten, dass der Schutz von nichtpersonenbezogenen genetischen Daten komplett fehlen würde.¹⁰⁰⁹ Technische und organisatorische Massnahmen der Datensicherheit würden entfallen (vgl. Art. 7 DSG, Art. 7 E-DSG, Art. 8 rev-DSG) und die Daten könnten veröffentlicht werden. In der Folge wäre es möglich, dass die Daten in falsche Hände geraten und jemand durch Korrelation mit einem anderen Datensatz den Personenbezug herstellen könnte.¹⁰¹⁰ Dies ist bei genetischen Daten wahrscheinlich, da sie ein Leben lang ihre Gültigkeit behalten.¹⁰¹¹ In solchen Fällen ist die Anwendbarkeit des DSG zu fordern.¹⁰¹²

¹⁰⁰⁶ DUHIGG CHARLES, How companies learn your secrets, The New York Times Magazine vom 16.02.2012, abrufbar unter <www.nytimes.com> (besucht am 31.05.2020); TENE/POLONETSKY, 66 und 68; TRINDEL.

¹⁰⁰⁷ WALDMAN, 64. Vgl. auch das folgende Beispiel: Verfolgt die Polizei einen Wagen mittels GPS-Sender auf öffentlichen Strassen, kann sie unschwer auf die politische und religiöse Überzeugung und sexuelle Neigungen des Fahrers schliessen, je nachdem, wo der Wagen parkiert: WALDMAN, 65.

¹⁰⁰⁸ Siehe S. 48–49. Vgl. zum amerikanischen Recht: BODIE *et al.*, 998–999.

¹⁰⁰⁹ Das GUMG verweist für den Schutz genetischer Daten im Wesentlichen auf das DSG und schreibt kaum strengere Schutzregeln vor (vgl. Art. 7 GUMG). Den ausbleibenden Schutz ablehnend: SIGRIST, N 12.

¹⁰¹⁰ SIGRIST, N 12.

¹⁰¹¹ Zu genetischen Informationen: SIGRIST, N 3. Vgl. SOLOVE/KEATS CITRON, 757–758.

¹⁰¹² Vgl. auch Europarat 2016b, 26.

5.4.5 Zwischenfazit: risikoorientierte Auslegung des Geltungsbereichs des Datenschutzgesetzes

Das soeben gewonnene Bild zeigt, dass der Geltungsbereich des DSG auf Personendaten beschränkt ist. Das Anknüpfungskriterium der Bestimmbarkeit bzw. Identifizierbarkeit verursacht hinsichtlich einer bedeutenden Zahl von People Analytics-Anwendungen Rechtsunsicherheit. Insbesondere bei Typisierungen ist unsicher, ob das DSG Geltung beanspruchen kann. Solange kein höchstrichterlicher Entscheid betreffend Typisierungen ergeht, wird eine gewisse Unsicherheit bestehen.

Vorliegend wird der Standpunkt vertreten, dass der Geltungsbereich des DSG risikoorientiert auszulegen ist. Typisierungen sollten vom DSG erfasst werden, sofern von ihnen ein hohes Risiko für die Persönlichkeit der Betroffenen ausgeht. Ob dies der Fall ist, beurteilt sich insbesondere nach den Parametern, die bei der Besprechung des Gesetzeszwecks erarbeitet worden sind.¹⁰¹³ Beispielsweise kann ein hohes persönlichkeitschutzrechtliches Risiko bestehen, wenn ein Mensch auf ein Profil reduziert wird, das als Grundlage für einschneidende Entscheidungen über ihn dient, obwohl es seiner Identität nicht entspricht. Ebenso können Gefahren bestehen, wenn durch die Typisierung das arbeitsrechtliche Frageverbot verletzt wird und wenn genetische Daten bearbeitet werden. Dagegen erscheint es vertretbar, Typisierungen mit geringem Verletzungsrisiko nicht dem DSG zu unterstellen, etwa das nicht personalisierte Scannen des Internetverkehrs am Arbeitsplatz zum Zweck des Virenschutzes.¹⁰¹⁴

Nach der Auseinandersetzung mit dem Geltungsbereich des DSG ist im Folgenden auf die wichtigsten Bearbeitungsregeln einzugehen, und zwar zunächst auf das Zweckbindungsgebot.

5.5 Zweckbindungsgebot

5.5.1 Doppelte Zweckbindung bei People Analytics

People Analytics unterliegt einer doppelten Zweckbindung von datenschutzrechtlicher und arbeitsrechtlicher Seite. Erstere ist sogleich zu erörtern, Letztere später (S. 181–199).

¹⁰¹³ Siehe S. 141–148.

¹⁰¹⁴ Siehe S. 161.

5.5.2 Datenschutzrechtliche Zweckbindung

a) Normzweck und Gesetzessystematik

Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wird, der aus den Umständen ersichtlich oder der gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG; vgl. Art. 5 Abs. 3 E-DSG, vgl. Art. 6 Abs. 3 rev-DSG). Die Norm bezweckt, dass die Verwendung von Daten innerhalb der begründeten Erwartungen der betroffenen Person erfolgt.¹⁰¹⁵ Ferner ist es auch aus betriebswirtschaftlicher Sicht zur Ressourcenplanung erstrebenswert, am Anfang eines People Analytics-Projekts eine klare Zielsetzung mit einer ebenso klaren Fragestellung zu definieren.¹⁰¹⁶

Gesetzessystematisch stellt die Zweckbindung eine spezifische Datenbearbeitungsregel dar.¹⁰¹⁷ Sie leitet sich von den allgemeinen Rechtsgrundsätzen der Rechtmässigkeit, des Verhaltens nach Treu und Glauben und der Verhältnismässigkeit (Art. 4 Abs. 1–2 DSG, Art. 5 Abs. 1–2 E-DSG, Art. 6 Abs. 1–2 rev-DSG) ab.¹⁰¹⁸

Die Regel der Zweckbindung ist an zwei Enden mit anderen Bestimmungen verknüpft. Zum einen besteht eine Verbindung mit der Bearbeitungsregel der Erkennbarkeit: Der Bearbeitungszweck muss für die betroffene Person erkennbar sein (Art. 4 Abs. 4 DSG, Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG). Somit muss der Zweck sowohl für den Betroffenen ersichtlich als auch für den Bearbeiter verbindlich sein.¹⁰¹⁹ Kritisch kommt THOUVENIN nach einer historischen Auslegung zum Ergebnis, dass die Regel der Zweckbindung ursprünglich aus dem Bereich des öffentlichen Rechts stamme.¹⁰²⁰ Eine Beschränkung des Bearbeitungszwecks

¹⁰¹⁵ Vgl. zur Zweckbindung nach der DSGVO: CUSTERS/URSIC, 337. In Nordamerika ist von «*mission creep*», «*data creep*» oder «*creepiness*» die Rede, wenn die Bearbeitung nicht kommunizierten Zwecken dient: BODIE *et al.*, 999, CAVOUKIAN/DIX/EL EMAM, 8, THIERER, 419, und TENE/POLONETSKY, 61.

¹⁰¹⁶ REINDL/KRÜGL, 127.

¹⁰¹⁷ Siehe zur Unterscheidung zwischen den allgemeinen Rechtsgrundsätzen und den spezifisch datenschutzrechtlichen Bearbeitungsregeln S. 134.

¹⁰¹⁸ SHK DSG-BAERISWYL, Art. 4 DSG, N 34.

¹⁰¹⁹ Vgl. SHK DSG-BAERISWYL, Art. 4 DSG, N 34–35. Vgl. THOUVENIN 2014, 74.

¹⁰²⁰ THOUVENIN 2014, 70–71. Private Datenbearbeiter waren ursprünglich nur an den Zweck gebunden, wenn dieser den betroffenen Personen effektiv bekannt gegeben worden oder aus den Umständen ersichtlich war; fehlte eine solche Information, war die Bearbeitung nicht auf einen bestimmten Zweck beschränkt: THOUVENIN 2014, 73.

stehe im Widerspruch zur Privatautonomie.¹⁰²¹ Eine extensive Auslegung des Zwecks, eine weitgehende Rechtfertigung der Datenbearbeitung und eine grosszügige Auslegung der Einwilligung seien daher im privatrechtlichen Kontext angezeigt.¹⁰²²

Zum andern verknüpft die Zweckbindung die Datenbearbeitung mit der Rechtfertigung.¹⁰²³ Der Rechtfertigungsgrund ergibt sich aus der Zwecksetzung und umgekehrt.¹⁰²⁴ Beispielsweise bildet die Zweckbindung die Grundlage der Einwilligung¹⁰²⁵ und aus der Einwilligungserklärung leiten sich Zweck und Umfang der Datenbearbeitung ab.¹⁰²⁶

b) Anforderungen an die Zweckfestsetzung

Der Zweck muss «angegeben», «aus den Umständen ersichtlich» oder «gesetzlich vorgesehen» sein (Art. 4 Abs. 3 DSG; vgl. Art. 5 Abs. 3 E-DSG, vgl. Art. 6 Abs. 3 rev-DSG). Nach dem revidierten DSG muss der Zweck, zusammenfassend, «bestimmt» sein (Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG). Ob die Voraussetzung der Bestimmtheit erfüllt ist, beurteilt sich normativ: Massgebend ist, von welchen Bearbeitungszwecken bzgl. ihrer Personendaten eine betroffene Person, die eine gewisse Aufmerksamkeit und ein Interesse am Schicksal ihrer Daten aufweist, aufgrund der konkreten Umstände in guten Treuen ausgehen durfte und musste, als die Daten erhoben worden sind.¹⁰²⁷ Nicht entscheidend sind die tatsächliche Vorstellung der betroffenen Person und die tatsächlichen Absichten der Datenbearbeiterin.¹⁰²⁸ Das Gesetz regelt den Konkretisierungsgrad des bei der Beschaffung der Daten anzugebenden Zwecks nicht und lässt damit auch inhaltlich weit gefasste Zweckangaben zu.¹⁰²⁹ Allerdings können zu allgemein gehaltene

¹⁰²¹ THOUVENIN 2014, 68.

¹⁰²² THOUVENIN 2014, 78.

¹⁰²³ PK IDG BS-RUDIN, § 12 IDG BS, N 1.

¹⁰²⁴ Vgl. SHK DSG-BAERISWYL, Art. 4 DSG, N 44.

¹⁰²⁵ BSK DSG-MAURER-LAMBROU/STEINER, Art. 4 DSG, N 13.

¹⁰²⁶ SHK DSG-BAERISWYL, Art. 4 DSG, N 44.

¹⁰²⁷ Zur Beurteilung der «Ersichtlichkeit» (Art. 4 Abs. 3 DSG): HK-ROSENTHAL, Art. 4 DSG, N 34.

¹⁰²⁸ HK-ROSENTHAL, Art. 4 DSG, N 34.

¹⁰²⁹ THOUVENIN 2014, 67.

Zwecksetzungsklauseln das Zweckänderungsverbot aushöhlen.¹⁰³⁰ Nicht hinreichend konkret erscheint die Bestimmung «für Zwecke des Arbeitsverhältnisses»; zumutbar ist eine genauere Erklärung, ob die Daten beispielsweise für die Zwecke der Lohnausrichtung, der beruflichen Vorsorge, der Weiterbildung oder für Beförderungseinscheidungen bearbeitet werden.¹⁰³¹ Die Datenbearbeitung kann mehreren Zwecken dienen,¹⁰³² wobei jeder von ihnen klar zum Ausdruck kommen muss.¹⁰³³

Die Zwecksetzung muss bereits im Zeitpunkt der Beschaffung der Personendaten feststehen («bei der Beschaffung», Art. 4 Abs. 3 DSG).¹⁰³⁴ Das DSG verbietet das Sammeln von Personendaten auf Vorrat,¹⁰³⁵ d.h. für Zwecke, welche sich erst in Zukunft oder möglicherweise niemals realisieren, weil es kein generelles, überwiegendes Interesse der Arbeitgeberin hierfür gibt.¹⁰³⁶ Dies verwehrt aber nicht etwa eine zukunftsbezogene Zwecksetzung; so ist etwa die Datenbearbeitung zum Zweck der Personalplanung und -entwicklung möglich.¹⁰³⁷

c) Konflikt zwischen People Analytics und Zweckbindung

Zwischen der Bearbeitungsregel der Zweckbindung und People Analytics besteht ein Konfliktpotenzial, weil Daten in ihrer Eigenschaft als unerschöpfliche Güter zu immer neuen Zwecken beliebig oft analysiert werden können.¹⁰³⁸ Daten können

¹⁰³⁰ Vgl. PK IDG ZH-HARB, § 9 IDG ZH, N 12. Pauschale Zielsetzungen nach deutschem Recht unzulässig: BMAS 2017, 146.

¹⁰³¹ Vgl. Europarat 2016b, 33.

¹⁰³² Implizit: PK IDG ZH-HARB, § 9 IDG ZH, N 8; zur DSGVO: HK-ROSENTHAL, Art. 4 DSG, N 25. Es ist dem Wortlaut der DSGVO zu folgen, der mehrere Zwecke zulässt («Zwecke», Art. 5 Abs. 1 lit. b DSGVO). Der schweizerische Wortlaut, der von einem einzigen Bearbeitungszweck auszugehen scheint («zu dem Zweck», Art. 4 Abs. 3 DSG; «zu einem bestimmten [...] Zweck», Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG), ist zu eng.

¹⁰³³ Bei einer Rechtfertigung durch Einwilligung muss der Betroffene die Wahl haben, einzelne Zwecke abzulehnen: DÄUBLER, N 148. Siehe S. 224.

¹⁰³⁴ Vgl. HK-ROSENTHAL, Art. 4 DSG, N 40.

¹⁰³⁵ BGE 125 II 473 E. 4b. Dagegen ist im Anwendungsbereich des BÜPF die Speicherung und Aufbewahrung von Randdaten der Telekommunikation im Hinblick auf strafrechtliche Ermittlungen zulässig: Urteil BGer 1C_598/2016 vom 02.03.2018 E. 8.4; JÖHRI.

¹⁰³⁶ Bzgl. Gesundheitsdaten: STEINER, 289.

¹⁰³⁷ CALLAGHAN/WIGMAN, 16–10.

¹⁰³⁸ Vgl. DIETRICH *et al.*, 23. Vgl. BBl 1988 II, 451. Konflikt zwischen Big Data und Zweckbindung: VON ARNAULD, 118; WEBER 2018, 101; SHK DSG-BAERISWYL, Art. 4

im Sinne des Daten-Lebenszyklus rezykliert werden.¹⁰³⁹ In dieser Möglichkeit zur Wiederverwertung und neuen Kombination mit anderen Datensätzen steckt der hauptsächliche Mehrwert von Daten.¹⁰⁴⁰ Der volle Wert von Daten kann den Wert, der bei der ersten Verwendung gewonnen wird, bei Weitem überschreiten.¹⁰⁴¹ Somit können Daten über die Zeit wesentlich an Wert gewinnen.¹⁰⁴² Beispielsweise die japanische Diebstahlsicherung für die Firmenautos, welche anhand der Sitzhaltung den am Steuer sitzenden Arbeitnehmer eindeutig identifiziert,¹⁰⁴³ könnte die Daten neu zusätzlich daraufhin auswerten, den Aufmerksamkeitszustand der Fahrer, etwa deren Schläfrigkeit, Trunkenheit oder Wut, zu evaluieren.¹⁰⁴⁴

Die Erkenntnis, dass der Wert von Daten in ihrer Wiederverwertung steckt, führt zu einem Umdenken in der Forschung: Während die herkömmliche Forschung mit einer Theorie oder Hypothese beginnt, um diese daraufhin mit Daten zu validieren, ist es mit dem üppigen Datenvorkommen und den sinkenden Speicherkosten möglich geworden, die Daten direkt zu analysieren, um sich von den resultierenden Korrelationen überraschen zu lassen.¹⁰⁴⁵ Solche explorativen Datenanalysen zur Entdeckung von noch unbekannten Zusammenhängen verstossen grundsätzlich gegen das Zweckbindungsgebot.¹⁰⁴⁶

d) Vereinbare Zwecke

Wegen des Konflikts zwischen People Analytics und der Zweckbindungsmaxime stellt sich die Frage, wie das Gesetz mit der Wiederverwertung von People Analytics-Daten umgeht. Das künftige schweizerische Datenschutzrecht und die

DSG, N 39; THOUVENIN 2014, 63 und 68. Vgl. Art.-29-Datenschutzgruppe 2013, 45. Vgl. HAMANN, N 55. Vgl. WILDHABER/KASPER, 765.

¹⁰³⁹ Siehe S. 19–20.

¹⁰⁴⁰ World Economic Forum 2013, 7; EDSB 2014, N 8. Vgl. CUSTERS/URSIC, 344. MAYER-SCHÖNBERGER/CUKIER, 122; WEICHERT, 255. Siehe aber auch zur Halbwertszeit und zum teilweise rasch abnehmenden Wert der Daten S. 159.

¹⁰⁴¹ MAYER-SCHÖNBERGER/CUKIER, 102.

¹⁰⁴² MAYER-SCHÖNBERGER/CUKIER, 103; POSNER/WEYL, 228.

¹⁰⁴³ Siehe S. 50.

¹⁰⁴⁴ MAYER-SCHÖNBERGER/CUKIER, 173–174.

¹⁰⁴⁵ Vgl. DIETRICH *et al.*, 23. Bei Big Data-Projekten «probieren Unternehmen Dinge aus, um zu schauen, ob sie funktionieren», und unternehmen «nur selten gezielte Versuche, um herauszufinden, welches Projekt am wichtigsten oder strategisch sinnvollsten wäre»: DAVENPORT, 142. Vgl. KASPER/WILDHABER, 206.

¹⁰⁴⁶ HORNING, 89. Vgl. HORNING, 84.

DSGVO erlauben eine Weiterbearbeitung zu Zwecken, die mit dem Zweck, der bei der Beschaffung bestimmt worden ist, «vereinbar» sind (Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG; Art. 5 Abs. 1 lit. b Teilsatz 1 DSGVO). Der Zweck muss somit nicht immer identisch bleiben, darf aber auch nicht derart stark mutieren, dass von einer eigentlichen Zweckänderung auszugehen ist.

Ob ein neuer Zweck mit dem alten kompatibel ist, muss anhand des Verwendungszusammenhangs beurteilt werden.¹⁰⁴⁷ Daten sind, stärker als andere Vermögenswerte wie Immobilien und Mobiliar, kontextabhängig.¹⁰⁴⁸ Alle Daten haben ein Janusgesicht, d.h., sie können sich positiv oder negativ auf den Betroffenen auswirken, je nachdem, in welchem Zusammenhang sie stehen.¹⁰⁴⁹ Im Sinne einer «kontextuellen Integrität» – einer massgeblich von NISSENBAUM für das Common Law entwickelten Idee¹⁰⁵⁰ – soll der Einzelne grundsätzlich davor bewahrt werden, in einem bestimmten Zusammenhang mit der eigenen Rolle aus einem anderen Zusammenhang ungewollt konfrontiert zu werden.¹⁰⁵¹

Zur Beurteilung, ob der Kontext unter der neuen Zwecksetzung gewahrt bleibt, sind verschiedene Parameter zusammenzuzählen: Zunächst ist der Wortlaut der ursprünglich kommunizierten Zwecksetzung zu konsultieren. Sodann hat, wie bereits besprochen, jede Person eine individuelle Erwartung an die Privatsphäre.¹⁰⁵² Diese ist geprägt durch die sozialen Prozesse und die Arbeitskultur, die den Arbeitnehmer umgeben.¹⁰⁵³ Auch aus dem Überwachungsinstrument selbst ergibt sich, welche Zwecke mit dem ursprünglichen vereinbar sind.¹⁰⁵⁴ Gemäss MATZ-

¹⁰⁴⁷ Vgl. HÄRTING, N 107–108.

¹⁰⁴⁸ Vgl. NISSENBAUM 2011, 44.

¹⁰⁴⁹ World Economic Forum 2013, 17.

¹⁰⁵⁰ NISSENBAUM 2011, 43. Das Konzept der kontextuellen Integrität (*contextual integrity*) ist auf NISSENBAUM zurückzuführen: NISSIM/WOOD, 6. Jede neue Verwendung von bestehenden Daten setzt voraus, dass sie mit den ursprünglichen informationellen Normen übereinstimmt: PELTZ-STEELE, 406.

¹⁰⁵¹ HERMSTRÜWER/HAMANN, 23.

¹⁰⁵² Siehe S. 85–86. BAMBERGER/MULLIGAN 2015, 25. Massgebend sind die normativen Erwartungen des Betroffenen zum Informationsfluss: NISSIM/WOOD, 6.

¹⁰⁵³ BAMBERGER/MULLIGAN 2015, 28; zu den sozialen Prozessen in einem überwachten Callcenter: BALL/MARGULIS, 114.

¹⁰⁵⁴ Z.B. durchlief der amerikanische Algorithmus COMPAS einen Veränderungsprozess, der öffentliche Kritik auslöste: Wurde der Algorithmus für die Phase der Resozialisierung eines Straftäters entwickelt, um knappe Ressourcen wie Therapieplätze an Personen auf Bewährung oder nach ihrer Haftentlassung zu verteilen, so verwenden inzwi-

NER ist bei der Beurteilung der Vereinbarkeit auch zu überlegen, ob die Datenbearbeitung sich auf Dritte, die nicht am Erhebungsprozess beteiligt sind, auswirkt. Gegebenenfalls sind solche Schutzinteressen Dritter zu berücksichtigen.¹⁰⁵⁵ Abstrahiert lässt sich resümieren, dass die Kompatibilität der Zwecke gegeben ist, wenn sich die weitere Datenbearbeitung als «logisch nächster Schritt» im Datenbearbeitungsprozess des ursprünglichen Zwecks präsentiert, d.h., wenn beide Bearbeitungszwecke auf solche Weise miteinander verknüpft sind, dass sie aufeinander aufbauen.¹⁰⁵⁶

Zur Umsetzung der Kontextberücksichtigung sind personelle und technische Massnahmen erforderlich. Auf der personellen Seite braucht es fachmännisches Personal, das fähig ist, den Kontext einer Datenbearbeitung zu würdigen. Die Beurteilung im Einzelfall, welche neuen Bearbeitungszwecke mit den ursprünglichen Erhebungszwecken vereinbar sind, überlässt das Gesetz der Arbeitgeberin qua Datenbearbeiterin.¹⁰⁵⁷ Die Arbeitnehmer können zwar mitreden, wenn es um Daten aus einer Anlage zur Verhaltensüberwachung (Art. 26 ArGV 3) geht.¹⁰⁵⁸ Doch bei andern Daten hat die Arbeitgeberin grundsätzlich keine Konsultationspflicht.¹⁰⁵⁹ Auf technischer Ebene können Metadaten die Eckpunkte des Kontexts festhalten und Bearbeitungsbeschränkungen festlegen, sodass die Wahrung der kontextuellen Integrität periodisch überprüft werden kann.¹⁰⁶⁰

schen Gerichte den gleichen Algorithmus bereits im Stadium der Urteilsfällung: ZWEIG/KRAFFT, 114.

¹⁰⁵⁵ Vgl. MATZNER, 101. NISSENBAUMS Theorie, die für jeden Menschen einzeln eine Sphäre definiert, in der bestimmte Normen und Erwartungen an die Privatsphäre gelten, müsse erweitert werden und gesellschaftliche Erwartungen an die Privatsphäre einbeziehen: MATZNER, 100. Vgl. auch S. 298.

¹⁰⁵⁶ CALDAROLA/SCHREY, N 221.

¹⁰⁵⁷ Vgl. RICHTER, 584: Die Entscheidung über die Vereinbarkeit obliegt nicht dem Gesetzgeber eines EU-Mitgliedstaats, weil die DSGVO als Verordnung direkt anwendbar ist.

¹⁰⁵⁸ Siehe S. 103.

¹⁰⁵⁹ Ist nach europäischer Rechtslage eine Datenschutz-Folgenabschätzung erforderlich, so sind die Arbeitnehmer «gegebenenfalls» anzuhören (vgl. Art. 35 Abs. 9 DSGVO). Eine entsprechende Bestimmung zur Konsultation der Arbeitnehmer besteht nach schweizerischem Recht nicht (vgl. Art. 20 E-DSG, Art. 22 rev-DSG).

¹⁰⁶⁰ Vgl. World Economic Forum 2013, 23. Siehe zum Begriff der Metadaten FN 213.

e) **Veränderte Zwecke**

Erweist sich der neue Bearbeitungszweck als nicht vereinbar mit dem ursprünglichen, so liegt eine Zweckänderung vor. Besonders bei der Verknüpfung von Datensätzen rücken die Daten in einen anderen Zusammenhang und müssen somit anders behandelt werden. Eine nicht mit dem ursprünglichen Bearbeitungszweck vereinbare Zweckänderung liegt beispielsweise in den folgenden Fällen vor: Wenn ein Arbeitnehmer einwilligt, dass sein Porträt in der Mitarbeiterzeitschrift veröffentlicht wird, darf die Arbeitgeberin nicht das gleiche Bild ungefragt auch in einer Werbebroschüre verwenden.¹⁰⁶¹ Auch hat der Name einer Person im Firmenverzeichnis eine völlig andere Bedeutung als in einem Adoptionsregister.¹⁰⁶² Informationen, die ein Arbeitnehmer in seinem sozialen Netzwerk veröffentlicht, darf die Arbeitgeberin grundsätzlich nicht überwachen (*social media monitoring*), um zu wissen, was über sie berichtet wird, und um die Kontrolle über ihre Darstellung im Netz (zurück) zu gewinnen.¹⁰⁶³ Daten aus Gesundheits-Fürsorgeprogrammen am Arbeitsplatz dürfen nicht ohne Weiteres Verwendung finden für die Analyse, welche Personen mehr und welche weniger produktiv sein könnten.¹⁰⁶⁴ Schliesslich kann eine ursprünglich rechtmässige Bearbeitung von Informationen nach Ablauf einer gewissen Zeit rechtswidrig werden.¹⁰⁶⁵

Die Zweckänderung bedarf einer erneuten Rechtfertigung.¹⁰⁶⁶ Nach der Rechtfertigung ist die Nutzung der Personendaten für den neuen Zweck möglich, ohne dass der ursprüngliche Zweck beachtet werden muss.¹⁰⁶⁷

Eine Zweckänderung kann jedoch nicht gerechtfertigt werden, wenn durch die Änderung des Zwecks derart viel Kontext verloren geht, dass Fehlinterpretationen

¹⁰⁶¹ SHK DSG-PÄRLI, Art. 328b OR, N 15.

¹⁰⁶² Vgl. Microsoft Corporation 2018b, 79, und BODDINGTON, 10 und 18.

¹⁰⁶³ Schweizerischer Bundesrat 2013b, 41–42. Dies gilt immerhin, solange die Arbeitgeberin und der Arbeitnehmer nicht im sozialen Netzwerk befreundet sind.

¹⁰⁶⁴ WILSON *et al.*, 25.

¹⁰⁶⁵ Vgl. zur DSRL: Urteil EuGH vom 13.05.2014, Google Spain, C-131/12, EU:C:2014:317, N 93; HÄRTING, N 429. Vgl. das Recht auf Vergessenwerden, Art. 17 DSGVO.

¹⁰⁶⁶ Vgl. PK IDG BS-RUDIN, § 12 IDG BS, N 1. Vgl. zur DSGVO: FRANZEN, 326–327. Vgl. zum Entwurf der DSGVO: WEBER/OERTLY, N 21.

¹⁰⁶⁷ PK IDG ZH-HARB, § 9 IDG ZH, N 11.

naheliegen. In diesem Fall liegt ein Verstoss gegen das Richtigkeitsgebot (Art. 5 DSG, Art. 5 Abs. 5 E-DSG, Art. 6 Abs. 5 rev-DSG) vor.¹⁰⁶⁸

5.5.3 Arbeitsrechtliche Zweckbeschränkung

a) Übersicht

Nach der Behandlung der datenschutzrechtlichen Schranken der Zwecksetzung ist nun auf das Arbeitsrecht einzugehen, das in Art. 328b Satz 1 OR ebenfalls den zulässigen Bearbeitungszweck eingrenzt. Hierfür ist zunächst auf den Normzweck und die gesetzessystematische Stellung von Art. 328b Satz 1 OR einzugehen (dazu sogleich). Danach sind der Geltungsbereich und der Norminhalt zu behandeln; Letzterer lässt Datenbearbeitungen entweder zur Eignungsabklärung oder zur Durchführung des Arbeitsvertrags zu (S. 182–193). Es ist zu prüfen, ob rechtsgültig eingewilligt werden kann in eine Datenbearbeitung, die gegen Art. 328b Satz 1 OR verstösst (S. 193–197). Schliesslich ist das Frageverbot zu besprechen, welches sich aus Art. 328b Satz 1 OR ergibt (S. 197–199).

b) Normzweck und Gesetzessystematik

Das Arbeitsrecht bestimmt, dass die Arbeitgeberin Daten über den Arbeitnehmer nur bearbeiten darf, soweit diese dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind (Art. 328b Satz 1 OR). Über den Zweck dieser Bestimmung und ihre systematische Stellung im Verhältnis zum DSG gehen die Meinungen auseinander. Gemäss der Botschaft zum DSG stellt der Artikel eine Konkretisierung des Verhältnismässigkeitsprinzips des DSG dar.¹⁰⁶⁹

Konträr zur Botschaft liegt für RIESELMANN-SAXER der eigenständige materielle Gehalt dieser Bestimmung im Bereich des Bearbeitungszwecks, nicht aber im Bereich der Verhältnismässigkeit.¹⁰⁷⁰ Dementsprechend ist zur Prüfung, ob die betreffende People Analytics-Anwendung nach Art. 328b Satz 1 OR zulässig ist, der Bearbeitungszweck – und nicht die Auswirkung der Datenbearbeitung – entscheidend.¹⁰⁷¹

¹⁰⁶⁸ GOLA/WRONKA, N 1261; ungenaue und veraltete Daten infolge einer Zweckänderung: UNO Generalversammlung, 13.

¹⁰⁶⁹ BBl 1988 II, 488.

¹⁰⁷⁰ RIESELMANN-SAXER, 6.

¹⁰⁷¹ RIESELMANN-SAXER, 109.

Richtigerweise ist WOLFER und MEIER zu folgen, die in Art. 328b Satz 1 OR sowohl eine Beschränkung des Zwecks als auch eine Konkretisierung des Verhältnismässigkeitsprinzips sehen.¹⁰⁷² Sie erkennen, dass mit dem Zweck der Überwachung gleichzeitig die dahinter stehenden Überwachungsinteressen gemeint sind.¹⁰⁷³ Indem Art. 328b Satz 1 OR arbeitsvertragsfremde Überwachungsinteressen zum Vornherein als unverhältnismässig qualifiziert, beeinflusst diese Bestimmung die Interessenabwägung, die Teil der Verhältnismässigkeitsprüfung ist. Hier zeigt sich die Scharnierstellung des Zweckbindungsgrundsatzes, der den Zweck mit dem Rechtfertigungsgrund (hier dem potenziell überwiegenden Interesse) verknüpft.¹⁰⁷⁴ Die Eignungsabklärung und die Durchführung des Arbeitsvertrags sind zugleich Bearbeitungszwecke und Rechtfertigungsgründe.

ROSENTHAL wiederum sieht in der identischen Norm gerade nicht eine Beschränkung des Bearbeitungszwecks, sondern nur des Kreises bzw. der Art der Daten.¹⁰⁷⁵ Er beruft sich hierfür primär auf den Wortlaut von Art. 328b Satz 1 OR.¹⁰⁷⁶ Eine kategorische Unterteilung nach dem Inhalt der Daten wäre aber äusserst unpraktisch, weil eine Überwachung häufig Daten aus Beruf und Privatleben simultan erfasst.¹⁰⁷⁷ Die Kritik zum DSG, dass ein binäres Unterscheiden zwischen bestehender oder fehlender Kategoriezugehörigkeit nicht zielführend ist,¹⁰⁷⁸ muss auch für das Arbeitsrecht nach OR gelten, womit eine starre Einteilung als berufliche oder private Daten zu verwerfen ist.

c) Geltungsbereich

In zeitlicher und persönlicher Beziehung gilt der Persönlichkeitsschutz bei Datenbearbeitungen nach verbreiteter, aber nicht unumstrittener Meinung und entgegen dem Wortlaut («Arbeitnehmer») bereits für Stellensuchende in der Phase der Ver-

¹⁰⁷² WOLFER, N 47 und 208; MEIER PHILIPPE, N 2037; gleicher Meinung, aber weniger differenziert: PAPA/PIETRUSZAK, N 17.5.

¹⁰⁷³ Vgl. WOLFER, N 614.

¹⁰⁷⁴ Siehe S. 174–175.

¹⁰⁷⁵ HK-ROSENTHAL, Art. 328b OR, N 29.

¹⁰⁷⁶ Zudem argumentiert ROSENTHAL mit der Botschaft (BB1 1988 II, 488) und der Rechtsprechung (BGE 130 II 425 E. 3.3). Beide Quellen lassen jedoch nach hier vertretener Meinung Raum offen, um aus Art. 328b Satz 1 OR eine Zweckbeschränkung abzulesen.

¹⁰⁷⁷ WOLFER, N 46.

¹⁰⁷⁸ Siehe S. 167.

tragsanbahnung (Art. 328b OR analog).¹⁰⁷⁹ Damit greift der arbeitsvertragliche datenbezogene Persönlichkeitsschutz früher als die allgemeine Fürsorgepflicht (nach Art. 328 OR).¹⁰⁸⁰ Allerdings kann nur die Eignungsabklärung (1. Variante von Art. 328b Satz 1 OR) die Analyse von Bewerbern rechtfertigen; nicht infrage kommt eine Berufung auf die Erforderlichkeit (2. Variante von Art. 328b Satz 1 OR), da diese nur die Zeit während einer Anstellung betrifft.¹⁰⁸¹

Der Schutz der Personendaten des Arbeitnehmers (Art. 328b OR) gilt genauso und ohne zeitliche Befristung nach Beendigung des Arbeitsverhältnisses.¹⁰⁸² Somit sind nach Austritt des Arbeitnehmers die Grundsätze des DSG anwendbar (vgl. Art. 328b Satz 2 OR). Hingegen erlischt die Fürsorgepflicht (Art. 328 OR) mit Ablauf des Arbeitsverhältnisses grundsätzlich. Nur eine beschränkte nachwirkende vertragliche Fürsorgepflicht überdauert.¹⁰⁸³

d) Norminhalt

Die arbeitsvertragliche Zweckbindung (gemäss Art. 328b Satz 1 OR) bedeutet eine Koppelung des Bearbeitungszwecks an den Arbeitsvertrag. Mit dieser Koppelung erweist sich das Arbeitsrecht restriktiver als das Datenschutzrecht: Das DSG enthält keine vergleichbare Koppelungsbestimmung. Die DSGVO verbietet vertragsfremde Koppelungen nur für Datenbearbeitungen, die mit einer Einwilligung gerechtfertigt werden (vgl. Art. 7 Abs. 4 DSGVO). Für Bearbeitungen, die anderweitig gerechtfertigt werden, etwa durch überwiegende Arbeitgeberinteressen oder Gesetz, stellt die DSGVO keine Koppelungsschranke auf.¹⁰⁸⁴

Die beiden Varianten «Eignungsabklärung» und «Erforderlichkeit» sind auseinanderzuhalten («oder», Art. 328b Satz 1 OR): Personendaten, die für die Vertragsdurchführung erforderlich sind, jedoch nicht zur Eignungsabklärung, dürfen nur zum Zweck der Durchführung bearbeitet werden. Beispielsweise Angaben über

¹⁰⁷⁹ Der vorvertragliche Schutz ist gerade auch vor dem Hintergrund einer im schweizerischen Recht nur unvollständig verankerten Antidiskriminierungsgesetzgebung notwendig: PÄRLI 2018, N 17.18. Bereits vor Stellenantritt gelten die Grenzen des Fragerechts und der Datenbearbeitung: RIESELNANN-SAXER, 5; KASPER/WILDHABER, 225. A.M. MEIER PHILIPPE, N 2068, m.w.H.: Art. 328b OR sei auf das Bewerbungsverfahren nicht anwendbar.

¹⁰⁸⁰ Vgl. RIESELNANN-SAXER, 7.

¹⁰⁸¹ EDÖB 2014b, 6.

¹⁰⁸² BGE 131 V 298 E. 6.1; RIESELNANN-SAXER, 70.

¹⁰⁸³ RIESELNANN-SAXER, 5.

¹⁰⁸⁴ Vgl. S. 224.

den Familienstand oder zur Gewerkschaftsmitgliedschaft sind notwendig für die Geltendmachung von Kinderzulagen oder zur Klärung, ob ein Arbeitnehmer einem Gesamtarbeitsvertrag untersteht. Für die Eignungsabklärung ist die Bearbeitung solcher Angaben aber nicht zulässig, da es an einem objektiven Arbeitsplatzbezug fehlt.¹⁰⁸⁵

e) Variante 1: Eignungsabklärung

aa) Objektivität der Eignungsabklärung

Zulässig ist eine Bearbeitung von Daten über den Arbeitnehmer, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen (1. Variante von Art. 328b Satz 1 OR). Erforderlich ist eine Personalunion von analysierter und interessierender Person («dessen Eignung», Art. 328b Satz 1 OR). An der Personalunion fehlt es beispielsweise, wenn Schlüsselmitarbeiter analysiert werden, aber nicht im Hinblick auf deren eigene Arbeitsverhältnisse, sondern zur Abklärung, nach welchen Parametern das Unternehmen künftig Bewerber auswählen und mit ihnen Arbeitsverhältnisse begründen soll.¹⁰⁸⁶

Die Daten müssen objektiv zur Abklärung der hinreichenden Eignung im Hinblick auf ein konkretes Arbeitsverhältnis beitragen.¹⁰⁸⁷ Die subjektive Wissensbegier der Arbeitgeberin genügt nicht.¹⁰⁸⁸

Sowohl die persönliche als auch die fachliche bzw. berufliche Qualifikation geben objektiven Aufschluss über die hinreichende Befähigung und können somit abgeklärt werden.¹⁰⁸⁹ Angaben zur beruflichen Qualifikation umfassen namentlich Aus- und Weiterbildung, Berufserfahrung, Sprachkenntnisse, Fahrerlaubnis, Auslandsaufenthalte, berufliche Pläne und Vorstrafen.¹⁰⁹⁰ Auch Soft Skills wie Belastbarkeit, Kreativität, Intuition, Lern-, Anpassungs-, Kommunikations-, Präsentations-, Teamfähigkeit, Empathie sowie die Fähigkeiten zum kritischen Denken

¹⁰⁸⁵ PÄRLI 2018, N 17.14.

¹⁰⁸⁶ KASPER/WILDHABER, 195; zum deutschen Recht: DZIDA, 542.

¹⁰⁸⁷ WILDHABER/HÄNSENBERGER 2016, 327; STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 5; «objektivierte Betrachtungsweise»: RIESSELMANN-SAXER, 22; KASPER/WILDHABER, 201.

¹⁰⁸⁸ KUKO OR-PIETRUSZAK, Art. 328b OR, N 6; KASPER/WILDHABER, 201.

¹⁰⁸⁹ KUKO OR-PIETRUSZAK, Art. 328b OR, N 6; KASPER/WILDHABER, 201.

¹⁰⁹⁰ KUKO OR-PIETRUSZAK, Art. 328b OR, N 6; REHBINDER/STÖCKLI, Art. 328b OR N 5; CHK OR BT 2-EMMEL, Art. 328b OR, N 4; WEDDE 2016c, 11; KASPER/WILDHABER, 201.

und Argumentieren stellen berufliche Qualifikationen dar.¹⁰⁹¹ Diese Fähigkeiten werden schon in der Primarschule bewertet und sind von zentraler Bedeutung im Berufsleben, besonders in der Zukunft.¹⁰⁹²

Zur persönlichen Qualifikation gehören demgegenüber beispielsweise die Weltanschauung¹⁰⁹³ und die Freizeitgestaltung.¹⁰⁹⁴ Grundsätzlich unzulässig ist die Abklärung persönlicher Verhältnisse und Eigenschaften, die nicht wesentlich die beruflichen Fähigkeiten mitbestimmen.¹⁰⁹⁵

Algorithmen werden mit dem technologischen Fortschritt immer neue Korrelationen zwischen Eigenschaften und dem beruflichen Erfolg aufdecken und Kriterien festmachen, die heute nicht als objektive Kriterien für die Beurteilung der Eignung bekannt sind.¹⁰⁹⁶ Ein Algorithmus zur Internetrecherche sammelt Millionen im Internet auffindbarer Datenpunkte über Bewerber, beispielsweise gesellschaftliche Vorlieben oder bevorzugter Browser.¹⁰⁹⁷ Ebenso werden Daten darüber erhoben, welche Webseiten die Person besucht, mit welcher Art Sprache (positiv oder negativ) die Person Technologien beschreibt und welche Fähigkeiten sich die Person auf LinkedIn selbst zuschreibt.¹⁰⁹⁸ Ferner interessieren Daten darüber, wie die arbeitsrelevanten Beiträge der Bewerber in Online-Foren von anderen bewertet werden¹⁰⁹⁹ oder ob jemand ein «Partylöwe» ist.¹¹⁰⁰ Anbieter wie Spokeo durchsuchen mit Computerprogrammen (sog. Webcrawler) sowohl den oberflächlichen, von

¹⁰⁹¹ KASPER/WILDHABER, 201, m.w.H.; Microsoft Corporation 2018b, 108; Microsoft Corporation 2018b, 114; Microsoft Corporation 2018b, 116; a.M. CHK OR BT 2-EMMEL, Art. 328b OR, N 4, und RIESSELMANN-SAXER, 22: Dies seien persönliche Qualifikationen.

¹⁰⁹² KASPER/WILDHABER, 201. Vgl. Microsoft Corporation 2018b, 120. «*In a world of big data, it is the most human traits that will need to be fostered – creativity, intuition, and intellectual ambition*»: CUKIER/MAYER-SCHÖNBERGER, 40. Vgl. Brian Simpson, emeritierter Professor der University of New England (Australia) School of Law, im Interview: «*The question that remains is the extent to which an algorithm can have a heart*»: GUIHOT *et al.*, 409.

¹⁰⁹³ KUKO OR-PIETRUSZAK, Art. 328b OR, N 6.

¹⁰⁹⁴ BAUMANN ROBERT, 640; KASPER/WILDHABER, 202.

¹⁰⁹⁵ EDÖB 2014b, 6; KASPER/WILDHABER, 202.

¹⁰⁹⁶ KASPER/WILDHABER, 202–203.

¹⁰⁹⁷ SNYDER, 243.

¹⁰⁹⁸ Z.B. die Funktion Smart Hiring Platform von Gild: KIM 2017, 862.

¹⁰⁹⁹ Z.B. Remarkable Hire: REINSCH/GOLTZ, 37.

¹¹⁰⁰ CUSTERS/URSIC, 324.

den gewöhnlichen Suchmaschinen indexierten Teil des Internets (sog. Surface Web) als auch das weitaus grössere, nicht indexierte (weil z.B. Login-geschützte) Deep Web.¹¹⁰¹ Nicht nur aus dem Internet, auch aus den Sensoren ergeben sich neue Eignungskriterien: Arbeitgeberinnen messen mit Wearables die Korrelation zwischen dem Schlafmuster und der Leistung am Arbeitsplatz, um Aufgaben an die am besten Geeigneten zu verteilen.¹¹⁰² Andere analysieren das Verhalten in Computerspielen.¹¹⁰³

Es ist nicht geklärt, inwiefern solche neuen Kriterien objektiv zur Eignungsabklärung in Bezug auf eine konkrete Stelle beitragen. Die wissenschaftliche Verlässlichkeit von solchen Analysen ist umstritten, weil sie induktiv¹¹⁰⁴ und untheoretisch¹¹⁰⁵ sind. Untheoretisch bedeutet, dass eine Theorie fehlt bzw. nicht im Voraus der Analyse bekannt ist, wonach gesucht wird.¹¹⁰⁶ People Analytics sucht nach unbekannten Mustern und auffälligen Korrelationen in einem Meer an Daten (sog.

¹¹⁰¹ Zum sog. Deep Web Crawler von Spokeo: KASPER/WILDHABER, 204; SNYDER, 275. Spokeo beschränkt sich nach eigenen Angaben auf die Durchsuchung der öffentlichen Teile des Deep Web: Spokeo, The deep web vs. the dark web: What's the difference?, 06.11.2017, abrufbar unter <www.spokeo.com> (besucht am 31.05.2020). – Das Volumenverhältnis zwischen dem kleineren Surface und dem grösseren Deep Web entspricht etwa dem Verhältnis zwischen dem über Meer sichtbaren Teil eines schwimmenden Eisbergs und dem Anteil unter dem Meeresspiegel. Vgl. BERGMAN.

¹¹⁰² Vgl. HAGGIN PATIENCE, Big issues in technology (a special report) – what's the best way for companies to handle data from employees' wearables?, The Wall Street Journal vom 23.05.2016, abrufbar unter <www.wsj.com> (besucht am 31.05.2020).

¹¹⁰³ KIM 2017, 863; KASPER/WILDHABER, 202.

¹¹⁰⁴ Empirisches, nicht theoretisch fundiertes Personalmanagement: KAISER, 14. Empirie und Induktion drücken der wissenschaftlichen Erkenntnisgewinnung den Stempel auf: MRKONICH *et al.*, 36; KASPER/WILDHABER, 205–206.

¹¹⁰⁵ KIM 2017, 879–880. A.M. MAYER-SCHÖNBERGER/CUKIER, 71: Es brauche nach wie vor Theorien, einfach vermehrt solche der Statistik, der Mathematik oder der Computerwissenschaft und weniger solche, die sich auf die kausale Dynamik eines spezifischen Phänomens beziehen.

¹¹⁰⁶ Big Data kehrt somit den konventionellen wissenschaftlichen Ansatz um, nach welchem zunächst eine Theorie formuliert und anschliessend Daten erhoben werden, um die Hypothese zu testen: ANDERSON CHRIS, The end of theory: the data deluge makes the scientific method obsolete, 23.06.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020). Die Umkehr wirkt sich auf die Prüfung der Validität von Forschungsergebnissen aus: MRKONICH *et al.*, 19 und 21. Die Reihenfolge «erst Theorie, dann mit Daten überprüfen» gilt für die gesamte Forschung, solange Daten karg sind, und somit für Analysen sowohl von Kausalitäten als auch von Korrelationen: MAYER-SCHÖNBERGER/CUKIER, 61. KASPER/WILDHABER, 206.

Bottom-up- oder datengetriebener Ansatz).¹¹⁰⁷ Eine theoretische Erklärung dafür, dass die Korrelationen auch Kausalitäten sind, fehlt.¹¹⁰⁸ Es ist zweifelhaft, ob die von Art. 328b OR geforderte berufliche Bezogenheit gegeben ist, wenn der Algorithmus Daten berücksichtigt, deren Informationsgehalt in der Korrelation zwischen nichtarbeitsbezogenen Daten und der Arbeitsleistung liegt.¹¹⁰⁹ Problematisch erscheint auch etwa die Ermittlung, ob ein Bewerber seiner Persönlichkeit nach generell zu Straftaten neigt.¹¹¹⁰ Wenn sich die Arbeitgeberin hierfür auf blosser Korrelationen stützt, müssen diese zumindest über möglichst lange Zeit stabil sein.¹¹¹¹ Versteht sich «objektiv» aber als sachlich nachvollziehbar, so darf eine blosser Korrelation noch kein genügend objektives Kriterium für die Eignungsabklärung sein.¹¹¹² Hier vertretener Auffassung zufolge ist auch eine Überprüfung der Stichhaltigkeit einer Korrelation bzw. der Nachweis einer Kausalität zwischen dem neuen Kriterium und der Arbeitseignung zu fordern, bevor das Kriterium bei der Selektion verwendet wird.¹¹¹³

bb) Persönlichkeitsdurchleuchtung

Durch den Einbezug immer neuer Kriterien in die Eignungsabklärung wird technisch eine regelrechte Durchleuchtung der Persönlichkeit des Arbeitnehmers möglich.¹¹¹⁴ Bei den geschilderten Anwendungen kann der Algorithmus die Persönlichkeit verletzen, indem er Daten aufspürt, die der Bewerber nicht zum Zweck einer solchen Analyse freigegeben hat (vgl. Art. 12 Abs. 3 i.V.m. Art. 4 Abs. 3 DSG; Art. 26 Abs. 3 i.V.m. Art. 5 Abs. 3 E-DSG; Art. 30 Abs. 3 i.V.m. Art. 6 Abs. 3 rev-DSG).¹¹¹⁵ Von den erhobenen Daten kann ein Algorithmus auf weitere Eigenschaften einer Person schliessen (z.B. von Körpergrösse und -gewicht auf

¹¹⁰⁷ KASPER/WILDHABER, 206. Gleichzeitig bleibt es aber möglich, vermutete Beziehungen durch Daten zu bestätigen (sog. Top-down- oder theoriegetriebener Ansatz), vgl.: CUSTERS *et al.*, 9.

¹¹⁰⁸ KASPER/WILDHABER, 206. Siehe S. 32–36 und 176.

¹¹⁰⁹ WILDHABER *et al.*, 480.

¹¹¹⁰ DZIDA, 545; KASPER/WILDHABER, 207.

¹¹¹¹ WILDHABER *et al.*, 462.

¹¹¹² KASPER/WILDHABER, 203.

¹¹¹³ So auch KASPER/WILDHABER, 203. Siehe zu den Begriffen der Korrelation und Kausalität S. 32–36.

¹¹¹⁴ So schon BBl 1988 II, 488; KASPER/WILDHABER, 205; Regelungsdruck bei Anwendungen zur Durchleuchtung der Persönlichkeit von Arbeitnehmern: BMAS 2017, 145.

¹¹¹⁵ KASPER/WILDHABER, 205.

das Geschlecht, von der Postleitzahl auf die Ethnie oder vom Essen auf die Religion).¹¹¹⁶

Grafologische Gutachten handgeschriebener Lebensläufe und psychologische Eignungstests sind wie People Analytics umstritten, weil ein tiefe Einblicke gewährendes Röntgenbild von zweifelhaftem wissenschaftlichem Wert erstellt wird.¹¹¹⁷ Es lohnt sich deshalb, die rechtliche Behandlung grafologischer Gutachten zu betrachten. Mitte der 90er-Jahre holten rund zwei Drittel (68 Prozent) der Unternehmen bei der Auswahl von Führungskräften regelmässig grafologische Gutachten über die Bewerber ein.¹¹¹⁸ Noch im Jahr 2011 waren grafologische Gutachten in der Schweiz verbreitet.¹¹¹⁹

Grafologische Gutachten müssen kumulativ die folgenden vier rechtlichen Voraussetzungen erfüllen: Erstens ist die vorgängige ausdrückliche Einwilligung des Bewerbers erforderlich, weil in der Regel besonders schützenswerte Personendaten beschafft und Persönlichkeitsprofile erstellt werden (vgl. Art. 4 Abs. 5 Satz 2 DSG, vgl. Art. 5 Abs. 6 Satz 2 E-DSG, vgl. Art. 6 Abs. 7 lit. b rev-DSG).¹¹²⁰ Diese Zustimmung kann konkludent erfolgen, beispielsweise wenn die Arbeitgeberin den handgeschriebenen Lebenslauf zur Anfertigung eines grafologischen Gutachtens fordert und der Bewerber ihn kommentarlos schickt.¹¹²¹ Das Einreichen einer Schriftprobe allein stellt hingegen keine Einwilligung dar.¹¹²² Ziel des Gutachtens und der Zusammenhang zur ausgeschriebenen Stelle müssen klar sein.¹¹²³ In der Regel genügt die vorgängige allgemeine «angemessene Information» (Art. 4 Abs. 5 Satz 1 DSG, Art. 5 Abs. 6 Satz 1 E-DSG, Art. 6 Abs. 6 rev-DSG) für die

¹¹¹⁶ SNYDER, 257; KASPER/WILDHABER, 205.

¹¹¹⁷ REHBINDER/STÖCKLI, Art. 320 OR N 2; KASPER/WILDHABER, 206.

¹¹¹⁸ ZÜST, 1476; KASPER/WILDHABER, 206.

¹¹¹⁹ Z.B. bei dem Bauunternehmen Implenja, dem Haushaltsgeräte-Hersteller Miele, der Netstal-Maschinen AG, dem Verkehrs-Club der Schweiz (VCS) und der Stadt Zürich: STEIGER MARTIN, Schweizerische Arbeitgeber auf graphologischen Abwegen, 21.10.2011, abrufbar unter <<https://steigerlegal.ch>> (besucht am 31.05.2020); KASPER/WILDHABER, 206.

¹¹²⁰ MEIER PHILIPPE, N 2107. Vgl. STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 10; zur Voraussetzung der Einwilligung KASPER/WILDHABER, 206.

¹¹²¹ DZIDA, 544.

¹¹²² STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 10.

¹¹²³ STEIGER MARTIN, Schweizerische Arbeitgeber auf graphologischen Abwegen, 21.10.2011, abrufbar unter <<https://steigerlegal.ch>> (besucht am 31.05.2020); HUGEN-TOBLER, 154.

rechtsgültige Einwilligung nicht; stattdessen gilt die spezifische Informationspflicht für das Beschaffen von besonders schützenswerten Personendaten und Persönlichkeitsprofilen (Art. 14 DSGVO).¹¹²⁴ Die Einwilligung muss freiwillig erfolgen (Art. 4 Abs. 5 Satz 1 DSGVO, Art. 5 Abs. 6 Satz 1 E-DSG, Art. 6 Abs. 6 rev-DSG).

Zweitens muss sich das grafologische Gutachten auf die Arbeitsplatzzeignung beschränken (Art. 328b Satz 1 OR).¹¹²⁵ In persönlicher Hinsicht bedeutet dies, dass die Stellung im Betrieb zu berücksichtigen ist. Bei Arbeitnehmern mit vorwiegend ausführenden Tätigkeiten darf sich die Datenbearbeitung nur auf die berufliche Qualifikation erstrecken.¹¹²⁶ Je höher jedoch die Position ist, desto umfassender darf die Abklärung ausfallen.¹¹²⁷ Für Stellen mit sehr grosser Verantwortung und hohen Anforderungen an die persönliche Integrität sind vertiefte Abklärungen wegen Haftungs- und Reputationsrisiken sogar geboten.¹¹²⁸ Demzufolge ist das Durchleuchten der ganzen Persönlichkeit mit der ausdrücklichen Einwilligung des Betroffenen möglich.¹¹²⁹ Eine unverhältnismässige Datenbearbeitung ist nicht *a priori* ungültig.¹¹³⁰ Allgemeine Charakterstudien sind aber unzulässig.¹¹³¹ Ferner kann die Natur der Arbeit und des Betriebs weitergehende Erkundigungen zulassen: Tendenzbetriebe dürfen in Bezug auf ihren ideellen Zweck Daten aus dem

¹¹²⁴ MEIER PHILIPPE, N 2110 und 2113.

¹¹²⁵ MEIER PHILIPPE, N 2114; STEIGER MARTIN, Schweizerische Arbeitgeber auf graphologischen Abwegen, 21.10.2011, abrufbar unter <<https://steigerlegal.ch>> (besucht am 31.05.2020). Vgl. Europarat 2015, N 19.1: Psychologische Tests sind nur zulässig, sofern sie für die konkrete Tätigkeit erforderlich sind und das nationale Recht angemessene Garantien bereithält. Zur Voraussetzung der Arbeitsplatzzeignung KASPER/WILDHABER, 207.

¹¹²⁶ STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 5.

¹¹²⁷ CHK OR BT 2-EMMEL, Art. 328b OR, N 2.

¹¹²⁸ SHK DSGVO-PÄRLI, Art. 328b OR, N 27. Auch vertiefte medizinische Abklärungen sind möglich. So kann z.B. der Betreiber eines Atomkraftwerks einen Medizintest anordnen und zusätzlich nach Krebsvorfällen und anderen Krankheiten in der Familie fragen: Europarat 2016b, 42.

¹¹²⁹ SHK DSGVO-PÄRLI, Art. 328b OR, N 27.

¹¹³⁰ RIESELMANN-SAXER, 37.

¹¹³¹ REHBINDER/STÖCKLI, Art. 320 OR N 6; STEIGER MARTIN, Schweizerische Arbeitgeber auf graphologischen Abwegen, 21.10.2011, abrufbar unter <<https://steigerlegal.ch>> (besucht am 31.05.2020).

Privatbereich bearbeiten, die keinen engen Bezug zur betreffenden Arbeit aufweisen, sofern der Arbeitnehmer Tendenzträger ist.¹¹³²

Drittens müssen nachvollziehbare, zuverlässige und objektive Ergebnisse resultieren. Die grafologischen Methoden müssen fachmännisch angewendet und ausgewertet werden.¹¹³³

Zu ergänzen ist eine vierte, allgemeine Voraussetzung, die für alle Datenbearbeitungen am Arbeitsplatz gilt. Die Analyse darf nicht gegen zwingendes oder höherrangiges Recht verstossen. Zu denken ist an das Strafrecht bei Untersuchungen, die den strafrechtlich geschützten Geheim- oder Privatbereich verletzen (vgl. Art. 179 ff. StGB). Ferner gelten sehr restriktive Schranken für präsymptomatische genetische Untersuchungen zur Verhütung von Berufskrankheiten und Unfällen (vgl. Art. 22 GUMG).¹¹³⁴

Die vier Voraussetzungen für grafologische Gutachten lassen sich auf Algorithmen, die die Persönlichkeit durchleuchten, in vergleichbarer Weise übertragen.¹¹³⁵ Die konkludente Einwilligung liegt beispielsweise vor, wenn die Arbeitgeberin die Einreichung einer wissenschaftlichen Arbeit im Wordformat zum Zweck einer Persönlichkeitsanalyse fordert und der Bewerber das Word-Dokument ohne weitere Stellungnahme zusendet.¹¹³⁶

Im Sinne eines risikoorientierten Verständnisses von Art. 328b Satz 1 OR ist jedoch zu vergegenwärtigen, dass es beim Einsatz von Algorithmen nicht immer zu einer Persönlichkeitsdurchleuchtung kommt. Keine Durchleuchtung der Persönlichkeit liegt vor, wenn sowohl die bearbeiteten Daten als auch die gezogene Schlussfolgerung vom Kern des Persönlichkeitsrechts sehr weit entfernt liegen.¹¹³⁷ Entscheidend ist ein objektiver Massstab.¹¹³⁸ Es stellt noch keine unzulässige Persönlichkeitsdurchleuchtung dar, wenn die Arbeitgeberin künftiges Verhalten über das einem traditionellen Vorgesetzten mögliche Mass hinaus prognostizieren

¹¹³² STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 5; OFK-PELLASCIO, Art. 328b OR, N 7.

¹¹³³ STEIGER MARTIN, Schweizerische Arbeitgeber auf graphologischen Abwegen, 21.10.2011, abrufbar unter <<https://steigerlegal.ch>> (besucht am 31.05.2020); zur Voraussetzung der objektiven Ergebnisse: KASPER/WILDHABER, 207.

¹¹³⁴ PÄRLI 2018, N 17.38.

¹¹³⁵ KASPER/WILDHABER, 207.

¹¹³⁶ DZIDA, 544; KASPER/WILDHABER, 207.

¹¹³⁷ DZIDA, 545; KASPER/WILDHABER, 207–208.

¹¹³⁸ Vgl. WOLFER, N 183–184; KASPER/WILDHABER, 208.

kann:¹¹³⁹ Äussert eine Person im öffentlich zugänglichen Teil eines sozialen Netzwerks Absichten über einen Stellenwechsel, kann der Algorithmus eine entsprechende Verhaltensprognose erstellen, während ein traditioneller Personalverantwortlicher keine Zeit für Diagnosen sozialer Netzwerke haben mag. Gleichwohl handelt es sich noch nicht um eine Ergründung der Persönlichkeit.¹¹⁴⁰ Ferner mangelt es an einer Persönlichkeitsdurchleuchtung beim Einsatz einer Plagiatsoftware zur Überprüfung der Dissertation daraufhin, ob der Verfasser den in der Bewerbung angegebenen akademischen Grad auf rechtmässigem Weg erlangt hat. Dies ist zur Eignungsabklärung zulässig.¹¹⁴¹

f) Variante 2: Erforderliche Daten zur Durchführung des Arbeitsvertrags

Die Arbeitgeberin darf Daten über den Arbeitnehmer bearbeiten, soweit diese zur Durchführung des Arbeitsvertrags erforderlich sind (2. Variante von Art. 328b Satz 1 OR). Zur Beurteilung der Erforderlichkeit müssen die für den betreffenden Arbeitsvertrag charakteristischen Rechte und Pflichten identifiziert werden.¹¹⁴² Die Überwachung kann zur Wahrnehmung der Fürsorgepflicht (Art. 328 OR) notwendig sein.¹¹⁴³ Zulässig kann es auch sein, den Arbeitnehmer hinsichtlich der Einhaltung der Sorgfalts- und Treuepflicht (Art. 321a OR) zu beaufsichtigen.¹¹⁴⁴ Die Abklärung medizinischer Angaben, etwa mittels Wearables, kann erforderlich sein, wenn Anzeichen bestehen, dass eine gesundheitliche Beeinträchtigung den Arbeitnehmer an der Erfüllung wesentlicher Arbeitsaufgaben hindert oder der Arbeitnehmer aufgrund seiner Krankheit eine direkte Bedrohung darstellt.¹¹⁴⁵

Nicht erforderlich zur Durchführung des Arbeitsvertrags sind in aller Regel Aufzeichnungen nach Arbeitsende.¹¹⁴⁶ Dies ist für geolokalisierte Geschäftsautos sowie geschäftliche Mobiltelefone und Laptops, welche auch privat benutzt werden

¹¹³⁹ DZIDA, 545; KASPER/WILDHABER, 208.

¹¹⁴⁰ DZIDA, 545; KASPER/WILDHABER, 208.

¹¹⁴¹ DZIDA, 544; KASPER/WILDHABER, 208.

¹¹⁴² Vgl. TREITL, 121.

¹¹⁴³ RIESSELMANN-SAXER, 109.

¹¹⁴⁴ RIESSELMANN-SAXER, 109.

¹¹⁴⁵ Mit Berufung auf die amerikanische EEOC: HASKINS, 72.

¹¹⁴⁶ EDÖB 2018a, 28.

dürfen, einzukalkulieren.¹¹⁴⁷ Gleiches gilt für implantierte Computerchips, die ohne einen medizinischen Eingriff nicht entfernt werden können.¹¹⁴⁸ Auch die Überwachung in datenschutzsensiblen Bereichen wie Pausenräumen oder Toiletten erscheint grundsätzlich nicht als erforderlich.¹¹⁴⁹

Bei der «Erforderlichkeit» handelt es sich um einen unbestimmten Rechtsbegriff.¹¹⁵⁰ Eine kompromisslose Auslegung würde bedeuten, dass eine Datenbearbeitung nur erforderlich ist, wenn ohne sie der Arbeitsvertrag nicht erfüllt werden könnte.¹¹⁵¹ Demgegenüber führt eine weite Auslegung dazu, dass Datenbearbeitungen bereits als erforderlich und somit zulässig gelten, wenn sie die Durchführung des Vertrags vereinfachen bzw. nützlich sind.¹¹⁵²

Die Einführung von People Analytics-Erfindungen wie Chip-Implantaten, Monitoring von Bewerbern in sozialen Netzwerken, algorithmischer Leistungsauswertung oder Gesundheitschecks mittels Wearables ist in vielen Fällen nicht im streng genommenen Sinne notwendig für die Durchführung des Arbeitsverhältnisses.¹¹⁵³ Die meisten Jobs lassen sich ohne Analytik ausüben; diese aber ermöglicht Entwicklung und Einsparungen. Letztlich trimmt sie das Unternehmen fit für den Wettbewerb, sichert bestehende und schafft neue Arbeitsstellen. Analysen, die für den Fortschritt des Gesamtunternehmens oder einer Abteilung erforderlich, für die Durchführung (oder den Erhalt) des einzelnen Arbeitsvertrags jedoch bloss nützlich sind, sollten nicht von Anfang an unterbunden werden.¹¹⁵⁴ Während die Eignungsabklärung (1. Variante von Art. 328b Satz 1 OR) die Personalunion von analysierter und interessierender Person verlangt,¹¹⁵⁵ erscheint bei der Erforder-

¹¹⁴⁷ Vgl. zu einem amerikanischen Fall, in dem die Arbeitnehmerin die Kündigung erhielt, weil sie die GPS-Tracking-Funktion nach Arbeitsschluss ausgeschaltet hatte: AKHTAR/MOORE, 116. Vgl. DETERMANN, 113.

¹¹⁴⁸ Unzulässig wäre es z.B., über ein Implantat die nächtlichen Toilettengänge zu messen und daraus Schlüsse über den Gesundheitszustand des Arbeitnehmers zu ziehen: CUSTERS/URSIC, 327. Siehe zu Chip-Implantaten S. 53–54.

¹¹⁴⁹ DAVIS PLÜSS JESSICA / REUSSER KAI, Your employer might be watching you. Should you care?, 13.05.2019, abrufbar unter <www.swissinfo.ch> (besucht am 31.05.2020).

¹¹⁵⁰ Vgl. GÄCHTER/EGLI, N 45.

¹¹⁵¹ Vgl. zu Art. 7 Abs. 4 DSGVO: TREITL, 122.

¹¹⁵² TREITL, 122.

¹¹⁵³ CUSTERS/URSIC, 334.

¹¹⁵⁴ Eine strikte Handhabung des Erforderlichkeitsprinzips wäre eine «*pain in the neck*», vgl. zum europäischen Recht: CUSTERS/URSIC, 336.

¹¹⁵⁵ Siehe S. 184.

lichkeit (2. Variante von Art. 328b Satz 1 OR) Fingerspitzengefühl angezeigt: Dient die Analyse nicht direkt der Durchführung des Arbeitsvertrags mit der analysierten Person, sondern (auch) dem Gesamtunternehmen oder der Abteilung, kann dies im Interesse des betroffenen Arbeitnehmers gelegen kommen.

Vermutlich führt ein Mittelweg zwischen der restriktiven und der extensiven Auslegung von Art. 328b Satz 1 OR zum Ziel: Eine Datenbearbeitung muss mehr als bloss nützlich sein, muss aber auch nicht absolut unerlässlich sein, um das Kriterium der Erforderlichkeit zu erfüllen.¹¹⁵⁶ Damit ist ein gewisser Raum für Innovationen sichergestellt, sodass das Unternehmen mit der Zeit gehen kann und die Arbeitsstellen erhalten bleiben. Mit dieser Auslegung können auch Reibungen zwischen Arbeitnehmerschutz und Gesellschaftsrecht gemildert werden: Das Unternehmen ist gegenüber den Gesellschaftern verpflichtet, den Unternehmenswert zu erhalten und zu steigern, sodass Investitionen im Bereich People Analytics geboten sein können.

g) Einwilligung zu Abweichungen von Artikel 328b Satz 1 Obligationenrecht

Die Bestimmung zum Persönlichkeitsschutz bei der Bearbeitung von Personendaten des Arbeitnehmers (Art. 328b Satz 1 OR) schafft einige Grauzonen. Es kann innerhalb des diskutierten Spielraums dafür oder dagegen argumentiert werden, ob ein Kriterium objektiv zur Eignungsabklärung dient, ob die Schwelle zur Persönlichkeitsthroughleuchtung erreicht ist und ob auch bloss nützliche Informationen zur Vertragsdurchführung bearbeitet werden dürfen.¹¹⁵⁷ Angesichts dieser Grenzfälle stellt sich die Frage, ob denn eine Abweichung von Art. 328b Satz 1 OR möglich und zulässig wäre.

Die arbeitsrechtliche Bestimmung zum Datenschutz (Art. 328b OR) ist grundsätzlich einseitig zwingender Natur: Von ihr darf nicht durch Abrede, Normalarbeitsvertrag oder Gesamtarbeitsvertrag zuungunsten des Arbeitnehmers abgewichen werden (Günstigkeitsprinzip, Art. 362 Abs. 1 OR). Da es sich um eine unabdingbare gesetzliche Vorschrift handelt, können Arbeitnehmer vor, während und einen Monat nach der Vertragsdauer nicht auf entsprechende Forderungen verzichten

¹¹⁵⁶ Vgl. zum europäischen Recht TREITL, 122. Bloss nützliche Datenbearbeitungen seien unzulässig: MEIER PHILIPPE, N 2043.

¹¹⁵⁷ Siehe S. 184–187 und 191–193.

(Art. 341 Abs. 1 OR).¹¹⁵⁸ Die Unverzichtbarkeit gilt bzgl. aller Arten von Ansprüchen des Arbeitnehmers gegenüber der Arbeitgeberin aus dem Arbeitsverhältnis; der Wortlaut, der nur Forderungen (vgl. Art. 184 OR) nennt, ist zu eng.¹¹⁵⁹ Deshalb kann auf den arbeitsrechtlichen Datenschutz (Art. 328b Satz 1 OR) in der Regel nicht durch Einwilligung verzichtet werden.¹¹⁶⁰ Eine Datenbearbeitung ohne genügenden Arbeitsplatzbezug und zulasten des Arbeitnehmers ist arbeitsrechtlich grundsätzlich selbst dann nicht erlaubt, wenn sie nach dem DSG (etwa mit einer Einwilligung, vgl. Art. 13 Abs. 1 DSG, Art. 27 Abs. 1 E-DSG, Art. 31 Abs. 1 rev-DSG) gerechtfertigt werden könnte.¹¹⁶¹ Eine Einwilligung wäre unwirksam bzw. nichtig (Art. 362 Abs. 2 OR analog).¹¹⁶² Dabei wird meistens nicht der gesamte Einzelarbeitsvertrag nichtig, sondern es gilt die Teilnichtigkeit (vgl. Art. 20 Abs. 2 OR). Die nichtige vertragliche Bestimmung wird durch die gesetzliche Vorschrift ersetzt.¹¹⁶³

Nach einer protektiven Meinung ist eine Datenbearbeitung, die gegen Art. 328b OR verstösst, nur so lange zulässig, als sie sich nicht zulasten des Arbeitnehmers auswirkt.¹¹⁶⁴ Bei ganzheitlicher Betrachtung unter Einschluss der *ratio legis* des Arbeitsrechts, «Schutz der schwächeren Vertragspartei», ist eine für den Arbeitnehmer nachteilige und nicht durch sachliche Gründe gerechtfertigte Datenbearbeitung durch die Arbeitgeberin unzulässig.¹¹⁶⁵ Eine Abweichung von Art. 328b

¹¹⁵⁸ Über den Gesetzeswortlaut hinaus gilt die Unverzichtbarkeit auch vor Beginn des Arbeitsvertrags: STREIFF/VON KAENEL/RUDOLPH, Art. 341 OR N 2.

¹¹⁵⁹ STREIFF/VON KAENEL/RUDOLPH, Art. 341 OR N 2.

¹¹⁶⁰ Einwilligung in eine den Arbeitnehmer benachteiligende, gegen Art. 328b OR verstossende Datenbearbeitung unmöglich: Urteil OGer ZH LA180019-O/U vom 15.03.2019 E. IV.2d/cc, bestätigt in: Urteil OGer ZH LA180031-O/U vom 20.03.2019 E. IV.2c/cc; PÄRLI 2018, N 17.20.

¹¹⁶¹ Urteil OGer ZH LA180019-O/U vom 15.03.2019 E. IV.2d/aa, bestätigt in: Urteil OGer ZH LA180031-O/U vom 20.03.2019 E. IV.2c/aa. Art. 328b OR beinhalte eine Abweichung zum DSG: PÄRLI 2018, N 17.22.

¹¹⁶² RIESELMANN-SAXER, 41. Art. 362 Abs. 2 OR kann keine direkte, sondern höchstens eine analoge Anwendung erfahren, weil dort die Einwilligung nicht genannt wird.

¹¹⁶³ RIESELMANN-SAXER, 41.

¹¹⁶⁴ EDÖB 2014b, 6; STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 3; BSK OR I-PORTMANN/RUDOLPH, Art. 328b OR, N 26; FLUECKIGER 2017, 8–9. Vgl. mit Bezug auf das Googeln von Arbeitnehmern: FLUECKIGER 2014, 89. OFK-PELLASCIO, Art. 328b OR, N 9; MÉTILLE, 106; HUGENTOBLE, 154. Vgl. die Darstellung der h.M. bei KASPER/WILDHABER, 196.

¹¹⁶⁵ PÄRLI 2018, N 17.22.

OR muss für den Arbeitnehmer gesamthaft von Vorteil sein bzw. in seinem Interesse erfolgen.¹¹⁶⁶ Ob insgesamt ein Vorteil resultiert, beurteilt sich nach einem objektiven Massstab.¹¹⁶⁷ Aus datenschutzrechtlicher Sicht ist zu fordern, dass die Einwilligung nur sehr eingeschränkt zum Einsatz kommen darf.¹¹⁶⁸

Eine liberalere Meinung sieht in Art. 328b Satz 1 OR aber keine selbständige Verbotsnorm, deren Verletzung automatisch eine unerlaubte Handlung darstellen würde.¹¹⁶⁹ Art. 328b Satz 1 OR verweise im Wesentlichen auf das DSG und habe einen verhältnismässig engen eigenständigen Regelungsbereich.¹¹⁷⁰ Es handle sich bloss um einen weiteren (auf Arbeitsverhältnisse beschränkten) datenschutzrechtlichen Bearbeitungsgrundsatz (vgl. Art. 12 Abs. 2 lit. a DSG, Art. 26 Abs. 2 lit. a E-DSG, Art. 30 Abs. 2 lit. a rev-DSG).¹¹⁷¹ Dies finde Rückhalt in einer historischen Auslegung, da der Gesetzgeber mit Art. 328b Satz 1 OR lediglich das datenschutzrechtliche Verhältnismässigkeitsprinzip (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG) konkretisieren wollte.¹¹⁷² Nach dieser

¹¹⁶⁶ BSK DSG-RAMPINI, Art. 13 DSG, N 7.

¹¹⁶⁷ Massgebend ist, wie ein vernünftiger, loyaler Arbeitnehmer unter Berücksichtigung seiner Stellung im Beruf und der Verkehrsanschauung die Bewertung vornehmen würde: RIESELMANN-SAXER, 40. Die Abweichung von Art. 328b OR durch Abrede, Normal- oder Gesamtarbeitsvertrag ist mit der Gruppe der eng zusammenhängenden gesetzlichen Vorschriften zu vergleichen. Es darf nicht jede einzelne einzel-, normal- oder gesamtarbeitsvertragliche Bestimmung isoliert mit den massgebenden Gesetzesvorschriften verglichen werden: RIESELMANN-SAXER, 40.

¹¹⁶⁸ Siehe dazu später, S. 231–234.

¹¹⁶⁹ WILDHABER/HÄNSENBERGER 2016, 317; PAPA/PIETRUSZAK, N 17.8; MEIER PHILIPPE, N 2037; HK-ROSENTHAL, Art. 328b OR, N 1, 5; so auch die frühere ständige kantonale Zürcher Rechtsprechung: Urteil OGer ZH LA160028-O/U vom 22.12.2016 E. 5.4, und Urteil OGer ZH LA180002-O/U vom 20.03.2018 E. 5.1. Nach der DSGVO und dem deutschen Recht sei nicht von einer generellen Unzulässigkeit der Einwilligung auszugehen: KAINER/WEBER, 2742, und DZIDA, 543. Darstellung der liberaleren Meinung und sich dieser anschliessend: KASPER/WILDHABER, 197.

¹¹⁷⁰ Frühere kantonale Zürcher Rechtsprechung: Urteil OGer ZH LA160028-O/U vom 22.12.2016 E. 5.4.

¹¹⁷¹ Urteil OGer ZH LA160028-O/U vom 22.12.2016 E. 5.4.

¹¹⁷² Siehe S. 181. Die Ständeratskommission war im Jahr 1991 der Ansicht, dass die Arbeitgeberin Daten über Angestellte mit «Zustimmung durch den Arbeitnehmer» und in den Schranken von Art. 9 DSG an Dritte weitergeben könne: AB SR 1991, 1066. Vgl. auch den Umstand, dass eine Arbeitgeberin in der Rolle als Verleiherin Daten über den Arbeitnehmer mit dessen ausdrücklicher schriftlicher Zustimmung an Dritte weitergeben darf, auch wenn die Daten zur Verleihung nicht erforderlich sind (Art. 18

Position kann eine Datenbearbeitung ohne sachlichen Bezug zur Arbeit durch eine Einwilligung gerechtfertigt werden, weil das Arbeitsrecht das DSG zum Bestandteil des Arbeitsvertrags macht (vgl. Art. 328b Satz 2 OR i.V.m. Art. 13 Abs. 1 DSG bzw. Art. 27 Abs. 1 E-DSG bzw. Art. 31 Abs. 1 rev-DSG).¹¹⁷³ Die liberalere Meinung hat zudem den Gesetzeswortlaut auf ihrer Seite, der eine Abweichung bloss mittels «Abrede, Normal- oder Gesamtarbeitsvertrag» (Art. 362 Abs. 1 OR) für unzulässig erklärt. An einer Abrede, einem Normalarbeitsvertrag oder Gesamtarbeitsvertrag sind mindestens zwei Parteien beteiligt, während sich Art. 362 Abs. 1 OR zur Einwilligung als einseitiger Willenserklärung nicht äussert.¹¹⁷⁴ Nach der liberaleren Meinung kann ein Arbeitnehmer rechtsgültig in die Speicherung von Daten über den Verlauf seiner privaten Internetnutzung einwilligen, indem er Internet-Guidelines unterschreibt.¹¹⁷⁵ Art. 362 OR lasse aber nur eine Einwilligung im Einzelfall zu, während ein Vorausverzicht auf den durch Art. 328b OR gewährten Schutz verboten sei.¹¹⁷⁶ Zu weit ginge somit die Einwilligung, die der Arbeitgeberin ein umfassendes Recht einräumen würde, in beliebiger Weise in den privaten E-Mails des Arbeitnehmers zu stöbern.¹¹⁷⁷

Solange kein höchstrichterlicher Entscheid ergeht, bleibt unsicher, ob der protektiven oder der liberaleren Meinung zu folgen ist. Nach der vorliegend vertretenen Ansicht unterscheidet RIESELMANN-SAXER zutreffend zwischen Satz 1 und Satz 2 von Art. 328b OR. Der erste Satz ist in dem Sinne relativ zwingend, dass eine Datenbearbeitung zu einem anderen Zweck als der Abklärung der Eignung oder der Durchführung des Arbeitsverhältnisses nur dann gültig ist, wenn sie für den Arbeitnehmer von Vorteil ist.¹¹⁷⁸ Damit durchbricht Art. 328b Satz 1 OR als

Abs. 3 AVG i.V.m. Art. 47 Abs. 4 AVV). Vgl. PAPA/PIETRUSZAK, N 17.8 FN 11, und SECO 2003, 91.

¹¹⁷³ Urteil OGer ZH LA180002-O/U vom 20.03.2018 E. 5.1; PAPA/PIETRUSZAK, N 17.8.

¹¹⁷⁴ Vgl. RIESELMANN-SAXER, 40. Die Aufzählung sei jedoch unvollständig: Betriebsordnungen (Art. 38 Abs. 3 ArG) unterlägen der identischen Beschränkung wie Abreden, Normal- und Gesamtarbeitsverträge: BSK OR I-PORTMANN/RUDOLPH, Art. 362 OR, N 1.

¹¹⁷⁵ WILDHABER/HÄNSENBERGER 2016, 318. Vgl. COSTA, N 17 FN 17: Im privaten Arbeitsbereich bilde hauptsächlich die Einwilligung den Rechtfertigungsgrund für die Internet- und E-Mail-Überwachung. Vgl. SHK DSG-PÄRLI, Art. 328b OR, N 27: Personen, die sich auf eine leitende Funktion bewerben, können bei hinreichender Transparenz ausdrücklich in die Durchleuchtung ihrer ganzen Persönlichkeit einwilligen.

¹¹⁷⁶ PAPA/PIETRUSZAK, N 17.8; MEIER PHILIPPE, N 2040.

¹¹⁷⁷ HK-ROSENTHAL, Art. 328b OR, N 14, 67.

¹¹⁷⁸ RIESELMANN-SAXER, 41.

lex specialis das DSG, das eine Bearbeitung zu einem beliebigen Zweck zulässt und lediglich die Zweckänderung verbietet (vgl. Art. 4 Abs. 3 DSG, Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG).¹¹⁷⁹ Der zweite Satz von Art. 328b OR ist insofern zwingend, als von den datenschutzrechtlichen Bestimmungen nicht zuungunsten des Arbeitnehmers abgewichen werden kann. Mit anderen Worten kann der Arbeitnehmer mittels Abrede, Normal- oder Gesamtarbeitsvertrag nicht schlechter gestellt werden, als wenn das DSG gelten würde. Jedoch kann durch Einwilligung der betroffenen Person zu deren Ungunsten von den datenschutzrechtlichen Einschränkungen abgewichen werden (Art. 13 Abs. 1 DSG, Art. 27 Abs. 1 E-DSG, Art. 31 Abs. 1 rev-DSG). Daher ist in Bezug auf Art. 328b Satz 2 OR die Bedeutung der relativ zwingenden Wirkung erheblich eingeschränkt.¹¹⁸⁰ Beispielsweise könnte ein Arbeitnehmer dazu einwilligen, dass die Arbeitgeberin im Rahmen einer arbeitsbezogenen Zwecksetzung übermässig viele Daten bearbeitet, dies entgegen den datenschutzrechtlichen Grundsätzen der Verhältnismässigkeit und Datenminimierung (vgl. Art. 4 Abs. 2 i.V.m. Art. 12 Abs. 2 lit. a DSG; Art. 5 Abs. 2 i.V.m. Art. 26 Abs. 2 lit. a E-DSG; Art. 6 Abs. 2 i.V.m. Art. 30 Abs. 2 lit. a rev-DSG). So erscheint etwa eine Einwilligung in die Aufzeichnung der Computeraktivitäten während der Arbeitszeit zur Betrugsprävention möglich, auch wenn kein konkreter Verdacht besteht, dass die einwilligende Person Betrugs handlungen begeht und eine Überwachung somit grundsätzlich unverhältnismässig ist.¹¹⁸¹ Unabhängig davon, welcher Lehrmeinung ein Gericht folgen wird, ist nach vorliegender Auffassung eine Einwilligung ohnehin nur mit grosser Zurückhaltung als Rechtfertigungsgrundlage zu wählen,¹¹⁸² weshalb die bereitgelegten Argumente selten ins Gefecht geführt werden müssen.

h) Frageverbot

Aus Art. 328b OR resultiert ein Frageverbot der Arbeitgeberin in Bezug auf die Privatsphäre des Arbeitnehmers.¹¹⁸³ Grundsätzlich unzulässig sind etwa Fragen nach Schwangerschaft(-sabsichten),¹¹⁸⁴ Rauchgewohnheiten,¹¹⁸⁵ Herkunft, Ge-

¹¹⁷⁹ RIESELMANN-SAXER, 41.

¹¹⁸⁰ RIESELMANN-SAXER, 41–42.

¹¹⁸¹ Vgl. auch das vorstehende Beispiel von WILDHABER und HÄNSENBERGER, S. 196 FN 1175. Vgl. KASPER/WILDHABER, 197.

¹¹⁸² Siehe zur Kritik am Rechtfertigungsgrund der Einwilligung später, S. 231–234.

¹¹⁸³ FLUECKIGER 2014, 78; KASPER/WILDHABER, 209.

¹¹⁸⁴ MEIER PHILIPPE, N 2090.

¹¹⁸⁵ KAINER/WEBER, 2742.

werkschaftszugehörigkeit, religiöser oder politischer Gesinnung.¹¹⁸⁶ Auch wie es um die allgemeine Gesundheit des Arbeitnehmers steht, ob er vegetarisch isst, Alkohol trinkt oder raucht, ist für die (potenzielle) Arbeitgeberin grundsätzlich tabu.¹¹⁸⁷ Bewerbern steht im Fall einer unzulässigen Frage ein Notwehrrecht auf Lüge zu.¹¹⁸⁸ Dem Arbeitnehmer wird das Notwehrrecht der Lüge teilweise auch im laufenden Arbeitsverhältnis zugestanden.¹¹⁸⁹ Wenn dem Arbeitnehmer aufgrund der unzulässigerweise gewonnenen Information gekündigt wird, ist eine missbräuchliche Kündigung (Art. 336 OR) anzunehmen.¹¹⁹⁰

Mit dem Frageverbot der Arbeitgeberin korrespondiert eine Mitteilungspflicht des Bewerbers nach den Regeln von Treu und Glauben (Art. 2 Abs. 1 ZGB) und des Arbeitnehmers gestützt auf die Treuepflicht (Art. 321a Abs. 1 OR). Beispielsweise muss ein Bewerber Informationen über seinen Gesundheitszustand offenlegen, wenn sie objektiv notwendig sind für die Beurteilung der künftigen Arbeitsfähigkeit.¹¹⁹¹

People Analytics wirft das Problem auf, dass die Technologie Informationen aufdecken kann, nach denen die Arbeitgeberin im Gespräch nicht fragen dürfte.¹¹⁹² Anders als bei einer direkten Frage erlangen die Arbeitnehmer keine Kenntnis davon, wenn ein Algorithmus Daten über sie aufspürt. Ihr Notwehrrecht zur Lüge können sie faktisch nicht ausüben. Daher ist zu fordern, dass die Arbeitgeberin den Algorithmus in der Weise programmiert, dass er von sich aus keine Daten zur Privatsphäre ermittelt.¹¹⁹³ Er darf beispielsweise nicht eruieren, ob sich die Bewerber

¹¹⁸⁶ EDÖB 2014b, 9; MEIER PHILIPPE, N 2090. Ausnahmsweise darf nach privaten Informationen gefragt werden. Vgl. die Ausführungen zur ausnahmsweise erlaubten Personlichkeitsdurchleuchtung auf S. 189.

¹¹⁸⁷ PÄRLI 2009, N 1361; MEIER PHILIPPE, N 2090; zum deutschen Recht: STEINER, 272.

¹¹⁸⁸ SHK DSG-PÄRLI, Art. 328b OR, N 36. Das Bundesgericht erwähnt das Notwehrrecht der Lüge in BGE 122 V 267 E. 4c. Wenn die Arbeitgeberin Dokumente verlangt, soll der Bewerber nach deutschem Recht ein Recht zur Fälschung haben: KAINER/WEBER, 2742. KASPER/WILDHABER, 209.

¹¹⁸⁹ RIESELMAANN-SAXER, 122.

¹¹⁹⁰ RIESELMAANN-SAXER, 122.

¹¹⁹¹ MEIER PHILIPPE, N 2101.

¹¹⁹² BIAS/BOGUE, 254.

¹¹⁹³ KASPER/WILDHABER, 209.

berin in sozialen Netzwerken äussert, in denen es um Schwangerschaftsthemen geht.¹¹⁹⁴

5.6 Erkennbarkeitsgebot

5.6.1 Normzweck und Norminhalt

Die spezifische Datenbearbeitungsregel der Erkennbarkeit verlangt, dass die Beschaffung von Personendaten und insbesondere der Zweck ihrer Bearbeitung für die betroffene Person erkennbar sein müssen (Art. 4 Abs. 4 DSG, Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG). Die Begriffe der «Erkennbarkeit» und «Transparenz» werden vorliegend gleichbedeutend verwendet, weil sich der letztere Fachausdruck auf internationaler Ebene etabliert hat (vgl. etwa Art. 5 Abs. 1 lit. a DSGVO).

Es handelt sich bei der Erkennbarkeit um einen der tragenden Pfeiler des Datenschutzrechts.¹¹⁹⁵ Denn er trägt zu verschiedenen Zwecken bei: Eine transparente Datenbearbeitung sensibilisiert die Bevölkerung für die Allgegenwärtigkeit von Datenbearbeitungen sowie deren Gefahren.¹¹⁹⁶ Transparenz ist eine Voraussetzung für die Ausübung der informationellen Selbstbestimmung, etwa um eine Algorithmen-unterstützte Personalentscheidung anzugreifen oder das eigene Verhalten anzupassen.¹¹⁹⁷ Die Durchsichtigkeit von Algorithmen steht auch am Anfang der Aufdeckung und Bekämpfung algorithmischer Diskriminierung.¹¹⁹⁸ Ferner

¹¹⁹⁴ DZIDA, 543. Das Frageverbot darf nicht durch eine Anfrage bei Google, Facebook, dem früheren Arbeitgeber oder dem Branchenauskunftsdienst umgangen werden: DAUBLER, N 241. KASPER/WILDHABER, 209.

¹¹⁹⁵ HILDEBRANDT/KOOPS, 448. Vgl. Erklärbarkeit von entscheidunterstützenden Systemen «*highly desirable*»: BIRAN/COTTON, 8. Vgl. Dr. iur. David Vasella, Rechtsanwalt, im Interview: DAVIS PLÜSS JESSICA / REUSSER KAI, Your employer might be watching you. Should you care?, 13.05.2019, abrufbar unter <www.swissinfo.ch> (besucht am 31.05.2020).

¹¹⁹⁶ BACHER/DUBOIS, 137; datenschutzrechtliche Aufklärungs- und Informationspflichten auch zum Ziel der Autonomiesicherung: KÖRNER, 148–149.

¹¹⁹⁷ HORNING, 87; HERMSTRÜWER, 103–104. Werden Informationen unbewusst preisgegeben, geht die bewusste Kontrolle systematisch verloren: DREYER, 142. Vgl. ANANNY/CRAWFORD, 975.

¹¹⁹⁸ ANANNY/CRAWFORD, 977.

kann Transparenz Vertrauen schaffen.¹¹⁹⁹ Welche Relevanz Transparenz in der Wahrnehmung der Betroffenen hat, zeigt eine Umfrage von 2015: Neun von zehn Befragten (91 Prozent) finden, dass ein Preisnachlass keine gerechte Gegenleistung für eine intransparente Datenerhebung ist. Auch eine verbesserte Dienstleistung vermag für über die Hälfte der Befragten (55 Prozent) die fehlende Erkennbarkeit nicht zu kompensieren.¹²⁰⁰ Der Transparenz wohnt aber auch ein direkter, intrinsischer Wert inne: Durch die Transparenz steigt die Erklärbarkeit und damit die Validität eines Algorithmus im Vergleich zu nebulösen Systemen.¹²⁰¹ Das System lässt sich verbessern, wenn Fehler offengelegt werden.¹²⁰²

Der Grundsatz der Erkennbarkeit leitet sich ab vom allgemeinen Rechtsgrundsatz des Handelns nach Treu und Glauben (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG),¹²⁰³ der ein schonendes und widerspruchsfreies Verhalten des Datenbearbeiters gegenüber dem Betroffenen verlangt.¹²⁰⁴ Daten dürfen nicht auf eine Art erhoben werden, mit der die betroffene Person nicht rechnen muss.¹²⁰⁵ Transparenz muss sowohl über die Tatsache, dass der Arbeitsplatz überwacht wird, als auch über die Methoden und Modalitäten der Überwachung geschaffen werden.¹²⁰⁶ In zeitlicher Hinsicht müssen die Arbeitnehmer und Bewerber informiert sein, bevor die Datenerhebungen beginnen.¹²⁰⁷ Heimliche Überwachungen sind in aller Regel unzulässig.¹²⁰⁸ Ausnahmsweise kann jedoch eine unangekün-

¹¹⁹⁹ DARPA, 5. Vgl. FOX *et al.*, 24. Mangelt es an Transparenz, entsteht ein «diffus bedrohliches Gefühl des Beobachtetseins»: Urteil Bundesverfassungsgericht [Deutschland] 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 vom 02.03.2010 N 212. Die Betroffenen fühlen sich dadurch in ihrer informationellen Selbstbestimmung gehemmt (sog. «*chilling effect*»): Urteil BGer 6B_908/2018 vom 07.10.2019 E. 3.2. HÄRTING, N 250. A.M. ANANNY/CRAWFORD, 980: Transparenz schafft nicht zwingend Vertrauen.

¹²⁰⁰ ZUBOFF 2019, 23.

¹²⁰¹ WÄLT/L/VOGL, 8.

¹²⁰² HÄNOLD, 131; WÄLT/L/VOGL, 9.

¹²⁰³ Vgl. EDÖB 2014a, 10.

¹²⁰⁴ AEBI-MÜLLER, N 564.

¹²⁰⁵ BBl 1988 II, 449.

¹²⁰⁶ DIMITROV *et al.*, 28.

¹²⁰⁷ Europarat 2015, N 19.2; EDÖB 2014a, 10.

¹²⁰⁸ STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 18; WOLFER, N 202; mit Bezug auf Videoüberwachung: STREIFF/VON KAENEL/RUDOLPH, Art. 328 OR N 8; Urteil BGer 6B_536/2009 vom 12.11.2009; mit Bezug auf Spyware: BAERISWYL 2013, 444,

digte Videoüberwachung des Verkaufspersonals in einem Supermarkt verhältnismässig sein, wenn der begründete Verdacht besteht, dass mehrere Arbeitnehmer aufeinander abgestimmte Diebstahlsdelikte zum Schaden der Arbeitgeberin begehen.¹²⁰⁹

5.6.2 Ungenügende Umsetzung der Erkennbarkeit

Auch wenn das DSGVO Transparenz verlangen mag, umgesetzt wird sie in der Praxis jedoch ungenügend.¹²¹⁰ So kann es vorkommen, dass diejenigen, die nicht an der Programmierung beteiligt sind, das Modell als algorithmische «Blackbox» wahrnehmen.¹²¹¹ Darunter ist ein komplexes Entscheidungsfindungssystem zu verstehen, von welchem nur das äussere Verhalten, nicht aber die innere Struktur sichtbar ist.¹²¹² Den Betroffenen sind nur die erhobenen Eingabedaten und das ausgegebene Ergebnis bekannt, während undurchsichtig bleibt, wie und warum es zum Resultat gekommen ist.¹²¹³ Aber nicht nur den betroffenen Arbeitnehmern, sondern auch vielen Arbeitgeberinnen ist das Innenleben dieser Blackbox, die sie von Entwick-

m.w.H.; mit Bezug auf das Googeln von Arbeitnehmern und Bewerbern: FLUECKIGER 2014, 87.

¹²⁰⁹ Urteil EGMR vom 17.10.2019, López Ribalda and others vs. Spain, Nr. 1874/13 und 8567/13, §§ 133–137.

¹²¹⁰ BOLLIGER *et al.*, 91; Prof. Dr. Florent Thouvenin im Interview: FAKI SERMÍN / WURM ANJA, Daten-Professor Florent Thouvenin verteidigt Facebook, Google und Co.: «Die beissen doch nicht!», Blick vom 30.05.2018, abrufbar unter <www.blick.ch> (besucht am 31.05.2020); keine Informationen zur Konzeption von Algorithmen im Einzelfall: HOFFMANN-RIEM, 47; fehlende Erklärungen zum Zustandekommen algorithmischer Entscheide: WATTL/VOGL, 9; mangelnde Information der Bewerber, warum sie vom Algorithmus abgewiesen worden sind: DREYER/SCHULZ, 7. Mehr Informationen sind darüber erforderlich, wie algorithmische Systeme gestaltet und getestet werden: MERCHANT BRIAN, Applying for your next job may be an automated nightmare, 24.04.2019, abrufbar unter <<https://gizmodo.com>> (besucht am 31.05.2020).

¹²¹¹ White House, Executive Office of the President 2016, 8. Oft sind die einzelnen Algorithmen Teile komplexer digitaler Entscheidungssysteme: HOFFMANN-RIEM, 13.

¹²¹² WILDHABER *et al.*, 480.

¹²¹³ Europäische Kommission 2019a, 5; GAY/KAGAN.

lernen einkaufen, unbekannt.¹²¹⁴ Sogar die Ingenieure selbst bekunden Mühe, die von ihnen persönlich programmierten Algorithmen zu verstehen.¹²¹⁵

Die Gründe für den Transparenzmangel sind vor allem technischer Natur:¹²¹⁶ Algorithmen entwickeln sich dank KI und maschinellem Lernen selbständig weiter, weshalb die algorithmischen Analyseergebnisse nicht vorhergesagt werden können.¹²¹⁷ Dies hat jedoch auch einen Vorteil: Selbständig lernende Modelle weisen im Vergleich zu leicht erklärbaren Modellen eine höhere Vorhersagegenauigkeit auf, weil sie mehr Beziehungen zwischen Variablen berücksichtigen.¹²¹⁸

5.6.3 Restriktive Auslegung der Erkennbarkeit

Beim Anblick der mangelhaften Verwirklichung der Transparenz bei People Analytics ist zu überlegen, welche Elemente der Datenbearbeitung erkennbar sein müssen und welche nicht. Das Gesetz verlangt Transparenz über die Beschaffung und den Bearbeitungszweck, doch ist diese Auflistung nicht abschliessend («insbesondere», Art. 4 Abs. 4 DSGVO).

Rechtliche Grenzen können einer vollständigen Transparenz von Algorithmen entgegenstehen. Zu denken ist einerseits an die Geschäftsgeheimnisse der Arbeitgeberin, die dazu dienen, Innovationsanreize zu setzen, indem gegenüber der Konkurrenz ein wirtschaftlicher Vorsprung entsteht und die betroffenen Arbeitnehmer

¹²¹⁴ MRKONICH *et al.*, 36.

¹²¹⁵ PURTOVA 2018, 53; HÄNOLD, 130–131; algo:aware [sic], 23–24; CRAWFORD/SCHULTZ, 99; ANANNY/CRAWFORD, 981. «*Something magical is happening*»: WALT/VOGL, 3. «*Technology indistinguishable from magic*»: BRYNJOLFSSON/MCAFEE, 13.

¹²¹⁶ ANANNY/CRAWFORD, 981.

¹²¹⁷ ANANNY/CRAWFORD, 982; CRAWFORD/SCHULTZ, 99; CUSTERS/URSIC, 340; HOFFMANN-RIEM, 34.

¹²¹⁸ LOHMANN MELINDA F., Blackbox, öffne dich, FAZ Einspruch Magazin vom 22.08.2018, abrufbar unter <<https://einspruch.faz.net>> (besucht am 31.05.2020); THELISSON *et al.*, 55. Neue, intransparente, aber effektive Techniken umfassen die Stützvektormethode (*support vector machine*), Klassifikationsverfahren anhand von Entscheidungsbäumen (*random forest*), probabilistische grafische Modelle (*probabilistic graphical models*), bestärkendes Lernen (*reinforcement learning*) und künstliche neuronale Netze zum tiefgehenden Lernen (*deep learning neural networks*): DARPA, 5. Lineare Modelle sind nicht unbedingt besser nachvollziehbar als künstliche neuronale Netze: LIPTON, 42.

das algorithmische System nicht manipulieren können.¹²¹⁹ Andererseits können Rechte Dritter einer Lüftung der Blackbox-Geheimnisse entgegenstehen, etwa weil ihre Personendaten in den Algorithmus eingeflossen sind und eine Veröffentlichung ihre Privatsphäre gefährden könnte.¹²²⁰

Eine totale Transparenz bei People Analytics kann nicht beabsichtigt werden, weil Persönlichkeitsverletzungen auch bei vollständiger Transparenz eintreten können.¹²²¹ Jemand kann seiner Authentizität verlustig gehen und wird sich verstellen, wenn er stets von einer Beobachtung ausgehen muss.¹²²² Zudem kann die Kenntnis der einzelnen Bearbeitungsschritte allein nicht gewährleisten, dass die Betroffenen verstehen, wie ein Modell als Ganzes funktioniert.¹²²³ Wenn alle, auch unwichtigen Eigenschaften des Algorithmus offengelegt werden, nimmt diese Lektüre für den Informationsempfänger so viel Zeit in Anspruch, dass er von den wesentlichen Informationen und der Ausübung seiner Betroffenenrechte abgelenkt wird.¹²²⁴ Die amerikanische Behörde DARPA (*Defense Advanced Research Projects Agency*) führt vor dem Hintergrund, dass für Betroffene kaum nachvollziehbar ist, wie sich selbständig lernende Algorithmen verändern, unter dem Titel XAI (*explainable artificial intelligence*) eigens ein Forschungsprogramm, das die Erklärbarkeit von KI verbessern will.¹²²⁵

Inspiration für eine geeignete Ausgestaltung der Transparenzpflicht können die Vorschläge zur Transparenz über automatisierte Entscheidungen im Einzelfall bieten. Während die entsprechenden Bestimmungen (Art. 19 E-DSG, Art. 21 rev-DSG;

¹²¹⁹ HOFFMANN-RIEM, 59; HOEREN 2018, 191; Manipulieren auch als «*to game the system*» bekannt: WACHTER *et al.*, 843; HÄNOLD, 130. Der Schutz der Berufsgeheimnisse wirkt positiv bzw. «performativ» auf die Wirtschaft: ANANNY/CRAWFORD, 980.

¹²²⁰ ANANNY/CRAWFORD, 978.

¹²²¹ Vgl. WOLFER, N 150. Kritik, der EGMR berücksichtige die Gefahren transparenter Überwachung zu wenig: JERVIS, 446.

¹²²² AEBI-MÜLLER, N 657.

¹²²³ «*Seeing inside a system does not necessarily mean understanding its behaviour or origins*»: ANANNY/CRAWFORD, 980 und 983. «*In most cases you cannot understand an automated decision system simply by looking at the source code*»: AI now institute, 5. Vgl. KROLL *et al.*, 661.

¹²²⁴ Zu viel Transparenz führt zu strategischer Verdunkelung wichtiger Informationen: ANANNY/CRAWFORD, 979. «*Transparency fallacy*»: EDWARDS/VEALE, 67; «*transparency paradox*»: NISSENBAUM 2011, 36.

¹²²⁵ DARPA, 7. Vgl. BIRAN/COTTON, 11. LOHMANN MELINDA F., Blackbox, öffne dich, FAZ Einspruch Magazin vom 22.08.2018, abrufbar unter <<https://einspruch.faz.net>> (besucht am 31.05.2020).

Art. 22 DSGVO) auf People Analytics nur selten Anwendung finden werden, weil eine beeinträchtigende Personalentscheidung kaum je ausschliesslich auf einer automatisierten Bearbeitung beruht,¹²²⁶ können sie vorliegend als Auslegungshilfe dienen. Vorgesehen ist kein verbindliches Recht auf Erklärung einer automatisierten Einzelentscheidung, sondern bloss eine Information darüber (vgl. Art. 19 Abs. 1 E-DSG, Art. 21 Abs. 1 rev-DSG).¹²²⁷

WACHTER, MITTELSTADT und RUSSEL schlagen vor, die Informationspflichten betreffend automatisierte Entscheidungen im Einzelfall auf kontrafaktische Erklärungen (*counterfactual explanations*) einzuschränken. Dabei würde die Information auf ein Minimum beschränkt, ohne Einblick in das Innenleben des Algorithmus zu gewähren.¹²²⁸ Eine kontrafaktische Erklärung beschreibt stattdessen die Abhängigkeit eines Entscheids von externen Umständen.¹²²⁹ Sie beschreibt, wie sich ein externer Umstand ändern müsste, damit der Algorithmus das gewünschte Resultat produzieren würde.¹²³⁰ Beispielsweise könnte eine kontrafaktische Erklärung lauten: «Die Beförderung des Arbeitnehmers wurde abgelehnt, weil er erst seit einem Jahr im Unternehmen arbeitet. Wäre er seit zwei Jahren angestellt, hätte der Algorithmus die Beförderung vorgeschlagen.»¹²³¹ Aus einer modellzentrierten Erklärung, die alle Bearbeitungsschritte einzeln erläutert, wird somit eine subjektzentrierte Erklärung, die sich auf das beschränkt, was die Betroffenen wissen wollen, nämlich, wie sie den Ausgang beeinflussen können.¹²³² Kontrafaktische Erklärungen können hingegen nicht genügen, wenn umfassende Kenntnis über die Systemfunktionalität erforderlich ist, beispielsweise, wenn Statistiken erforderlich sind, um zu prüfen, ob der Algorithmus diskriminiert.¹²³³

Der Vorschlag von THOUVENIN und FRÜH im Zusammenhang mit der Information über automatisierte Entscheidungen im Einzelfall (Art. 19 Abs. 1 E-DSG, Art. 21

¹²²⁶ THOUVENIN/FRÜH 2020, 16; GLATTHAAR, 19; zur DSGVO WACHTER *et al.*, 842.

¹²²⁷ Bzgl. Art. 22 DSGVO: WACHTER *et al.*, 842. Die DSGVO konkretisiere den Zweck und Inhalt von Erklärungen kaum: WACHTER *et al.*, 880.

¹²²⁸ WACHTER *et al.*, 851. Vgl. WACHTER *et al.*, 843: «*without opening the black box*».

¹²²⁹ WACHTER *et al.*, 845.

¹²³⁰ WACHTER *et al.*, 844. Dementsprechend hat eine kontrafaktische Erklärung die Form einer «Warum nicht»-Begründung: algo:aware [sic], 25.

¹²³¹ Vgl. das Beispiel zu einer Darlehensgewährung: WACHTER *et al.*, 844.

¹²³² Algo:aware [sic], 25. Vgl. WALT/VOGL, 5.

¹²³³ WACHTER *et al.*, 883.

Abs. 1 rev-DSG) zielt auf eine Zweiteilung der Informationspflicht. Eine rudimentäre allgemeine Transparenzpflicht soll in allen Fällen offenlegen, dass Methoden der automatisierten Entscheidungsfindung verwendet werden. Eine erweiterte Transparenzpflicht soll dagegen nur für Fälle gelten, in denen die Betroffenen ein Rechtsmittel oder einen Rechtsbehelf zur Hand haben, um den Entscheid anzufechten, und somit ein genügendes Interesse an weiterer Information besteht.¹²³⁴ Dabei ist davon auszugehen, dass die allgemeine Transparenz dem Entscheid zeitlich vorausgeht (*ex ante*), die erweiterte hingegen nachfolgt (*ex post*).

Vorliegend wird gestützt auf die vorgestellten Argumente eine eher restriktive Auslegung der Bearbeitungsregel der Erkennbarkeit vertreten in dem Sinne, dass ein Übermass an Information nicht erstrebenswert ist. Die Erkennbarkeit ist wortwörtlich so auszulegen, dass die Arbeitnehmer die Vorgänge in Algorithmen «erkennen» bzw. verstehen und es nicht bei der blossen Sichtbarkeit durch Transparenz bleibt.¹²³⁵ Anzupeilen ist eine qualitativ hochwertige Transparenz, die sich nur schwer quantitativ ausdrücken lässt. Die Pflicht zur Transparenz sollte sich am Informationsinteresse des Betroffenen ausrichten. Interessieren dürften etwa die Form der Überwachung (z.B. Video oder GPS), der Zweck (z.B. Diebstahlschutz oder Leistungsoptimierung) und die Dauer der Überwachung sowie gegebenenfalls die Möglichkeit zum Ergreifen von Rechtsmitteln.¹²³⁶ Auch die Bearbeitungsart und die Natur der Daten beeinflussen den Grad der nötigen Transparenz. Informationen über die Grundzüge eines Datenbearbeitungssystems können allenfalls bereits genügen.¹²³⁷ Dagegen erscheint die Offenlegung von Systemdetails (z.B. des Algorithmenquellcodes) in der Regel nicht zielführend: Einerseits resultiert daraus kaum ein Verständnissgewinn für die Arbeitnehmer (all jene, die der Programmiersprache nicht mächtig sind, können den Quellcode nicht lesen). Andererseits bestehen oft schützenswerte Geheimhaltungsinteressen der Arbeitgeberin.

¹²³⁴ THOUVENIN/FRÜH 2019, 8. Vgl. THOUVENIN/FRÜH 2020, 14–15.

¹²³⁵ Vgl. auf internationaler Ebene: World Economic Forum 2013, 4.

¹²³⁶ Vgl. SECO 2018, 326–5 – 326–6.

¹²³⁷ ROSSNAGEL, 274. «*Less [transparency] can sometimes be more*»: World Economic Forum 2013, 18. Vgl. ANANNY/CRAWFORD, 979. Mangelnde Sachkunde kann ein Indiz dafür sein, dass das Datenschutzinteresse in dem betreffenden Bereich eher tief ist: ROSENTHAL 2012, 81.

5.7 Richtigkeitsgebot

Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern. Er hat alle angemessenen Massnahmen zu treffen, damit die Daten berichtigt oder vernichtet werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind (Art. 5 Abs. 1 DSGVO, vgl. Art. 5 Abs. 5 E-DSG, vgl. Art. 6 Abs. 5 rev-DSG). Beim Prinzip der Richtigkeit geht es um die Regulierung der Informationsqualität. Anstatt Informationsflüsse als solche zu verbieten, wird verlangt, dass personenbezogene Information bestimmten qualitativen Anforderungen genügen und insbesondere zutreffen soll.¹²³⁸ Entscheidend ist nicht nur die absolute Zahl von Fehlern, sondern auch das Verhältnis zur gesamten Datenmenge: Wer bei der Bearbeitung von zehn Datensätzen fünf Fehler begeht, verletzt die Persönlichkeit der Betroffenen häufiger als derjenige, dem bei hundert Datensätzen «nur» zehn Fehler unterlaufen.¹²³⁹

Einige der von People Analytics ausgehenden Rechtsprobleme bestehen jedoch gerade darin, dass die Arbeitgeberin über qualitativ hochwertige Informationen verfügt, die ihr präzise Einsicht in das Leben der Arbeitnehmer gewähren.¹²⁴⁰ Beispielsweise können zu präzise Ableitungen zu einer unverhältnismässigen Persönlichkeitsdurchleuchtung führen.¹²⁴¹ Somit kann die Einhaltung der Informationsqualität (allein) nicht ausreichen, um die Privatsphäre der Arbeitnehmer zu bewahren.

5.8 Datenminimierung und Speicherbegrenzung

Die DSGVO statuiert explizit die Grundsätze der Datenminimierung und Speicherbegrenzung. Die Datenerhebung muss sich auf das für die Zwecke der Bearbeitung notwendige Mass beschränken (Datenminimierung, Art. 5 Abs. 1 lit. c DSGVO). Zudem müssen Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange zulässt, wie es für die Zwecke,

¹²³⁸ MATZNER, 102; «*need for intervention [...] to regulate information quality*»: GASSER 2004, 13–15; zum Regulierungsansatz der Informationsqualität: AEBI-MÜLLER, N 845. Vgl. DRUEY 1995, 243–246, und KASPER, N 95–102.

¹²³⁹ ROSENTHAL 2012, 91.

¹²⁴⁰ AEBI-MÜLLER, N 621.

¹²⁴¹ Siehe S. 187.

für die die Daten bearbeitet werden, erforderlich ist (Speicherbegrenzung, Art. 5 Abs. 1 lit. e DSGVO).

Im geltenden und im künftigen schweizerischen Datenschutzrecht sind die beiden Bearbeitungsregeln der Datenminimierung und Speicherbegrenzung nicht explizit verankert. Sie stehen zwar in enger Verwandtschaft mit dem Verhältnismässigkeitsprinzip (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG).¹²⁴² Auch umschreibt das künftige Datenschutzrecht die Speicherbegrenzungspflicht, indem er verlangt, dass Personendaten vernichtet oder anonymisiert werden müssen, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind (Art. 5 Abs. 4 E-DSG, Art. 6 Abs. 4 rev-DSG).¹²⁴³ Insgesamt zeigen jedoch sowohl das DSG als auch das rev-DSG eine gewisse Zurückhaltung bei der Aufnahme der beiden Bearbeitungsregeln. Dies ist zu begrüßen, wie sogleich gezeigt wird.

Der Grundsatz der Datenminimierung steht quer zu anderen Rechtsbestimmungen. Das Gebot der Datenminimierung kann mit dem Grundsatz der Datensicherheit (Art. 7 DSG, Art. 7 E-DSG, Art. 8 rev-DSG) in Konflikt geraten.¹²⁴⁴ Dieser verlangt, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden (Art. 7 Abs. 1 DSG, Art. 8–12 VDSG; Art. 7 Abs. 1 E-DSG, Art. 8 Abs. 1 rev-DSG). Integrität und Vertraulichkeit, aber auch Verfügbarkeit ist zu gewährleisten.¹²⁴⁵ Die Protokollierung der automatisierten Bearbeitung besonders schützenswerter Personendaten oder von Persönlichkeitsprofilen ist per Verordnung vorgeschrieben (vgl. Art. 10 VDSG). Als Vorkehrung gegen Angriffe und Datenverluste ist die Speicherung von Back-ups über längere Zeit erforderlich.¹²⁴⁶ Jede Anomalieerkennung basiert auf einer umfassenden Logfile-Analyse, die zwangsläufig eine Speicherung des normalen Benutzerverhaltens als Referenz und somit ein Profiling voraussetzt.¹²⁴⁷

¹²⁴² Der Grundsatz der Speicherbegrenzung werde aus dem allgemeinen Verhältnismässigkeitsprinzip abgeleitet: BBI 2017, 7026.

¹²⁴³ BBI 2017, 7026.

¹²⁴⁴ SCHNABL, N 4. Vgl. PÄRLI 2018, N 17.5.

¹²⁴⁵ SIGRIST, N 24. Vgl. GILBERT, 272.

¹²⁴⁶ Löschfrist von «vielen Monaten oder Jahren» erforderlich, um Angriffe zu erkennen: SCHNABL, N 14; Back-ups für längere Zeit zu speichern, weil sich Schadsoftware nicht immer sofort zeigt und dadurch in Back-ups mitgespeichert werden kann: DOMENIG/MITSCHERLICH, N 451–452; Konflikt zwischen Löschpflicht und der Pflicht zur Datenintegrität (vgl. Art. 5 Abs. 1 lit. f DSGVO): STIEMERLING, 95.

¹²⁴⁷ SCHNABL, N 17. Die Informationsgewinnung aus frei verfügbaren Quellen (*open source intelligence*, OSINT) als Mittel zur Detektion und Repression von Sicherheits-

Die Aufzeichnung von Metadaten, die für das Funktionieren des Systems selbst nicht erforderlich wären, kann zur Gewährleistung der Datensicherheit angezeigt sein.¹²⁴⁸ Somit verlangen die Informationssicherheit und die effiziente Abwehr von Gefahren nach umfangreichem Wissen über Vorgänge im digitalen, aber auch analogen Umfeld.¹²⁴⁹ Der Grundsatz der Datensicherheit strebt nach einem Maximum an Information, während das Ideal der Datenminimierung das Gegenteil verkörpert. Ein Kompromiss zwischen den gegensätzlichen Prinzipien der Datenminimierung und der Datensicherheit ist erstrebenswert, da der Datenschutz als Ganzes durch eine erhöhte Datensicherheit gewinnen wird.¹²⁵⁰

Sodann schwelt ein Konflikt zwischen der Datenminimierung und dem Auskunftsrecht: Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden (Art. 8 DSG, Art. 23 E-DSG, Art. 25 rev-DSG). Der Auskunftsanspruch besteht grundsätzlich jederzeit; niemand kann im Voraus auf das Auskunftsrecht verzichten (Art. 8 Abs. 6 DSG, Art. 23 Abs. 5 E-DSG, Art. 25 Abs. 5 rev-DSG).¹²⁵¹ Problematisch ist, dass die Arbeitgeberin aufgrund der möglichen Ausübung des Rechts auf Auskunft durch einen Arbeitnehmer praktisch dazu gezwungen ist, alle entscheidungsrelevanten Daten zu speichern und für den Fall der Auskunft vorzuhalten – auch dann, wenn dies zur Durchführung des Arbeitsvertrags (Art. 328b OR) gar nicht nötig wäre.¹²⁵²

Der Grundsatz der Datensparsamkeit ist relativ zum Bearbeitungszweck zu verstehen. D.h., dass es je nach Zwecksetzung erforderlich sein kann, mehr oder weniger Daten zu bearbeiten.¹²⁵³

Auch über die DSG-internen Widersprüche hinaus gibt es Konfliktpotenzial: Eine Diskrepanz besteht zwischen dem Grundsatz der Datenminimierung und der

vorfällen kann unter dem Aspekt der IT-Compliance zwingend sein: VON MALTZAN, 213. Flächendeckende Durchleuchtung des Computersystems notwendig zum Schutz gegen externe Saboteure: RIEDY/WEN, 91.

¹²⁴⁸ KOOPS/LEENES, 166–167. Siehe zum Begriff der Metadaten FN 213.

¹²⁴⁹ SCHNABL, N 3.

¹²⁵⁰ SAARENPÄÄ, 99. Vgl. HARTZOG 2013, 1022.

¹²⁵¹ Erfolgreiche Geltendmachung eines Auskunftsanspruchs durch einen juristischen Sekretär des eidgenössischen Versicherungsgerichts rund 20 Jahre (!) nach seiner Entlassung: Urteil Eidgenössische Datenschutzkommission VPB 62.38 vom 26.05.1995 E. 3c; RUDOLPH, 1679.

¹²⁵² DREYER/SCHULZ, 30.

¹²⁵³ ROSENTHAL 2012, 83.

Nichtdiskriminierung.¹²⁵⁴ Die Erstellung eines nicht diskriminierenden Algorithmus setzt voraus, dass umfassend Daten zu den betroffenen Personen, auch zu ihren geschützten verpönten Merkmalen, in den Modellierungsprozess einbezogen werden, wie noch gezeigt werden wird.¹²⁵⁵ Das (Datenschutz-)Recht muss diesen Einbezug auf angemessene Art zulassen.¹²⁵⁶

Schliesslich können Grundrechte der Datenminimierung entgegenstehen, so beispielsweise die Grundrechte auf Meinungs- und Informationsfreiheit (Art. 16 BV), Wissenschaftsfreiheit (Art. 20 BV) und Wirtschaftsfreiheit (Art. 27 BV).

Zusammenfassend bestehen zwischen den am Bearbeitungsprozess orientierten Bestimmungen der Datenminimierung und der Speicherbegrenzung einerseits und diversen Rechtsbestimmungen andererseits Konfliktpotenziale. Infolgedessen ist es unrealistisch, an einer strengen Minimierung der Bearbeitung von Personendaten festzuhalten.¹²⁵⁷ Stattdessen ist eine «behutsame Neuinterpretation» zu erwägen.¹²⁵⁸ Die widerstreitenden Grundsätze sollten in ein ausgewogenes Verhältnis zueinander gesetzt werden. Leitstern muss dabei der Persönlichkeitsschutz (Art. 1 DSG, Art. 1 E-DSG, Art. 1 rev-DSG) bzw. das Risiko einer Persönlichkeitsverletzung sein. Eine risikoorientierte Auslegung der entsprechenden Datenschutzbestimmungen ist daher zu befürworten.¹²⁵⁹ Beispielsweise könnte es für die Einhaltung des Datenminimierungs-Grundsatzes genügen, die Daten bloss zu anonymisieren oder pseudonymisieren, statt gänzlich auf sie zu verzichten.¹²⁶⁰

5.9 Löschpflicht

5.9.1 Norminhalt

Aus dem allgemeinen Rechtsgrundsatz der Verhältnismässigkeit (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG) fliesst die Pflicht der Arbeit-

¹²⁵⁴ ŽLIOBAITĖ/CUSTERS, 183.

¹²⁵⁵ Siehe S. 342–343. ŽLIOBAITĖ/CUSTERS, 199.

¹²⁵⁶ ŽLIOBAITĖ/CUSTERS, 199.

¹²⁵⁷ TAMÒ-LARRIEUX, 192.

¹²⁵⁸ Bzgl. der DSGVO und mit der Forderung nach einer Neuinterpretation auch der Grundsätze der Zweckbindung und der datenschutzfreundlichen Voreinstellungen: HERMSTRÜWER, 115.

¹²⁵⁹ Siehe bereits S. 140.

¹²⁶⁰ TAMÒ-LARRIEUX, 192.

geben, die Daten nach einer bestimmten Zeit zu löschen.¹²⁶¹ Der spezifische Datenbearbeitungsgrundsatz der Zweckbindung (Art. 4 Abs. 3 DSG, Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG) konkretisiert, dass die Aufbewahrung (eine Form des Bearbeitens, vgl. Art. 3 lit. e DSG, Art. 4 lit. d E-DSG, Art. 5 lit. d rev-DSG) unzulässig ist, sobald die Daten für den Zweck, der zu ihrer Erhebung geführt hat, nicht mehr benötigt werden.¹²⁶² Werden Daten zu mehreren Zwecken analysiert, sind sie zu löschen, wenn der letzte Zweck erfüllt worden ist.¹²⁶³ Korrespondierend fließt aus dem Recht auf informationelle Selbstbestimmung für den Arbeitnehmer ein Anspruch auf Datenvernichtung (vgl. Art. 12 Abs. 2 lit. b DSG, Art. 26 Abs. 2 lit. b E-DSG, Art. 30 Abs. 2 lit. b rev-DSG).¹²⁶⁴ Die Begriffe der «Löschung» und «Vernichtung» von Daten werden vorliegend gleichbedeutend verwendet.

Der Löschpflicht des DSG liegt der Schutz der subjektiven Persönlichkeitsrechte des Betroffenen zugrunde (vgl. Art. 1 DSG, Art. 1 E-DSG, Art. 1 rev-DSG). Die Löschpflicht ist nach vorliegender Auffassung nicht an eine starre Frist gebunden.¹²⁶⁵ Es handelt sich somit um eine implizit zeitbezogene Norm; dies im Gegensatz zu explizit zeitbezogenen Normen, die den Informationsbestand an sich schützen und Aufbewahrungszeiträume vordefinieren.¹²⁶⁶ Somit ist im Sinne einer risikoorientierten Auslegung in jedem Einzelfall abzuwägen, ob das Interesse des Betroffenen an der Löschung oder dasjenige der Verantwortlichen an der Daten-

¹²⁶¹ AEBI-MÜLLER, N 565; BSK OR I-PORTMANN/RUDOLPH, Art. 328b OR, N 42.

¹²⁶² BSK DSG-MAURER-LAMBROU/STEINER, Art. 4 DSG, N 14. Vgl. die ausdrückliche Normierung in Art. 17 Abs. 1 lit. a DSGVO. FRANZEN, 327. Vgl. Europarat 2016b, 49.

¹²⁶³ WARTER, 4.

¹²⁶⁴ RIESELMANN-SAXER, 69.

¹²⁶⁵ Keine starre Frist, sondern «unverzügliche Löschung» gebietet Art. 17 Abs. 1 DSGVO, was so viel wie «ohne schuldhaftes Zögern» bedeutet: Hessischer Beauftragter für Datenschutz und Informationsfreiheit, Häufig gestellte Fragen, abrufbar unter <<https://datenschutz.hessen.de>> (besucht am 31.05.2020). Nach wohl **a.M.** gelten abstrakte, aber zwischen den einzelnen Meinungen stark variierende Aufbewahrungszeiträume von einer «sehr kurzen Frist» (in Bezug auf Daten abgewiesener Bewerber: Europarat 2016b, 33), «drei Wochen» (so die österreichische Datenschutzkommission im Jahr 2008 bzgl. Logfiles: Bescheid Beschwerde Datenschutzkommission [Österreich] K121.358/0009-DSK/2008 vom 20.06.2008 E. 2.3c/bb) oder zwei (MATHYS, 100) bis fünf Jahren (je nach Datenkategorie: EDÖB 2014b, 14).

¹²⁶⁶ Zu implizit und explizit zeitbezogenen Normen: EGGIMANN, 37.

nutzung, etwa durch Wiederverwertung oder Lizenzierung an Dritte, überwiegt.¹²⁶⁷

5.9.2 Umsetzung der Löschung

Von technischer Seite her sollten die Daten der Arbeitnehmer mit Metadaten versehen werden, die den Zeitpunkt der Datenerhebung und die voraussichtliche Gültigkeitsdauer der Daten und des erlaubten Bearbeitungszwecks festhalten.¹²⁶⁸ Für die Löschung braucht es ein Zusammenwirken von unterschiedlichen Lösungsverfahren und begleitenden Schutzmassnahmen gegen eine Datenwiederherstellung über alle vernetzten Systeme und Datenträger hinweg.¹²⁶⁹ Es wird ins Feld geführt, anstelle einer Löschung von Personendaten könne auch ihre Anonymisierung genügen.¹²⁷⁰ Dies ist angesichts der Schwierigkeiten zur Bewerkstelligung einer irreversiblen Anonymisierung nur mit Zurückhaltung zu bejahen.¹²⁷¹

Bevor die Daten endgültig gelöscht oder anonymisiert werden, kann ein vorläufiges Sperren bzw. eine Einschränkung der Bearbeitung (vgl. Art. 18 DSGVO) sinnvoll sein. Dies erlaubt ein Entsperren von Datensätzen, falls aufgrund fachlicher oder technischer Fehler ein Datensatz irrtümlich gesperrt wurde.¹²⁷² Dienen die Daten mehreren Zwecken, ist Sperren das Mittel, um sicherzustellen, dass die gesperrten Datensätze nur noch für die übrigen, noch aktuellen Zwecke von den dafür zuständigen Personen bearbeitet werden.¹²⁷³ Umgesetzt wird das Sperren durch Verschlüsselung und Verteilung der Zugangsschlüssel nur an die berechtigten Personen.¹²⁷⁴ Der EDÖB empfiehlt, am letzten Arbeitstag das E-Mail-Konto des aus-

¹²⁶⁷ Kritik an einer generellen Pflicht zur Löschung: EGGIMANN, 213–214; für eine Aufhebung der Löschpflicht und dafür strengere Inpflichtnahme der Datenbearbeiter: MAYER-SCHÖNBERGER/CUKIER, 174.

¹²⁶⁸ Vgl. SCHÜRER, 64. Siehe zum Begriff der Metadaten FN 213.

¹²⁶⁹ VALERSI MICHAEL, Definitiv lassen sich Daten nicht löschen, NZZ online vom 07.12.2016, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

¹²⁷⁰ Zum europäischen Recht der DSGVO: VASELLA DAVID, Österreichische Datenschutzbehörde: Anonymisierung von Personendaten als Form der Löschung, 01.02.2019, abrufbar unter <https://datenrecht.ch> (besucht am 31.05.2020); zum amerikanischen Recht: White House, Executive Office of the President 2014, 8.

¹²⁷¹ Siehe zur Re-Identifizierbarkeit: S. 157.

¹²⁷² WARTER, 4.

¹²⁷³ WARTER, 4.

¹²⁷⁴ Vgl. STIEMERLING, 96.

tretenden Mitarbeiters sowie alle anderen EDV-Konten zu sperren, um sie nach einer gewissen Zeit zu löschen.¹²⁷⁵

Eine definitive Vernichtung von Daten ist technisch schwierig umzusetzen, weil dieselben Daten oft automatisch an verschiedenen physischen Speicherorten und in verschiedenen Systemen im Unternehmen sowie, im Fall der Auftragsdatenbearbeitung, auch bei Dritten abgelegt werden.¹²⁷⁶ Es kommt praktisch nie vor, dass nur eine einzige Kopie existiert. Deshalb sind hohe Anforderungen an die Datenvernichtung zu stellen. Nach der Rechtsprechung des Bundesverwaltungsgerichts genügt es nicht, nur den Datenträger unbrauchbar zu machen (z.B. durch Durchbohrung oder Durchlochung einer CD oder eines USB-Sticks), sondern auch alle Kopien (inkl. sämtlicher Back-ups) müssen so behandelt werden, dass die Daten nicht mehr lesbar gemacht werden können.¹²⁷⁷

Zur Löschung sind auch rechtliche Massnahmen zu ergreifen: Die anwendbaren abstrakten Grundsätze sind in einem für die Belegschaft zugänglichen betriebsinternen Reglement über die Nutzung von Informatikmitteln festzuhalten und durch Schulungen zu vertiefen.¹²⁷⁸ Der (automatisierte oder manuelle) Lösungsprozess im konkreten Fall ist detailliert zu dokumentieren.¹²⁷⁹ Dies hilft bei Beweisschwierigkeiten; denn die Tatsache der Löschung selbst lässt sich naturgemäss nicht nachweisen, wenn das Datum nicht mehr da ist.

5.10 Rechtfertigungsmöglichkeiten

5.10.1 Übersicht zu den relevanten Bestimmungen

Ein Verstoß gegen Datenschutzbestimmungen und eine daraus resultierende Persönlichkeitsverletzung ist nicht schlechthin widerrechtlich. Das DSG beschreibt drei Rechtfertigungsgründe, bei deren Vorliegen eine Persönlichkeitsverletzung zulässig ist: Einwilligung, überwiegendes privates oder öffentliches Interesse sowie Gesetz (Art. 13 DSG, Art. 27 E-DSG, Art. 31 rev-DSG, dazu S. 219–240). In

¹²⁷⁵ EDÖB 2018a, 27.

¹²⁷⁶ STIEMERLING, 96; VALERSI MICHAEL, Definitiv lassen sich Daten nicht löschen, NZZ online vom 07.12.2016, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

¹²⁷⁷ BVGE 2015/13 E. 3.3.4.

¹²⁷⁸ EDÖB 2018a, 27.

¹²⁷⁹ VALERSI MICHAEL, Definitiv lassen sich Daten nicht löschen, NZZ online vom 07.12.2016, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

diesem Zusammenhang ist vorneweg klarzustellen, dass Grundsatzverstöße (Art. 12 Abs. 2 lit. a DSG, Art. 26 Abs. 2 lit. a E-DSG, Art. 30 Abs. 2 lit. a rev-DSG) rechtfertigbar sind und die Bearbeitung allgemein zugänglich gemachter Personendaten (Art. 12 Abs. 3 DSG, Art. 26 Abs. 3 E-DSG, Art. 30 Abs. 3 rev-DSG) gegebenenfalls einer Rechtfertigung bedarf (dazu sogleich).

5.10.2 Rechtfertigungsmöglichkeit für Grundsatzverstöße

Die Arbeitgeberin darf nicht Personendaten entgegen den Grundsätzen von Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG bearbeiten (Art. 12 Abs. 2 lit. a DSG, Art. 26 Abs. 2 lit. a E-DSG, Art. 30 Abs. 2 lit. a rev-DSG). Nach dem scharfen Gesetzeswortlaut kann ein Grundsatzverstoss nie gerechtfertigt werden, während bei anderen Persönlichkeitsverletzungen eine Rechtfertigungsmöglichkeit besteht (vgl. Art. 12 Abs. 2 lit. b und c DSG: «Rechtfertigungsgrund»). Ein Blick zurück auf die Gesetzgebungsgeschichte scheint diese Auslegung zu bestätigen: Im Zuge der Revision des DSG vom 24.03.2006 wurde der Vorbehalt des Rechtfertigungsgrunds bei einer Verletzung von Grundsätzen der Datenbearbeitung gestrichen.¹²⁸⁰ Dies hat Anlass zur Annahme gegeben, das Gesetz fingiere eine unwiderlegbare widerrechtliche Persönlichkeitsverletzung, wenn die Arbeitgeberin die Datenbearbeitungsgrundsätze missachte.¹²⁸¹ Die Datenschutzbestimmungen sind nicht im Hinblick auf die Besonderheiten von People Analytics entwickelt worden, und so tun sich Zielkonflikte im Verhältnis zu den datenschutzrechtlichen Prinzipien der Zweckbindung, der Erkennbarkeit, der Datenminimierung und der Löschpflicht auf.¹²⁸² In der Konsequenz würde dies bedeuten, dass People Analytics in aller Regel widerrechtlich wäre.

Der Gesetzeswortlaut ist jedoch zu relativieren: Der Berichterstatter der ständerrätlichen Kommission erläuterte ausführlich, dass es sich bei der Änderung von Art. 12 Abs. 2 lit. a DSG (bzw. Art. 26 Abs. 2 lit. a E-DSG bzw. Art. 30 Abs. 2 lit. a rev-DSG) um eine Klarstellung dessen handle, was bereits bis dahin gegolten habe. Datenbearbeitungen entgegen den Grundsätzen können somit mit den üblichen Gründen gerechtfertigt werden (vgl. Art. 13 DSG, Art. 27 E-DSG, Art. 31

¹²⁸⁰ Bundesamt für Justiz 2006, 1.

¹²⁸¹ So die Annahme von: WOLFER, N 200; ebenso: EPINEY, § 9 N 6.

¹²⁸² Siehe S. 176, 201, 206 und 209–212. Vgl. zum Konfliktpotenzial zwischen Datenschutz und Big Data: HOFFMANN-RIEM, 45 und 57. Big Data widerspricht diametral den datenschutzrechtlichen Prinzipien: RICHTER, 582.

rev-DSG).¹²⁸³ Trotz der Abwiegung durch den Ständerat behält Art. 12 Abs. 2 lit. a DSG (bzw. Art. 26 Abs. 2 lit. a E-DSG bzw. Art. 30 Abs. 2 lit. a rev-DSG) eine eigenständige Bedeutung: Das Bundesgericht bejaht die Rechtfertigungsgründe für einen Grundsatzverstoss im konkreten Fall nur mit grosser Zurückhaltung.¹²⁸⁴

5.10.3 Bearbeitbarkeit allgemein zugänglich gemachter Daten

a) Tatbestandsmerkmale und Rechtsfolge

In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person ihre Personendaten «allgemein zugänglich» gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Art. 12 Abs. 3 DSG, Art. 26 Abs. 3 E-DSG, Art. 30 Abs. 3 rev-DSG).¹²⁸⁵ Die allgemeine Zugänglichkeit ist ein unbestimmter Rechtsbegriff. Zur Prüfung, ob sie vorliegt, können die Erkenntnisse zur Informationsverbreitung in sozialen Netzwerken herangezogen werden.¹²⁸⁶ Demnach ist der Kontext einer informationellen Interaktion für die Verbreitungsgeschwindigkeit der Daten mindestens so entscheidend wie die Tatsache der Informationsbekanntgabe selbst.¹²⁸⁷ Die Beschaffenheit der Information und der Empfängerkreis beeinflussen die Geschwindigkeit.¹²⁸⁸ Eine interessante oder schockierende Information wird sich in Windeseile in weitem Umkreis verbreiten, sodass sie bald allgemein zugänglich sein wird.¹²⁸⁹ Demgegenüber wird eine komplexe Information in einem locker verbundenen Netzwerk schwerlich die Runde machen.¹²⁹⁰ Hier dürfte allein mit der Bekanntgabe der Information an ein anderes Netzwerkmitglied noch keine allgemeine Zugänglichkeit vorliegen.

¹²⁸³ Bundesamt für Justiz 2006, 2.

¹²⁸⁴ BGE 136 II 508 E. 5.2.4; BGE 138 II 346 E. 7.2.

¹²⁸⁵ Im weitesten Sinne geht es bei der Qualifikation als allgemein zugängliche Daten um den Rechtfertigungsgrund der konkludenten Einwilligung: KASPER/WILDHABER, 217 FN 175.

¹²⁸⁶ Vgl. STRAHILEVITZ' «*social networks theory of privacy*»: STRAHILEVITZ 2005.

¹²⁸⁷ WALDMAN, 104; STRAHILEVITZ 2005, 922.

¹²⁸⁸ WALDMAN, 103.

¹²⁸⁹ Vgl. STRAHILEVITZ 2005, 972.

¹²⁹⁰ WALDMAN, 102–103.

Die Formulierung, dass die Information allgemein zugänglich «gemacht» worden ist (vgl. Art. 12 Abs. 3 DSG, Art. 26 Abs. 3 E-DSG, Art. 30 Abs. 3 rev-DSG), enthält ein subjektives Element. Nicht nur die tatsächliche Zugänglichkeit für die Allgemeinheit, sondern auch der aus den Umständen ersichtliche Veröffentlichungszweck ist zu würdigen.¹²⁹¹ Stellt die betroffene Person eine Information einem begrenzten Publikum zur Verfügung mit der impliziten Auflage, die Nachricht für sich zu behalten, muss die Betroffene sich nicht gefallen lassen, dass die Daten an die Allgemeinheit weitergereicht werden.¹²⁹²

Die gesetzliche Vermutung der fehlenden Persönlichkeitsverletzung greift nur, wenn die betroffene Person die Datenbearbeitung «nicht ausdrücklich untersagt hat» (Art. 12 Abs. 3 DSG, Art. 26 Abs. 3 E-DSG, Art. 30 Abs. 3 rev-DSG). Auszuscheiden sind Informationen, die erkennbar gegen den Willen des Arbeitnehmers ins Internet gestellt worden sind (Art. 12 Abs. 2 lit. b DSG, Art. 26 Abs. 2 lit. b E-DSG, Art. 30 Abs. 2 lit. b rev-DSG).¹²⁹³ Nach einer restriktiven Meinung, die jedoch im Wortlaut keine Stütze findet, dürften nach einer Suche im Internet nur Daten bearbeitet werden, deren Veröffentlichung der Betroffene explizit wollte.¹²⁹⁴

Die Bearbeitung allgemein zugänglich gemachter Daten ist «in der Regel» zulässig (Art. 12 Abs. 3 DSG, Art. 26 Abs. 3 E-DSG, Art. 30 Abs. 3 rev-DSG). Das Gesetz behält somit Ausnahmen vor, in denen selbst für die Bearbeitung allgemein zugänglich gemachter Daten ein Rechtfertigungsgrund erforderlich ist. In Art. 328b OR ist eine solche Ausnahmeregel zu sehen, sodass im Arbeitsverhältnis auch öffentlich zugängliche Daten des Arbeitnehmers nur bearbeitet werden dürfen, wenn ein Zusammenhang mit dem Arbeitsplatz besteht.¹²⁹⁵ Die Arbeitgeberin darf nicht gezielt nach privaten Daten suchen.¹²⁹⁶ Untersagt ist auch eine generelle For-

¹²⁹¹ BSK DSG-RAMPINI, Art. 12 DSG, N 18.

¹²⁹² Vgl. SPRAGUE 2015, 17. Vgl. WALDMAN, 99–100, verweisend auf einen amerikanischen Fall, in dem eine verdeckte Reporterin Aussagen eines Arbeitnehmers, die nur für das Arbeitsumfeld gedacht gewesen waren, unzulässigerweise mit der Allgemeinheit teilte. Vgl. RICHARDS/KING, 396, und SPRAGUE 2015, 18.

¹²⁹³ KASPER/WILDHABER, 218. Vgl. zum deutschen Recht: DZIDA, 545.

¹²⁹⁴ Vgl. KUKO OR-PIETRUSZAK, Art. 328b OR, N 8, nach welchem in der Regel nicht davon ausgegangen werden könne, dass der Arbeitnehmer Daten, die mit Googleⁿ gefunden werden, allgemein zugänglich gemacht habe. Siehe auch, aber **a.M.**: THÜSING/TRAUT, N 7, und KASPER/WILDHABER, 218.

¹²⁹⁵ PÄRLI 2018, N 17.27; GEISER 2015, 376.

¹²⁹⁶ KUKO OR-PIETRUSZAK, Art. 328b OR, N 9; KASPER/WILDHABER, 217–218.

schung nach Informationen über Arbeitnehmer im Internet (*screening*), weil die Arbeitgeberin regelmässig auf Personendaten stossen wird, die weder der Eignungsabklärung dienen noch für die Vertragsdurchführung erforderlich sind, und zudem die Datenrichtigkeit nicht gewährleistet ist.¹²⁹⁷

Die Rechtsfolge von allgemein zugänglich gemachten Daten (im Sinne von Art. 12 Abs. 3 DSG bzw. Art. 26 Abs. 3 E-DSG bzw. Art. 30 Abs. 3 rev-DSG) ist eine gesetzliche Vermutung, dass die Datenbearbeitung zulässig ist. Es handelt sich nicht um eine unumstössliche Fiktion.¹²⁹⁸ Der betroffenen Person steht es offen, die Vermutung zu widerlegen. Bei der Annahme, dass trotz allgemeiner Zugänglichkeit eine Persönlichkeitsverletzung vorliege, ist Zurückhaltung geboten.¹²⁹⁹

b) Zugänglichkeit von Internetdaten

Der Begriff der allgemein zugänglich gemachten Daten sei am Beispiel von Internetdaten, die hergeben, ob ein Mitarbeiter abwanderungswillig ist, illustriert: Die Arbeitgeberin kann mithilfe des Active Sourcings individuelle Fluktuationsprognosen erstellen.¹³⁰⁰

Auszugehen ist von einer Fluktuationsprognose anhand einer Internetrecherche, die ein Mensch mit einer gewöhnlichen Suchmaschine durchführt (sog. Googeln).¹³⁰¹ Die Arbeitgeberin muss dem Arbeitnehmer gegenüber klar zu verstehen geben, dass sie eine solche Nachforschung durchführt.¹³⁰² Zu fordern ist eine organisatorische Trennung zwischen der Person, welche das Googeln und die Fluktuationsprognose durchführt, und dem Personal-Entscheidungsträger, sodass Erstere Letzterem bloss die gefilterten Daten mit Arbeitsplatzbezug zur Kenntnis bringt.¹³⁰³

¹²⁹⁷ KUKO OR-PIETRUSZAK, Art. 328b OR, N 9; SHK DSG-PÄRLI, Art. 328b OR, N 28; KASPER/WILDHABER, 217 FN 178. Trotzdem sei das Screening von Stellensuchenden weit verbreitet: PÄRLI 2018, N 17.46.

¹²⁹⁸ BB1 2017, 7072; KASPER/WILDHABER, 217.

¹²⁹⁹ BSK DSG-RAMPINI, Art. 12 DSG, N 16. Vgl. zum amerikanischen Recht: WALDMAN, 42.

¹³⁰⁰ Siehe S. 44 und 57.

¹³⁰¹ Zum Googeln von Arbeitnehmern: KASPER/WILDHABER, 217–218, m.w.H.

¹³⁰² FLUECKIGER 2014, 82.

¹³⁰³ KUKO OR-PIETRUSZAK, Art. 328b OR, N 9.

Quasi ein Unterfall des Googelns ist die Suche nach Informationen in den immer beliebteren sozialen Netzwerken. Mehr als ein Drittel (36 Prozent) der Unternehmen weltweit überwachte 2012 die Benutzung von sozialen Netzwerken durch ihre Arbeitnehmer.¹³⁰⁴ Es ist zwischen den verschiedenen Arten sozialer Netzwerke zu unterscheiden.

Die Analyse berufsbezogener sozialer Netzwerke (z.B. LinkedIn oder Xing) erscheint generell zulässig, da die Mitglieder ihr Profil bewusst zu beruflichen Zwecken allgemein zugänglich machen und mit der Einsichtnahme durch einen Personalverantwortlichen rechnen oder rechnen müssen.¹³⁰⁵ Gleiches muss in Bezug auf Daten von Arbeitnehmern in unternehmensinternen Foren gelten (z.B. Yammer von Microsoft, SuccessFactors von SAP, Chatter von Salesforce oder Workplace von Facebook).¹³⁰⁶

Die Zulässigkeit der Analyse freizeitorientierter sozialer Netzwerke (z.B. Facebook) ist umstritten.¹³⁰⁷ Restriktiv ist die Haltung, die solche Datenerhebungen wegen des privaten Zwecks des Netzwerks generell verbieten will.¹³⁰⁸ Dies gelte unabhängig von den konkreten Datenschutzeinstellungen, da diese oft schwierig zu handhaben seien und von den Anbietern laufend geändert würden. Selbst bei jüngeren Arbeitnehmern, die mit Social Media aufgewachsen und technisch versiert sind, könne die Arbeitgeberin nicht von einer Zustimmung zur Analyse ausgehen.¹³⁰⁹ Ausser Acht bleibt dabei, dass es jedem frei steht, ein soziales Netzwerk zu verlassen. Mit der Nutzung geht die Selbstverantwortung zur Kontrolle der Einstellungen und eine wachsende Netzkompetenz des Betroffenen einher.¹³¹⁰ Nach hier vertretener Meinung kann es nicht allein auf den Zweck des sozialen Netzwerks ankommen, weil gewisse soziale Netzwerke genauso gut zu privaten wie

¹³⁰⁴ AUBERT/DELLEY, 142; KASPER/WILDHABER, 218.

¹³⁰⁵ KUKO OR-PIETRUSZAK, Art. 328b OR, N 8; AUBERT/DELLEY, 147; DZIDA, 544.

¹³⁰⁶ Zur Analyse berufsbezogener sozialer Netzwerke: KASPER/WILDHABER, 218–219.

¹³⁰⁷ Zur Analyse freizeitorientierter sozialer Netzwerke: KASPER/WILDHABER, 219–220.

¹³⁰⁸ So STUTZ/VALLONI, N 5.10. Vgl. AUBERT/DELLEY, 158, und STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 10.

¹³⁰⁹ STUTZ/VALLONI, N 5.11.

¹³¹⁰ Vgl. EDÖB, Erläuterungen zu sozialen Netzwerken, abrufbar unter <www.edoeb.admin.ch> (besucht am 31.05.2020); Beobachtung und Steuerung der Daten im Internet zumutbar: THÜSING/TRAUT, N 16; DZIDA, 545.

beruflichen Zwecken genutzt werden können (z.B. Instagram oder Twitter).¹³¹¹ Entscheidend für die Kategorisierung als allgemein zugänglich muss der öffentliche (oder eben private) Charakter der einzelnen Inhalte sein.¹³¹² Orientierungspunkt sind die Umstände des Einzelfalls,¹³¹³ insbesondere die Kontoeinstellungen.¹³¹⁴ In Anwendung der beschriebenen Erkenntnisse zur Informationsverbreitung in sozialen Netzwerken muss sich der Arbeitnehmer verhalten lassen, mit wem er die Daten teilt.¹³¹⁵ Zulässig erscheint selbst bei freizeitorientierten sozialen Netzwerken die Analyse von Daten, auf die ein praktisch unbegrenzter Kreis von Personen zugreifen kann.¹³¹⁶ Letzteres ist der Fall, wenn die Mitglieder bewusst die Öffentlichkeit suchen und auf die Weiterverbreitung ihrer Mitteilungen keinen Einfluss haben (z.B. bei Twitter).¹³¹⁷ Unklar ist, ob die Arbeitgeberin, die nicht direkt mit dem Arbeitnehmer über das soziale Netzwerk befreundet ist, Beiträge einsehen darf, die dieser für «Freunde von Freunden» geöffnet hat.¹³¹⁸ Nach der hier vertretenen Ansicht dürfte dies zulässig sein, weil diese Einstellung gerade für solche Situationen geschaffen wurde, in denen lediglich eine indirekte Online-Bekanntschaft zwischen der schreibenden und der lesenden Person besteht. Mit der Wahl dieser Einstellung nimmt der Arbeitnehmer in Kauf, dass die Arbeitgeberin die Information liest.

Die Arbeitgeberin kann die Suche durch einen Algorithmus ausführen lassen.¹³¹⁹ Im Gegensatz zu einem Menschen kann ein Algorithmus zur Internetrecherche einerseits im Deep Web Daten aufspüren, die nicht im Sinne von Art. 12 Abs. 3 DSG (bzw. Art. 26 Abs. 3 E-DSG bzw. Art. 30 Abs. 3 rev-DSG) allgemein zu-

¹³¹¹ Vgl. die Unterscheidung zwischen rein privat und rein geschäftlich genutzten Social Media-Profilen sowie sog. Mischaccounts. Letztere dienen sowohl der privaten als auch der geschäftlichen Kontaktpflege: WILDHABER/HÄNSENBERGER 2017, 533–534.

¹³¹² Vgl. AUBERT/DELLEY, 157: Facebook stelle sowohl einen öffentlichen als auch einen privaten Raum dar. – Der Begriff der Öffentlichkeit wird im Schweizer Recht nicht einheitlich verwendet (vgl. Art. 259 ff. StGB, Art. 652a OR, Art. 54 ZPO, Art. 19 Abs. 1 lit. a URG): WILDHABER/HÄNSENBERGER 2015, 408.

¹³¹³ WILDHABER/HÄNSENBERGER 2015, 407.

¹³¹⁴ AUBERT/DELLEY, 158; KUKO OR-PIETRUSZAK, Art. 328b OR, N 8.

¹³¹⁵ Siehe zur Informationsverbreitung in sozialen Netzwerken S. 214.

¹³¹⁶ DZIDA, 545.

¹³¹⁷ Vgl. mit Bezug auf Twitter: Urteil BGer 5A_195/2016 vom 04.07.2016 E. 5.3.

¹³¹⁸ Verneinend, jedoch ohne zwingende Argumente: DZIDA, 545.

¹³¹⁹ Zur Internetrecherche mit Algorithmen: KASPER/WILDHABER, 220.

gänglich gemacht sind.¹³²⁰ Andererseits kann er allgemein zugängliche Daten zusammenführen, Folgerungen ableiten und Informationen zu Tage fördern, die der Arbeitnehmer so nie offenlegen wollte.¹³²¹ Der Arbeitnehmer kann seine Daten gegenüber einer derart ungleich mächtigeren Arbeitgeberin nicht kontrollieren.¹³²² Entsprechende kommerzielle Dienste zur Kontrolle stehen in der Regel nicht zur Verfügung.¹³²³ Es wird daher vorliegend vertreten, dass Big Data-Internetrecherchen, im Gegensatz zum Googeln,¹³²⁴ höchstens im Einzelfall zulässig sein sollten.¹³²⁵ Zu denken ist an einen Algorithmus, der der Arbeitgeberin zwar die Sucharbeit abnimmt, ihr aber im Endeffekt nicht mehr vermittelt, als ein Mensch mit Googeln und genügend Zeit hätte herausfinden können und dürfen.

5.10.4 Einwilligung im Arbeitskontext

a) Rückblick auf die arbeitsrechtlichen Bedingungen der Einwilligung

Die Frage der Einwilligung ist bereits unter dem Aspekt der arbeitsvertragsrechtlichen Zweckbeschränkung aktuell geworden. Es ist dafür argumentiert worden, dass eine Einwilligung in eine Datenbearbeitung ohne sachlichen Bezug zum Arbeitsplatz (d.h. entgegen Art. 328b Satz 1 OR) nur zulässig ist, wenn die Datenbearbeitung zugunsten des Arbeitnehmers erfolgt.¹³²⁶ Kumulativ zu den arbeitsrechtlichen Schranken der Einwilligung sind jedoch auch die datenschutzrechtlichen Anforderungen zu erfüllen (vgl. Art. 328b Satz 2 OR). Diese werden im Folgenden erläutert.

¹³²⁰ Siehe zum Begriff des Deep Web S. 186 und FN 1101.

¹³²¹ Mit den Verfahren OSINT (*open source intelligence*) und SOCMINT (*social media intelligence*) lassen sich aus verschiedenen allgemein zugänglichen Datensätzen Informationen generieren, die in ihrem Aussagegehalt weit über den Informationsgehalt einzelner Daten hinausgehen: VON MALTZAN, 208.

¹³²² Die Erkenntnisse, die eine Arbeitgeberin mittels Suchmaschine über einen Bewerber erlangt, sind für ihn «nicht kontrollierbar»: BROY, 342. «*Predictive analytics is not necessarily fair game*»: SPRAGUE 2015, 42.

¹³²³ THÜSING/TRAUT, N 29.

¹³²⁴ KUKO OR-PIETRUSZAK, Art. 328b OR, N 9.

¹³²⁵ Ebenso THÜSING/TRAUT, N 29; a.M. BROY, 343: automatisierte Bewerberrecherche im Internet generell unzulässig.

¹³²⁶ Siehe S. 193–197.

b) Datenschutzrechtliche Voraussetzungen der Einwilligung

aa) Übersicht

Das DSG nennt als ersten von drei möglichen Rechtfertigungsgründen einer Persönlichkeitsverletzung die Einwilligung des Verletzten (Art. 13 Abs. 1 DSG, Art. 27 Abs. 1 E-DSG, Art. 31 Abs. 1 rev-DSG). Das Recht, in eine persönlichkeitsverletzende Datenbearbeitung einzuwilligen, ist Teil des informationellen Selbstbestimmungsrechts und Eckpfeiler der privatrechtlichen Datenschutzerlasse rund um den Globus.¹³²⁷

Eine Einwilligung ist unter den Voraussetzungen gültig, dass sie freiwillig, informiert und – bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen – ausdrücklich erfolgt (vgl. Art. 4 Abs. 5 DSG, vgl. Art. 5 Abs. 6 E-DSG, vgl. Art. 6 Abs. 6–7 rev-DSG; zu diesen Voraussetzungen sogleich). Umstritten ist, ob eine Einwilligung sich auf eine spezifische Bearbeitung beziehen muss.¹³²⁸ Nach dem vorliegend vertretenen Standpunkt muss die Spezifikation unter schweizerischem Datenschutzrecht nicht als selbständige Voraussetzung abgehandelt werden; stattdessen wird sie im Rahmen der (spezifischen) angemessenen Information thematisiert.¹³²⁹ Eine Einwilligung darf ferner nicht gegen zwingende Schutznormen und höherrangiges Recht verstossen; zu denken ist an das Verbot der übermässigen Selbstbindung (Art. 27 Abs. 2 ZGB).¹³³⁰

¹³²⁷ CAVOUKIAN/DIX/EL EMAM, 6.

¹³²⁸ Eine Einwilligung in eine unbestimmte Datenbearbeitung, deren Zweck nicht bekannt ist, ist nicht rechtsgültig: SHK DSG-BAERISWYL, Art. 4 DSG, N 31. A.M. THOUVENIN 2014, 81–82: Eine informierte und bewusste global erteilte Einwilligung in jede künftige Bearbeitung der infrage stehenden Daten sei zulässig. – Dagegen verlangt das europäische Recht Bestimmtheit («für den bestimmten Fall», Art. 4 Nr. 11 DSGVO). Eine Pauschaleinwilligung für diverse Arbeitnehmerdatenbearbeitungen ist dort deshalb unzulässig: GRAF/KRIŽANAC, 94. Zu unterscheiden sind die Einwilligung in eine Datenbearbeitung (Art. 6 Abs. 1 lit. a, Art. 7 DSGVO) und diejenige im Rahmen eines automatisierten Entscheidverfahrens (Art. 22 Abs. 2 lit. c DSGVO); hierzu näher bei DREYER/SCHULZ, 27.

¹³²⁹ Siehe S. 225.

¹³³⁰ RIESELMANN-SAXER, 37; WOLFER, N 629; BYERS, N 359. Ein Bewerber kann nicht eine pauschale Einwilligung zur Bearbeitung aller Fundstellen im Internet erteilen: BROY, 325–326.

bb) Freiwilligkeit

Die Freiwilligkeit einer Einwilligung muss im Arbeitsbereich grundsätzlich äußerst kritisch betrachtet werden, da der Arbeitnehmer von der Stelle abhängig ist und sich wegen des strukturellen Machtungleichgewichts unter Druck fühlen kann.¹³³¹ Eine freiwillige Einwilligung im Arbeitsverhältnis ist jedoch nicht schlechthin ausgeschlossen. Das deutsche Recht¹³³² und die DSGVO (E. 155: «auf der Grundlage einer Einwilligung»)¹³³³ lassen eine Einwilligung zu, solange die konkreten Umstände im Einzelfall eine «echte und freie Wahl» (E. 42 DSGVO) zulassen.¹³³⁴

Es ist eine Einzelfallbetrachtung erforderlich, um zu beurteilen, ob eine eingeholte Einwilligung freiwillig erfolgt ist.¹³³⁵ Dabei sind die folgenden Kriterien massgeblich: Negativ definiert darf kein Willensmangel vorliegen.¹³³⁶ D.h., die Einwilligung darf nicht infolge einer Überrumpelung oder Übervorteilung (Art. 21 OR), eines Irrtums (Art. 23 ff. OR), einer Täuschung (Art. 28 OR) oder einer Furchterregung bzw. Drohung (Art. 29 OR) erfolgen.¹³³⁷ Ebenso wenig darf es zur Inaus-

¹³³¹ KASPER/WILDHABER, 196; EDÖB 2013, 5; MÉTILLE, 106; «sehr hohe» Anforderungen an die Einwilligung im Arbeitsverhältnis: WILDHABER 2017, 216. Arbeitnehmer gefährden mit der Verweigerung der Einwilligung ihre eigenen Interessen: RIESELMANN-SAXER, 35. CUSTERS/URSIC, 334. Arbeitnehmer gehen im Vertrauen auf den Fortbestand der Einkommensquelle finanzielle Verpflichtungen ein: OTTO 2016, 182; EU/Europarat, 332; AKHTAR/MOORE, 116; BALL/MARGULIS, 115. «*It is questionable whether regard for one's privacy is capable of commoditization in the way the theory of independent bargaining might suggest*»: DEBEER, 407.

¹³³² Eine freiwillige Einwilligung ist möglich, selbst wenn eine Datenbearbeitung für den Arbeitnehmer nachteilig ist: DZIDA/GRAU, 189; WYBITUL/SCHULTZE-MELLING, N 170; SCHULZE, 142.

¹³³³ Kritisch jedoch die Art.-29-Datenschutzgruppe, derzufolge die Einwilligung in der Regel «höchst unwahrscheinlich» als Rechtsgrundlage der Datenbearbeitung am Arbeitsplatz genüge: Art.-29-Datenschutzgruppe 2017b, 3, und Art.-29-Datenschutzgruppe 2017d, 7.

¹³³⁴ Entscheidend sei, dass der Betroffene die Möglichkeit erhalte, sein Recht auf informationelle Selbstbestimmung wirksam auszuüben: WYBITUL/SCHULTZE-MELLING, N 171. KASPER/WILDHABER, 198.

¹³³⁵ Vgl. zur DSGVO GRAF/KRIŽANAC, 94.

¹³³⁶ RIESELMANN-SAXER, 36.

¹³³⁷ Ein Willensmangel dürfte z.B. vorliegen, wenn die Arbeitgeberin die Zugangsdaten zum privaten Chatroom-Konto oder sozialen Netzwerk des Arbeitnehmers verlangen würde, wie dies in den USA verbreitet geschieht (*shoulder viewing*, auch *shoulder surfing*, weil die Arbeitgeberin dem Arbeitnehmer «über die Schulter» schaut): MRKO-

sichtstellung übermässiger Vorteile kommen, wie dies etwa der Fall wäre, wenn die Arbeitgeberin im Rahmen eines Gewinnspiels ein Extra-Monatsgehalt verlosen würde.¹³³⁸ Tendenziell unfreiwillig dürfte die Zustimmung erfolgen, wenn die Datenbearbeitung ausschliesslich die Handlungs- und Kontrollmöglichkeiten der Arbeitgeberin erweitert.¹³³⁹

Die negative Formel «ohne Willensmangel», bisweilen auch «ohne Zwang», hat eine enge Bedeutung: Es kann nicht die Rede von Willensmangel oder Zwangsausübung sein, wenn ein Arbeitnehmer bloss befürchtet, bei einem Nein möglicherweise Nachteile zu erleiden, oder wenn ein Bewerber auch nach der Verweigerung der Zustimmung noch die Wahl zwischen anderen vergleichbaren Angeboten hat; und doch handelt er nicht wirklich freiwillig.¹³⁴⁰ Freiwilligkeit bedeutet mehr als das Fehlen von Willensmängeln.¹³⁴¹ Das DSG stellt nicht auf die Abwesenheit von Willensmängeln oder Zwang ab, sondern wählt eine positive Formulierung («freiwillig», «*exprime sa volonté librement*», «*espresso liberamente*», Art. 4 Abs. 5 Satz 1 DSG, Art. 5 Abs. 6 Satz 1 E-DSG, Art. 6 Abs. 6 rev-DSG).¹³⁴² Freiwilligkeit kann vorliegen, wenn für den Arbeitnehmer ein gewisser «Verhandlungsspielraum»¹³⁴³ oder eine mögliche Alternative¹³⁴⁴ besteht. Ein deutlicher Hinweis der Arbeitgeberin, dass der Arbeitnehmer berechtigt ist, die Zustimmung ohne übermässige nachteilige Folgen zu verweigern, stellt ein Indiz für die Frei-

NICH *et al.*, 14, BIAS/BOGUE, 253, m.w.H., AUBERT/DELLEY, 148, und STUTZ/VALLONI, N 5.13.

¹³³⁸ DÄUBLER, N 159a–160. Verbreitet ist der Austausch von Daten gegen andere Vorteile (z.B. Krankenkassen-Prämienreduktion oder kostenlose Wearables) in den amerikanischen Gesundheitsprogrammen am Arbeitsplatz: ROWLAND CHRISTOPHER, With fitness trackers in the workplace, bosses can monitor your every step – and possibly more, The Washington Post vom 16.02.2019, abrufbar unter <www.washingtonpost.com> (besucht am 31.05.2020), und The Economist vom 05.01.2019, The spy who hired me, abrufbar unter <www.economist.com> (besucht am 31.05.2020). Vgl. auch HERMSTRÜWER, 108.

¹³³⁹ DÄUBLER, N 429c.

¹³⁴⁰ DÄUBLER, N 150. Vgl. SCHMIDT, 88.

¹³⁴¹ Vgl. DÄUBLER, N 153.

¹³⁴² So auch die DSGVO: DÄUBLER, N 150.

¹³⁴³ SCHULZE, 143.

¹³⁴⁴ «Exzessiv» wäre ein Koppelungsverbot in einem funktionierenden Markt, in dem Alternativangebote bestehen, die nicht die Bearbeitung sachfremder Daten voraussetzen: TREITL, 124. Vgl. HOFFMANN-RIEM, 42. Fehlende Freiwilligkeit in einer «Take it or leave it»-Situation: BUCHNER/KÜHLING, 546.

willigkeit dar.¹³⁴⁵ Beispielsweise ist die Freiwilligkeit gewahrt, wenn auf dem Betriebsareal für einen Werbeclip gefilmt wird und die Arbeitgeberin denjenigen Arbeitnehmern, die nicht im Hintergrund der Aufnahmen erscheinen möchten, für die Dauer der Videoarbeiten einen gleichwertigen anderen Arbeitsplatz anbietet.¹³⁴⁶ Auf Freiwilligkeit deutet es hin, wenn ein rechtlicher oder wirtschaftlicher Vorteil für den Arbeitnehmer resultiert oder Arbeitnehmer und Arbeitgeberin gleichgelagerte Interessen verfolgen.¹³⁴⁷

Die Phase des Arbeitnehmer-Lebenszyklus, in welcher sich der Einwilligende gerade befindet, ist für die Beurteilung der Freiwilligkeit wegweisend: In der Rekrutierungsphase steht der Bewerber unter besonderem Druck, weshalb Einwilligungen in der Regel nicht als Rechtfertigungsgrund taugen können.¹³⁴⁸ Nur ausnahmsweise ist eine Einwilligung sinnvoll, etwa wenn Bewerbungsunterlagen für eine bestimmte, im Voraus festgelegte Dauer aufbewahrt werden und anzunehmen ist, dass die Daten demnächst wieder gebraucht werden.¹³⁴⁹ Eine solche Aufbewahrung kann im Interesse des Bewerbers liegen, wenn dieser die Anforderungen der Stellenbeschreibung zwar nicht erfüllt, aber zu einem späteren Zeitpunkt für eine andere Stelle infrage kommen könnte.¹³⁵⁰ Es braucht hierfür eine Einwilligung, weil die übrigen Rechtfertigungsgründe ausscheiden: Weder existiert eine gesetzliche Aufbewahrungspflicht, noch sind überwiegende Interessen erkennbar (vgl. Art. 13 Abs. 1 DSGVO, Art. 27 Abs. 1 E-DSG, Art. 31 Abs. 1 rev-DSG), noch sind die Daten zur Eignungsabklärung für eine konkrete Stelle oder Vertragsdurchführung erforderlich (vgl. Art. 328b OR).¹³⁵¹

¹³⁴⁵ Vgl. DETERMANN/SPRAGUE, 1028.

¹³⁴⁶ Art.-29-Datenschutzgruppe 2017d, 7.

¹³⁴⁷ DÄUBLER, N 151a.

¹³⁴⁸ Stattdessen sollte die Arbeitgeberin den Rechtfertigungsgrund des überwiegenden Interesses wählen, weil sie vor Eingehung des Dauerschuldverhältnisses ein ausgeprägtes Informationsinteresse hat: CULIK, 300.

¹³⁴⁹ EDÖB 2014b, 11.

¹³⁵⁰ Vgl. Europarat 2016b, 49.

¹³⁵¹ Art. 328b OR ist auf die Aufbewahrung von Dossiers abgewiesener Bewerber analog anwendbar: STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 13, und KASPER/WILDHABER, 225. Vgl. zur Rechtslage unter der EMRK: «*Prospective employees should benefit from the same protection and rights as employees, even if their candidature does not lead to a contract of employment. Similarly, [...] the principles [...] apply to former employees*»: Europarat 2016b, 28.

Im laufenden Arbeitsverhältnis würde ein genereller Ausschluss der Einwilligung zu weit führen.¹³⁵² Die Stellung des Arbeitnehmers ist zu berücksichtigen: Schlüsselmitarbeiter haben insoweit eine stärkere und freiere Verhandlungsposition, als die Arbeitgeberin sie mehr als andere behalten will.¹³⁵³

Bei der Beendigung des Arbeitsverhältnisses ist wiederum zu differenzieren: Solange das Arbeitszeugnis noch nicht ausgestellt ist, verfügt die Arbeitgeberin über ein starkes Druckmittel.¹³⁵⁴ Danach wird die für laufende Arbeitsverträge und Bewerbungsverfahren typische Machtasymmetrie entfallen, weshalb eine freiwillige Zustimmung vorstellbar ist.¹³⁵⁵ Die Einwilligung muss sich auf einen bestimmten Bearbeitungszweck beziehen, etwa auf die Pflege des Alumni-Netzwerks des Unternehmens.

Ein Indiz für eine unfreiwillige Einwilligung ist schliesslich gegeben, wenn die Vertragserfüllung von der Einwilligung in eine Datenbearbeitung, die für die Erfüllung des Vertrags nicht erforderlich ist, abhängig gemacht wird. Nach dem europäischen Datenschutzrecht muss «in grösstmöglichem Umfang» berücksichtigt werden, ob die Einwilligung wegen einer vertragsfremden Koppelung erteilt worden ist (vgl. Art. 7 Abs. 4 DSGVO). Das schweizerische DSG enthält dagegen kein explizites Koppelungsverbot. Für den EDÖB ist es eine Frage des Arbeitsrechts, wenn eine Arbeitgeberin eine Anstellung an die Bedingung knüpft, dass der Arbeitnehmer der Erfassung des Fingerabdrucks zustimmt. Datenschutzrechtlich sei es (lediglich) «wünschenswert», auch Alternativen zur biometrischen Zeiterfassung zur Verfügung zu haben.¹³⁵⁶ Wie dargelegt verlangt das schweizerische Arbeitsrecht einen sachlichen Zusammenhang zwischen der Datenbearbeitung und der Arbeit (vgl. Art. 328b OR), welcher nicht nur «wünschenswert», sondern einseitig zwingend ist.¹³⁵⁷

¹³⁵² CULIK, 301.

¹³⁵³ KASPER/WILDHABER, 198.

¹³⁵⁴ CULIK, 301.

¹³⁵⁵ CULIK, 301.

¹³⁵⁶ EDÖB 2018a, 28.

¹³⁵⁷ Siehe S. 193–197.

cc) Informiertheit

Voraussetzung einer gültigen Einwilligung ist eine «angemessene Information» (Art. 4 Abs. 5 Satz 1 DSGVO, Art. 5 Abs. 6 Satz 1 E-DSG, Art. 6 Abs. 6 rev-DSG).¹³⁵⁸ Diese muss insbesondere enthalten, welche Daten erhoben werden, zu welchem Bearbeitungszweck, wer die verantwortliche Stelle ist und wer Zugriff auf die Daten hat. Zudem muss die Information aktuell, spezifisch und verständlich sein.¹³⁵⁹ Die Einwilligung darf nicht auf einseitiger Beratung basieren. Entscheidend ist, dass der Betroffene die Konsequenzen der Datenbearbeitung abschätzen kann. Es kommt auf dessen Urteilsfähigkeit (vgl. Art. 16 ZGB), nicht aber auf dessen Handlungsfähigkeit (vgl. Art. 13 ZGB) an.¹³⁶⁰

Die Informiertheit ist bereits dadurch infrage gestellt, dass die Information nicht beim Betroffenen ankommt. Datenschutzerklärungen werden nicht gelesen¹³⁶¹ oder nicht verstanden.¹³⁶² Wenn ein gewöhnlicher Internetbenutzer alle Datenschutz-Erklärungen, denen er während eines Jahres begegnet, mit eiserner Disziplin lesen würde, bräuchte er dafür mindestens 30 Arbeitstage – ein volkswirtschaftlicher Unsinn.¹³⁶³ Hinzu kommt, dass ein Unternehmen seine Datenschutzerklärung ändern kann, sodass die Betroffenen sie mehrfach lesen müssten.¹³⁶⁴ Niemand kann all diese Datenschutz-Erklärungen bewältigen.¹³⁶⁵ Auch im

¹³⁵⁸ In Europa ist von «informierter Einwilligung» bzw. «*informed consent*» und in Nordamerika von «*notice-and-consent*» die Rede: NISSENBAUM 2011, 34.

¹³⁵⁹ Datenschutzerklärungen erfüllen diese Kriterien in der Regel: CUSTERS/VAN DER HOF/SCHERMER, 277.

¹³⁶⁰ Vgl. SCHULZE, 140: Entscheidend ist die Einsichtsfähigkeit, nicht die Geschäftsfähigkeit.

¹³⁶¹ 72 Prozent der Betroffenen lesen Datenschutzerklärungen nie, selten oder bloss manchmal: CUSTERS/VAN DER HOF/SCHERMER, 282. Durchschnittlich besteht eine Bereitschaft, 1–5 Minuten pro Jahr für das Lesen von Datenschutz-Erklärungen aufzuwenden: CUSTERS/DECHESNE *et al.*, 240, m.w.H. NISSENBAUM 2011, 35.

¹³⁶² Auch nach der Revision des DSGVO werden wir «nicht wirklich besser verstehen und kontrollieren können, was mit unseren Daten geschieht»: ROSENTHAL DAVID, Eine Mogelpackung, NZZ vom 03.05.2017, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020). NISSENBAUM 2011, 32; HÄNOLD, 131. Vgl. ANANNY/CRAWFORD, 975.

¹³⁶³ 250 Stunden oder 30 Arbeitstage pro Jahr: World Economic Forum 2013, 11; 244 Stunden pro Jahr: McDONALD/CRANOR, 563; a.M. RICHARDS/HARTZOG 2016, 444: sogar 76 Arbeitstage pro Jahr.

¹³⁶⁴ NISSENBAUM 2011, 35.

¹³⁶⁵ HARTZOG 2017, 974. Die Vervielfachung der Datenbearbeitungs-Vorgänge in allen Lebensbereichen übersteige die mögliche Aufmerksamkeit: ROSSNAGEL, 273.

Arbeitsverhältnis werden die Datenschutzerklärungen im Zuge von People Analytics zunehmen (müssen), sodass die hier gemachten Ausführungen über Internetbenutzer zumindest sinngemäss auch für Arbeitnehmer gelten. Die Flut an Datenschutz-Erklärungen ist rechtlich zu kritisieren, führt sie doch zu einer «Informationsvergiftung»;¹³⁶⁶ Der vermeintliche Schutz durch Transparenz ist nicht nur ineffektiv,¹³⁶⁷ sondern entmachtet letztlich die Individuen, indem er sie mit endlosen Schriftstücken überfordert und von einer rationalen Entscheidung über die Aushändigung ihrer Daten abhält.¹³⁶⁸ Eine Anfrage um Zustimmung sollte den Betroffenen eigentlich dazu veranlassen, innezuhalten und aktiv über die Folgen der Einwilligung nachzudenken.¹³⁶⁹ Transparenz und Informationspflicht führen aber zu einer «Abstumpfung» (*«consent desensitisation»*), sodass Einwilligungen meistens blind erteilt werden.¹³⁷⁰

Neben der Masse an Information kämpfen die Betroffenen auch mit der Qualität der Texte. Diese sind schwer verständlich, weil sie rechtliches Vokabular einerseits und Fachbegriffe der Informatik und Analytik andererseits miteinander vereinen.¹³⁷¹ Gewisse Webseiten bemühen sich zwar um eine Vereinfachung, etwa im Zusammenhang mit Cookies: Hier kann der Besucher mancherorts unkompliziert wählen, ob nur die Cookies aufgezeichnet werden sollen, die für den Betrieb der Seite notwendig sind, oder ob Informationen zu weiteren Zwecken (z.B. Marketing oder Personalisierung der Dienste) gespeichert werden dürfen.¹³⁷² Doch

¹³⁶⁶ *«Information poisoning»* beim Abschluss von Verträgen online: FAIRFIELD, 602. Auch als «Daten-Schmutz» oder «Informationsverschmutzung» bezeichnet: DRUEY 1990, 379, 383.

¹³⁶⁷ *«Disempowering and ineffective»*: World Economic Forum 2013, 11. WALDMAN, 84. *«Stricter legal requirements [...] further weaken the effectiveness of the consent mechanism»*: SCHERMER *et al.*, 171.

¹³⁶⁸ *«The weight of too much control will crush us»*: HARTZOG 2017, 976. WALDMAN, 84.

¹³⁶⁹ SCHERMER *et al.*, 172.

¹³⁷⁰ SCHERMER *et al.*, 178. Datenschutzerklärungen schafften ein «falsches Gefühl der Sicherheit» und steigerten letztlich das Risiko für die Privatsphäre der Betroffenen: SCHERMER *et al.*, 171–172. Paradoxerweise führten Datenschutzerklärungen dazu, dass Individuen noch mehr sensible Daten preisgaben: BAMBERGER/MULLIGAN 2015, 23.

¹³⁷¹ NISSENBAUM 2011, 35; WATTL/VOGL, 5.

¹³⁷² Zwei Beispiele für solchermassen einfache Modelle finden sich statt vieler bei der Fluggesellschaft Swiss und der British Telecom: Swiss International Air Lines AG, <www.swiss.com> (besucht am 31.05.2020); British Telecom Public Limited Company, <<https://btplc.com/>> (besucht am 31.05.2020).

selbst solchermassen simpel ausgestaltete Informationen (auch warnende Boxen oder standardisierte Labels und Symbole) tragen weder zur Informiertheit der Nutzer bei noch wirken sie sich auf das Einwilligungsverhalten aus.¹³⁷³ Diese Idee einer selbstbestimmten Einwilligung scheitert somit in der Praxis.¹³⁷⁴

Ein mögliches rechtliches Linderungsmittel für das Problem der blind erteilten Einwilligungen könnte in einer Rechtsprechung bestehen, die die Einwilligenden vor unklaren und ungewöhnlichen Klauseln schützt, so wie dies in Bezug auf AGB praktiziert wird.¹³⁷⁵ Auch AGB werden in der Regel global übernommen, da es ähnlich lange wie bei den Datenschutz-Erklärungen dauern würde, um alle AGB, denen man begegnet, zu lesen.¹³⁷⁶ Begleitend dazu könnte die Einwilligung eine Aufwertung erfahren, wenn sie an den Browser oder an ein technisches Gerät der betroffenen Person delegiert werden könnte. Dieses könnte bei jedem signalisierten Bearbeitungsvorgang im Hintergrund die Datenschutzerklärungen prüfen, akzeptieren oder verwerfen.¹³⁷⁷ Diese Ansätze sind jedoch nicht mehr als Symptombekämpfung, da sie die Informationsschwemme nicht an der Quelle zu stoppen vermögen.

Ein weiterer wunder Punkt bzgl. der Informiertheit über Datenbearbeitungen liegt darin, dass sich die Wirkung von Informationen über die Zeit kaum kontrollieren lässt.¹³⁷⁸ Bei People Analytics akzentuiert sich dieses Problem, weil die Daten, einmal elektronisch aufgezeichnet, in der Regel verewigt sind.¹³⁷⁹ Beispielsweise lässt sich im Zeitpunkt der Einwilligung nicht vorhersagen, in welchem Kontext

¹³⁷³ HERMSTRÜWER, 113. «*Increased simplification of privacy policies is not going to magically make consumers start reading them*»: THIERER, 447. Mozilla hat vorgeschlagen, die Beschreibung der Datenbearbeitung durch Symbole zu vereinfachen, was sich jedoch nicht durchgesetzt hat: Mozilla, Privacy icons, 28.06.2011, abrufbar unter <<https://wiki.mozilla.org>> (besucht am 31.05.2020); World Economic Forum 2013, 17.

¹³⁷⁴ SCHERMER *et al.*, 171.

¹³⁷⁵ Rechtsprechung zu AGB: BGE 135 III 1 E. 2.1; Rechtsprechung zu allgemeinen Versicherungsbedingungen: BGE 138 III 411 E. 3.1. Die gleichen Grundsätze gelten für die Gültigkeit von Einwilligungen im Datenschutz: ROSENTHAL DAVID, Cookies: comment la CJUE lutte-t-elle contre la mentalité du «cliquer et fermer sans regarder», abrufbar unter <www.lawinside.ch> (besucht am 31.05.2020).

¹³⁷⁶ 244 Stunden im Jahr für das Lesen von AGB: BAUMANN MAX-OTTO, 5.

¹³⁷⁷ ROSSNAGEL, 280.

¹³⁷⁸ Vgl. HERMSTRÜWER, 105.

¹³⁷⁹ Siehe zur zeitlichen Ubiquität S. 72.

die Daten künftig bearbeitet werden. Werden zwei scheinbar harmlose, aggregierte Datensätze übereinandergelegt, können sie «Babydaten» erzeugen, deren Aussagekraft für den Betroffenen unvorhersehbar ist.¹³⁸⁰ Der Einzelne kämpft mit einer «invisible visibility»: Für ihn ist nicht erkennbar, wie durchsichtig er infolge der Ableitungen aus Datensätzen ist.¹³⁸¹ Wie überrascht war doch die Kundin im dargestellten Beispiel,¹³⁸² als Target von ihrer Schwangerschaft wusste, noch ehe sie es ihrem Vater verkünden konnte. Der Mangel an Kontrollierbarkeit über die Zeit zeigt sich auch etwa, wenn ein einziger Arbeitnehmer den Betrieb verlässt und daher aus einer monatlich durch die Arbeitgeberin erstellten anonymen Statistik herausfällt: Ist einerseits erkennbar, dass die Statistik im Vergleich zum Vormonat genau einen Datensatz weniger aufweist, und ist andererseits bekannt, wer das Unternehmen verlassen hat, so ist es ein Leichtes, aus der vormals anonymen Statistik personenbezogene Aussagen über den ehemaligen Arbeitskollegen abzuleiten.¹³⁸³ Ferner stellen mutierende Algorithmen, wie sie bei maschinellem Lernen vorkommen, eine Herausforderung für die informierte Einwilligung dar. Selbst wenn der Arbeitnehmer die Parameter der algorithmischen Verwandlung kennen würde, kann sich der Algorithmus derart grundlegend ändern, dass er das mit der Einwilligung abgesteckte Feld verlässt.¹³⁸⁴ Ein Algorithmus verfügt nicht über die Selbstreflexions-Kompetenz eines Menschen, um einzuschätzen, wann er eine neue Einwilligung einholen muss.¹³⁸⁵

Mit einer nachträglichen Einwilligung liesse sich dem Problem der fehlenden Informiertheit begegnen: Anders als bei einer vorgängigen Einwilligung besteht im Nachhinein eine Übersicht über die Datenbearbeitung. Beispielsweise könnte die Arbeitgeberin den Arbeitnehmer nachträglich über einen neuen Bearbeitungszweck für die bereits beschafften Daten informieren. Nach der schweizerischen Rechtslage kann die nachträgliche Genehmigung die Persönlichkeitsverletzung

¹³⁸⁰ Informierte Einwilligung «kaum zu bewerkstelligen»: WEBER 2018, 103–104; Aussagekraft von aggregierten Informationen unvorhersehbar: HERMSTRÜWER, 104. «*Two innocuous pieces of data [...] can breed and generate baby data*»: Europarat 2016a, 14. Siehe S. 38 und 74.

¹³⁸¹ Hypothetisch könne die «invisible visibility» mit dem Auskunftsrecht bekämpft werden: HÄNOLD, 150.

¹³⁸² Siehe S. 172.

¹³⁸³ Vgl. das Beispiel, in dem genau ein Schüler in einer anonymen Statistik fehlt im Vergleich zum vorhergehenden Semester: WOOD *et al.*, 228.

¹³⁸⁴ WRIGLEY, 192.

¹³⁸⁵ WRIGLEY, 192.

heilen, wobei die Voraussetzungen einer gültigen Einwilligung (Art. 4 Abs. 5 DSGVO, Art. 5 Abs. 6 E-DSG, Art. 6 Abs. 6–7 rev-DSG) erfüllt sein müssen.¹³⁸⁶ Ungeklärt ist, ob die Einwilligung auch unter der DSGVO nachträglich erfolgen darf.¹³⁸⁷

dd) **Ausdrücklichkeit**

Die Einwilligung kann grundsätzlich formlos erfolgen, insbesondere auch stillschweigend.¹³⁸⁸ Selbst eine hypothetische Einwilligung ist nicht durchs Band weg ausgeschlossen.¹³⁸⁹ Jedoch ist mit zunehmender Schwere der Persönlichkeitsverletzung eine stillschweigende Einwilligung zurückhaltender anzunehmen.¹³⁹⁰ Aus Beweisgründen ist die Schriftlichkeit zu bevorzugen.¹³⁹¹

Wird eine Einwilligung eingeholt, so muss diese ausdrücklich erfolgen, wenn die Bearbeitung besonders schützenswerte Personendaten (Art. 3 lit. c DSGVO, Art. 4 lit. c E-DSG, Art. 5 lit. c rev-DSG) oder Persönlichkeitsprofile (Art. 3 lit. d DSGVO, vgl. zum Profiling Art. 4 lit. f E-DSG und Art. 5 lit. f–g rev-DSG) betrifft (Art. 4 Abs. 5 Satz 2 DSGVO, Art. 5 Abs. 6 Satz 2 E-DSG, Art. 6 Abs. 7 lit. a rev-DSG). Dies dürfte in der Praxis oft vorkommen.¹³⁹² Für die Ausdrücklichkeit genügt das Ankreuzen eines Kästchens (*Opt-in-Modell*). Nicht genügen kann jedoch ein bereits angekreuztes Kästchen, das die Einwilligung signalisiert, sodass diese durch Klicken aus der Welt geschafft werden muss (*Opt-out-Modell*), ebenso wenig das Stillschweigen und die Untätigkeit der betroffenen Person.¹³⁹³

¹³⁸⁶ PRIEUR, 1651; HK-ROSENTHAL, Art. 4 DSGVO, N 40.

¹³⁸⁷ Verneinend: Eine nachgeholte Einwilligung könne den rechtswidrigen Charakter des Datenbearbeitungsvorgangs nicht mehr mit Rückwirkung ändern: CALDAROLA/SCHREY, N 172.

¹³⁸⁸ RIESSELMANN-SAXER, 37; zum europäischen Recht: EPINEY/KERN, 52; WYBITUL/SCHULTZE-MELLING, N 179.

¹³⁸⁹ RIESSELMANN-SAXER, 38. A.M. DÄUBLER, N 144: Die DSGVO sehe eine mutmassliche Einwilligung nicht vor.

¹³⁹⁰ RIESSELMANN-SAXER, 37.

¹³⁹¹ Zum deutschen Recht: WEDDE 2016c, 9.

¹³⁹² WEBER 2018, 104.

¹³⁹³ Vgl. zum europäischen Recht: E. 32 Sätze 2–3 DSGVO. DÄUBLER, N 144; CALDAROLA/SCHREY, N 197.

c) Jederzeitiges Widerrufsrecht

Eine Einwilligung kann nur als informiert gelten, wenn der Arbeitnehmer Kenntnis von seinem Widerrufsrecht hat. Aus dem Verbot der übermäßigen Selbstbindung (Art. 27 ZGB) folgt, dass der Arbeitnehmer seine Einwilligung jederzeit widerrufen kann.¹³⁹⁴ Dem Arbeitnehmer dürfen aus dem Widerruf keine oder höchstens die Nachteile entstehen, die allein darin begründet sind, dass er die Vorteile des datenintensiveren Systems nicht nutzt.¹³⁹⁵

Der Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG; Art. 2 Abs. 1 ZGB) kann dem Widerrufsrecht Schranken setzen.¹³⁹⁶ Ein Widerruf der Einwilligung wäre beispielsweise rechtsmissbräuchlich, wenn der Betroffene seine Einwilligung allein widerruft, um der verantwortlichen Stelle zusätzlichen Aufwand zu verursachen.¹³⁹⁷ Nach der bundesgerichtlichen Rechtsprechung können ausserdem Persönlichkeitsgüter, die nicht zum Kernbereich der menschlichen Existenz gehören, Gegenstand von vertraglichen und unwiderruflichen Verpflichtungen sein, wenn bei der fraglichen Verpflichtung wirtschaftliche Interessen im Vordergrund stehen.¹³⁹⁸ Beispielsweise ist es möglich, Rechte am eigenen Bild und Namen oder an der eigenen Stimme zum Zweck der Vermarktung rechtlich verbindlich abzutreten, sodass ein Widerruf nicht mehr jederzeit und frei möglich ist.¹³⁹⁹ Diese Rechtsprechung kommt zum Tragen, wenn wirtschaftliche Interessen des Arbeitnehmers an einer Abtretung bestehen. Bei People Analytics stehen aber in der Regel wirtschaftliche Interessen der Arbeitgeberin im Vordergrund, da sie aus der Analyse Vorteile ziehen will. Somit erscheint ein Widerruf der Einwilligung zu keiner Zeit *a priori* als treuwidrig.

Wenn ein Arbeitnehmer seine Einwilligung widerruft, liegt für die Arbeitgeberin nichts näher, als retrospektiv auf einen anderen Rechtfertigungsgrund – etwa das überwiegende private Interesse – auszuweichen, um die Datenbearbeitung fortzusetzen. Ein solches Ansinnen ist kritisch zu würdigen. Unter der DSGVO stehen

¹³⁹⁴ Zum Widerrufsrecht: KASPER/WILDHABER, 199; BSK DSG-RAMPINI, Art. 13 DSG, N 14.

¹³⁹⁵ Mit Bezug auf das deutsche und das europäische Recht: HOFMANN, 14.

¹³⁹⁶ Zu den Schranken des Widerrufsrechts: KASPER/WILDHABER, 199; zur deutschen Rechtsprechung: DZIDA/GRAU, 190; DZIDA, 543.

¹³⁹⁷ WYBITUL/SCHULTZE-MELLING, N 163.

¹³⁹⁸ BGE 136 III 401 E. 5.2.2.; BSK DSG-RAMPINI, Art. 13 DSG, N 14.

¹³⁹⁹ BGE 136 III 401 E. 5.2.2.

die möglichen Rechtfertigungsgründe alternativ zueinander, d.h., die Arbeitgeberin muss sich von Anfang an für einen (den richtigen) von ihnen entscheiden.¹⁴⁰⁰ Beschreitet sie den Weg der Einwilligung, muss sie einen allfälligen Widerruf respektieren und die Datenbearbeitung stoppen.¹⁴⁰¹ Die Bitte um Zustimmung schürt beim Arbeitnehmer eine Erwartung zur betreffenden Datenbearbeitung; möglicherweise schafft die Arbeitgeberin gar einen vertraglichen Anspruch auf Einholung der Einwilligung bei künftigen Änderungen der Datenbearbeitung.¹⁴⁰² Ein Ignorieren des Widerrufs würde gegen Treu und Glauben verstossen.¹⁴⁰³ Dies muss nach der hier vertretenen Ansicht für People Analytics-Projekte in der Schweiz erst recht gelten, da der Grundsatz von Treu und Glauben im Datenschutz- (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG) und im Vertragsrecht (Art. 328 OR i.V.m. Art. 2 ZGB) gleich doppelt verankert ist.¹⁴⁰⁴

d) Zwischenfazit zur Einwilligung

Zusammenfassend erweist sich die Vorstellung eines informationell selbstbestimmt einwilligenden Arbeitnehmers als Traumfigur.¹⁴⁰⁵ Die Voraussetzung der

¹⁴⁰⁰ «If a controller seeks to process personal data that are in fact necessary for the performance of a contract [Art. 6 Abs. 1 lit. b DSGVO], then consent is not the appropriate lawful basis»: Art.-29-Datenschutzgruppe 2017d, 8. «[...] It is impossible to swap to a different legal basis»: Hellenic Data Protection Authority, Summary of Hellenic DPA's decision no 26/2019, abrufbar unter <www.dpa.gr> (besucht am 31.05.2020). Griechischer Volltext dieses Urteils: Urteil Αρχή Προστασίας Δεδομένων, «Archē Prostatías Dedoménon» [Datenschutz-Aufsichtsbehörde von Griechenland] Γ/ΕΞ/5230/26-07-2019 vom 26.07.2019.

¹⁴⁰¹ Art.-29-Datenschutzgruppe 2017d, 23.

¹⁴⁰² DETERMANN, 108–109.

¹⁴⁰³ Vgl. Art.-29-Datenschutzgruppe 2017d, 23. Nach deutschem Recht liegt ein unlauteres Handeln vor: CALDAROLA/SCHREY, N 163. Wohl a.M. WYBITUL/SCHULTZE-MELLING, N 157: Das Einholen einer Einwilligung sei auch dann rechtlich zulässig, wenn bereits ein anderer Erlaubnistatbestand einschlägig sei.

¹⁴⁰⁴ Anders dürfte die Rechtslage beim Widerspruchsrecht sein: Der Arbeitnehmer riskiert bei der Ausübung seines Rechts auf informationelle Selbstbestimmung (Art. 12 Abs. 2 lit. b DSG, Art. 26 Abs. 2 lit. b E-DSG, Art. 30 Abs. 2 lit. b rev-DSG), dass die Arbeitgeberin unter Berufung auf den Rechtfertigungsgrund des überwiegenden privaten Interesses die Daten trotz der Untersagung durch den Arbeitnehmer bearbeiten darf: WOLFER, N 214.

¹⁴⁰⁵ «Transparency-and-choice has failed»: NISSENBAUM 2011, 34. «Transparency-and-choice is meaningless»: WALDMAN, 84. Die ablehnende Haltung gegenüber der Einwilligung muss auch Konsequenzen für den Grundsatz der Erkennbarkeit haben. Die Betroffenen müssen zurückhaltend mit Informationen über die Datenbearbeitung ver-

Freiwilligkeit ist wegen des arbeitsrechtlichen Subordinationsverhältnisses kritisch zu sehen, und an der Voraussetzung der Informiertheit nagen Zweifel angesichts der regelmässig blinden Erteilung von Einwilligungen. Aus Sicht der Arbeitgeberin bildet die Einwilligung ein fragiles Rechtfertigungsfundament, weil jederzeit ein Widerruf droht.¹⁴⁰⁶ Gerade im Arbeitsverhältnis kann bereits das Nein einer relativ geringen Zahl von Arbeitnehmern der analytischen Untersuchung die Repräsentativität nehmen.¹⁴⁰⁷

Nebenbei bemerkt entfaltet die Einwilligung auch negative Externalitäten, denn je mehr Arbeitnehmer eines Betriebs ihre Einwilligung erteilen, desto stärker schrumpft der verbleibende Pool der durch Privatheit Geschützten.¹⁴⁰⁸ Aus den Daten der Einwilligenden können Ableitungen über einen Dritten resultieren, welcher seine Daten gerade nicht preisgeben wollte.¹⁴⁰⁹ Wenn beispielsweise eine genügende Anzahl Arbeitnehmer mit dem Stirnband «Muse» ihre Stressgefühle aufzeichnen lässt,¹⁴¹⁰ so kann die Arbeitgeberin Aussagen zum inneren Gefühlszustand von Arbeitskollegen treffen, die sich in einer vergleichbaren Situation befinden (z.B. Erledigung gleicher Aufgaben), die aber das Stirnband nicht tragen wollen.

Das Abstellen auf eine Einwilligung sollte somit nur die «ultima ratio» sein,¹⁴¹¹ wenn das Gesetz es ausdrücklich anordnet (etwa bei automatisierten Entscheidungen im Einzelfall, Art. 19 Abs. 3 lit. b E-DSG, Art. 21 Abs. 3 lit. b rev-DSG, Art. 22 Abs. 2 lit. c DSGVO) oder wenn kein anderer Rechtfertigungsgrund zur

sorgt werden. Weniger Transparenz ist manchmal mehr, vgl. S. 202–205. Kritik an der Behauptung, Transparenz sei ein universales Allheilmittel: DREYER/SCHULZ, 16. Es sei unklar, ob irgendeine Form der Transparenz mehr Gerechtigkeit schaffen könne: WACHTER *et al.*, 853. Es sei «naiv», zu meinen, Transparenz hinsichtlich Quellcode sowie Eingabe- und Ausgabedaten des Algorithmus erhöhe die verfahrensrechtliche Gerechtigkeit: KROLL *et al.*, 657.

¹⁴⁰⁶ KASPER/WILDHABER, 199; BISSELS *et al.*, 3045.

¹⁴⁰⁷ DÄUBLER, N 135.

¹⁴⁰⁸ HERMSTRÜWER, 109.

¹⁴⁰⁹ Vgl. HERMSTRÜWER, 106, und MATZNER, 99.

¹⁴¹⁰ Siehe zu diesem Stirnband S. 46.

¹⁴¹¹ GRAF/KRIŽANAC, 95. «For the majority of data processing at work, the lawful basis cannot and should not be the consent of the employees»: Art.-29-Datenschutzgruppe 2017d, 7. «Decisions only need consent when it really matters»: SCHERMER *et al.*, 172. A.M. AJUNWA 2017: «Employers should always obtain employees' informed consent about wellness programs.»

Verfügung steht.¹⁴¹² Nach europäischem Datenschutzrecht ist das Einholen einer Einwilligung im Arbeitsverhältnis sogar verboten, wenn eine andere Rechtsgrundlage (z.B. eine gesetzliche Pflicht oder ein überwiegendes Interesse der Arbeitgeberin) für die Datenbearbeitung zur Verfügung steht.¹⁴¹³ Dies geht aus einem rechtskräftigen¹⁴¹⁴ Urteil der griechischen Datenschutz-Aufsichtsbehörde hervor.¹⁴¹⁵ Es handelt sich hierbei zwar «nur» um ein Urteil eines EU-Mitgliedstaats, doch auch der Europäische Datenschutzausschuss verweist auf seiner öffentlich zugänglichen Webseite darauf.¹⁴¹⁶ Dem griechischen Entscheid zufolge ist aufgrund der Prinzipien der Rechtmässigkeit, der Datenbearbeitung nach Treu und Glauben und der Transparenz (Art. 5 Abs. 1 lit. a DSGVO) das Ausweichen auf die Einwilligung erst dann gestattet, wenn es an jeder anderen Rechtsgrundlage (im Sinne von Art. 6 Abs. 1 DSGVO) mangelt.¹⁴¹⁷ Das griechische Urteil nimmt eine Pionierstellung ein: Soweit ersichtlich und gemäss Direktauskunft der griechischen Datenschutz-Aufsichtsbehörde an den Autor der vorliegenden Arbeit ist es das erste Mal, dass eine europäische Datenschutz-Aufsichtsbehörde entschieden hat, dass das Anfragen einer Zustimmung der Arbeitnehmer unzulässig ist, wenn eine andere, angemessenere Rechtsgrundlage besteht.¹⁴¹⁸

Gestützt auf die vorangehenden Ausführungen resultiert, dass die Einwilligung zwar theoretisch als Rechtfertigungsgrund für Datenbearbeitungen im Arbeitsverhältnis vorgesehen ist, dass aber in der Praxis aus Sicht der Arbeitgeberin kaum Möglichkeiten bestehen, eine rechtsgültige Einwilligung zu erlangen. Im Hinblick

¹⁴¹² Siehe das Beispiel der Aufbewahrung von Bewerbungsunterlagen auf S. 223.

¹⁴¹³ Hellenic Data Protection Authority, Summary of Hellenic DPA's decision no 26/2019, abrufbar unter <www.dpa.gr> (besucht am 31.05.2020), 2. Vgl. auch Art.-29-Datenschutzgruppe 2017b, 23. Siehe bereits S. 230.

¹⁴¹⁴ Direktauskunft an den Autor durch die Αρχή Προστασίας Δεδομένων, «Arché Prostatías Dedoménon» [Datenschutz-Aufsichtsbehörde von Griechenland] 2020: «The decision 26/2019 is final, as it has not been appealed to a higher instance.»

¹⁴¹⁵ Der Volltext dieses Urteils ist, soweit ersichtlich, nur auf Neugriechisch verfügbar: Urteil Αρχή Προστασίας Δεδομένων, «Arché Prostatías Dedoménon» [Datenschutz-Aufsichtsbehörde von Griechenland] Γ/ΕΞ/5230/26-07-2019 vom 26.07.2019.

¹⁴¹⁶ EDSA, Company fined 150,000 euros for infringements of the GDPR, 31.07.2019, abrufbar unter <https://edpb.europa.eu> (besucht am 31.05.2020).

¹⁴¹⁷ Hellenic Data Protection Authority, Summary of Hellenic DPA's decision no 26/2019, abrufbar unter <www.dpa.gr> (besucht am 31.05.2020), 1.

¹⁴¹⁸ Αρχή Προστασίας Δεδομένων, «Arché Prostatías Dedoménon» [Datenschutz-Aufsichtsbehörde von Griechenland] 2020.

auf die zentrale Forschungsfrage,¹⁴¹⁹ nämlich wie eine Neuausrichtung des Datenschutzrechts aussehen könnte, bei welcher die Rechtsdurchsetzung im Zusammenhang mit People Analytics gewährleistet ist, kann jetzt schon festgehalten werden, dass die Einwilligung bei dieser Neuausrichtung höchstens eine untergeordnete Rolle spielen wird.

5.10.5 Überwiegendes Interesse

a) Gesetzessystematik

Der zweite Rechtfertigungsgrund von drei möglichen bei einer Persönlichkeitsverletzung ist das überwiegende private oder öffentliche Interesse des Datenbearbeiters (Art. 13 Abs. 1 DSG, Art. 27 Abs. 1 E-DSG, Art. 31 Abs. 1 rev-DSG). Dieser Rechtfertigungsgrund ist untrennbar mit dem Verhältnismässigkeitsprinzip (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG) verbunden, weil Letzteres eine Interessenabwägung impliziert.¹⁴²⁰ Deshalb ist es im zivilrechtlichen Anwendungsbereich des DSG dogmatisch richtig, die Verhältnismässigkeit auf der Stufe der Widerrechtlichkeit zu prüfen.¹⁴²¹

b) Privates Interesse

WOLFER wägt die widerstreitenden Interessen bei der elektronischen Überwachung im privatrechtlichen Arbeitsverhältnis sorgfältig und ausführlich gegeneinander ab.¹⁴²² An dieser Stelle ist daher nur an die wichtigsten Interessen der Arbeitgeberin zu erinnern: Zunächst hat sie ein Interesse an wirtschaftlicher Entfaltung (vgl. Art. 27 BV),¹⁴²³ Informationsbeschaffung (vgl. Art. 16 BV) und betrieblichem Fortschritt durch datenbasierte Forschung (vgl. Art. 20 BV).¹⁴²⁴ Sie ist

¹⁴¹⁹ Siehe S. 11.

¹⁴²⁰ Vgl. S. 181–182.

¹⁴²¹ WOLFER, N 207.

¹⁴²² WOLFER, N 238–320.

¹⁴²³ DREYER/SCHULZ, 25. Gerade in den USA ist das Verständnis von Daten als Handelsware stark ausgeprägt: VON ARNAULD, 119, und THIERER, 412.

¹⁴²⁴ PASSADELIS NICOLAS, Am überkommenen Primat der informationellen Selbstbestimmung festzuhalten, bedeutet, noch mehr wertvolle Zeit zu verlieren, NZZ vom 17.05.2017, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020). Informationsfreiheit (Art. 17 Abs. 3 lit. a DSGVO) und Wissenschaftsfreiheit (Art. 85 Abs. 1 DSGVO) sind im europäischen Recht keine eigenen Erlaubnistatbestände, jedoch von Behörden und Gerichten zu berücksichtigen: HAAS, N 25.

letztlich für die Produktivität der Angestellten verantwortlich (allenfalls gegenüber den Besitzern des Unternehmens, vgl. zur Aktiengesellschaft: Art. 716a Abs. 1 Ziff. 1 und 5, Art. 754 Abs. 1 OR).¹⁴²⁵ Auch besteht ein Interesse am Vermögensschutz (vgl. Art. 26 Abs. 1 BV, Art. 641 ZGB).¹⁴²⁶ Mit der zunehmenden Verbreitung von Arbeitssituationen, in denen die Arbeitgeberin den Arbeitnehmer aus den Augen verliert, wie beispielsweise bei der Telearbeit, wächst das Interesse der Arbeitgeberin an elektronischer Kontrolle der Tätigkeiten.¹⁴²⁷

Nach Beendigung eines Arbeitsverhältnisses sind die den Ehemaligen betreffenden Daten grundsätzlich zu vernichten.¹⁴²⁸ Eine befristete Aufbewahrung von Daten kann ausnahmsweise zur Beweissicherung bei Rechtsstreitigkeiten¹⁴²⁹ oder zur Durchsetzung eines Konkurrenzverbotes gerechtfertigt werden.¹⁴³⁰ Nur diejenigen Daten dürfen aufbewahrt werden, die dazu weiterhin erforderlich (Art. 328b Satz 1 OR) sind.¹⁴³¹

c) Öffentliches Interesse

Die Machtverschiebung zugunsten der Arbeitgebenden kann eine Vielzahl von Arbeitsverhältnissen betreffen,¹⁴³² da People Analytics sektorübergreifend zur Anwendung kommt.¹⁴³³ Somit können öffentliche Interessen an der Regulierung von People Analytics bestehen. Diese müssen in die Interessenabwägung einfließen (vgl. Art. 13 Abs. 1 DSG, Art. 27 Abs. 1 E-DSG, Art. 31 Abs. 1 rev-DSG). Sie sind zum Teil gleichläufig mit den Individualinteressen.

Zu gewährleisten ist eine pluralistische Gesellschaft, in deren Zentrum die Menschenwürde steht und in welcher der Einzelne nicht als austauschbar gilt, etwa

¹⁴²⁵ Vgl. BIAS/BOGUE, 262.

¹⁴²⁶ Vgl. S. 50–51.

¹⁴²⁷ Schweizerischer Bundesrat 2016b, 55. Vgl. zur schwindenden Bedeutung des Standard-Arbeitsvertrags S. 68–69.

¹⁴²⁸ Bzgl. der Personalakte: RIESSELMANN-SAXER, 70; bzgl. grafologischer Gutachten, psychologischer oder medizinischer Tests und Untersuchungsberichte sowie Qualifikationsunterlagen: SCHÜRER, 76.

¹⁴²⁹ CHK OR BT 2-EMMEL, Art. 328b OR, N 6; RIESSELMANN-SAXER, 71.

¹⁴³⁰ STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 13.

¹⁴³¹ KASPER/WILDHABER, 224–226.

¹⁴³² Siehe zur Machtverschiebung S. 79–82.

¹⁴³³ Siehe S. 61.

weil ihm das gleiche Profil wie anderen zugeschrieben wird.¹⁴³⁴ Ein «Daten-Determinismus» in der Art, dass Personen hauptsächlich aufgrund von Korrelationen und Gruppenwahrscheinlichkeiten beurteilt werden, läuft der bisher meritokratischen Gesellschaft, in der die tatsächlichen Handlungen und Leistungen am Arbeitsplatz von entscheidendem Belang sind, zuwider.¹⁴³⁵ Die grobe Einteilung in Gruppen kann eine Polarisierung der ohnehin schon gegensätzlichen Interessen der Arbeitgeber und -nehmer sowie eine Polarisierung unter den Arbeitnehmern zur Folge haben.¹⁴³⁶ Zudem können die Meinungsfreiheit und die Demokratie bedroht sein, wenn sich Personen wegen der Überwachung nicht trauen, sich nichtkonform zu äussern und zu verhalten.¹⁴³⁷

Kollektiv bedeutsam ist das Interesse am Schutz vor Manipulation von persönlichen Einstellungen und Werthaltungen, beispielsweise zwecks Verhaltenssteuerung.¹⁴³⁸ Nur wenn alle Beteiligten wissen, was beim Einsatz von People Analytics

¹⁴³⁴ OTTO 2016, 199. Dem Datenschutz kommt somit ein «gesellschaftlicher Wert» zu: WALTER, 117. Vgl. ROESSLER/MOKROSINSKA, 785: Ein öffentliches Interesse an einer Geheimsphäre für Individuen bestehe, weil einer vollkommen transparenten Gesellschaft sinnstiftende soziale Beziehungen fehlen würden.

¹⁴³⁵ WILSON *et al.*, 21. Ein Daten-Determinismus ist problematisch: ZARSKY, 1409.

¹⁴³⁶ «*Workforce polarisation*»: STAN, 293. Vgl. BOEHME-NESSLER. Algorithmen in Suchmaschinen und sozialen Netzwerken führen zur Polarisierung der Gesellschaft: THELISSON *et al.*, 54. «*We must pause to ask whether emerging technologies are disruptive to the very fabric of our democracy [...] in the freedom to direct the course of our everyday work lives*»: AJUNWA IFEOMA, Corporate Surveillance Is Turning Human Workers Into Fungible Cogs, The Atlantic vom 19.05.2017, abrufbar unter <www.theatlantic.com> (besucht am 31.05.2020). Befürchtet wird ein Überwachungskapitalismus («*surveillance capitalism*»), weil Unternehmen imstande seien, das Verhalten von Bevölkerungen, Gruppen und Individuen vorherzusagen: ZUBOFF 2019, 21. Die Folgen des Einsatzes von Algorithmen seien auf der Makroebene, etwa für die Bevölkerung, noch nicht abschätzbar: SMITH ANDREW, Franken-algorithms: the deadly consequences of unpredictable code, The Guardian vom 30.08.2018, abrufbar unter <www.theguardian.com> (besucht am 31.05.2020).

¹⁴³⁷ BELSER 2011b, 1. Kapitel N 5.

¹⁴³⁸ Vgl. KASPER/WILDHABER, 216. HOFFMANN-RIEM, 58. Wichtig sei es, dass die Menschen frei handelten und die Algorithmen beaufsichtigten («*human agency and oversight*») und nicht umgekehrt: Europäische Kommission 2019b, 14. «*As a society we need to decide whether we want to live in a world that is increasingly determined by algorithms*»: HÄNOLD, 151.

passiert, können wir noch behaupten, in einer freien Demokratie zu leben.¹⁴³⁹ Die Daten sollten genutzt und nicht die Arbeitnehmer ausgenutzt werden.¹⁴⁴⁰

Arbeitsmarktpolitische Argumente stehen hinter der Antidiskriminierungs-Gesetzgebung. In dem Masse, wie es gelingt, durch privatrechtlichen Diskriminierungsschutz soziale Ausgrenzung (vom Arbeitsmarkt) zu vermeiden, müssen die Kosten für die sozialen Ausgleichsmassnahmen nicht vom Staat bzw. von den Sozialversicherungen und Institutionen der sozialen Hilfe getragen werden.¹⁴⁴¹

Umgekehrt sollte aber zugunsten von People Analytics auch das öffentliche Interesse an einem soliden Arbeitsmarkt sowie am innovativen Wirtschafts- und Forschungsstandort Schweiz in der Waagschale Platz finden.¹⁴⁴² Auch das öffentliche Archivwesen kann ein Interesse an den Daten haben, um einen rationalen Umgang mit der Vergangenheit zu ermöglichen.¹⁴⁴³ Schliesslich sollte berücksichtigt werden, ob eine Technologie sozial akzeptiert ist.¹⁴⁴⁴

d) Forschung, Planung und Statistik

Das DSG konkretisiert, dass ein überwiegendes Interesse der bearbeitenden Person insbesondere in Betracht fällt, wenn diese Personendaten zu nicht personenbezogenen Zwecken namentlich in der Forschung, Planung und Statistik bearbeitet und die Ergebnisse so veröffentlicht werden, dass die betroffenen Personen nicht bestimmbar sind (Art. 13 Abs. 2 lit. e DSG, vgl. Art. 27 Abs. 2 lit. e Ziff. 1–3 E-DSG, vgl. Art. 31 Abs. 2 lit. e Ziff. 1–3 rev-DSG). Dieser Rechtfertigungsgrund ist näher zu beleuchten, weil People Analytics dazu dient, das Humankapital zu

¹⁴³⁹ Vgl. BLATTNER MARCEL / NONNER TIM, Algorithmen gefährden die Demokratie, Tagesanzeiger vom 10.04.2018, abrufbar unter <www.tagesanzeiger.ch> (besucht am 31.05.2020). Je schwerwiegender die Einmischung von Algorithmen in politisch-gesellschaftliche Normen sei, desto mehr bedürfe sie gesellschaftlicher Kontrolle: BAUMANN MAX-OTTO, 4.

¹⁴⁴⁰ RICHARDS/HARTZOG 2017, 1188.

¹⁴⁴¹ PÄRLI 2009, N 18. Vgl. DAÜBLER, N 208. Zu den Folgeproblemen, wenn benachteiligte Gruppen ausgeschlossen werden: ROBERTS, 575.

¹⁴⁴² Für eine offene Haltung gegenüber der Forschung mit Daten aus Medizinakten: DÜBENDORFER THOMAS, Paradoxe beim Datenschutz, NZZ vom 22.03.2017, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020); HOFFMANN-RIEM, 44. Vgl. HÄRTING, N 254: «Datenminimierung ist innovationsfeindlich.» WEBER 2018, 101.

¹⁴⁴³ RUDIN 1998, N 10–11.

¹⁴⁴⁴ ROSENTHAL 2012, 78.

erforschen, die Personalplanung und Gebäudeplanung zu optimieren,¹⁴⁴⁵ und weil die dabei gesuchten Korrelationen aus Statistiken hervorgehen.¹⁴⁴⁶

Der Begriff der Forschung ist ein unbestimmter Rechtsbegriff.¹⁴⁴⁷ Die EU legt den Begriff der «wissenschaftlichen Forschungszwecke» (E. 159 Satz 2 DSGVO) weit aus und versteht darunter jedes Forschungsprojekt, das nach fachspezifischen methodischen und ethischen Regeln und bewährten Verfahren durchgeführt wird.¹⁴⁴⁸ Eingeschlossen ist auch die privat finanzierte Forschung (E. 159 Satz 2 DSGVO),¹⁴⁴⁹ was auch unter dem schweizerischen DSG zutreffen dürfte. Umstritten ist, ob nur die Forschung in einem engeren Sinn privilegiert werden soll und somit nicht jede Analyse oder Aufbereitung von Daten in Zeiten von People Analytics.¹⁴⁵⁰ Eine solche Einschränkung des Forschungsbegriffs wird vorliegend abgelehnt, würde sie doch bedeuten, dass die meisten People Analytics-Projekte der Praxis nicht vom Forschungsprivileg profitieren könnten.

Die Forschungsergebnisse müssen «veröffentlicht werden» (Art. 13 Abs. 2 lit. e DSG, Art. 27 Abs. 2 lit. e Ziff. 3 E-DSG, Art. 31 Abs. 2 lit. e Ziff. 3 rev-DSG). Die Arbeitgeberin kann nur vom Forschungsprivileg profitieren, wenn sie die Resultate jedermann zur Verfügung stellt. Es wird vermutet, dass das Forschungsprivileg im privatrechtlichen Arbeitsverhältnis wenig von Bedeutung ist, weil die Arbeitgeberin hier in der Regel ein starkes Interesse an der Wahrung der Geschäftsgeheimnisse hat.¹⁴⁵¹

Vorausgesetzt wird weiter, dass die Personendaten «nicht zu personenbezogenen Zwecken» bearbeitet werden und die betroffenen Personen anhand der Ergebnisse nicht re-identifizierbar sind (Art. 13 Abs. 2 lit. e DSG, vgl. Art. 27 Abs. 2 lit. e E-DSG, vgl. Art. 31 Abs. 2 lit. e rev-DSG).¹⁴⁵² Somit sind beispielsweise Gene-

¹⁴⁴⁵ Z.B. die Software Jobfeed zur strategischen Personalplanung (siehe S. 45), die Software Sopre zur Personal- und Rollmaterial-Einsatzplanung (siehe S. 53) oder die Infrarotsender zur Gebäudeplanung (siehe S. 53).

¹⁴⁴⁶ Siehe zum Begriff der Korrelation S. 32–36.

¹⁴⁴⁷ Fehlende Definition der «wissenschaftlichen Forschung» in der DSGVO: Art.-29-Datenschutzgruppe 2017d, 27.

¹⁴⁴⁸ Art.-29-Datenschutzgruppe 2017d, 27–28.

¹⁴⁴⁹ GAMPER/KASTELITZ, 3.

¹⁴⁵⁰ Vgl. GAMPER/KASTELITZ, 3.

¹⁴⁵¹ KASPER/WILDHABER, 196; MITTLÄNDER 2016b, 175.

¹⁴⁵² Für eine möglichst rasche Pseudonymisierung oder Anonymisierung unter der DSGVO: DÄUBLER, N 425.

alogen und Historiker, die explizit personenbezogene Forschung betreiben, nicht von dieser Bestimmung erfasst.¹⁴⁵³ People Analytics kann folglich nicht vom Forschungsprivileg profitieren, wenn einzelne Arbeitnehmer bestimmbar sind.

Im Arbeitskontext ist für den Rechtfertigungsgrund der Forschung zusätzlich vorausgesetzt, dass People Analytics letztlich einen Arbeitsplatzbezug aufweist (vgl. Art. 328b OR). Das OR findet kumulativ zum DSG Anwendung.¹⁴⁵⁴

Sind die geschilderten Voraussetzungen der Spezialnorm erfüllt, kann die Persönlichkeitsverletzung gerechtfertigt werden. Unter der DSGVO ist eine erleichterte Weiterbearbeitung der Daten nach Erfüllung des Zwecks möglich, weil die Datenbearbeitung zu Forschungszwecken nicht als unvereinbar mit den ursprünglichen Zwecken gilt (Art. 5 Abs. 1 lit. b Teilsatz 2 DSGVO). Die Daten dürfen länger gespeichert werden als für den Bearbeitungszweck erforderlich (Art. 5 Abs. 1 lit. e Teilsatz 2 DSGVO). Die Betroffenenrechte auf Information (Art. 14 Abs. 5 lit. b DSGVO) und Löschung (Art. 17 Abs. 3 lit. d DSGVO) und gegebenenfalls weitere Rechte (vgl. Art. 89 Abs. 2–4 DSGVO) erfahren Einschränkungen.

e) Arbeitnehmerinteressen

Den arbeitgeberseitigen Interessen steht das Interesse der Arbeitnehmer entgegen, dass sich die dem beschriebenen Machtungleichgewicht innewohnenden Risiken von People Analytics nicht verwirklichen. Dies betrifft die diskutierten Rechtsprobleme der Persönlichkeitsverletzung (Manipulation, Verlust von Autonomie und Persönlichkeitsdurchleuchtung), Diskriminierung (etwa durch ungerechtfertigte, auf falschen Daten beruhende Nichtanstellung, Nichtbeförderung, Kündigung oder überhöhte Leistungsvorgabe)¹⁴⁵⁵ und Mitwirkung.¹⁴⁵⁶

f) Fehlende Methode zur Interessenabwägung

Eine Methode der Interessenabwägung spezifisch für das privatrechtliche Datenschutzrecht gibt es nicht; jede Bewertung der einzelnen Interessen verlangt letztlich ein Werturteil.¹⁴⁵⁷ Dies führt zu Rechtsunsicherheit.¹⁴⁵⁸ Nach der bundesge-

¹⁴⁵³ BB1 1988 II, 463; BSK DSG-RAMPINI, Art. 13 DSG, N 42; a.M. HK-ROSENTHAL, Art. 13 DSG, N 59.

¹⁴⁵⁴ Vgl. zum deutschen § 26 Abs. 1 BDSG: DÄUBLER, N 427.

¹⁴⁵⁵ Vgl. PARISI, 333.

¹⁴⁵⁶ Siehe Kapitel 3, S. 79–106.

¹⁴⁵⁷ WOLFER, N 631.

¹⁴⁵⁸ CULIK, 300.

richtlichen Rechtsprechung darf ein überwiegendes privates oder öffentliches Interesse an einer Datenbearbeitung nur zurückhaltend bejaht werden.¹⁴⁵⁹ Als übergeordnete Erwägung gegen die Zulässigkeit von People Analytics kann auf die durch People Analytics verursachte Machtverschiebung hingewiesen werden.¹⁴⁶⁰ Für die Zulässigkeit spricht hingegen, dass die rechtlichen und tatsächlichen Folgen einer Datenanalyse für den Arbeitnehmer gering ausfallen, wenn Personalmassnahmen unterstützt werden, die auch ohne die Datenbearbeitung hätten getroffen werden können.¹⁴⁶¹

Das Fehlen einer Methodik zur Interessenabwägung bedeutet, dass die Gesamtheit aller Umstände des konkreten Einzelfalls einzubeziehen ist. Der Kontext der Datenbearbeitung erlangt somit eine starke Bedeutung.¹⁴⁶² Gerade bei Daten ist der Kontext bedeutsam, weil sie in ihrer Eigenschaft als Wertchance erst einen Wert erlangen, wenn sie in einen Kontext gesetzt werden.¹⁴⁶³ Der hohe Stellenwert des Kontexts verlangt, dass die Personen, die mit People Analytics umgehen, fähig sind, die Situation umfassend zu analysieren und sich in die verschiedenen Interessenspositionen, die zu gewichten sind, hineinzusetzen.

5.10.6 Gesetzliche Rechtfertigung

Zunächst können aus dem DSG herrührende Pflichten eine Datenbearbeitung notwendig machen. Zu denken ist insbesondere an die Pflicht zur Gewährleistung der Datensicherheit (Art. 7 DSG, Art. 7 E-DSG, Art. 8 rev-DSG) und an die Auskunftspflicht (Art. 8 DSG, Art. 23 E-DSG, Art. 25 rev-DSG), die eine Aufbewahrung von Daten gebieten und einer Löschung oder Datenminimierung entgegenstehen können.¹⁴⁶⁴

Sodann trifft die Arbeitgeberin eine arbeitsrechtliche Schutzpflicht gegenüber dem Arbeitnehmer (vgl. Art. 328 OR). Beispielsweise kann es zur Vermeidung von

¹⁴⁵⁹ BGE 136 II 508 E. 6.3.3; ROSENTHAL 2012, 79.

¹⁴⁶⁰ Siehe S. 79. CULIK, 151.

¹⁴⁶¹ CULIK, 293.

¹⁴⁶² Der Kontext umfasst insbesondere die Art der Daten, die beteiligten Personen, das zwischenparteiliche Vertrauen, die Erhebungsmethoden, die verwendeten Geräte und Programme sowie die Wertgenerierung durch die Datenbearbeitung: World Economic Forum 2013, 11. Vgl. auch PELTZ-STEELE, 406.

¹⁴⁶³ Siehe S. 21–22. Wie Geld unter einer Matratze bleiben Daten inert, bis sie jemand für einen bestimmten Zweck verwendet: World Economic Forum 2013, 11.

¹⁴⁶⁴ Siehe S. 207–208.

Verletzungen bei der Zusammenarbeit von Mensch und Roboter geboten sein, Daten über Bewegung und Standort der Arbeitskraft zu erheben.¹⁴⁶⁵ Eine solche Datenerhebung kann auch deshalb angezeigt sein, weil die Arbeitgeberin Dritten gegenüber delikts- und strafrechtlich für die Handlungen ihrer Arbeitnehmer haften muss (vgl. Art. 55 und Art. 101 OR; Art. 102 StGB).¹⁴⁶⁶ Die gesetzliche Pflicht zur Ausstellung oder späteren Berichtigung eines Zeugnisses und zur Erteilung von Referenzen (Art. 330a OR) kann eine Aufbewahrung von Personendaten über die Beendigung des Arbeitsvertrags hinaus rechtfertigen.¹⁴⁶⁷ Der Arbeitnehmer hat während zehn Jahren (Art. 127 OR) nach Beendigung des Arbeitsverhältnisses einen Anspruch darauf.¹⁴⁶⁸ Verlangt er die Vernichtung seiner Daten, ist dies – unter Vorbehalt der Unverzichtbarkeit im ersten Monat nach dem Austritt (Art. 341 Abs. 1 OR) – als konkludenter (unwiderruflicher) Verzicht auf die Ausstellung eines Zeugnisses zu werten.¹⁴⁶⁹

Ferner existieren andere gesetzliche Aufbewahrungspflichten. Zu nennen ist die Pflicht zur zehnjährigen Aufbewahrung der Geschäftsbücher (Art. 958f OR). Sie kann E-Mails erfassen, wenn diese buchhaltungsrelevante Daten enthalten.¹⁴⁷⁰ Sie kann aber nicht als Rechtfertigungsgrund für eine allgemeine E-Mail-Aufbewahrung greifen, wenn bloss ein kleiner Teil der E-Mails Informationen zu den Geschäftsbüchern enthält.¹⁴⁷¹ Art. 328b OR geht in diesem Fall als *lex specialis* vor.¹⁴⁷² Gleiches muss in Bezug auf sozialversicherungs-,¹⁴⁷³ steuer- und aufsichtsrechtliche Aufbewahrungspflichten gelten.¹⁴⁷⁴ Aus den Bestimmungen zu finanzmarktrechtlichen Organisations- und Risikomanagement-Pflichten (z.B. Gewährspflicht) kann kein Rechtfertigungsgrund für die Bearbeitung von Personendaten entgegen den Datenschutz-Grundsätzen (vgl. Art. 12 Abs. 2 lit. a DSGVO, Art. 26 Abs. 2 lit. a E-DSG, Art. 30 Abs. 2 lit. a rev-DSG) abgeleitet werden. Sie

¹⁴⁶⁵ BMAS 2017, 72.

¹⁴⁶⁶ Vgl. GRÜNANGER, N 4.1. Vgl. zur Haftung für Arbeitnehmer nach amerikanischem Recht: BIAS/BOGUE, 256.

¹⁴⁶⁷ KASPER/WILDHABER, 225–226.

¹⁴⁶⁸ RIESELMANN-SAXER, 71; SCHÜRER, 76.

¹⁴⁶⁹ RIESELMANN-SAXER, 72.

¹⁴⁷⁰ DUNAND, 58; KASPER/WILDHABER, 226.

¹⁴⁷¹ Vgl. MATHYS, 100. KASPER/WILDHABER, 226.

¹⁴⁷² STREIFF/VON KAENEL/RUDOLPH, Art. 328b OR N 13; KASPER/WILDHABER, 226.

¹⁴⁷³ Vgl. zur Aufbewahrung von Pensionskassendaten: Europarat 2016b, 49.

¹⁴⁷⁴ KASPER/WILDHABER, 226.

stellen zwar Spezialnormen dar, die Vorrang gegenüber dem allgemeinen Gesetz genießen, in diesem Fall vor dem DSG. Nur sehen sie inhaltlich keine gegenteilige Regelung zu den Datenschutz-Grundsätzen vor.¹⁴⁷⁵ Unzulässig wäre es somit, unter dem Vorwand der Compliance aus den (nicht anonymisierten) Daten eines erfolglosen Ex-Arbeitnehmers ein Profil unerwünschter Bewerber zu erstellen oder ihn auf eine schwarze Liste zu setzen, um seinen Wiedereintritt in einer anderen Unternehmensabteilung oder Konzerngesellschaft zu verhindern.¹⁴⁷⁶

Einzelne der genannten gesetzlichen Pflichten vermögen eine Datenbearbeitung in stärkerem Ausmass zu rechtfertigen. So können die eingangs bekannt gemachten Lösungen zur Einhaltung der Arbeitssicherheits-Richtlinien (z.B. die Drohnen, die Bahngeleise-Arbeiter beaufsichtigen)¹⁴⁷⁷ zur Erfüllung der Fürsorgepflicht behilflich sein. Die Mehrheit der mit People Analytics verfolgten Zwecke dürfte aber nicht durch das Gesetz gedeckt sein, denn die meisten der beschriebenen Anwendungen in den Bereichen Rekrutierung, Leistungssteuerung, Arbeits- und Arbeitsplatzgestaltung sowie Mitarbeiterbindung sind betriebswirtschaftlich motiviert und nicht etwa durch ein allgemeines Interesse, das gesetzlich verankert ist.¹⁴⁷⁸ In diesen Fällen ist auf den Rechtfertigungsgrund der überwiegenden privaten Interessen der Arbeitgeberin zurückzugreifen. Insgesamt spielt von der Trias der Rechtfertigungsgründe – Einwilligung, überwiegende Interessen und Gesetz (Art. 13 Abs. 1 DSG, Art. 27 Abs. 1 E-DSG, Art. 31 Abs. 1 rev-DSG) – der Rechtfertigungsgrund der überwiegenden privaten Interessen bei People Analytics im privatrechtlichen Arbeitsverhältnis eine dominante Rolle.

5.11 Umsetzung der Datenschutznormen in der Praxis

5.11.1 NFP75-Daten zur Umsetzung

Das Abwägen der verschiedenen Datenbearbeitungsregeln gegeneinander und die Prüfung der Rechtfertigungsgründe im Einzelfall erfordert ein bedeutendes Mass an rechtlicher Reflexionskompetenz – ein Befund, der auch aus der Betrachtung

¹⁴⁷⁵ EDÖB 2014a, 5.

¹⁴⁷⁶ KASPER/WILDHABER, 226.

¹⁴⁷⁷ Siehe S. 52.

¹⁴⁷⁸ Siehe S. 42–59.

der relevanten Erlasse in Kapitel 4 hervorgegangen ist.¹⁴⁷⁹ Die empirischen Daten aus der Online-Umfrage des NFP75-Projekts lassen aber Zweifel aufkeimen, ob die Arbeitgeberinnen das Datenschutzrecht korrekt umsetzen.¹⁴⁸⁰

Zunächst erfolgt nicht immer die gesetzlich zwingende Trennung von Beruf und Privatleben (vgl. Art. 328b OR). Einige Teilnehmer gaben an, sie stimmten der Aussage völlig oder beinahe völlig zu, dass ihr Unternehmen nichtberufsbezogene Daten von Arbeitnehmern (3 Prozent) oder Bewerbern (7 Prozent) analysiere. Dies verstösst grundsätzlich gegen das arbeitsrechtliche Erfordernis eines sachlichen Bezugs der Datenbearbeitung zur Arbeit (Art. 328b OR). Zudem können die Arbeitnehmer das Gerät oder das Programm, über das People Analytics betrieben wird, in drei von fünf Fällen nicht ausschalten (62 Prozent), während sie sich in zwei von fünf Fällen durch Ausschalten des Geräts der Analyse entziehen können (38 Prozent). Hier ist im Einzelfall zu beurteilen, ob die fehlende Ausschaltfunktion (unter Verstoß gegen Art. 328b OR) zur Erhebung nicht erforderlicher Daten aus der Freizeit führt. Dies wäre grundsätzlich der Fall, wenn ein über GPS geortetes Geschäftsauto auch privat benutzt werden darf und Aufzeichnungen stattfinden. Weniger problematisch erscheint die permanente Aufzeichnung, wenn die Sensoren am Arbeitsplatz fest installiert sind und die Arbeitnehmer aus den «Augen» verlieren, sobald sie das Gebäude verlassen.¹⁴⁸¹

Jeder fünfte Umfrageteilnehmer stimmt der Aussage völlig oder fast völlig zu, dass sein Unternehmen das Verhalten von Arbeitnehmern und deren Zusammenarbeit untereinander beobachtet (22 Prozent). Diese Unternehmen verstossen grundsätzlich gegen das Verbot von Verhaltens-Überwachungssystemen (Art. 26 ArGV 3). Aber die Rechtsprechung hat dieses Verbot gelockert. Somit sind die genannten Systeme trotzdem zulässig, solange sie nicht durch ihre Auswirkungen die Gesundheit oder das Wohlbefinden der Arbeitnehmer beeinträchtigen.¹⁴⁸²

Bedenklich ist, wie die Praxis die Bearbeitungsregel der Erkennbarkeit lebt: Von den Unternehmen, die People Analytics einsetzen, stimmt (nur) etwas mehr als die Hälfte der Aussage völlig oder nahezu völlig zu, dass die Mitarbeiter und Bewerber verstehen, was das Unternehmen über sie analysiert (53 Prozent).¹⁴⁸³

¹⁴⁷⁹ Siehe S. 131–132.

¹⁴⁸⁰ Siehe zur Publikation der Resultate: FN 76.

¹⁴⁸¹ Siehe auch WILDHABER/KASPER, 767–768. Siehe zu den Datenaufzeichnungen nach Arbeitsende S. 191.

¹⁴⁸² Siehe S. 150–154.

¹⁴⁸³ Siehe auch WILDHABER/KASPER, 768–769.

Offensichtlich auf Kollisionskurs mit der Praxis sind die Bearbeitungsregeln zur Speicherbegrenzung und zum Löschen (siehe Abb. 9). Eine unbegrenzte Speicherdauer ist immer mehr an der Tagesordnung. (Nur) jedes fünfte Unternehmen, das People Analytics betreibt, löscht die Daten gänzlich, sobald der Zweck, zu dem sie erhoben worden sind, erfüllt ist (20 Prozent). Doppelt so viele Arbeitgebende bewahren die erhobenen Daten generell während zehn Jahren auf (44 Prozent). Jedes vierte Unternehmen bewahrt die Daten während der gesamten Dauer des Arbeitsverhältnisses des jeweiligen Arbeitnehmers auf (27 Prozent). Jedes zwanzigste Unternehmen gibt an, dass es Datensätze und Analysen überhaupt nicht lösche (5 Prozent).¹⁴⁸⁴

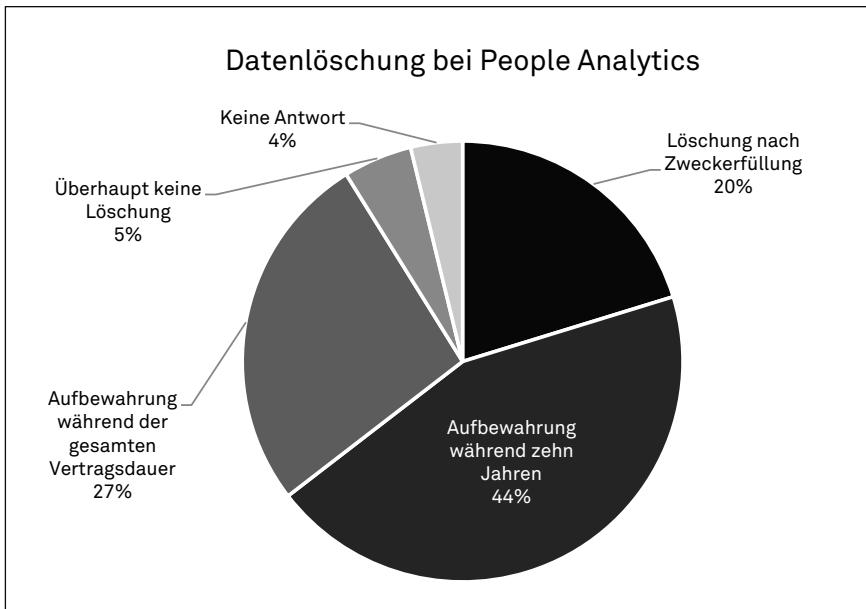


Abb. 9: Datenlöschung in der schweizerischen People Analytics-Praxis

Das Gebot der Datensicherheit (Art. 7 Abs. 1 DSG, Art. 7 Abs. 1 E-DSG, Art. 8 Abs. 1 rev-DSG) verlangt die Ausarbeitung eines firmeninternen Berechtigungskonzepts, damit nicht jeder Mitarbeitende alle Daten einsehen kann.¹⁴⁸⁵ Doch ein Unternehmen gibt an, dass alle Angestellten im Unternehmen nahezu vollen Zu-

¹⁴⁸⁴ Siehe auch WILDHABER/KASPER, 768.

¹⁴⁸⁵ Zumindest Firmen, die in den Anwendungsbereich der DSGVO fallen, sind zu einem Berechtigungsmanagement verpflichtet: DOMENIG/MITSCHERLICH, N 444–445.

griff auf die Daten hätten (*open company access*, 1 Prozent). In jedem dritten Unternehmen haben allein die analysierten Mitarbeiter vollen oder nahezu vollen Zugriff auf die über sie erhobenen Daten (35 Prozent). In den übrigen Fällen haben oft allein die Personalabteilung (57 Prozent), allein die Linienvorgesetzten (39 Prozent), sowohl die analysierten Mitarbeiter als auch ihre Linienvorgesetzten (30 Prozent) oder auch interne Expertenausschüsse (39 Prozent) vollen oder nahezu vollen Zugriff auf die über die Arbeitnehmer erhobenen Daten. Drei Unternehmen gewähren externen Drittparteien (z.B. beauftragten IT-Dienstleistern) vollen Zugriff auf die erhobenen Daten (3 Prozent).¹⁴⁸⁶

Auf den Rechtfertigungsgrund der Einwilligung verlässt sich die Praxis trotz der vorliegend aufgestellten Warningschilder in beinahe neun von zehn Fällen (86 Prozent, siehe Abb. 10). Dabei holt jedes vierte Unternehmen (27 Prozent) eine Einwilligung für jede einzelne People Analytics-Anwendung ein. Doch die übrigen drei von fünf Unternehmen (59 Prozent) holen eine vorgängige generelle Einwilligung zu People Analytics mittels einer Klausel im Arbeitsvertrag ein. Dies ist kritisch zu sehen, weil bei der Vertragsunterzeichnung eine erhebliche Drucksituation bestehen kann, wodurch die Freiwilligkeit der Einwilligung infrage gestellt ist. Auch droht eine allgemein gehaltene Einwilligungsklausel am Erfordernis der Informiertheit zu scheitern, wenn sie die Datenbearbeitung, der zugestimmt werden soll, nicht genügend bestimmt umschreibt. Bemerkenswert und in der Regel zu begrüßen ist, dass jedes zehnte Unternehmen keine Einwilligung einholt, weil es die Analysen anderweitig rechtfertigt (11 Prozent).¹⁴⁸⁷

¹⁴⁸⁶ Siehe auch WILDHABER/KASPER, 769–770.

¹⁴⁸⁷ Siehe auch WILDHABER/KASPER, 769.

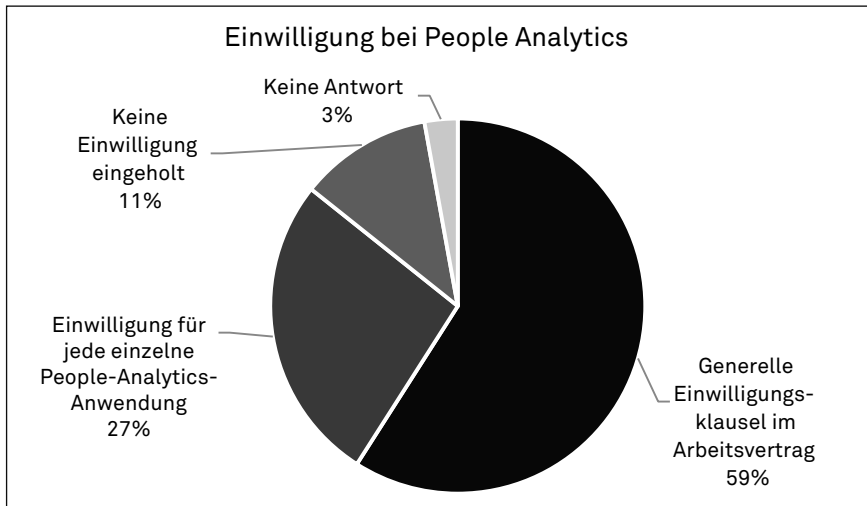


Abb. 10: Einwilligung in der schweizerischen People Analytics-Praxis

5.11.2 Öffentlich bekannt gewordene Datenskandale

Was die NFP75-Zahlen suggerieren, trifft auf Bestätigung in der Literatur: Es wird festgestellt, dass den hohen Erwartungen des Gesetzgebers eine «ziemlich unbedarfte betriebliche Praxis» gegenübersteht.¹⁴⁸⁸ Unternehmen handeln «nicht aus Erkenntnis, sondern aus Zwang» und bestenfalls «gerade einmal so, dass es keine Sanktionen gibt».¹⁴⁸⁹

Oft kommt es aber zum öffentlichen Datenskandal: In der Schweiz hat sich die Grossbank Credit Suisse 2019 in die negativen Schlagzeilen manövriert, als sie in Zusammenarbeit mit einem Detektivbüro Beschattungen hochrangiger Mitarbeiter durchführte.¹⁴⁹⁰ Im gleichen Jahr ist in Südkorea der Verwaltungsratspräsident von Samsung Electronics zu 18 Monaten Gefängnis verurteilt worden, weil das Unter-

¹⁴⁸⁸ PÄRLI 2018, N 17.2.

¹⁴⁸⁹ ROSENTHAL DAVID, Eine Mogelpackung, NZZ vom 03.05.2017, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

¹⁴⁹⁰ Beschattungsaffäre Iqbal Khan: EISENRING CHRISTOPH / SCHÜRPF THOMAS, Die Credit-Suisse-Spitze bleibt unter Druck – die wichtigsten Antworten, NZZ vom 04.10.2019, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020); Beschattungsaffäre Peter Goerke: GALLAROTTI ERMES / BACHES ZOÉ, Die Credit Suisse bestätigt eine weitere Beschattung – und entlässt Thiems ehemalige rechte Hand fristlos, NZZ vom 23.12.2019, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

nehmen die Gewerkschaftsmitglieder bespitzelt hatte.¹⁴⁹¹ Ähnliches trug sich bei der Deutschen Telekom zu, die Telefonate von Aufsichtsratsmitgliedern abhörte, und bei der Deutschen Bank, die das persönliche Umfeld von Führungskräften recherchierte.¹⁴⁹² Der Discounter Lidl kontrollierte 2008 die Häufigkeit und Dauer des Toilettengangs seiner Mitarbeitenden, montierte unzulässigerweise Videokameras in den Umkleidekabinen und heuerte zur systematischen Mitarbeiterüberwachung Detektive an; im Jahr darauf wurde bekannt, dass Lidl unrechtmässig detaillierte Informationen zu den Krankheitsgründen und dem Krankheitsverlauf seiner Mitarbeiter erfasste.¹⁴⁹³ Die Deutsche Bahn wiederum liess bis 2009 ohne konkreten Missbrauchsverdacht personenbezogene Daten von 173'000 Arbeitnehmern mit Daten von Lieferanten abgleichen. Zudem hat das Unternehmen in den Jahren 2006 und 2007 den E-Mail-Verkehr aller Beschäftigten, die einen externen E-Mail-Anschluss am Arbeitsplatz hatten, systematisch überwacht.¹⁴⁹⁴

5.12 Zwischenfazit: hoher Fachwissensbedarf bei gleichzeitigen Mängeln in der Datenschutzpraxis

Das vorliegende Kapitel 5 hat sich eingangs mit der *ratio legis* des DSG auseinandergesetzt. Der Gesetzeszweck des DSG besteht im privatrechtlichen Bereich im Schutz der Persönlichkeit bei Datenbearbeitungen. Während der Persönlichkeitsschutz das Endziel ist, werden als Mittel zur Zielerreichung die zulässigen Bearbeitungsprozesse definiert. In der Gesetzgebungstechnik äussert sich dies dadurch, dass einerseits risikoorientierte Normen den Schutz der Persönlichkeit im privatrechtlichen Bereich statuieren, andererseits aber auch prozedurale Normen den Persönlichkeitsschutz in Bezug auf Datenbearbeitungen konkretisieren. Beide Normtypen haben ihre Defizite, entweder weil sie zu abstrakt sind (die risikoorientierten) oder zu starr und formalistisch (die prozessorientierten). Nach der vorliegend vertretenen Meinung sind die prozessbezogenen Normen notwendig,

¹⁴⁹¹ Reuters, Haftstrafe für Samsung-Manager [sic] wegen Sabotage von Gewerkschaften, 17.12.2019, abrufbar unter <www.reuters.com> (besucht am 31.05.2020).

¹⁴⁹² HÄFNER-BEIL, 94.

¹⁴⁹³ NEU, 327; PÄRLI 2018, N 17.2.

¹⁴⁹⁴ NEU, 327–328.

doch müssen sie in jedem Einzelfall risikoorientiert ausgelegt werden. Die datenschutzrechtlichen Bearbeitungsregeln gelten deshalb oft nicht absolut.¹⁴⁹⁵

Die Flexibilität und Auslegungsbedürftigkeit zeigt sich bei verschiedenen Normen. Beispielsweise fallen gemäss der Auffassung des Autors Typisierungen nicht generell unter das DSG, sondern nur, wenn ihnen hohe Persönlichkeitsrisiken innewohnen.¹⁴⁹⁶ Das datenschutzrechtliche Prinzip der Zweckbindung lässt neue Bearbeitungszwecke zu, solange sie mit dem ursprünglichen vereinbar sind.¹⁴⁹⁷ Arbeitsrechtlich muss der Bearbeitungszweck einen Bezug zum Arbeitsplatz aufweisen; es besteht aber ein gewisser Spielraum zur Auslegung, welche Datenbearbeitungen objektiv zur Eignungsabklärung beitragen und welche Daten zur Durchführung des Arbeitsvertrags erforderlich sind.¹⁴⁹⁸ Die Erkennbarkeit ist nach der hier entwickelten restriktiven Auslegung so umzusetzen, dass die Arbeitnehmer die Datenbearbeitung verstehen, was individuell verschiedene Massnahmen bedingen kann.¹⁴⁹⁹ Das Prinzip der Richtigkeit darf nicht zu einer derart hohen Datenqualität führen, dass Persönlichkeitsdurchleuchtungen möglich sind.¹⁵⁰⁰ Die Pflichten zur Datenminimierung, Speicherbegrenzung und Löschung sind auszu-tarieren mit gegenläufigen Vorschriften wie beispielsweise der Pflicht zur Gewährleistung der Datensicherheit, der Auskunftspflicht, dem Diskriminierungs-verbot und dem Schutz der Grundrechte Anderer.¹⁵⁰¹

Auch die Anwendung der Rechtfertigungsgründe veranlasst zu einer sorgfältigen Betrachtung jedes Einzelfalls. Entgegen dem Gesetzeswortlaut kann eine Datenbearbeitung gerechtfertigt werden, selbst wenn sie gegen die Grundsätze des DSG verstösst.¹⁵⁰² Die gesetzliche Vermutung der Zulässigkeit der Bearbeitung allgemein zugänglich gemachter Daten ist im Arbeitsverhältnis relativ leicht widerlegbar.¹⁵⁰³ Zu einer Einwilligung des Arbeitnehmers als Rechtfertigungsgrund sollte höchstens als *ultima ratio* gegriffen werden.¹⁵⁰⁴ Zur Anwendung des Rechtferti-

¹⁴⁹⁵ Siehe S. 135–154.

¹⁴⁹⁶ Siehe S. 167–172.

¹⁴⁹⁷ Siehe S. 177–179.

¹⁴⁹⁸ Siehe S. 184–193.

¹⁴⁹⁹ Siehe S. 202–205.

¹⁵⁰⁰ Siehe S. 206.

¹⁵⁰¹ Siehe S. 206–209.

¹⁵⁰² Siehe S. 213.

¹⁵⁰³ Siehe S. 214–219.

¹⁵⁰⁴ Siehe S. 231–234.

gungsgrunds der überwiegenden Interessen fehlt eine einfache Methode;¹⁵⁰⁵ auch das gesetzlich privilegierte Interesse an der Forschung, Planung und Statistik untersteht strengen Voraussetzungen.¹⁵⁰⁶ Die meisten People Analytics-Projekte können ferner nicht mit generellen gesetzlichen Verpflichtungen gerechtfertigt werden.¹⁵⁰⁷

Es bedarf somit eines hohen Masses an Fachwissen in den Betrieben vor Ort, um die Datenbearbeitungsregeln und Rechtfertigungsgründe im Einzelfall korrekt anzuwenden und geeignete Schutzmassnahmen anzuordnen.¹⁵⁰⁸ Dass sich die Technik und das Recht in diesem Bereich ständig entwickeln, trägt zu den Rechtsunsicherheiten bei.¹⁵⁰⁹ Diese können Unternehmen davon abhalten, People Analytics einzusetzen.¹⁵¹⁰

In der betrieblichen Praxis fehlt das nötige Fachwissen aber oft. Die empirischen Daten des NFP75-Projekts fördern Ungereimtheiten zwischen dem gesetzlichen Ideal und der Umsetzung zu Tage.¹⁵¹¹ Auch kommen Datenskandale vor.¹⁵¹² Insgesamt ist festzuhalten, dass Probleme bei der Umsetzung des Datenschutzrechts durch die Arbeitgeberinnen verbreitet sind.

Das Bedürfnis nach mehr Fachwissen wird ein zentraler Punkt sein bei der späteren Beantwortung der Forschungsfrage. Diese sucht nach den Möglichkeiten, wie eine Neuausrichtung des Datenschutzrechts aussehen könnte, bei welcher die Rechtsdurchsetzung *ex ante* gewährleistet ist.¹⁵¹³ Damit die Arbeitgeberin die Datenschutznormen von vornherein korrekt anwendet, benötigt sie genügend fachli-

¹⁵⁰⁵ Siehe S. 239–240.

¹⁵⁰⁶ Siehe S. 237–239.

¹⁵⁰⁷ Siehe S. 240–242.

¹⁵⁰⁸ PÄRLI 2018, N 17.6; einzelfall- und argumentationsbezogene Betrachtungsweise erforderlich: EGGIMANN, 213; Erfahrung und kritische Distanz erforderlich: GEISER THOMAS / UTTINGER URSULA, Big Data und das Individuum, NZZ vom 14.07.2016, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

¹⁵⁰⁹ Vgl. REINSCH/GOLTZ, 35.

¹⁵¹⁰ Vgl. CULIK, 49, zu deutschen Unternehmen, die wegen des Datenschutzrechts auf People Analytics verzichten. – Die im NFP75-Projekt befragten Schweizer Unternehmen verwenden dagegen mehrheitlich People Analytics (siehe S. 60). In der Schweiz bestehen im Vergleich zum EU-Raum geringere datenschutzrechtliche Sanktionsrisiken (siehe S. 275, 278 und 348–350).

¹⁵¹¹ Siehe S. 242–246.

¹⁵¹² Siehe S. 246–247.

¹⁵¹³ Siehe S. 11.

che Ressourcen, die sie etwa durch die Anstellung eines Datenschutzberaters und durch Schulungen ihres Personals erlangt. Auch sollte sie die möglichen Folgen der Datenbearbeitungen frühzeitig abschätzen und jederzeit in der Lage sein, Rechenschaft über ihre Bearbeitungstätigkeiten abzulegen.¹⁵¹⁴

¹⁵¹⁴ Siehe später zu den verschiedenen Professionalisierungsvorschlägen S. 319–344.

6 Rechtsdurchsetzung

6.1 Übersicht: Individualrechtsschutz und weitere Rechtsbehelfe

Im vorhergehenden Kapitel 5 wurde festgestellt, dass für eine korrekte Anwendung des DSG ein hohes Mass an Fachwissen vorausgesetzt wird, das in den Betrieben jedoch nicht überall vorhanden ist, weswegen Datenschutzverstösse in der Praxis nicht selten vorkommen. Es besteht ein Problem bei der arbeitgeberseitigen Umsetzung des Datenschutzrechts bei People Analytics. Um dieser Tendenz entgegenzuwirken, ist zu prüfen, mit welchen Kontrollinstrumenten die Gegenseite auf die Rechtsdurchsetzung hinwirken kann. Einerseits kommen individualrechtliche Klagen infrage, andererseits sind auch kollektive Instrumente der Rechtsdurchsetzung zu prüfen.

Das DSG stellt für die Durchsetzung des privatrechtlichen Datenschutzes zu einem wesentlichen Teil auf die individuell betroffenen Arbeitnehmer ab. Sie sind zunächst berufen, den Datenschutz *ex ante* zu steuern, indem sie ihre Einwilligung erteilen, beschränken oder verweigern (vgl. Art. 13 Abs. 1 DSG, Art. 27 Abs. 1 E-DSG, Art. 31 Abs. 1 rev-DSG).¹⁵¹⁵ Sie müssen aber auch *ex post*, im Nachgang einer Datenschutzverletzung, ihre Rechtsansprüche mittels zivilrechtlicher Klage zum Schutz der Persönlichkeit durchsetzen (vgl. Art. 15 Abs. 1 DSG bzw. Art. 28 Abs. 2 E-DSG bzw. Art. 32 Abs. 2 rev-DSG i.V.m. Art. 28 ZGB). Der Datenschutz ist hier mehr oder weniger dem zivilrechtlichen Persönlichkeitsschutz gemäss Art. 28 ZGB gleichgestellt. Der Grund dafür ist darin zu finden, dass der Gesetzgeber im Jahr 1992 bei Erlass des DSG bzgl. der Datenbearbeitung durch Private (noch) keine ähnlichen Risiken wie in der staatlichen Datenbearbeitung eruiert hat.¹⁵¹⁶ Als Folge davon kommt der Datenschutz im privatrechtlichen Bereich im Konzept des DSG faktisch als rein individuelles Anliegen zum Tragen.¹⁵¹⁷

¹⁵¹⁵ BAERISWYL 2010, 145.

¹⁵¹⁶ BAERISWYL 2010, 140. Im öffentlich-rechtlichen Bereich wirkt auch der Gesetzgeber aktiv auf die Durchsetzung des Datenschutzrechts hin. Dies zeigt sich darin, dass für Datenbearbeitungen durch Bundesorgane – anders als für Datenbearbeitungen durch Private – zum Vornherein eine gesetzliche Grundlage erforderlich ist (Art. 17 Abs. 1 DSG, Art. 30 Abs. 1 E-DSG, Art. 34 Abs. 1 rev-DSG).

¹⁵¹⁷ BAERISWYL 2010, 145.

Im Grundsatz verfolgt das DSG einen «eindimensionalen» Ansatz.¹⁵¹⁸ Auch die Datenschutz-Rechtsordnungen der EU und der USA weisen eine «atomistische» Struktur auf,¹⁵¹⁹ indem sie primär die Individualrechte schützen und sich weitgehend auf das Zweipersonenverhältnis zwischen der betroffenen und der verantwortlichen Person konzentrieren.¹⁵²⁰

Im Folgenden ist zunächst zu untersuchen, inwieweit die Individualklage zur Durchsetzung des Datenschutzrechts im privatrechtlichen Umfeld taugt. Nach der hier vertretenen Ansicht besteht keine Möglichkeit zur effizienten Kontrolle der Einhaltung des Datenschutzes durch die betroffenen Arbeitnehmer. Die Defizite sind sogleich zu erläutern.¹⁵²¹

Wegen der Mängel der Individualklage ist anschliessend zu fragen, ob das Rechtssystem dem Individuum Verbündete zur Seite stellen kann, die es bei der Rechtsdurchsetzung (indirekt) unterstützen könnten. Würden Dritt- oder öffentliche Interessen einfließen, die sich mit den Individualinteressen teilweise überschneiden,¹⁵²² so könnte der unzureichende Individualrechtsschutz zu einem gewissen Grad kompensiert werden. Der EDÖB könnte allenfalls im Interesse von Gruppen wirken, weil er insbesondere einschreitet, wenn eine grössere Anzahl von Personen betroffen ist (vgl. Art. 29 Abs. 1 lit. a DSG). Zu suchen ist auch nach datenschutzentfernteren Steuerungsansätzen, insbesondere in den Rechtsgebieten, die in Kapitel 4 über die relevanten Rechtsbestimmungen genannt worden sind:¹⁵²³ Anzuschauen sind somit die ArG-Aufsicht, das Strafrecht, das Mitwirkungsrecht, das Gesellschaftsrecht sowie die arbeitsrechtlichen Mittel der Arbeitsverweigerung, des Streiks und der Kündigung (dazu Unterkapitel 6.3–6.8, S. 275–291).

¹⁵¹⁸ PASSADELIS NICOLAS, Am überkommenen Primat der informationellen Selbstbestimmung festzuhalten, bedeutet, noch mehr wertvolle Zeit zu verlieren, NZZ vom 17.05.2017, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

¹⁵¹⁹ Zur EU: HORNING, 92; «atomistic, individual-oriented understanding of privacy» in den USA und Europa: BAMBERGER/MULLIGAN 2015, 22.

¹⁵²⁰ Bzgl. der DSGVO: HORNING, 92, und DREYER/SCHULZ, 39. Das Datenschutzrecht gehe «von überschaubaren Konstellationen aus: hier die betroffene Person als Individuum, dort der Verantwortliche»: HORNING, 91. Bzgl. des amerikanischen Rechts: WALDMAN, 70; «one-on-one interaction between the data controller and the individual»: SPRAGUE 2015, 14.

¹⁵²¹ Dazu nachfolgend S. 256–258 und 263–274.

¹⁵²² Vgl. S. 235.

¹⁵²³ Siehe S. 107.

6.2 Zivilrechtliche Individualklagen

6.2.1 Zivilrechtliche Ansprüche der Arbeitnehmer

Der Arbeitnehmer kann bei unrechtmässigem Betrieb von People Analytics die arbeitsvertraglichen Ansprüche aus einer Verletzung der Fürsorgepflicht (Art. 328 OR) geltend machen.¹⁵²⁴ Zunächst kommt ein Anspruch auf Schadenersatz (Art. 97 Abs. 1 i.V.m. Art. 328 OR) infrage. Führt People Analytics beispielsweise zu einer erheblichen Beeinträchtigung der psychischen Integrität und zur Arbeitsunfähigkeit, so kann der Schaden in einer Lohneinbusse bestehen.¹⁵²⁵ Bei einer schweren Persönlichkeitsverletzung, die nicht anders wiedergutmachtet worden ist, besteht ein Anspruch auf Genugtuung (Art. 49 Abs. 1 i.V.m. Art. 99 Abs. 3 i.V.m. Art. 328b OR). Denkbar ist ferner eine Konventionalstrafe, falls die Parteien eine solche vereinbart haben (vgl. Art. 160 OR).¹⁵²⁶ Die Arbeitgeberin haftet für den Schaden, den ihre Hilfsperson oder andere Arbeitnehmer in Ausübung ihrer Verrichtungen verursachen (Art. 97 Abs. 1 i.V.m. Art. 101 Abs. 1 OR).

Das öffentlich-rechtliche Arbeitnehmerschutzrecht kann zivilrechtliche Ansprüche vermitteln: Wenn Vorschriften des Bundes oder der Kantone über die Arbeit der Arbeitgeberin oder dem Arbeitnehmer eine öffentlich-rechtliche Verpflichtung auferlegen und die Verpflichtung Inhalt des Einzelarbeitsvertrags sein könnte, so steht der jeweils anderen Vertragspartei ein zivilrechtlicher Anspruch auf Erfüllung zu (Art. 342 Abs. 2 OR). Der Arbeitnehmer kann auf diesem Weg beispielsweise verlangen, dass ein Überwachungssystem mit gesundheitsschädigenden Auswirkungen abgeschaltet werde (vgl. Art. 6 ArG, Art. 26 ArGV 3).¹⁵²⁷

Kumulativ zu den vertraglichen kann der Arbeitnehmer ausservertragliche Ansprüche geltend machen.¹⁵²⁸ Vorderhand ist an die Ansprüche aufgrund einer Persönlichkeitsverletzung durch eine unzulässige Datenbearbeitung zu denken (Art. 15 Abs. 1 Satz 1 DSG i.V.m. Art. 28 und Art. 28a ZGB; Art. 28 Abs. 2

¹⁵²⁴ Das Haftungsrisiko aus Art. 328 Abs. 2 OR bleibt bestehen, selbst wenn die Arbeitgeberin die Arbeitnehmer für die Gesundheitsvorsorge korrekt angehört hat (Art. 6 ArGV 3); KUKO ArG-NÖTZLI, Art. 6 ArG, N 15.

¹⁵²⁵ WOLFER, N 590.

¹⁵²⁶ ROSENTHAL 2015, N 7.7.

¹⁵²⁷ Vgl. KUKO ArG-NÖTZLI, Art. 6 ArG, N 13. Vgl. WOLFER, N 58.

¹⁵²⁸ WYLER, 253.

Satz 1 E-DSG, Art. 32 Abs. 2 Satz 1 rev-DSG).¹⁵²⁹ Mit der Klage auf Unterlassung einer drohenden Verletzung (Art. 28a Abs. 1 Ziff. 1 ZGB) kann der Arbeitnehmer beispielsweise die Sperrung der Datenbearbeitung verlangen oder dass keine Daten an Dritte bekanntgegeben werden (Art. 15 Abs. 1 Satz 2 DSG, Art. 28 Abs. 2 lit. a–c E-DSG, Art. 32 Abs. 2 lit. a–c rev-DSG), gegebenenfalls unter Anordnung vorsorglicher Massnahmen (Art. 261 ff. ZPO). Der Arbeitnehmer kann die Beseitigung einer bestehenden Verletzung verlangen (Art. 28a Abs. 1 Ziff. 2 ZGB), was durch die Vernichtung der Daten geschehen kann (Art. 15 Abs. 1 Satz 2 DSG, Art. 28 Abs. 2 lit. c E-DSG, Art. 32 Abs. 2 lit. c rev-DSG). Der Anspruch auf Feststellung der Widerrechtlichkeit einer Verletzung besteht dann, wenn sich diese weiterhin störend auswirkt (Art. 28a Abs. 1 Ziff. 3 ZGB). Auch die Berichtigung der Daten (Art. 28a Abs. 2 ZGB; Art. 15 Abs. 1 Satz 2 DSG) und die Mitteilung des Urteils an Dritte oder die Veröffentlichung des Urteils (Art. 28a Abs. 2 ZGB, Art. 28 Abs. 4 E-DSG, Art. 32 Abs. 4 rev-DSG) können verlangt werden. Neben diesen spezifischen Rechtsbehelfen des Persönlichkeitsschutzes sind allgemeine vermögensrechtliche Ansprüche möglich (Art. 28a Abs. 3 ZGB: Schadenersatz, Genugtuung, Gewinnherausgabe nach den Bestimmungen über die Geschäftsführung ohne Auftrag), die der Arbeitnehmer auf vertraglicher Basis geltend machen muss.

Unter dem europäischen Datenschutzrecht hat jede Person, der wegen eines Verstosses gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegenüber dem Verantwortlichen oder dem Auftragsbearbeiter (Art. 82 Abs. 1 DSGVO).

6.2.2 Persönlichkeitsschutz als Abwehrrecht (*privacy-as-secrecy*)

a) Abwehrrecht im Zivilgesetzbuch

Es bestehen Schwierigkeiten, die Ansprüche des Arbeitnehmers auf dem Weg der Individualklage durchzusetzen. Dies begründet sich zunächst mit der Konzeption des Persönlichkeitsschutzes als Abwehrrecht. Der schweizerische zivilrechtliche Persönlichkeitsschutz (Art. 28 ZGB) ist ein Abwehrrecht, das den Schutz vor Eingriffen Dritter bezweckt. Der Persönlichkeitsschutz vermittelt keinen Entfaltungs-

¹⁵²⁹ Das DSG ergänzt in privatrechtlicher Hinsicht den allgemeinen Persönlichkeitsschutz (Art. 28 ff. ZGB) und ist nicht *lex specialis* dazu: WOLFER, N 29.

anspruch; die Nutzung der Persönlichkeitsattribute steht nicht im Vordergrund.¹⁵³⁰ Somit wirkt das Persönlichkeitsrecht negativ, repressiv und defensiv.¹⁵³¹

b) Geheimsphäreschutz im Common Law

Zur Illustration des Abwehrcharakters des Persönlichkeitsschutzes dient ein Vergleich mit dem amerikanischen Common Law. Dort lautet die Leitidee, dass Probleme rund um Personendaten letztlich die Geheimhaltung von persönlicher Information betreffen (*privacy-as-secrecy*).¹⁵³² Das Recht auf Privatsphäre schützt das Interesse, in Ruhe gelassen zu werden (*right to be let alone*).¹⁵³³ Darunter sind vier konkretisierbare Teilinteressen zu verstehen: Schutz vor verletzendem Eindringen in die Zurückgezogenheit oder die privaten Angelegenheiten (*intrusion upon seclusion*), Schutz vor Veröffentlichung peinlicher privater Tatsachen (*public disclosure*), Schutz vor Publizität, die einen in den Augen der Öffentlichkeit in ein falsches Licht rückt (*publicity*), und Schutz vor unrechtmässiger Aneignung des Namens oder der Identität (*appropriation of name or likeness*).¹⁵³⁴

Eine konkrete technische Umsetzung des Privatsphäreschutzes durch Geheimhaltung des Common Law besteht darin, Information gegenüber den Datenbearbeitern zu verschleiern. Die Verschleierung (*obfuscation*) soll durch absichtliches Verheimlichen von Information vor der Überwachungswirtschaft und durch das Einspeisen von fehlerhaften, unbrauchbaren Daten in die Analysesysteme gelingen.¹⁵³⁵ Eine Verschleierungstaktik behindert jedoch den Informationsfluss, der für die Informationswirtschaft essenziell ist, und kann somit «höchstens die zweit-

¹⁵³⁰ AEBI-MÜLLER, N 20.

¹⁵³¹ AEBI-MÜLLER, N 20.

¹⁵³² PURTOVA 2011, 255. Vgl. die Definition von *privacy* als Recht, Informationen über einen selbst zurückzuhalten: RULE, 3. Das Paradigma des Geheimnisschutzes komme vom Schutz der Geschäftsgeheimnisse; demnach könnten nur Geheimnisse rechtlich geschützt werden; einmal veröffentlichte Information sei «Freiwild» der Öffentlichkeit: PELTZ-STEELE, 407.

¹⁵³³ WARREN/BRANDEIS, 205.

¹⁵³⁴ PROSSER, 389; DETERMANN/SPRAGUE, 990; OTTO 2016, 5; Recht auf Privatsphäre bestehend aus den zwei Delikten *publicity* und *intrusion into the seclusion*: FINKIN, xxxiii–xxxiv. Die Voraussetzungen für das Delikt *intrusion upon seclusion* sind einerseits beim Verletzten eine begründete Erwartung von Privatsphäre, andererseits der Umstand, dass das Eindringen für eine vernünftige Person sehr verletzend ist: RIEDY/WEN, 92.

¹⁵³⁵ RICHARDS/HARTZOG 2017, 1186.

beste Lösung» zur Gewährleistung der Privatsphäre darstellen.¹⁵³⁶ Insgesamt ist der Schutz der Privatsphäre im amerikanischen Verfassungsrecht im Vergleich zum europäischen Datenschutzrecht schwach ausgebildet.¹⁵³⁷

c) Sphärentheorie in der bundesgerichtlichen Rechtsprechung

Zur Beurteilung, ob eine Information vor Einblicken geschützt werden soll, unterteilt das Bundesgericht das gesamte Leben eines Menschen in die drei Bereiche Geheim-, Privat- und Gemeinsphäre (sog. Drei-Sphären-Theorie oder Sphärentheorie).¹⁵³⁸ Demnach sind der Geheim- (oder Intim-)Sphäre Tatsachen zuzuordnen, die niemandem oder nur ganz bestimmten Personen zugänglich sein sollen. Zur Privatsphäre im Sinne der Sphärentheorie gehören Tatsachen, die nur einem bestimmten, nahe verbundenen Personenkreis zugänglich sein sollen. Die Gemein- (oder Öffentlichkeits-)Sphäre umfasst Tatsachen, die sich an allgemein zugänglichen Orten abspielen oder denen die betroffene Person eine gewisse Publizität verleiht.¹⁵³⁹ In der Schweiz wurde die Sphärentheorie, der deutschen Lehre entstammend, soweit ersichtlich, durch JÄGGI im Jahr 1960 und ausschliesslich im Zusammenhang mit Persönlichkeitsverletzungen durch personenbezogene Informationen eingeführt.¹⁵⁴⁰

d) Ungenügen der Sphärentheorie

Die Sphärentheorie wird kritisiert, weil sie mit der Gemeinsphäre einen vollständig ungeschützten Bereich aussondert, dies in Abweichung von der Doktrin und Praxis vor Einführung der Sphärentheorie.¹⁵⁴¹ Die Persönlichkeit bedarf des Schutzes, auch wenn sie den Privatbereich verlässt und sich in die Öffentlichkeit

¹⁵³⁶ RICHARDS/HARTZOG 2017, 1184.

¹⁵³⁷ PELTZ-STEELE, 368; US-Abwehrrechte dem europäischen Datenschutzrecht deutlich unterlegen: PURTOVA 2011, 255.

¹⁵³⁸ Sphärentheorie erstmals explizit angewendet in: BGE 97 II 97 E. 3; später ebenfalls explizit etwa: Urteil BGer 5A_195/2016 vom 04.07.2016 E. 5.1.

¹⁵³⁹ WOLFER, N 111–113.

¹⁵⁴⁰ JÄGGI, 226a–227a; AEBI-MÜLLER, N 513, m.w.H.; Sphärentheorie in der Schweiz erstmals Mitte des 20. Jh. vertreten: WOLFER, N 110. Vor Einführung der Sphärentheorie kannten die schweizerische Rechtsprechung und Lehre keine eigentliche Theorie der informationellen Privatheit: AEBI-MÜLLER, N 842.

¹⁵⁴¹ AEBI-MÜLLER, N 843; BSK DSG-MAURER-LAMBROU/KUNZ, Art. 1 DSG, N 14.

begibt.¹⁵⁴² Die Sphärentheorie unterschätzt die Bedeutung der Öffentlichkeit und der sozialen Interaktion für das Individuum.¹⁵⁴³ Dass die Gemeinsphäre ohne Schutz bleibt, lässt sich mit Blick auf die deutsche Herkunft der Sphärentheorie nachvollziehen: In Deutschland leitet sich das allgemeine Persönlichkeitsrecht aus dem Verfassungsrecht ab (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und ist im Sinne einer allgemeinen Handlungsfreiheit ausserordentlich weit gefasst. Somit stellt sich dort unweigerlich die Frage nach einer vernünftigen Begrenzung dieses Rechts, womit die Sphärentheorie auf fruchtbaren Boden fällt.¹⁵⁴⁴ Demgegenüber wurzelt der Persönlichkeitsschutz in der Schweiz im Privatrecht (Art. 27 ff. ZGB). Für die Schweiz eignet sich jedenfalls im privatrechtlichen Bereich eine Rezeption der Sphärentheorie nur beschränkt und nicht mit dem deutschen umfassenden, auf den gesamten Bereich der Persönlichkeit bezogenen Gehalt.¹⁵⁴⁵ Der schweizerische Gesetzgeber hat die Schutzlücke, die sich durch die Erfindung der Gemeinsphäre ergibt, mit dem Erlass des DSG und den darin aufgestellten, immer geltenden Datenbearbeitungsgrundsätzen teilweise wieder geschlossen.¹⁵⁴⁶

Die Sphärentheorie bietet des Weiteren keine allgemeingültige Abgrenzung der Privatsphäre im Sinne der Sphärentheorie: Der Arbeitsplatz zählt zur Privatsphäre im Sinne der Sphärentheorie.¹⁵⁴⁷ Angesichts der ubiquitären Datenerfassungen und der Tendenz zum Arbeiten aus dem Homeoffice verschwimmt aber die Trennlinie zwischen dem Büro und dem Zuhause und somit zwischen Privat- und Geheimsphäre.¹⁵⁴⁸ Auch ist die Privatsphäre, wie bereits besprochen, je nach Person verschieden:¹⁵⁴⁹ Eine identische Tatsache kann für einen Menschen in den Privatbereich, für einen anderen in die Geheimsphäre fallen.¹⁵⁵⁰

¹⁵⁴² AEBI-MÜLLER, N 538. Vgl. JÄGGLI, 228a: Die erhöhte technische Macht müsse ausgeglichen werden, indem die Privatsphäre im Sinne der Sphärentheorie zulasten der Gemeinsphäre ausgedehnt werde. Vgl. BBl 1997 I, 152.

¹⁵⁴³ AEBI-MÜLLER, N 533.

¹⁵⁴⁴ AEBI-MÜLLER, N 466.

¹⁵⁴⁵ AEBI-MÜLLER, N 513.

¹⁵⁴⁶ WOLFER, N 121. Vgl. ROSSNAGEL, 280: Datenschutzrechtliche Bearbeitungsregeln seien permanent zu beachten.

¹⁵⁴⁷ WOLFER, N 115.

¹⁵⁴⁸ CUSTERS/URSIC, 324. Siehe S. 69 und 71.

¹⁵⁴⁹ Siehe S. 85–86.

¹⁵⁵⁰ BSK DSG-MAURER-LAMBROU/KUNZ, Art. 1 DSG, N 14.

Schwierigkeiten bereitet die Sphärentheorie auch, weil selbst hinsichtlich Tatsachen der Geheimsphäre stets ein überwiegendes Interesse Dritter bestehen kann. Zu denken ist etwa an das Recht auf Kenntnis der eigenen Abstammung, das die Aufdeckung intimster Sachverhalte aus dem Sexualleben der Eltern bedingt.¹⁵⁵¹

Das Hauptproblem der Sphärentheorie besteht somit darin, dass die Einordnung in eine bestimmte Persönlichkeitssphäre keine Hilfe leistet, um über die Rechtswidrigkeit des Eingriffs zu entscheiden. Für die Feststellung der Widerrechtlichkeit ist immer eine Abwägung zwischen dem Geheimhaltungs- und dem Informationszugriffs-Interesse erforderlich.¹⁵⁵² Es braucht Kriterien, um zu beurteilen, ob ein Privatsphäreneingriff schwerer oder weniger schwer wiegt.¹⁵⁵³ Aus all diesen Gründen wird geltend gemacht, dass die Sphärentheorie im DSG nicht anwendbar sein soll.¹⁵⁵⁴

6.2.3 Persönlichkeitsschutz durch informationelle Selbstbestimmung (*privacy-as-control*)

a) Deutsches Konzept der informationellen Selbstbestimmung

Das Ungenügen der Sphärentheorie verlangte nach einer inhaltlich «radikal» neuen Betrachtungsweise des Privaten.¹⁵⁵⁵ Dies war die Stunde des Konzepts der informationellen Selbstbestimmung (im angelsächsischen Rechtsraum häufig als *privacy-as-control* bezeichnet).¹⁵⁵⁶ Mit der informationellen Selbstbestimmung im Zentrum verpufft die unter der Sphärentheorie begründete schutzlose Gemeinsphäre vollständig: Grundsätzlich können keine Daten mehr unabhängig vom Willen des Betroffenen bearbeitet werden.¹⁵⁵⁷ Nach dem Konzept der informationellen Selbstbestimmung ist Schutzobjekt nicht eine Geheimsphäre, sondern die

¹⁵⁵¹ AEBI-MÜLLER, N 529.

¹⁵⁵² HÄRTING, N 433. Der Ansatz der Sphärentheorie ist daher «gescheitert»: AEBI-MÜLLER, N 529.

¹⁵⁵³ WOLFER, N 119.

¹⁵⁵⁴ BSK DSG-MAURER-LAMBROU/KUNZ, Art. 1 DSG, N 14.

¹⁵⁵⁵ AEBI-MÜLLER, N 591. Siehe zur Kritik an der Sphärentheorie S. 256.

¹⁵⁵⁶ Für die USA: «*privacy-as-control*» (VEALE *et al.*, 105) und «*privacy [...] is the control*» (SPRAGUE 2015, 1). Arbeitnehmer gäben umso mehr Daten über sich preis, je mehr informationelle Kontrolle sie darüber hätten: SHOOK *et al.* – Für Kanada: «*exercise control over [...] their personal data*» (CAVOUKIAN 2014, 176).

¹⁵⁵⁷ AEBI-MÜLLER, N 611.

informationelle Selbstbestimmung, ein Teil der Autonomie des Menschen.¹⁵⁵⁸ Die Geheimsphäre ist demnach nicht ein Rechtsgut, sondern bloss die Folge dessen, dass eine Person gewisse Sachverhalte geheim halten will und darf.¹⁵⁵⁹

Das Konzept der informationellen Selbstbestimmung ist in Deutschland entwickelt worden.¹⁵⁶⁰ Das Bundesverfassungsgericht hat das Recht auf informationelle Selbstbestimmung im Volkszählungsurteil vom 15.12.1983 erstmals in aller Deutlichkeit formuliert.¹⁵⁶¹ Das Grundrecht der informationellen Selbstbestimmung (abgeleitet aus dem allgemeinen Persönlichkeitsrecht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.¹⁵⁶² Das Recht auf informationelle Selbstbestimmung hat seither in Deutschland eine Vorrangstellung erlangt, hinter der die allgemeinen Datenschutzprinzipien zurückstehen.¹⁵⁶³

Im Volkszählungsurteil hat das Bundesverfassungsgericht das allgemeine Persönlichkeitsrecht rechtsdogmatisch aus dem Grundgesetz und somit aus dem öffentlich-rechtlichen Verfassungsrecht abgeleitet. Dies ergibt eine besondere Nähe zum grundrechtlichen Persönlichkeitsschutz.¹⁵⁶⁴ Trotzdem orientieren sich auch private deutsche Unternehmen wegen der mittelbaren Drittwirkung der Grundrechte an den Grundsätzen, die das Bundesverfassungsgericht 1983 aufgestellt hat.¹⁵⁶⁵

Der grundrechtliche Persönlichkeitsschutz in Deutschland geht von der allgemeinen Handlungsfreiheit aus.¹⁵⁶⁶ Die deutsche Rechtsprechung legt den grundrechtlichen Entfaltungsschutz extensiv aus, sodass «jedes menschliche Verhalten»

¹⁵⁵⁸ RUDIN 2004b, 421; RUDIN 2007, 25.

¹⁵⁵⁹ DRUEY 1995, 253. Unklar ist, was im Zentrum der Sphärentheorie steht, ob sich die Sphären um die Tatsache des Geheimseins oder um den Willen nach Kontrolle bilden: DRUEY 1995, 354 und 356.

¹⁵⁶⁰ Siehe S. 257. CAVOUKIAN 2013, 9.

¹⁵⁶¹ Urteil Bundesverfassungsgericht [Deutschland] 1 BvR 209/83 vom 15.12.1983; CAVOUKIAN 2011, 6.

¹⁵⁶² Urteil Bundesverfassungsgericht [Deutschland] 1 BvR 209/83 vom 15.12.1983 N 147; so auch die jüngere Rechtsprechung: Urteil Bundesverfassungsgericht [Deutschland] 1 BvR 3309/13 vom 19.04.2016 N 56.

¹⁵⁶³ Datensparsamkeit und Zweckbindung treten zurück: BAUMANN MAX-OTTO, 6.

¹⁵⁶⁴ AEBI-MÜLLER, N 465.

¹⁵⁶⁵ WYBITUL/SCHULTZE-MELLING, N 9; private Arbeitgeber indirekt gebunden: GASCHER, 128.

¹⁵⁶⁶ BeckOK GG-LANG, Art. 2 GG, N 1; ErfK-SCHMIDT, Art. 2 GG, N 1.

geschützt wird, «ohne Rücksicht darauf, welches Gewicht ihm für die Persönlichkeitsentfaltung zukommt».¹⁵⁶⁷ Geschützt werden soll der Selbstbestimmungswille, unabhängig davon, ob die Respektierung dieses Willens im konkreten Fall für die Persönlichkeitsentfaltung wesentlich ist.¹⁵⁶⁸ Das Recht auf informationelle Selbstbestimmung ist somit «nichts anderes als eine Neufassung der allgemeinen Handlungsfreiheit unter den Bedingungen der modernen Datenverarbeitung».¹⁵⁶⁹

b) Schweizerische Rezeption der informationellen Selbstbestimmung

Das schweizerische Recht hat den der deutschen Lehre und Rechtsprechung entstammenden Schutz des informationellen Selbstbestimmungsrechts rezipiert.¹⁵⁷⁰ Dies ergibt sich aus dem DSG, auch wenn der Begriff der informationellen Selbstbestimmung darin fehlt:¹⁵⁷¹ Eine widerrechtliche Persönlichkeitsverletzung liegt immer vor, wenn jemand Daten einer Person gegen deren ausdrücklichen Willen ohne Rechtfertigungsgrund bearbeitet (Art. 12 Abs. 2 lit. b DSG, Art. 26 Abs. 2 lit. b E-DSG, Art. 30 Abs. 2 lit. b rev-DSG). Zudem kann die betroffene Person die Bearbeitung ihrer Daten selbst dann untersagen, wenn sie sie zuvor allgemein zugänglich gemacht hat (Art. 12 Abs. 3 DSG, Art. 26 Abs. 3 E-DSG, Art. 30 Abs. 3 rev-DSG *e contrario*). Das Bundesgericht hat bereits 1987 anerkannt, dass das damals noch ungeschriebene Grundrecht der persönlichen Freiheit punktuell auch Schutz vor unbefugtem Bearbeiten von personenbezogenen Daten bietet.¹⁵⁷² Der Ausdruck «informationelle Selbstbestimmung» taucht erstmals 1994 in einem

¹⁵⁶⁷ Urteil Bundesverfassungsgericht [Deutschland] 1 BvR 2007/10 vom 21.12.2011 N 17. Z.B. schliesst die Handlungsfreiheit sogar das Füttern von Tauben ein. Da dies jedoch nicht zum absolut geschützten Kern privater Lebensgestaltung gehört, kann ein städtisches Fütterungsverbot zulässig sein: Urteil Bundesverfassungsgericht [Deutschland] 2 BvR 854/79 vom 23.05.1980 E. 2d; ErfK-SCHMIDT, Art. 2 GG, N 1.

¹⁵⁶⁸ AEBI-MÜLLER, N 596.

¹⁵⁶⁹ GÄCHTER/EGLI, N 24.

¹⁵⁷⁰ Vgl. AEBI-MÜLLER, N 546.

¹⁵⁷¹ AEBI-MÜLLER, N 592; WOLFER, N 137.

¹⁵⁷² Unter expliziter Bezugnahme auf das Zensus-Urteil des deutschen Bundesverfassungsgerichts: BGE 113 Ia 1 E. 4b/bb; BGE 113 Ia 257 E. 3c; persönliche Freiheit 1963 erstmals durch die Rechtsprechung als ungeschriebenes Grundrecht anerkannt: RUDIN 2004b, 417.

veröffentlichten Bundesgerichtsurteil auf, in dem ein Recht des Arbeitnehmers auf Einsicht in seine Personalakte aus Art. 328 OR abgeleitet wurde.¹⁵⁷³

Das Bundesgericht zeigte jedoch eine gewisse Zurückhaltung in der Anerkennung eines informationellen Selbstbestimmungsrechts und verneinte 1998 ein «generelles Recht [...], jederzeit zu wissen, wer was über [einen] weiss».¹⁵⁷⁴ Auch das von der informationellen Selbstbestimmung hergeleitete Einsichtsrecht des Arbeitnehmers versteht das Bundesgericht nicht als umfassend. Das Einsichtsrecht hat lediglich instrumentalen Charakter für den Fall, dass die in der Personalakte vorhandenen Angaben die Persönlichkeitsrechte des Arbeitnehmers verletzen, weil sie falsch sind oder keinen Bezug zum Arbeitsverhältnis haben.¹⁵⁷⁵ Es wird ein berechtigtes Interesse an der Einsichtnahme vorausgesetzt.¹⁵⁷⁶ Das Bundesgericht gewährt dem Arbeitnehmer keinen unbedingten Anspruch auf Einsicht in sämtliche Dokumente über Geschäftsvorgänge der Arbeitgeberin, an denen der Arbeitnehmer in irgendeiner Weise beteiligt war.¹⁵⁷⁷ Die Arbeitgeberin muss keine Auskunft über interne Dokumente zur Willensbildung erteilen, wie beispielsweise E-Mails zwischen Vorgesetzten.¹⁵⁷⁸ Ausserdem ist das DSG und damit auch das Auskunftsrecht nicht anwendbar auf Personendaten, die eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet und nicht an Aussenstehende bekannt gibt (Art. 2 Abs. 2 lit. a DSG, vgl. Art. 2 Abs. 2 lit. a E-DSG, vgl. Art. 2 Abs. 2 lit. a rev-DSG). Hierunter sind etwa persönliche Notizen eines Vorgesetzten als Gedächtnisstütze für ein Mitarbeitergespräch zu subsumieren.¹⁵⁷⁹ Im Übrigen besteht von Gesetzes wegen kein Anspruch des Arbeitnehmers auf physische Einsichtnahme vor Ort in das Original der Personalakte (vgl. Art. 3 Satz 1 VD SG).¹⁵⁸⁰ In der Regel genügt eine schriftliche Auskunftserteilung in der Form eines Ausdrucks oder einer Fotokopie (Art. 8 Abs. 5 Satz 1 DSG).

¹⁵⁷³ BGE 120 II 118 E. 3a; RUDIN 2004b, 418.

¹⁵⁷⁴ Dieser Entscheid betraf einen öffentlich-rechtlichen Sachverhalt: BGE 124 I 176 E. 6a. Mit Hinweisen auf Widersprüche in der Rechtsprechung: GÄCHTER/EGLI, N 29.

¹⁵⁷⁵ BGE 120 II 118 E. 3b; AEBI-MÜLLER, N 593.

¹⁵⁷⁶ BGE 120 II 118 E. 3c.

¹⁵⁷⁷ BGE 120 II 118 E. 3b.

¹⁵⁷⁸ Urteil BGer 8C_467/2013 vom 21.11.2013 E. 3.2; RUDOLPH, 1680.

¹⁵⁷⁹ RUDOLPH, 1679.

¹⁵⁸⁰ RUDOLPH, 1675, m.w.H. Die Bundesversammlung hat ein vom Bundesrat vorgeschlagenes (BBi 1988 II, 489) explizites Einsichtsrecht des Arbeitnehmers als Ergänzung zum Auskunftsrecht des DSG abgelehnt: AB SR 1990, 162, und AB NR 1991, 979.

Die Einschränkung des Rechts auf informationelle Selbstbestimmung im Fall des Einsichtsrechts des Arbeitnehmers in die Personalakte vermag zu erstaunen angesichts des Umstands, dass der Arbeitnehmer in einem persönlichkeitsrechtlich besonders schutzbedürftigen Sonderverhältnis zur Arbeitgeberin steht.¹⁵⁸¹ Die limitierte Geltung des Rechts auf informationelle Selbstbestimmung in der Schweiz lässt sich aber mit Blick auf dessen geschichtliche Entwicklung und systematische Einordnung in zweifacher Hinsicht erklären: Erstens leitet sich für schweizerische privatrechtliche Arbeitsverhältnisse der Anspruch auf informationelle Selbstbestimmung direkt aus dem privatrechtlichen Persönlichkeitsschutz ab. Die Schweiz war der internationalen Entwicklung weit voraus, als sie 1907 einen umfassenden privatrechtlichen Persönlichkeitsschutz verankerte (Art. 28 ZGB), der nicht nur einzelne, sondern alle wesentlichen Ausprägungen der menschlichen Persönlichkeit schützte.¹⁵⁸² Dieser privatrechtliche Persönlichkeitsschutz ist älter als der grundrechtliche Persönlichkeitsschutz.¹⁵⁸³ Da das schweizerische Recht im Unterschied zum deutschen keine eigentliche Verfassungsgerichtsbarkeit kennt, wird über die verfassungskonforme Gesetzesauslegung von Art. 28 ZGB wie auch über die Einhaltung der grundrechtlichen Kerngehaltsschranke (Art. 36 Abs. 4 BV) im Zivilprozess entschieden. Der zivilrechtliche Persönlichkeitsschutz folgt in der Schweiz eigenen, spezifisch auf das Privatrechtsverhältnis zugeschnittenen Regeln.¹⁵⁸⁴

Zweitens kennt die Schweiz kein Grundrecht der allgemeinen Handlungsfreiheit:¹⁵⁸⁵ Das Grundrecht auf persönliche Freiheit (Art. 10 Abs. 2 BV) schützt nur elementare Erscheinungsformen der Persönlichkeitsentfaltung.¹⁵⁸⁶ Auch das Grundrecht auf Schutz vor Missbrauch der persönlichen Daten (Art. 13 Abs. 2 BV) sieht keine allgemeine Handlungsfreiheit vor, weshalb bei der Übernahme der informationellen Selbstbestimmung in die Schweizer Rechtsordnung Vorsicht

¹⁵⁸¹ AEBI-MÜLLER, N 593.

¹⁵⁸² Dagegen kennt Deutschland den Schutz der «besonderen Persönlichkeitsrechte»: AEBI-MÜLLER, N 10. Der Schweizer Gesetzgeber lehnte jedoch jede, auch nur beispielhafte Aufzählung von geschützten Persönlichkeitsbereichen ausdrücklich ab, um die Rechtsfortbildung nicht zu behindern: AEBI-MÜLLER, N 11.

¹⁵⁸³ Rechtsvergleichende «Pionierstellung» des Art. 28 ZGB: AEBI-MÜLLER, N 464.

¹⁵⁸⁴ AEBI-MÜLLER, N 467.

¹⁵⁸⁵ BELSER 2011a, § 6 N 119.

¹⁵⁸⁶ Ständige Rechtsprechung, statt vieler: BGE 138 IV 13 E. 7.1, BGE 132 I 49 E. 5.2 und BGE 130 I 369 E. 2. GÄCHTER, 184; BELSER 2011a, § 6 N 10.

geboten ist.¹⁵⁸⁷ Dieses Grundrecht ist nicht verhaltensbezogen in dem Sinne, dass die betroffene Person völlig frei handeln oder über etwas, an dem sie Eigentumsrechte hat, nach Belieben verfügen könnte. Der Schutzzweck ist stattdessen informationsorientiert in dem Sinne, dass es auf den Schutz vor allumfassender, unbegrenzter und intransparenter Daten- und Informationsbearbeitung abzielt.¹⁵⁸⁸ Das Grundrecht auf Information und Meinungsbildung (Art. 16 BV) ist grundsätzlich gleichwertig wie der informationelle Selbstbestimmungswille, sodass nicht von vornherein von einem Verfügungsrecht des Betroffenen die Rede sein kann.¹⁵⁸⁹

c) **Zwei Stossrichtungen der Kritik am Recht auf informationelle Selbstbestimmung**

aa) **Übersicht**

Die schweizerische Rezeption des Rechts auf informationelle Selbstbestimmung stösst auf Kritik. Diese zielt in zwei Richtungen: Einerseits wird bemängelt, dass der Einzelne ungeachtet seines Rechtsschutzbedürfnisses jederzeit Datenbearbeitungen untersagen kann (dazu sogleich). Nach der vorliegend vertretenen Auffassung muss andererseits ergänzt werden, dass die heute ubiquitären Datenbearbeitungen die Kontrollressourcen von Einzelpersonen übersteigen, sodass eine Ausübung des Selbstbestimmungsrechts *de facto* unmöglich geworden ist (dazu nachfolgend S. 267–273).

bb) **Informationsverbot infolge ausufernder Kontrollrechte**

AEBI-MÜLLER, RUDIN, GÄCHTER und BELSER kritisieren ein weites Verständnis des informationellen Selbstbestimmungsrechts.¹⁵⁹⁰ Die Erstgenannte stösst sich am «völlig konturlosen» Anspruch, der jedes personenbezogene Datum zum absoluten Recht erhebe und dem begriffsimmanente Schranken fehlten, sodass «praktisch ein Informationsverbot» bestehe.¹⁵⁹¹ Sachverhalte würden als Verletzungstatbestände fingiert, obwohl bei näherem Hinsehen keine (wesentlichen) Beeinträchtigungen der Persönlichkeit vorlägen.¹⁵⁹² Für jeden Verstoss gegen den

¹⁵⁸⁷ AEBI-MÜLLER, N 595. In Deutschland geniesst zudem die Gefühlswelt geringeren Schutz als in der Schweiz: AEBI-MÜLLER, N 476. HAUSHEER/AEBI-MÜLLER, N 12.124.

¹⁵⁸⁸ GÄCHTER, 185. Siehe auch S. 136–138.

¹⁵⁸⁹ AEBI-MÜLLER, N 601.

¹⁵⁹⁰ AEBI-MÜLLER, N 597. RUDIN 1998, 248, warnt vor einem «Verfügungsmonopol», das jegliche Kommunikation verhindern könnte. GÄCHTER, 186; BELSER 2011a, § 6 N 118.

¹⁵⁹¹ AEBI-MÜLLER, N 597.

¹⁵⁹² AEBI-MÜLLER, N 708.

geäusserten Willen der betroffenen Person müsse die Datenbearbeiterin ein rechts-erhebliches und überwiegendes Interesse vorweisen.¹⁵⁹³ RUDIN will den Ausdruck «informationelle Selbstbestimmung» durch denjenigen der «informationellen Integrität» ablösen, um den Eindruck zu verhindern, jedes Individuum würde ein «Verfügungsmonopol» über «seine» Daten besitzen.¹⁵⁹⁴

Die Befürchtung ist berechtigt, dass das Recht auf informationelle Selbstbestimmung zu einem eigentlichen Herrschaftsrecht an den eigenen Daten hochstilisiert werden könnte.¹⁵⁹⁵ Eine derart starke Betonung des Willens der Betroffenen wäre jedoch aus drei Gründen nicht mit dem geltenden Recht vereinbar: Erstens ist persönlichkeitsrechtlich zu berücksichtigen, dass sich die Persönlichkeit in der sozialen Gemeinschaft entfaltet.¹⁵⁹⁶ Somit sind Eingriffe im Rahmen des sozialüblichen Handelns zu dulden, ohne dass eine Anrufung des Persönlichkeitsschutzes (Art. 28 ZGB) möglich ist.¹⁵⁹⁷ Ein Modell, das auf persönlicher Herrschaft über die Daten beruht, stösst spätestens dann an seine praktischen Grenzen, wenn die Daten eine Mehrzahl von Personen betreffen und es unklar ist, wem das Selbstbestimmungsrecht zustehen soll.¹⁵⁹⁸ Zweitens besteht datenschutzrechtlich kaum Raum für ein Herrschaftsrecht an Daten, weil Datenbearbeitungen unter Privaten grundsätzlich zulässig sind.¹⁵⁹⁹ Damit stellt das DSG einen Gegenpol zur DSGVO dar, nach welcher die Datenbearbeitung grundsätzlich verboten ist, ausser einer der abschliessend aufgezählten Rechtfertigungsgründe (Art. 6 Abs. 1 DSGVO) treffe zu (sog. Verbot mit Erlaubnisvorbehalt).¹⁶⁰⁰ Drittens dürfte wegen des ar-

¹⁵⁹³ AEBI-MÜLLER, N 598.

¹⁵⁹⁴ RUDIN 1998, 249; gegen ein Verfügungsmonopol auch BELSER 2011a, § 6 N 118.

¹⁵⁹⁵ Siehe etwa die Aussage von BACHER/DUBOIS, 141: «Die Herrschaft über persönliche Daten ist das zentrale Element der informationellen Selbstbestimmung.»

¹⁵⁹⁶ UTTINGER, 6.

¹⁵⁹⁷ AEBI-MÜLLER, N 379; MEIER PHILIPPE, N 334.

¹⁵⁹⁸ AEBI-MÜLLER, N 603; ebenso White House, Executive Office of the President 2014, 9.

¹⁵⁹⁹ Siehe S. 143. Vorzubehalten ist, dass sich im öffentlich-rechtlichen Bereich die Vorstellung einer Herrschaftsbefugnis über die eigenen Daten eher rechtfertigen lassen könnte als im Privatrecht, weil bei Vorliegen einer entsprechenden gesetzlichen Verpflichtung auch sensible Daten nicht verweigert werden können: AEBI-MÜLLER, N 556.

¹⁶⁰⁰ CUSTERS/URSIC, 333; Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, 26; für Deutschland: PILTZ CARLO, Ihr Arzt muss nicht alles sehen, 28.03.2019, abrufbar unter <www.lto.de> (besucht am 31.05.2020). Das Verbot mit Erlaubnisvorbehalt steht im Konflikt mit der Informations- und Kommunikationsfrei-

beitsrechtlichen Weisungsrechts der Arbeitgeberin (Art. 321d OR) die Ausübung des Rechts auf informationelle Selbstbestimmung im Arbeitsverhältnis faktisch eine begrenzte Tragweite haben.¹⁶⁰¹

Die Idee der Herrschaft an Daten steht derjenigen von Dateneigentum nahe. Ein Eigentumsrecht an Daten ist aber aus drei Gründen ebenfalls abzulehnen:¹⁶⁰² Erstens kann aus sachenrechtlicher Sicht kein Eigentum an Daten bestehen, weil Daten keine Sachen (im Sinne von Art. 641 ZGB) sind. Der Grund dafür liegt in der Nichtrivalität im Konsum von Daten (und nicht etwa in ihrer fehlenden Körperlichkeit).¹⁶⁰³ Zweitens ist persönlichkeitsrechtlich ein Eigentum an Daten unvorstellbar, weil Eigentum veräusserlich ist, Persönlichkeitsrechte aber unveräusserlich sind. Ein kompletter Verkauf der eigenen Persönlichkeitsrechte würde dem persönlichkeitsrechtlichen Verbot der übermässigen Bindung zuwiderlaufen (vgl. Art. 27 ZGB).¹⁶⁰⁴ Zudem besteht Eigentum an Objekten, während der Persönlichkeitsschutz die Eigenschaften von Menschen zum Gegenstand hat.¹⁶⁰⁵ Ferner ge-

heit (vgl. Art. 11 GrCh): HÄRTING, N 96. «Überzeugende Argumente für ein Festhalten am Verbotsprinzip gibt es nicht»: HÄRTING, N 99–100.

¹⁶⁰¹ Vgl. WOLFER, N 214.

¹⁶⁰² Weder das traditionelle Recht auf Privat- und Geheimsphäre noch das neuere Recht auf informationelle Selbstbestimmung können als Parallelordnung zum Eigentum verstanden werden: DRUEY 1995, 101. Vgl. MEIER PHILIPPE, N 18. Auch für den europäischen Rechtsraum wird die Einführung von Eigentumsrechten an Daten verworfen: PURTOVA 2011, 270. A.M. FLÜCKIGER, 864: «*il faut renforcer le droit à l'autodétermination, en particulier dans les relations entre les particuliers [...], en lui conférant un effet direct valable erga omnes qui le fera évoluer vers un droit de propriété sui generis, lui conférant un véritable pouvoir de maîtrise, et non plus de contrôle seulement.*»

¹⁶⁰³ MACCABE, N 18; HOFFMANN-RIEM, 17; Vorrat von Daten unbegrenzt: HOFFMANN-RIEM, 16; unbegrenzte Verteilbarkeit von Information: DRUEY 1995, 33; unbeschränkte Agglomerier- und Teilbarkeit sowie fehlende Einheit von Information: DRUEY 1995, 10; Fahrniseigentum an Energie und flüchtigen Gasen trotz fehlender Körperlichkeit analog möglich: Art. 713 ZGB und BSK ZGB II-SCHWANDER, Art. 713 ZGB, N 6. Das Vertragsrecht könnte mit Eigentumsrechten an Daten umgehen; so werden Daten zum Gegenstand vertraglicher Vereinbarungen gemacht, gehandelt und kommerzialisiert: HOEREN 2018, 187.

¹⁶⁰⁴ GLASS, 104. Ein Grad an Bestimmung über die Personendaten muss nach europäischem Recht immer beim Betroffenen verbleiben: PURTOVA 2011, 265. Verbot der freien und unbegrenzten Veräusserung von Kontrollrechten nach europäischem Recht: PURTOVA 2011, 211.

¹⁶⁰⁵ AEBI-MÜLLER, N 20.

niesst jeder Mensch den privatrechtlichen Persönlichkeitsschutz, auch wenn die Fähigkeiten zur Herrschaft, Kontrolle und Selbstbestimmung teilweise oder ganz fehlen – etwa bei Kleinkindern, Bewusstlosen oder geistig behinderten Personen.¹⁶⁰⁶ Drittens spricht aus wirtschaftlicher Sicht gegen die Einführung eines Dateneigentums das Bedürfnis der Datenwirtschaft, Daten zum Fliessen zu bringen. Eigentumsrechte würden den Datenfluss behindern, weil sie auf Behalten statt auf Teilen fokussieren.¹⁶⁰⁷ Die Geschäftsmodelle vieler unentgeltlicher Datendienstleistungen wären infrage gestellt.¹⁶⁰⁸

Aufgrund der geäusserten Bedenken fügt sich das dem deutschen Rechtssystem entsprungene Konzept der informationellen Selbstbestimmung nicht nahtlos in das schweizerische Rechtssystem ein. AEBI-MÜLLER postuliert daher in Abkehr vom voluntativen Primat der informationellen Selbstbestimmung, dass das Private insofern begründungspflichtig sei, als auch das menschliche Dasein (zwar nicht ausschliesslich, aber auch) gemeinschaftsbezogen sei – ebenso wie die Rechtsordnung als solche nicht primär auf das einzelne Individuum, sondern auf eine angemessene Koordination der Interessen angelegt sei. Nach dieser Konzeption stehen Information, Transparenz, Bildung und Wahrheit dem Anspruch auf Privatheit von vornherein entgegen.¹⁶⁰⁹ Der Betroffene muss demnach ein konkretes und wesentliches Interesse daran zeigen, dass eine fragliche Datenbearbeitung unterbleibt. Er muss nachweisen, dass seine Persönlichkeit (in ihrem ganzen Entfaltung- und Entwicklungspotenzial, d.h. in ihren körperlichen, geistig-seelischen und sozialen Anlagen) durch die Bearbeitung von personenbezogenen Informationen so wesentlich beeinträchtigt wird, dass von einer eigentlichen Verletzung auszugehen und entsprechender Schutz zu gewähren ist.¹⁶¹⁰

Durch die Begründungspflicht tritt das mit der Privatsphäre zu schützende Interesse, nämlich das Interesse an individueller Autonomie, in den Fokus.¹⁶¹¹ Bildlich gesprochen geht es bei der Privatsphäre nicht mehr um drei konzentrische Kugeln bzw. «Sphären» im Sinne der Sphärentheorie, sondern um drei Vektoren: Die

¹⁶⁰⁶ AEBI-MÜLLER, N 377.

¹⁶⁰⁷ «Zentral ist bei Daten nicht das Haben, sondern das Nutzen»: THOUVENIN/WEBER/FRÜH, 194. Kein Bedarf nach Einführung eines Dateneigentums: THOUVENIN/WEBER/FRÜH, 56; WEBER 2018, 105. Vgl. AEBI-MÜLLER, N 602.

¹⁶⁰⁸ WEBER 2018, 105.

¹⁶⁰⁹ AEBI-MÜLLER, N 630.

¹⁶¹⁰ AEBI-MÜLLER, N 846 und 851.

¹⁶¹¹ AEBI-MÜLLER, N 840; WOLFER, N 123.

Autonomie findet ihre Ausprägung in drei «Dimensionen der Privatheit»: lokale, dezisionale und informationelle Privatheit.¹⁶¹² Die lokale Privatheit bezeichnet die Möglichkeit, sich räumlich zurückzuziehen, um in Ruhe gelassen zu werden. Die dezisionale Privatheit umfasst Freiräume für persönliche Entscheidungen. Sie wird im Arbeitsrecht durch das Weisungsrecht der Arbeitgeberin eingeschränkt, beispielsweise durch Kleider-, Frisur- oder Hygienevorschriften.¹⁶¹³ Die informationelle Privatheit sichert die freie Selbstdarstellung im Hinblick auf die autonome Gestaltung von Beziehungen. Sie schützt die Fähigkeit des Subjekts, den Informationsstand anderer über es zu kontrollieren.¹⁶¹⁴

Nach vorliegend vertretener Meinung weist die vorgestellte Theorie der Privatheit jedoch zwei Schwachpunkte auf. Einerseits erodieren die Grenzen zwischen den beschriebenen drei Dimensionen. Beispielsweise verschmelzen die lokale und die informationelle Privatheit im Online-Bereich.¹⁶¹⁵ Somit vermag die Theorie von den drei Dimensionen der Privatheit das zu schützende Private nicht klar zu beschreiben. Andererseits sind die Individuen mit der fortwährenden Begründungspflicht überfordert. Darauf ist sogleich einzugehen.

cc) Überforderung durch informationelle Selbstbestimmung

i. Last der informationellen Selbstbestimmung

Würde man der Forderung, dass das Private begründungspflichtig sein soll,¹⁶¹⁶ stattgeben, so erhielte das Recht auf informationelle Selbstbestimmung eine neue Färbung. Es würde gleichsam zur Last und Pflicht, die eigenen Interessen geltend zu machen und zu begründen. Hier setzt der vorliegend vertretene zweite Kritikpunkt betreffend die informationelle Selbstbestimmung an: In einer Welt von People Analytics, in der Datenbearbeitungen ubiquitär erfolgen, Daten über interoperable Systeme im ganzen Unternehmen und rund um den Erdball verteilt werden und die Prozesse infolge der künstlichen Intelligenz immer komplexer

¹⁶¹² Ausführlich RÖSSLER 2001, 144–304. Ebenso RÖSSLER 2002, 107–108; AEBI-MÜLLER, N 491–497; WOLFER, N 125 und 619–622; RUDIN 2004b, 422.

¹⁶¹³ AEBI-MÜLLER, N 840; WOLFER, N 132.

¹⁶¹⁴ RÖSSLER 2001, 40; WOLFER, N 144; AEBI-MÜLLER, N 840. Eine Persönlichkeitsverletzung ist bei der informationellen Privatheit in dreierlei Hinsicht denkbar: Verlust der Verhaltensauthenzität, Verlust der Kontrolle über die Selbstdarstellung und Störung der Beziehungsgestaltung: WOLFER, N 622–625.

¹⁶¹⁵ Vgl. GILBERT, 291, ausgehend von vier Kategorien: informationelle, physische, dezisionale und eigentumsrechtliche Privatheit.

¹⁶¹⁶ Siehe S. 263–267.

werden, ist der Einzelne mit der Kontrolle der ihn betreffenden Datenflüsse völlig überfordert.¹⁶¹⁷ Individuen sind zusehends ausser Stande, die sie betreffenden Informationsströme in informationeller Selbstbestimmung zu kontrollieren. Stattdessen bestimmen die Arbeitgeberinnen, die die Überwachungen durchführen, das Geschehen.¹⁶¹⁸ Das liberale Leitbild des (informationell) selbstbestimmten Individuums scheitert aus ähnlichen Gründen, aus denen es unsinnig wäre, dem Nutzer die Verantwortung für sauberes Wasser, gesunde Lebensmittel oder sichere Produkte zu überlassen.¹⁶¹⁹ Der Primat der informationellen Selbstbestimmung ist somit «überkommen».¹⁶²⁰

Das Phänomen der Überforderung der Individuen hat sich bereits am Beispiel des Rechtfertigungsgrunds der Einwilligung, die zumindest im Arbeitskontext selten in informationell selbstbestimmter Weise erteilt wird, bemerkbar gemacht.¹⁶²¹ Nun ist aufzuzeigen, dass auch im zivilrechtlichen Verfahren Hürden für die Ausübung der informationellen Selbstbestimmung gestellt sind.

ii. *Materiell-rechtliche Beweisschwierigkeiten
von Persönlichkeitsschutzklagen*

Im Zivilprozess haben die Parteien dem Gericht die Tatsachen, auf die sie ihre Begehren stützen, darzulegen und die Beweismittel anzugeben (Verhandlungsgrundsatz, Art. 55 Abs. 1 ZPO). In erster Linie trägt der klagende Arbeitnehmer die materiell-rechtliche Beweislast (Art. 8 ZGB).¹⁶²² Da viele Algorithmen geheim

¹⁶¹⁷ Bereits im Gesetzgebungsverfahren zum DSG im Jahr 1990 wurde vorausgesehen, dass der Einzelne mit der Führung von Datenschutzklagen «überfordert ist»: AB SR 1990, 147. «Die technisierte, vorab computergestützte Verarbeitung von Personendaten bietet für den einzelnen Bürger oft unüberwindliche Hindernisse, um sich Überblick und Klarheit zu verschaffen»: AB SR 1990, 127. «Überforderung»: BOLLIGER *et al.*, 90. Vgl.: «*Information sharing [...] makes [...] privacy control [...] significantly more difficult*»: THIERER, 431.

¹⁶¹⁸ Arbeitnehmer «machtlos» gegenüber der Arbeitgeberin: AJUNWA IFEOMA, Corporate Surveillance Is Turning Human Workers Into Fungible Cogs, The Atlantic vom 19.05.2017, abrufbar unter <www.theatlantic.com> (besucht am 31.05.2020); Macht bei grossen Unternehmen und dem Staat: RICHARDS/HARTZOG 2017, 1182.

¹⁶¹⁹ BAUMANN MAX-OTTO, 4; THELISSON *et al.*, 55.

¹⁶²⁰ PASSADELIS NICOLAS, Am überkommenen Primat der informationellen Selbstbestimmung festzuhalten, bedeutet, noch mehr wertvolle Zeit zu verlieren, NZZ vom 17.05.2017, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020).

¹⁶²¹ Siehe S. 231–234.

¹⁶²² Kritisierend, dass im Common Law der Betroffene die Beweislast trägt: CAVOUKIAN/DIX/EL EMAM, 11.

sind,¹⁶²³ muss er zur Beweisführung das Auskunftsrecht (Art. 8 DSG, Art. 23 E-DSG, Art. 25 rev-DSG) nutzen.¹⁶²⁴ Ein Recht auf Übertragung der Daten in einem strukturierten, gängigen und maschinell lesbaren Format, wie es das EU-Recht kennt (Art. 20 DSGVO), gesteht ihm das schweizerische DSG nicht zu.¹⁶²⁵ Wird die Auskunft erteilt, bietet die technisierte Datenbearbeitung «oft unüberwindliche Hindernisse, um sich einen Überblick und Klarheit zu verschaffen».¹⁶²⁶

Der Kläger muss eine Persönlichkeitsverletzung (Art. 12 DSG, Art. 26 E-DSG, Art. 30 rev-DSG) nachweisen. Eine Persönlichkeitsverletzung ist eine durch menschliches Verhalten herbeigeführte Störung fremder Persönlichkeitsgüter, bestehend aus der Missachtung von Rechten, welche die Persönlichkeit schützen.¹⁶²⁷ Es handelt sich um eine negative Zustandsänderung des Persönlichkeitsguts, welche durch einen Vergleich des entsprechenden Zustands vor und nach der Eingriffshandlung festgestellt wird.¹⁶²⁸ Der Begriff «Verletzung» kann sich sowohl auf die menschliche Handlung, die eine (schwerwiegende) Beeinträchtigung der Persönlichkeit einer anderen Person nach sich zieht, als auch auf den Erfolg als (negatives) Resultat der verletzenden Handlung beziehen.¹⁶²⁹ Der Nachweis einer Persönlichkeitsverletzung durch People Analytics ist schwierig, weil mit der Privatsphäre und der psychischen Integrität zwei Persönlichkeitsaspekte zur Diskussion stehen, die sich kaum in messbaren Grössen ausdrücken lassen: Während der Arbeitnehmer bei einer Beeinträchtigung der Privatsphäre mit einer Einschränkung oder Verkleinerung eines bestimmten Freiheits- und Entfaltungsraums argumentieren muss, geht es bei der psychischen Integrität um die Veränderung eines

¹⁶²³ ANGWIN JULIA, Make algorithms accountable, The New York Times vom 01.08.2016, abrufbar unter <www.nytimes.com> (besucht am 31.05.2020).

¹⁶²⁴ Die Datenbearbeiterin muss eine vollständige Auskunft erteilen (vgl. Art. 8 Abs. 2 DSG, Art. 23 Abs. 2 E-DSG, Art. 25 Abs. 2 rev-DSG). Vermutet die Auskunft ersuchende Person, dass weitere Daten über sie existieren, trägt sie hierfür die Beweislast: Urteil BGer 1C_59/2015 vom 17.09.2015 E. 3.2.

¹⁶²⁵ Ein Recht auf Datenportabilität würde die Prozessführung vereinfachen: MEIER REGINA, N 19.

¹⁶²⁶ AB SR 1990, 127.

¹⁶²⁷ BGE 120 II 369 E. 2.

¹⁶²⁸ WOLFER, N 182.

¹⁶²⁹ WOLFER, N 176.

(seelischen) Zustandes.¹⁶³⁰ Die negativen Folgen von People Analytics sind oft immateriell und diffus.¹⁶³¹

Rechtserheblich ist nicht jede noch so leichte Veränderung des Persönlichkeitsguts.¹⁶³² Der Rechtsschutz kommt erst bei einer erheblichen Beeinträchtigung der Persönlichkeit zum Tragen (vgl. Art. 49 Abs. 1 OR).¹⁶³³ People Analytics tangiert nicht immer elementare Lebensäusserungen. Bei einer Video- oder Telefonüberwachung, die das Erscheinungsbild und die Stimme erfasst, ist dies schon eher zu bejahen als bei der Überwachung von Internet- und E-Mail-Aktivitäten.¹⁶³⁴

Scheitern wird auch die Berufung auf das verfassungsrechtliche Willkürverbot (vgl. Art. 9 i.V.m. Art. 35 Abs. 3 BV), etwa weil sich das algorithmische Analyseresultat unsorgfältig nur auf wenige Parameter stütze und andere ausser Acht lasse. Die Arbeitgeberin wählt den Algorithmus gerade deswegen aus, weil er einen wesentlichen statistischen Zusammenhang zwischen den Daten und der Leistung des Arbeitnehmers erkannt hat.¹⁶³⁵ Wäre es nicht der beste, würde sie einen anderen Algorithmus wählen.¹⁶³⁶

Am Rande sei vermerkt, dass auch die Arbeitgeberin mit Beweisproblemen zu kämpfen haben kann, wenn sie das Datenschutzrecht verletzt.¹⁶³⁷ Rechtswidrig beschaffte Beweismittel sind grundsätzlich nicht verwertbar (vgl. Art. 152 Abs. 2

¹⁶³⁰ WOLFER, N 182. Auch im amerikanischen Rechtssystem sind Forderungen aus immateriellen Schäden schwierig durchzusetzen: WALDMAN, 70. Forderung nach Kompensierbarkeit von Ängsten und Risiken, die durch Datensicherheitsverletzungen hervorgerufen wurden, unter amerikanischem Recht: SOLOVE/KEATS CITRON, 744.

¹⁶³¹ «Kaum denkbar, dass dem Arbeitnehmer durch unzulässige Kontrollmassnahmen materielle Schäden entstehen»: BYERS, N 378. Der Schaden aus einer Verletzung der Datensicherheit kann z.B. in dem «Risiko» bestehen, dass Dritte entwichene Daten unrechtmässig verwenden: SOLOVE/KEATS CITRON, 737.

¹⁶³² WOLFER, N 108.

¹⁶³³ WOLFER, N 154.

¹⁶³⁴ WOLFER, N 531.

¹⁶³⁵ MRKONICH *et al.*, 36.

¹⁶³⁶ MRKONICH *et al.*, 37; sorgfältige Durchführung von Big Data-Analysen: WEBER 2018, 98; mangelnde Sorgsamkeit bei der Programmierung der eingesetzten Softwareanwendung oder der Aufsicht über sie schwierig nachzuweisen: MARTINI, 1024.

¹⁶³⁷ Siehe zu den Datenschutzverletzungen der Praxis die empirischen Zahlen des NFP75-Projekts (S. 242–246) und die Aufzählung öffentlicher Datenskandale (S. 246–247).

ZPO).¹⁶³⁸ Allerdings ist hierauf nicht näher einzugehen, weil die Durchsetzung des Datenschutzrechts auf dem Wege des Zivilprozesses aufgrund der vorstehend erwähnten Bedenken als nicht zielführend erscheint.

iii. *Verfahrensrechtliche Hürden von Persönlichkeitsschutzklagen*

Der Streitwert und damit das Interesse an der Klage werden gering sein, weil Einzelpersonen in der Regel nur einen Streuschaden erleiden und sich daher mit der Persönlichkeitsschutzklage nicht viel gewinnen lässt.¹⁶³⁹ Ist ein Schaden an den Daten selbst entstanden, so ist zu vergegenwärtigen, dass der Datensatz einer Person einen Wert von wenigen Rappen hat.¹⁶⁴⁰ Wenn auf weiteren Schadenersatz geklagt werden sollte, etwa wegen angefallener Kosten aus gesundheitlichen Beeinträchtigungen, sieht das Zivilprozessrecht keine mit den angloamerikanischen *punitive damages* vergleichbaren Schadenersatzhöhen vor.¹⁶⁴¹ Eine streitige missbräuchliche Kündigung, die gestützt auf einen Vorschlag des Algorithmus ausgesprochen wird, ist gültig; der Entschädigungsanspruch ist auf sechs Monatslöhne beschränkt (Art. 336a OR). Sie zieht nicht die für rechtsmissbräuchliche Handlungen grundsätzlich vorgesehene Rechtsfolge der Ungültigkeit (Art. 2 Abs. 2 ZGB) nach sich.¹⁶⁴² Klagen wegen einer Verletzung der Persönlichkeit müssen in der Regel auf eine Genugtuung lauten (vgl. Art. 49 Abs. 1 OR). Doch ist die Bezifferung des Streitwerts schwierig, weil es kaum möglich ist, abzuschätzen, welche weiteren Folgen sich aus einer Datenschutzverletzung ergeben können, etwa was passiert, wenn die Daten in die Hände unbekannter Dritter gelangen.¹⁶⁴³

Die tiefen möglichen finanziellen Ersatzansprüche des Arbeitnehmers stehen in keinem vernünftigen Verhältnis zu den potenziellen Risiken. Hierzu gehören die

¹⁶³⁸ In einem betreffenden Fall wurde eine fristlose Kündigung als ungerechtfertigt qualifiziert, weil sie sich auf Bildschirmfotos von Chatverläufen einer Mitarbeiterin stützte und die Arbeitgeberin die Fotos rechtswidrig beschafft hatte: Urteil OGER ZH LA180019-O/U vom 15.03.2019 E. 3c/ff.

¹⁶³⁹ MEIER REGINA, N 8.

¹⁶⁴⁰ Die Financial Times hat basierend auf Branchenpreisen einen Rechner entwickelt, mit dem sich der Wert der eigenen Daten berechnen lässt: STEEL EMILY / LOCKE CALLUM / CADMAN EMILY / FREESE BEN, How much is your personal data worth?, 12.06.2013, abrufbar unter <<https://ig.ft.com>> (besucht am 31.05.2020).

¹⁶⁴¹ RUDIN 2002, 408.

¹⁶⁴² PÄRLI 2009, N 1567.

¹⁶⁴³ BOLLIGER *et al.*, 91.

Verfahrenskosten.¹⁶⁴⁴ Auch die lange Dauer des Verfahrens zur Durchsetzung des Datenschutzrechts ist einzuberechnen.¹⁶⁴⁵ Im Arbeitsbereich kommt ferner das Risiko einer Kündigung des Arbeitsverhältnisses hinzu, wenn der Arbeitnehmer gegen seine Arbeitgeberin klagt.¹⁶⁴⁶

Einem kollektiven Vorgehen der Arbeitnehmer in Form der einfachen Streitgenossenschaft (auch subjektive Klagenhäufung, Art. 71 ZPO) und der Nebenintervention (Art. 74 ZPO) steht im Weg, dass die Arbeitgeberin den Algorithmus periodisch ändern kann (und sollte), sobald sich eine neue Korrelation als zutreffender erweist als die alte.¹⁶⁴⁷ Wenn Angestellte zu verschiedenen Zeiten befördert werden, wird sich der Entscheid auf unterschiedliche Algorithmen stützen.¹⁶⁴⁸ Dadurch sind die geforderte Gleichartigkeit der Tatsachen (Art. 71 Abs. 1 ZPO) und das rechtliche Interesse des Nebenintervenienten (Art. 74 Abs. ZPO) infrage gestellt.¹⁶⁴⁹ Möglich wäre zudem eine objektive Klagenhäufung (Art. 90 ZPO). Hierfür müssten die Betroffenen vorgängig ihre Forderungen an eine Person oder einen Verband abtreten (Art. 164 OR). Doch dieses Vorgehen hat in der Praxis kaum Bedeutung erlangt.¹⁶⁵⁰ Auf die Möglichkeit einer Verbandsklage wird später eingegangen.¹⁶⁵¹

Angesichts der materiell- und verfahrensrechtlichen Klagehindernisse treten die Vorteile aus dem Umstand, dass sämtliche Bestimmungen des DSG über Art. 328b Satz 2 OR vertragliche Natur erlangen, in den Hintergrund.¹⁶⁵² Diese Vorteile bestehen darin, dass der Arbeitnehmer von der Verschuldensvermutung (Art. 97 Abs. 1 OR), der Haftung für Hilfspersonen (Art. 101 OR), der längeren

¹⁶⁴⁴ BOLLIGER *et al.*, 91; RUDIN 2002, 407. «Der Einzelne [...] wird wahrscheinlich nur in den seltensten Fällen datenschutzrechtliche Prozesse führen können, weil das Prozessrisiko ausgesprochen hoch ist»: AB NR 1991, 967.

¹⁶⁴⁵ Z.B. benötigte die erste Instanz zur Vorabkontrolle eines Berner Klinikinformationssystems 18 Monate, und das zweitinstanzliche Verfahren dauerte 12 Monate: SIEGENTHALER, 113.

¹⁶⁴⁶ BOLLIGER *et al.*, II.

¹⁶⁴⁷ MRKONICH *et al.*, 23; tägliche Änderung der Algorithmen: MRKONICH *et al.*, 22.

¹⁶⁴⁸ MRKONICH *et al.*, 23.

¹⁶⁴⁹ Vgl. HORNUNG, 92–93: Betroffene bildeten nicht eine zur Willensbildung fähige homogene Gruppe.

¹⁶⁵⁰ KERN/EPINEY, 48–49.

¹⁶⁵¹ Siehe S. 353–361.

¹⁶⁵² RIESELMANN-SAXER, 10.

Verjährungsfrist (Art. 127 f. OR) und dem kostenlosen arbeitsrechtlichen Verfahren (Art. 113 Abs. 2 lit. d und Art. 114 lit. c ZPO) profitiert.

iv. *Diskriminierungsklagen*

Für diskriminierungsrechtliche Klagen stellen sich Probleme, die mit den geschilderten Problemen beim zivilrechtlichen Persönlichkeitsschutz vergleichbar sind, weil in der Schweiz ein Diskriminierungsschutz nur ansatzweise vorhanden ist und kaum abschreckende Sanktionen gegen diskriminierendes Verhalten vorgesehen sind.¹⁶⁵³ Klagen wegen Diskriminierung sind schwierig zu gewinnen und dementsprechend auch rar.¹⁶⁵⁴ Der Bundesrat hat am 25.05.2016 festgestellt, dass die geringe Zahl der Gerichtsfälle zu Diskriminierungsproblemen darauf hindeuten könne, dass die bestehenden Rechtsinstrumente für Betroffene entweder zu wenig bekannt oder zu kompliziert seien oder dass verfahrensrechtliche Hindernisse bestünden.¹⁶⁵⁵ Der Bundesrat lehnt jedoch die Einführung einer expliziten Diskriminierungsnorm im Privatrecht in Ergänzung zum geltenden Persönlichkeitsschutz (Art. 27 ZGB) ab.¹⁶⁵⁶

Einem Beweisproblem sieht sich der Kläger ausgesetzt, wenn er geltend macht, dass die Annahmen des Algorithmus falsch seien.¹⁶⁵⁷ Beispielsweise könnte sich die Klage gegen die Funktion Talent Match von LinkedIn richten, welche der Arbeitgeberin gestützt auf deren eigenes Nutzerverhalten Stellenkandidaten vorschlägt.¹⁶⁵⁸ Um die Kandidatenauswahl als falsch zu widerlegen, müsste der Kläger Daten zu den nicht erkorenen Lebensläufen haben und den hypothetischen Beweis erbringen, dass er bzw. die Abgewiesenen mit ebenso hoher Wahrscheinlichkeit leistungsstarke Mitarbeiter geworden wären.¹⁶⁵⁹ Dies ist naturgemäss un-

¹⁶⁵³ Vgl. WILDHABER *et al.*, 471. KASPER/WILDHABER, 209–210. Siehe auch S. 115–122. Während in der Schweiz griffige Sanktionen fehlen, besteht in Deutschland eine Schadenersatzpflicht der Arbeitgeberin nach dem Allgemeinen Gleichbehandlungsgesetz (vgl. § 15 AGG): DZIDA, 543.

¹⁶⁵⁴ Rechtsdurchsetzungsprobleme: WILDHABER *et al.*, 476. Vgl. zum amerikanischen Recht: KIM 2017, 868.

¹⁶⁵⁵ Schweizerischer Bundesrat 2016a, 2–3.

¹⁶⁵⁶ Schweizerischer Bundesrat 2016a, 17.

¹⁶⁵⁷ WILDHABER *et al.*, 470–471.

¹⁶⁵⁸ Siehe S. 43.

¹⁶⁵⁹ REINSCH/GOLTZ, 43.

möglich. Dessen ungeachtet stuft der Bundesrat die Einführung einer generellen Beweislast erleichterung in Diskriminierungsfällen als nicht realistisch ein.¹⁶⁶⁰

6.2.4 Zwischenfazit zu den Individualklagen

Zusammenfassend weisen sowohl die Konzeption des Persönlichkeitsschutzes als Abwehrrecht (*privacy-as-secrecy*) als auch der Persönlichkeitsschutz durch informationelle Selbstbestimmung (*privacy-as-control*) Defizite auf. Die Vorstellung des Gesetzgebers, der das DSG 1992 – in den Anfängen des WWW-Zeitalters – verabschiedet hat, dass die Betroffenen das Datenschutzrecht eigenständig durchsetzen würden, entspricht nicht der heutigen Realität. Die Durchsetzung des Datenschutzrechts auf dem Wege der Individualklage (Art. 15 DSG, Art. 28 E-DSG, Art. 32 rev-DSG) durch einzelne Arbeitnehmer ist im Umfeld von ubiquitären Datenerhebungen, interoperablen Systemen und steigender künstlicher Intelligenz realitätsfern (geworden).¹⁶⁶¹ Sowohl materiell-rechtliche als auch verfahrensrechtliche Hürden schrecken den einzelnen Arbeitnehmer ab.¹⁶⁶² Deshalb sind Persönlichkeitsschutzklagen nach Art. 15 DSG (bzw. Art. 28 E-DSG bzw. Art. 32 rev-DSG) «sehr selten».¹⁶⁶³ Zum Vergleich sei erwähnt, dass die Durchsetzung der individuellen Rechte selbst in den USA, wo das Verfahrensrecht die Individuen mehr als in Festlandeuropa zur Prozessführung befähigt, schwierig ist.¹⁶⁶⁴

¹⁶⁶⁰ Schweizerischer Bundesrat 2016a, 18.

¹⁶⁶¹ Siehe zur Ubiquität, Interoperabilität und KI S. 71–76.

¹⁶⁶² Siehe S. 268–273.

¹⁶⁶³ BOLLIGER *et al.*, 83 und 85; BACHER/DUBOIS, 144. Wesentlich häufiger sind dagegen Auskunftsansprüche (gestützt auf Art. 8 DSG [Art. 23 E-DSG, Art. 25 rev-DSG]): BOLLIGER *et al.*, 84 und 104. Auskunftsansprüche sind zudem vor Gericht relativ erfolgreich: BOLLIGER *et al.*, 104.

¹⁶⁶⁴ Zum Vergleich zwischen den USA und der EU: EDWARDS/VEALE, 74. Vgl. REINSCH/GOLTZ, 55: In den USA profitiert der Kläger von einer Beweislastumkehr, wenn er nachweisen kann, dass ein Algorithmus der Arbeitgeberin mit Daten arbeitet, die zu einer geschützten Gruppe von Personen gehören. – In den USA sind «*finances and liability [...] as important as ever*»: HARTZOG 2018, 87.

6.3 Datenschutzrechtliche Aufsicht

6.3.1 Abklärungen und Empfehlungen des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten

Wegen der geringen Wirkungskraft der zivilrechtlichen Individualklagen ist nach anderen Möglichkeiten zur Durchsetzung des Datenschutzrechts zu suchen. Der EDÖB stellt neben der Individualklage den zweiten zentralen Wirkungsmechanismus des DSG im privatrechtlichen Bereich dar.¹⁶⁶⁵

Das DSG vermittelt dem EDÖB die Kompetenz zu Abklärungen und Empfehlungen im Privatrechtsbereich (Art. 29 DSG). Der EDÖB interveniert im öffentlichen Interesse (vgl. Art. 5 Abs. 2 BV), wenn die Verteidigung einer Vielzahl von Personen angezeigt ist.¹⁶⁶⁶ Es handelt sich um eine öffentlich-rechtliche Bestimmung im DSG, das ansonsten in der systematischen Rechtssammlung des Bundes als Privatrecht klassifiziert ist (SR 235.1).¹⁶⁶⁷

Von sich aus oder auf Meldung Dritter hin klärt der EDÖB den Sachverhalt näher ab, insbesondere wenn die Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (sog. Systemfehler, Art. 29 Abs. 1 lit. a DSG). Bei einem Systemfehler geht es um konzeptionell falsch bzw. rechtswidrig angelegte Datenbearbeitungen, nicht um einmalige Datenschutzpannen.¹⁶⁶⁸ Die Kompetenz des EDÖB zur Sachverhaltsabklärung ist erforderlich, weil Einzelpersonen mit gerichtlichen Klagen jeweils nur ihre eigenen Daten verändern, nicht aber einen Systemfehler, der eine ganze Reihe anderer Personen tangiert, beheben können.¹⁶⁶⁹ Ein Systemfehler kann bei People Analytics auftreten, da es sich um Systeme der Überwachung und Kontrolle handelt. Eine Sachverhaltsabklärung ist zudem möglich, wenn Datensammlungen registriert werden müssen (Art. 29 Abs. 1 lit. b DSG) und wenn eine Informationspflicht betreffend die grenzüberschreitende Bekanntgabe von Daten besteht (Art. 29 Abs. 1 lit. c DSG). Der EDÖB kann bei einer Sachverhaltsabklärung die Akten herausverlan-

¹⁶⁶⁵ BOLLIGER *et al.*, I.

¹⁶⁶⁶ THÜR, 74. Vgl. DREYER/SCHULZ, 42: Behörden könnten auf Fehlentwicklungen wie die Monopolisierung von automatisierten Entscheidungssystemen oder Algorithmen in bestimmten Lebensbereichen aufmerksam machen.

¹⁶⁶⁷ Schweizerischer Bundesrat, Systematische Rechtssammlung, Landesrecht, abrufbar unter <www.admin.ch> (besucht am 31.05.2020); FLUECKIGER 2014, 79.

¹⁶⁶⁸ BBl 1988 II, 479; ROSENTHAL 2015, N 7.60.

¹⁶⁶⁹ Vgl. AB NR 1991, 967.

gen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen (Art. 29 Abs. 2 Satz 1 DSG).¹⁶⁷⁰ Für die Sachverhaltsabklärungen hat der EDÖB keine Zwangsmittel.¹⁶⁷¹

Der EDÖB kann aufgrund seiner Abklärungen empfehlen, das Bearbeiten zu ändern oder zu unterlassen (Art. 29 Abs. 3 DSG). Die Empfehlungen des EDÖB enthalten konkrete Anweisungen zur Anpassung oder (teilweisen) Einstellung der Datenbearbeitung unter Ansetzung einer Frist zur Einhaltung der Empfehlung.¹⁶⁷² Eine Empfehlung ist nicht bindend.¹⁶⁷³ Der EDÖB hat keine Kompetenz zum Erlass von Verfügungen. Somit kommt das Verwaltungsverfahrenrecht nicht (direkt)¹⁶⁷⁴ zur Anwendung.¹⁶⁷⁵ Die Empfehlungen des EDÖB werden grossmehrheitlich umgesetzt.¹⁶⁷⁶ Beispielsweise hat der EDÖB im Jahr 2006 der Aldi Suisse AG empfohlen, die Videoüberwachung zum Schutz des Verkaufspersonals anzupassen, worauf der Detailhändler datenschutzfreundliche Technologien (Privacy-Filter) eingeführt hat.¹⁶⁷⁷

Bei Nichtbefolgung oder Ablehnung einer Empfehlung des EDÖB kann dieser die Angelegenheit dem Bundesverwaltungsgericht zur Entscheid vorlegen (Art. 29 Abs. 4 Satz 1 DSG). Ein Verbot oder eine vorgeschriebene Änderung des Bundesverwaltungsgerichts gilt typischerweise für alle von der Verantwortlichen bearbeiteten Daten.¹⁶⁷⁸ Dieser Umstand kann für die Datenbearbeiterin weitreichendere Konsequenzen haben als eine zivilprozessuale Klage, bei der lediglich die Daten des Klägers betroffen sind. Verbote des Bundesverwaltungsgerichts können zeitlich unbefristet, d.h. bis auf Weiteres, gelten.¹⁶⁷⁹ In persönlicher Dimension treffen die Verbote des Bundesverwaltungsgerichts nur die adressierte Datenbearbeiterin. Konkurrenten, die eine vergleichbare Datenbearbeitung praktizieren, können diese

¹⁶⁷⁰ Dabei gilt das Zeugnisverweigerungsrecht nach Art. 16 VwVG sinngemäss (Art. 29 Abs. 2 Satz 2 DSG, Art. 43 Abs. 3 Satz 2 E-DSG, Art. 49 Abs. 3 Satz 2 rev-DSG).

¹⁶⁷¹ ROSENTHAL 2015, N 7.60.

¹⁶⁷² ROSENTHAL 2015, N 7.61.

¹⁶⁷³ ROSENTHAL 2015, N 7.61.

¹⁶⁷⁴ Zum Verfahren vor Bundesverwaltungsgericht sogleich.

¹⁶⁷⁵ ROSENTHAL 2015, N 7.60.

¹⁶⁷⁶ Umsetzung der Empfehlungen entweder direkt oder nach einem Gerichtsentscheid: BOLLIGER *et al.*, III.

¹⁶⁷⁷ EDÖB 2007, 59–61.

¹⁶⁷⁸ ROSENTHAL 2015, N 7.62.

¹⁶⁷⁹ ROSENTHAL 2015, N 7.62.

weiterführen und einen gewichtigen Wettbewerbsvorteil erlangen.¹⁶⁸⁰ Stellt der EDÖB im Rahmen einer Sachverhaltsabklärung in einem Unternehmen Mängel fest, verzichtet er häufig aus Ressourcengründen bei ähnlichen Bearbeitern auf stichprobenartige Kontrollen.¹⁶⁸¹ Das Rechtsrisiko eines Verfahrens des EDÖB ist somit nicht gleichmässig auf die Unternehmen verteilt, sondern konzentriert sich bei den auf irgendeine Weise besonders exponierten Datenbearbeitern.¹⁶⁸² Dies hat eine gewisse Rechtsungleichheit und -unsicherheit zur Folge. Manche Unternehmen beugen einem Verfahren des EDÖB dadurch vor, dass sie ihre geplante Datenbearbeitung dem EDÖB vorgängig konsultativ unterbreiten.¹⁶⁸³

Prozessual gesehen handelt es sich vor dem Bundesverwaltungsgericht um ein verwaltungsrechtliches Verfahren.¹⁶⁸⁴ Das Verfahren stellt eine Art «Popularklage» des EDÖB gegen die betreffende Datenbearbeiterin dar, d.h. mit dem EDÖB als Kläger anstelle der (potenziell) betroffenen Personen und der Datenbearbeiterin als beklagter Partei.¹⁶⁸⁵ Der EDÖB ist berechtigt, gegen den Entscheid des Bundesverwaltungsgerichts Beschwerde zu führen (Art. 29 Abs. 4 Satz 2 DSG).

Insgesamt ist die Sensibilisierungs- und Schutzwirkung, die vom EDÖB ausgeht, zwar stärker als diejenige der einklagbaren Individualrechte.¹⁶⁸⁶ Jedoch erscheinen die Möglichkeiten des EDÖB zur Intervention bei People Analytics begrenzt.¹⁶⁸⁷ Das DSG verwehrt dem EDÖB jede Kompetenz zum Erlass von Zwangsmassnahmen, Verfügungen und Verwaltungssanktionen. Verfahren nach Art. 29 DSG sind vergleichsweise selten.¹⁶⁸⁸ Dies ist auf die beschränkten Ressourcen des EDÖB

¹⁶⁸⁰ ROSENTHAL 2015, N 7.62.

¹⁶⁸¹ BOLLIGER *et al.*, IV.

¹⁶⁸² ROSENTHAL 2015, N 7.93.

¹⁶⁸³ ROSENTHAL 2015, N 7.63.

¹⁶⁸⁴ Legt der EDÖB eine Angelegenheit dem Bundesverwaltungsgericht vor (Art. 29 Abs. 4 DSG), so richtet sich das Verfahren nach dem VwVG, soweit das VGG nichts anderes bestimmt (Art. 37 VGG). Das Verfahren basiert allerdings grösstenteils auf den Grundsätzen eines Zivilprozesses: ROSENTHAL 2015, N 7.61.

¹⁶⁸⁵ ROSENTHAL 2015, N 7.61.

¹⁶⁸⁶ BOLLIGER *et al.*, IV.

¹⁶⁸⁷ BOLLIGER *et al.*, 222.

¹⁶⁸⁸ Nicht mehr als fünf bis zehn Verfahren jährlich: ROSENTHAL 2015, N 7.62.

zurückzuführen.¹⁶⁸⁹ Den künftig erweiterten Kompetenzen des EDÖB gemäss rev-DSG widmet sich diese Arbeit zu einem späteren Zeitpunkt.¹⁶⁹⁰

6.3.2 Aufsichtskompetenzen nach der Datenschutz-Grundverordnung

Fällt ein People Analytics-Sachverhalt in den Anwendungsbereich der DSGVO, muss die Arbeitgeberin mit Interventionen der zuständigen ausländischen Aufsichtsbehörde rechnen, welche griffiger als diejenigen des EDÖB sind.¹⁶⁹¹ Zunächst verfügen die Aufsichtsbehörden ähnlich wie der EDÖB über Untersuchungsbefugnisse (Art. 58 Abs. 1 DSGVO) zur Wahrnehmung ihrer Aufgaben (Art. 57 DSGVO). Die Untersuchungsbefugnisse umfassen sowohl Anweisungen zur Bereitstellung von Informationen als auch Datenschutzüberprüfungen, Überprüfungen von Zertifizierungen, Hinweise auf Verstösse gegen die DSGVO sowie den Zugang zu allen personenbezogenen Daten und zu den Geschäftsräumen des Verantwortlichen und des Auftragsbearbeiters (Art. 58 Abs. 1 lit. a–f DSGVO).

Die Aufsichtsbehörden haben aber auch eine Kompetenz zum Erlass von Verfügungen zur Durchsetzung ihrer Aufgaben (Art. 58 Abs. 2 DSGVO). Die sog. Abhilfebefugnisse umfassen Warnungen vor beabsichtigten Bearbeitungsvorgängen, Verwarnungen bei Verstössen gegen die DSGVO und Anweisungen. Sodann bestehen die Befugnisse in der vorübergehenden oder endgültigen Beschränkung der Bearbeitung einschliesslich eines Verbots, in der Anordnung der Berichtigung oder Löschung von personenbezogenen Daten und im Widerruf einer Zertifizierung. Die Aufsichtsbehörde kann schliesslich Geldbussen verhängen und die Aussetzung der Übermittlung von Daten anordnen (Art. 58 Abs. 2 lit. a–j DSGVO).

Schliesslich können die Aufsichtsbehörden im EU-Raum ein rechtswidriges Verhalten mit Geldbussen sanktionieren. Diese werden bei Verstössen gegen die DSGVO und bei Nichtbefolgung einer Anweisung der zuständigen Aufsichtsbehörde je nach den Umständen des Einzelfalls zusätzlich oder anstelle von Massnahmen verhängt (Art. 83 Abs. 2 Satz 1 DSGVO). Die Geldbussen betragen bis zu EUR 20 Mio. oder im Fall eines Unternehmens bis zu vier Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs, je

¹⁶⁸⁹ ROSENTHAL 2015, N 7.93.

¹⁶⁹⁰ Siehe S. 348–350.

¹⁶⁹¹ Vgl. BOLLIGER *et al.*, V.

nachdem, welcher Betrag höher ist (Art. 83 Abs. 5–6 DSGVO).¹⁶⁹² Von der Busenkompetenz wurde bereits intensiv Gebrauch gemacht.¹⁶⁹³ Zudem sind andere Sanktionen für DSGVO-Verstöße, insbesondere solche, die keiner Geldbusse (Art. 83 DSGVO) unterliegen, möglich (Art. 84 DSGVO).

6.4 Arbeitsgesetzliche Aufsicht

Die Vollzugsbehörden des ArG können von der Arbeitgeberin Einsicht in sämtliche Unterlagen und Daten der betriebenen Überwachungs- und Kontrollsysteme verlangen.¹⁶⁹⁴ Das Einsichtsrecht der Aufsichtsbehörde geht weiter als das Auskunftsrecht von Individuen (nach Art. 8 DSG, Art. 23 E-DSG bzw. Art. 25 rev-DSG): Die Arbeitgeberin und ihre Arbeitnehmer sowie Personen, die im Auftrag der Arbeitgeberin Aufgaben nach dem ArG wahrnehmen, haben den Voll-

¹⁶⁹² Der Höchstbetrag der Geldbusse ist auf die Hälfte (EUR 10 Mio. oder 2 Prozent des globalen Jahresumsatzes) begrenzt beim Verstoss gegen ausgewählte Bestimmungen der DSGVO (Art. 83 Abs. 4 DSGVO).

¹⁶⁹³ Eine aktuelle Übersicht aller verhängten datenschutzrechtlichen Bussen findet sich unter: CMS, GDPR Enforcement Tracker, abrufbar unter <<https://enforcementtracker.com>> (besucht am 31.05.2020). Die Aufsichtsbehörden von elf EWR-Staaten haben im ersten Jahr, als die DSGVO anwendbar war, Bussen in der Höhe von rund EUR 55 Mio. verhängt: EDSA 2019, 8. Die Höhe der ersten Busse unter der DSGVO betrug EUR 4'800, zzgl. Verfahrenskosten, und wurde in Österreich verhängt: VASELLA DAVID, Erste Busse unter der DSGVO verhängt, 20.09.2018, abrufbar unter <<https://datenrecht.ch>> (besucht am 31.05.2020). Busse in Höhe von EUR 20'000 gegen das soziale Netzwerk «Knuddels» durch die Datenschutz-Aufsichtsbehörde von Baden-Württemberg: VASELLA DAVID, Nur, aber immerhin: «Knuddels» zahlt verkräftbare DSGVO-Busse, 22.11.2018, abrufbar unter <<https://datenrecht.ch>> (besucht am 31.05.2020); Busse von EUR 150'000 gegen den Wirtschaftsprüfer PricewaterhouseCoopers (PwC) durch die griechische Datenschutz-Aufsichtsbehörde: Hellenic Data Protection Authority, Summary of Hellenic DPA's decision no 26/2019, abrufbar unter <www.dpa.gr> (besucht am 31.05.2020); Busse von umgerechnet rund EUR 220'000 gegen einen polnischen Verantwortlichen: VASELLA DAVID, Polen: DSGVO-Busse von EUR 220'000 (Verletzung der Transparenz), 27.03.2019, abrufbar unter <<https://datenrecht.ch>> (besucht am 31.05.2020); Busse von EUR 50 Mio. gegen Google in Frankreich im Jahr 2019: Commission nationale de l'informatique et des libertés, bestätigt in: Décision Conseil d'Etat [Frankreich] N° 430810 vom 19.06.2020 N 28.

¹⁶⁹⁴ Zudem kann der betroffene Arbeitnehmer seine Daten im Einvernehmen mit der Arbeitgeberin oder auf deren Vorschlag hin einsehen. Eine mündliche Auskunftserteilung ist möglich, sofern der Arbeitnehmer einwilligt und die Arbeitgeberin den Arbeitnehmer identifizieren kann: SECO 2018, 326–327.

zugs- und Aufsichtsbehörden alle Auskünfte zu erteilen, die diese zur Erfüllung ihrer Aufgaben benötigen (Art. 45 Abs. 1 ArG). Darüber hinaus hat die Arbeitgeberin den Vollzugs- und Aufsichtsorganen den Zutritt zum Betrieb, die Vornahme von Feststellungen und die Entnahme von Proben zu gestatten (Art. 45 Abs. 2 ArG). Die Arbeitgeberin hat die Verzeichnisse oder andere Unterlagen, aus denen die für den Vollzug des ArG und seiner Verordnungen erforderlichen Angaben ersichtlich sind, den Vollzugs- und Aufsichtsorganen zur Verfügung zu halten, wobei die Bestimmungen des DSG gelten (Art. 46 ArG; insbesondere die Mitwirkungspflicht, vgl. Art. 34 DSG, Art. 54 E-DSG, Art. 60 rev-DSG).

In einem weiteren Schritt können die Vollzugsbehörden die Arbeitgeberin darauf aufmerksam machen, dass eine People Analytics-Anwendung gegen das ArG verstösst, und sie können eine Reduktion auf ein zulässiges Mass (z.B. Anonymisierung der Daten) verlangen (Art. 51 Abs. 1 ArG). Leistet die Arbeitgeberin dem Verlangen keine Folge, erlässt die kantonale Vollzugsbehörde eine entsprechende Verfügung, unter Androhung einer Busse im Widerhandlungsfall (Art. 51 Abs. 2 ArG i.V.m. Art. 292 StGB). Missachtet die Arbeitgeberin die Verfügung, ergreift die kantonale Behörde als äusserstes Mittel die zur Herbeiführung des rechtmässigen Zustands erforderlichen Massnahmen des Verwaltungszwangs, bis zur vorübergehenden Betriebsschliessung (Art. 52 ArG).¹⁶⁹⁵ Bei People Analytics fällt die Beschlagnahmung einer Überwachungsanlage als Massnahme zur direkten Vollstreckung in Betracht.¹⁶⁹⁶

Für den Vollzug des ArG sind grundsätzlich die kantonalen Arbeitsinspektorate zuständig (vgl. Art. 41 ArG) und für die Oberaufsicht über den Vollzug hauptsächlich das SECO (Art. 42 Abs. 3 ArG).¹⁶⁹⁷ Das Verfahren wird auf Anzeige hin eingeleitet (vgl. Art. 54 ArG) und ist öffentlich-rechtlich.¹⁶⁹⁸ Der Arbeitnehmer hat gegenüber den Vollzugsorganen des ArG einen Anspruch auf Durchsetzung der notwendigen Gesundheitsschutz-Massnahmen (vgl. Art. 54 ArG). Vor allem in kleineren Betrieben, in denen die Arbeitnehmer nicht organisiert sind und der Einzelne mit einer Klage gegen die Arbeitgeberin sein faktisches Interesse an einer

¹⁶⁹⁵ Massnahmen des Verwaltungszwangs sind insbesondere bei Verletzung von Informations-, Konsultations- und Mitwirkungsrechten möglich: KUKO ArG-BLESI, Art. 48 ArG, N 24.

¹⁶⁹⁶ WOLFER, N 606.

¹⁶⁹⁷ KUKO ArG-KASPER/WILDHABER, Art. 41 ArG, N 2; KUKO ArG-KASPER/WILDHABER, Art. 42 ArG, N 11.

¹⁶⁹⁸ KUKO ArG-NÖTZLI, Art. 6 ArG, N 23.

Weiterbeschäftigung gefährden würde,¹⁶⁹⁹ kann eine Anzeige ein passendes Mittel zur Durchsetzung der arbeitsrechtlichen Schutzvorschriften sein.

Die Mittel der ArG-Vollzugsbehörden sind insgesamt besonders aufgrund der Kompetenz zum Erlass von Verfügungen und zur Anwendung von Verwaltungszwang stärker als diejenigen des EDÖB im Bereich Datenschutz. Nach der besprochenen bundesgerichtlichen Rechtsprechungsänderung zu den Systemen der Verhaltensüberwachung (Art. 26 ArGV 3) werden die Arbeitsinspektorate hingegen erst sanktionierend einschreiten, wenn es effektiv zu einer Gesundheitsbeeinträchtigung kommt.¹⁷⁰⁰ Dies stellt eine relativ hohe Schwelle dar, sodass Datensicherheitsverletzungen und geringere Datenschutzverletzungen arbeitsschutzrechtlich in den meisten Fällen folgenlos bleiben werden.

6.5 Strafverfolgung

Die Strafverfolgungsbehörden können einschreiten bei einer Verletzung der Auskunft-, Melde- und Mitwirkungspflichten durch private Personen (Art. 34 DSG, vgl. Art. 54 E-DSG, Art. 60 rev-DSG) sowie bei einer Verletzung der beruflichen Schweigepflichten (Art. 35 DSG, Art. 56 E-DSG, Art. 62 rev-DSG). Hierbei handelt es sich um Sonderdelikte, sodass die Unternehmensvertreter (insbesondere die vorgesetzte Führungsperson und die Organe) bestraft werden können (vgl. Art. 29 StGB).¹⁷⁰¹ Die Delikte sind grundsätzlich nur auf Antrag der verletzten Person (d.h. des Arbeitnehmers) strafbar (vgl. Art. 34 Abs. 1 und Art. 35 Abs. 1 DSG; Art. 54 Abs. 1 und Art. 56 Abs. 1 E-DSG; Art. 60 Abs. 1 und Art. 62 Abs. 1 rev-DSG; Art. 30 StGB). Jedoch kann der EDÖB bei unterlassenen Meldungen an ihn, bei falschen Auskünften und bei einer Mitwirkungsverweigerung (Art. 34 Abs. 2

¹⁶⁹⁹ Z.B. Klagen von Arbeitnehmerinnen nach dem Gleichstellungsgesetz sind «ausnehmend selten und nur dort zu verzeichnen, wo das Arbeitsverhältnis bereits aufgelöst worden ist»: HÄNER, N 1047.

¹⁷⁰⁰ Siehe zur Rechtsprechung S. 150–154.

¹⁷⁰¹ Die beiden Tatbestände des DSG stellen Sonderdelikte dar, da als Täter nur infrage kommt, wer informations- oder auskunftspflichtig ist (Art. 34 DSG, Art. 54 E-DSG, Art. 60 rev-DSG) bzw. wer einen Beruf ausübt, der die Kenntnis geheimer, besonders schützenswerter Personendaten oder Persönlichkeitsprofile vermittelt (Art. 35 DSG, Art. 56 E-DSG, Art. 62 rev-DSG): HK-ROSENTHAL, Art. 34 DSG, N 14, 25, und HK-ROSENTHAL, Art. 35 DSG, N 6. Die Strafbarkeit der Unternehmensvertreter gilt bei allen Sonderdelikten: BSK StGB I-WEISSENBERGER, Art. 29 StGB, N 3.

DSG, Art. 54 Abs. 2 E-DSG, Art. 60 Abs. 2 rev-DSG) Strafanzeige (Art. 301 Abs. 1 StPO) erstatten; diese Straftaten sind keine Antragsdelikte.

Der EDÖB kann die Strafverfolgungsbehörden zudem einschalten, indem er ein Rechtsbegehren um Androhung einer Ungehorsamsstrafe (Busse nach Art. 292 StGB) stellt.¹⁷⁰² Dieses Begehren kann er vor Bundesverwaltungsgericht anbringen für den Fall, dass seine Empfehlung nicht befolgt werden sollte (vgl. Art. 29 Abs. 4 DSG).

Bei sämtlichen Delikten handelt es sich um Übertretungen (vgl. Art. 103 ff. StGB). Eine Strafbarkeit des Unternehmens fällt daher ausser Betracht (Art. 102 Abs. 1 Satz 1 i.V.m. Art. 10 StGB *e contrario*). Die höchstmögliche strafrechtliche Sanktion für Widerhandlungen gegen das DSG ist eine Busse von CHF 10'000 (Art. 106 Abs. 1, Art. 333 Abs. 1 StGB).

Ferner sind Strafverfahren bei Zuwiderhandlungen gegen die Vorschriften über den Gesundheitsschutz (vgl. Art. 59 Abs. 1 lit. a ArG) und über genetische Untersuchungen möglich (Art. 36 ff. GUMG).¹⁷⁰³ Hierbei handelt es sich im Gegensatz zur Mehrheit der DSG-Tatbestände um Offizialdelikte. Insgesamt aber spielen strafrechtliche Sanktionen im Schweizer Datenschutzrecht in der Praxis keine wesentliche Rolle.¹⁷⁰⁴ Dies kann zur Folge haben, dass dem Datenschutz im unternehmensinternen Verteilungskampf der Ressourcen im Vergleich zu anderen Themen wie etwa der Korruptionsbekämpfung oder dem Kartellrecht kein besonders hohes Gewicht beikommt.¹⁷⁰⁵

6.6 Mitwirkungsrechtliche Behelfe

6.6.1 Grosses Potenzial für die Durchsetzung des Datenschutzrechts

Die betriebsverfassungsrechtlichen Instrumente, die das MitwG vorsieht, können eine zentrale Rolle für die Rechtsdurchsetzung einnehmen, weil hier das rechts-

¹⁷⁰² ROSENTHAL 2015, N 7.61. Vgl. BSK StGB II-RIEDO/BONER, Art. 292 StGB, N 66: Das Bundesverwaltungsgericht ist kompetent, im Entscheid eine Busse für den Fall einer Widerhandlung gegen das Urteil anzudrohen, weil auch Gerichte vom Begriff der «Behörden» (Art. 292 StGB) erfasst sind.

¹⁷⁰³ Siehe S. 127.

¹⁷⁰⁴ ROSENTHAL 2015, N 7.88.

¹⁷⁰⁵ ROSENTHAL 2015, N 7.89.

konforme Verhalten durch das Kollektiv eingefordert wird, wobei einzelne Arbeitnehmer anonym bleiben können. Demgegenüber ist das persönliche Einfordern durch die Arbeitnehmer, die im Berufsleben Datenschutzverstösse ihrer Arbeitgeberin erkennen, problematisch.¹⁷⁰⁶ Selbst wenn ihnen im gerichtlichen oder aufsichtsrechtlichen Verfahren Erfolg beschieden sein sollte, kann die Arbeitgeberin in der Praxis anschliessend das Arbeitsverhältnis unter anderen Vorwänden kündigen.¹⁷⁰⁷ Aufgrund solcher Probleme sollte gemäss Direktauskunft des SECO an den Autor der vorliegenden Arbeit die Gesundheitsvorsorge am Arbeitsplatz, wozu die Überwachung zählt (vgl. Art. 26 ArGV 3), primär über kollektive Wege erfolgen. Zu individuellen Ansätzen sollte nur dann gegriffen werden, wenn die gemeinschaftlichen untauglich sind.¹⁷⁰⁸

Die Mitsprache bei People Analytics muss nicht zwingend betriebsverfassungsrechtlich durch den Gesetzgeber auf dem Wege des MitwG initiiert werden. Alternativ könnten kollektivrechtliche Instrumente gewählt werden (z.B. Interaktion der Sozialpartnerschaft, Abschluss von Betriebsvereinbarungen, Tarifverträgen und Gesamtarbeitsverträgen, vgl. Art. 2 MitwG i.V.m. Art. 356 ff. OR). Die Möglichkeit zum sozialpartnerschaftlichen Austausch basierend auf dem Grundsatz der Vertragsfreiheit führt in der Schweiz zu einem im internationalen Vergleich flexiblen Arbeitsrecht, das eine schnelle Anpassung an strukturelle Veränderungen sowie an die Bedürfnisse der Wirtschaft erlaubt.¹⁷⁰⁹ Vorteile einer kollektivrechtlichen Regelung wären die Rücksichtnahme auf Branchenverhältnisse und eine im Verhältnis zum schwerfälligen Gesetzgebungsprozess agile Anpassung an die sich schnell ändernden Technologien.¹⁷¹⁰ Jedoch zeigte eine Untersuchung von 15 Gesamtarbeitsverträgen, dass von dieser Gelegenheit zur Präzisierung und Einschränkung wenig Gebrauch gemacht wird: Die Bestimmungen zur Arbeitssicherheit und zum Gesundheitsschutz (vgl. Art. 26 ArGV 3) verweisen lediglich auf die

¹⁷⁰⁶ WEDDE 2016c, 3.

¹⁷⁰⁷ WEDDE 2016c, 7.

¹⁷⁰⁸ SECO 2019. Der Autor dankt Herrn lic. iur. Alain Vuissoz und Herrn Dr. sc. Marc Arial, Ressortleiter Grundlagen Arbeit und Gesundheit des SECO, für die bereitwillige Auskunftserteilung.

¹⁷⁰⁹ Schweizerischer Bundesrat 2017a, 58.

¹⁷¹⁰ CIRIGLIANO/EGGER, N 265–266. Übermässig restriktiv erscheint die Haltung, Überwachungen am Arbeitsplatz sollten nur zulässig sein, wenn ein «*collective agreement*» bestehe: AKHTAR/MOORE, 122. Etwas unklar bleibt die Forderung, Einwilligungen in einer «kollektiven Form» durchzusetzen, etwa durch Gewerkschaften, Betriebsräte oder gemischte Ausschüsse: OTTO 2016, 193.

rechtlichen Grundlagen.¹⁷¹¹ Daher werden im Folgenden primär die Instrumente des betriebsverfassungsrechtlichen Mitwirkungsrechts analysiert. Wenn aber später¹⁷¹² künftige Verbesserungsmöglichkeiten des Mitwirkungsrechts thematisiert werden, so ist im Kopf zu behalten, dass nicht nur der Gesetzgeber, sondern auch die Sozialpartner diese Reformen herbeiführen könnten.

6.6.2 Öffentlich-rechtliches Anzeigeverfahren

Für die Durchsetzung des MitwG stehen die zwei Wege über eine öffentlich-rechtliche Anzeige oder eine privatrechtliche Klage frei. Die öffentlich-rechtliche Anzeige wegen eines Verstosses gegen das Mitspracherecht geht an die zuständige Vollzugsstelle des ArG (vgl. Art. 54 Abs. 1 lit. a i.V.m. Art. 48 ArG). Auch die Verletzung des Informationsrechts ist ein tauglicher Anzeigegrund.¹⁷¹³

Anzeigeberechtigt ist jedermann.¹⁷¹⁴ Weder eine Rechtsmittellegitimation noch eine Prozess- oder Rechtsfähigkeit sind für eine Anzeige vorausgesetzt.¹⁷¹⁵ Somit können die Arbeitnehmer, ihre Vertretungen, aber auch Dritte eine Anzeige erstatten.

Für Verstösse gegen das MitwG sind keine Sanktionen (z.B. Bussen) vorgesehen.¹⁷¹⁶ Das Fehlen der Sanktion stellt eine vom Gesetzgeber beabsichtigte Geset-

¹⁷¹¹ CIRIGLIANO/EGGER, N 262, 265. Z.B. der Gesamtarbeitsvertrag der SBB wiederholt nur das gesetzlich vorgeschriebene Mitspracherecht in Fragen der Arbeitssicherheit und des Gesundheitsschutzes: SBB, Anhang 10 Ziff. 8 GAV SBB; wenige Gesamtarbeitsverträge, die sich der Mitwirkungsthematik widmen: KASPER, N 428. Diverse Gesamtarbeitsverträge verweisen lediglich auf die Bestimmungen im MitwG und OR: KASPER, N 447. WILDHABER 2011, 369. A.M. FRITZ/SCHULER, 29, und DERRER BALLADORE, 185: Anfang der 1990er-Jahre enthielt rund die Hälfte aller Gesamtarbeitsverträge Mitwirkungsregeln und eine Pflicht zur Schaffung von Arbeitnehmervertretungen. Im Jahr 2009 sahen die meisten Gesamtarbeitsverträge in Branchen mit grösseren Betrieben Arbeitnehmervertretungen vor und gingen in der Regel über die Vorschriften des MitwG hinaus: DERRER BALLADORE, 186.

¹⁷¹² Siehe S. 346–347.

¹⁷¹³ KUKO ArG-BLESI, Art. 48 ArG, N 24.

¹⁷¹⁴ KUKO ArG-HÄGGI FURRER, Art. 54 ArG, N 2.

¹⁷¹⁵ KUKO ArG-HÄGGI FURRER, Art. 54 ArG, N 2.

¹⁷¹⁶ FURER 2009a, 173.

zeslücke dar.¹⁷¹⁷ Das MitwG wird deshalb als zahnloser «Papiertiger» verspottet.¹⁷¹⁸

6.6.3 Privatrechtliche Klage

a) Zuständigkeit und Verfahren

Alternativ zur Anzeige besteht die Möglichkeit einer privatrechtlichen Klage (Art. 15 MitwG). Zuständig sind die für Streitigkeiten aus dem Arbeitsverhältnis kompetenten Instanzen (arbeitsrechtliche Schlichtungsbehörde, vgl. Art. 197, Art. 34 ZPO); vorbehalten bleiben vertragliche Schlichtungs- und Schiedsstellen (Art. 15 Abs. 1 MitwG).

Weder im Schlichtungs- (Art. 113 Abs. 2 lit. e ZPO i.V.m. Art. 15 Abs. 1 MitwG) noch im Entscheidverfahren (Art. 114 lit. d ZPO i.V.m. Art. 15 Abs. 1 MitwG) werden Gerichtskosten gesprochen. Es gilt ohne Rücksicht auf den Streitwert das vereinfachte Verfahren (Art. 243 Abs. 2 lit. e ZPO). Oft bestehen Beweisschwierigkeiten.¹⁷¹⁹ Urkunden über Leistungen nach dem MitwG sind nicht direkt vollstreckbar (Art. 348 lit. c ZPO).

b) Aktivlegitimation

Klageberechtigt sind zunächst die beteiligten Arbeitnehmer (ebenso die Arbeitgeberin: Art. 15 Abs. 2 Satz 1 MitwG). Ihnen steht ein direkter Anspruch auf die Informations- und Mitspracherechte zu, wenn keine Arbeitnehmervertretung bestellt worden ist (Art. 4 MitwG). Der Anspruch steht den Arbeitnehmern gesamthänderisch zu, da die Mitwirkungsrechte nicht individualisiert sind¹⁷²⁰ und der Belegschaft als nicht rechtsfähigem Verband keine Parteifähigkeit zukommt.¹⁷²¹ Die Arbeitnehmenden bilden somit eine notwendige Streitgenossenschaft, was bedeutet, dass sämtliche Arbeitnehmende gemeinsam klagen müssen (vgl. Art. 70

¹⁷¹⁷ Vgl. bzgl. der Mitwirkung bei Betriebsübergängen: WILDHABER 2011, 387.

¹⁷¹⁸ FURER 2009a, 150.

¹⁷¹⁹ FURER 2009a, 173.

¹⁷²⁰ FRITZ/SCHULER, 32.

¹⁷²¹ KASPER, N 193.

Abs. 1 ZPO).¹⁷²² Für grosse Belegschaften wird damit eine Klageerhebung illusorisch.¹⁷²³

Zur Klage legitimiert sind auch die Verbände der Arbeitnehmer und der Arbeitgeber (Art. 15 Abs. 2 MitwG).

Ob ein (nicht positiviertes) Klagerecht der Arbeitnehmervertretung besteht, sofern eine solche bestellt ist (vgl. Art. 3 MitwG), ist umstritten.¹⁷²⁴ Die Arbeitnehmervertretung wird nicht namentlich als klageberechtigte Partei aufgeführt (vgl. Art. 15 Abs. 2 MitwG). Doch suggeriert das Gesetz, dass die Mitwirkungsrechte der Arbeitnehmervertretung zustehen, sofern eine bestellt ist, und nicht direkt den Arbeitnehmern (Art. 4 *e contrario*; vgl. Art. 9–10 MitwG). Die Arbeitnehmervertretung ist verpflichtet, aktiv mitzuwirken (vgl. Art. 8 MitwG),¹⁷²⁵ während in Betrieben ohne Arbeitnehmervertretung die einzelnen Arbeitnehmer frei wählen, ob sie die Mitwirkungsrechte wahrnehmen oder darauf verzichten.¹⁷²⁶ Ob ein Klagerecht der Arbeitnehmervertretung zu befürworten ist, hängt davon ab, wie die Rechtsnatur der Arbeitnehmervertretung eingeschätzt wird. Richtigerweise ist mit WILDHABER und PORTMANN eine praktikable Lösung im Hinblick auf eine effiziente Mitwirkung der Arbeitnehmerschaft zu fordern. Der Arbeitnehmervertretung ist daher die Partei- und Prozessfähigkeit oder gar partielle Rechtsfähigkeit zuzugestehen, d.h., sie sollte im eigenen Namen oder im Namen der Belegschaft handeln können, nicht nur im Namen der einzelnen Arbeitnehmer.¹⁷²⁷ Solange ein höchstrichterlicher Entscheid betreffend das Klagerecht der Arbeitnehmervertretung fehlt, empfiehlt es sich, im Falle eines Streits mittels Prozessabrede unter den

¹⁷²² KASPER, N 193.

¹⁷²³ Deshalb flammt die Forderung auf, den Arbeitnehmenden das Recht auf eine individuelle Durchsetzbarkeit der Mitwirkungsrechte zu gewähren: KASPER, N 193.

¹⁷²⁴ Der Schweizerische Arbeitgeberverband lehnt ein Klagerecht der Arbeitnehmervertretung ab: FRITZ/SCHULER, 79. Der Schweizerische Gewerkschaftsbund hat das Klagerecht zunächst abgelehnt (NORDMANN, 20), später aber befürwortet (GABATHULER THOMAS, N 29). Klagelegitimation *sui generis* der Arbeitnehmervertretung bejahend: WYLER/HEINZER, 1237.

¹⁷²⁵ FRITZ/SCHULER, 48.

¹⁷²⁶ FRITZ/SCHULER, 48–49.

¹⁷²⁷ WILDHABER 2011, 370; PORTMANN/WILDHABER. Die Repräsentationstheorie (MÜLLER, 358) wird mit der vorgeschlagenen praktikablen Lösung nicht verworfen: WILDHABER 2011, 370.

Parteien den Auftritt der Arbeitnehmervertretung als Prozesspartei zu vereinbaren.¹⁷²⁸

Eine Arbeitnehmervertretung existiert jedoch nicht überall: Nur in Betrieben mit mindestens 50 Arbeitnehmern besteht ein Anspruch auf Vertretung (Art. 3 MitwG).¹⁷²⁹ People Analytics findet vorwiegend in grossen Betrieben Anwendung, sodass ein Anspruch auf Vertretung in der Regel besteht. Arbeitnehmervertretungen können auch für einzelne Betriebsbereiche (vgl. Art. 4 MitwG)¹⁷³⁰ oder Standorte¹⁷³¹ bestellt werden. Dies kann sinnvoll sein, wenn die Arbeitgeberin ein People Analytics-Pilotprojekt nur in einem Betriebsbereich lanciert.

Schwierigkeiten können bei der erstmaligen Bestellung der Arbeitnehmervertretung (Art. 5 MitwG) auftreten. Denn es braucht von den Betroffenen Freiwilligenarbeit und gehörigen Mut, sich zu exponieren, um die Unterschriften von einem Fünftel der Arbeitnehmer oder von 100 Beschäftigten (vgl. Art. 5 Abs. 1 MitwG) zu sammeln.¹⁷³² Solange die Arbeitnehmervertretung nicht bestellt ist, geniessen die Arbeitnehmer den Schutz hinsichtlich der Ausübung des Mitwirkungsrechts (vgl. Art. 12 MitwG) noch nicht.¹⁷³³ Bei relativ schwachem Kündigungsschutz¹⁷³⁴ bleiben auch missbräuchliche Kündigungen (vgl. Art. 336 Abs. 2 lit. b OR) wirksam, wobei sie eine Entschädigungspflicht auslösen.

c) **Rechtsbegehren**

Die Klage der Arbeitnehmer wird in der Regel eine Leistungsklage sein (vgl. Art. 84 ZPO). Das Rechtsbegehren kann lauten, dass die geschuldete Information geliefert und die versäumte Anhörung nachgeholt werden.

Für die Arbeitnehmerverbände geht der Anspruch hingegen nur auf Feststellung (Art. 15 Abs. 2 Satz 2 MitwG). Die Feststellung der Verletzung der Mitwirkungsrechte kann für eine vertragliche oder ausservertragliche Haftung der Arbeitgeberin Relevanz erlangen, sofern das Unterbleiben der Mitwirkung für eine Gesund-

¹⁷²⁸ ILG, 98–99.

¹⁷²⁹ Auch die Arbeitgeberin kann eine Arbeitnehmervertretung verlangen: FRITZ/SCHULER, 31. Daran kann sie ein Interesse haben, um die Verhandlungen effizient zu gestalten.

¹⁷³⁰ Mehrere Vertretungen innerhalb eines Betriebs oder ein Nebeneinander von Betriebsbereichen mit und ohne Arbeitnehmervertretung sind möglich: FRITZ/SCHULER, 32.

¹⁷³¹ FURER 2009a, 158.

¹⁷³² FURER 2009a, 157.

¹⁷³³ FURER 2009a, 157.

¹⁷³⁴ BIANCHI, 194. Vgl. S. 253.

heitsschädigung kausal war. Ein Anspruch auf Veröffentlichung eines Urteils könnte ein Unternehmen empfindlich treffen, ist aber nicht gesetzlich vorgesehen.¹⁷³⁵ Insgesamt spielen die Verbände eine subsidiäre Rolle bei der Durchsetzung der Mitwirkungsordnung.¹⁷³⁶

6.6.4 NFP75-Daten zur Mitwirkung

Wie die empirischen Daten des NFP75-Projekts suggerieren, wird das Potenzial des Mitwirkungsrechts für die Rechtsdurchsetzung nicht ausgeschöpft. Die Belegschaft wird nicht einmal in jedem zehnten Unternehmen vor dem Entscheid über die Beschaffung eines Analysetools konsultiert (Arbeitnehmervertretung, Einkauf und Fachstellen auf Konzernstufe zusammen 9 Prozent). Stattdessen sind am Entscheid über den Kauf von Analyse-Produkten in erster Linie die Personalabteilung (in 90 Prozent aller Fälle), die Unternehmensführung (81 Prozent) und die IT (64 Prozent) beteiligt. Des Weiteren werden die Rechtsabteilung (44 Prozent) sowie die Compliance- (36 Prozent), Finanz- (27 Prozent) und Ethik-Verantwortlichen beigezogen (11 Prozent).¹⁷³⁷ Bei der darauffolgenden Gestaltung und Anwendung des Analysetools wird die Meinung von Gewerkschaften (nur) in rund jedem zehnten Fall (11 Prozent) abgeholt. Das grosse Potenzial, das dem MitwG innewohnt,¹⁷³⁸ wird insgesamt unzulänglich ausgeschöpft.

6.7 Gesellschaftsrechtliche Haftung der exekutiven Organe

Die Mitglieder des Verwaltungsrats und alle mit der Geschäftsführung oder mit der Liquidation befassten Personen sind sowohl der Gesellschaft als auch den einzelnen Aktionären und Gesellschaftsgläubigern gegenüber für den Schaden verantwortlich, den sie durch absichtliche oder fahrlässige Verletzung ihrer Pflichten verursachen (Art. 754 Abs. 1 OR). Eine Haftung des Verwaltungsrats setzt eine Pflichtverletzung, einen kausal resultierenden Schaden und ein Verschulden voraus.

¹⁷³⁵ Vgl. FURER 2009a, 173.

¹⁷³⁶ KASPER, N 192.

¹⁷³⁷ WILDHABER/KASPER, 770.

¹⁷³⁸ Siehe S. 282–284.

Unübertragbare und unentziehbare Pflicht des Verwaltungsrats ist die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen (Art. 716a Abs. 1 Ziff. 5 OR). Hierzu gehört die Einhaltung der rechtlichen Bestimmungen beim Einsatz von People Analytics.¹⁷³⁹ Diese Aufgabe müssen die Mitglieder des Verwaltungsrats sowie Dritte, die mit der Geschäftsführung befasst sind, mit aller Sorgfalt erfüllen und die Interessen der Gesellschaft in guten Treuen wahren (Art. 717 Abs. 1 OR). Nur drei von zehn Führungskräften (30 Prozent) sind aber zuversichtlich, dass ihr Unternehmen mit Arbeitnehmerdaten verantwortungsvoll umgeht.¹⁷⁴⁰ Nicht einmal jedes fünfte Unternehmen weltweit (weniger als 20 Prozent) betraut ein Verwaltungsrats- oder Geschäftsführungsmitglied mit der Aufgabe der verantwortungsbewussten und ethisch vertretbaren Verwendung von arbeitsplatzbezogenen Daten und Technologien.¹⁷⁴¹ Der Verwaltungsrat ist in der Regel nicht nahe genug an den komplexen Datenbearbeitungsprozessen, um diese lückenlos erklären zu können.¹⁷⁴²

Zur Pflicht des Verwaltungsrats gehört ferner das Management der Rechtsrisiken, die aus People Analytics fließen.¹⁷⁴³ Dies ergibt sich sowohl aus der Pflicht zur Oberleitung der Gesellschaft (Art. 716a Abs. 1 Ziff. 1 OR)¹⁷⁴⁴ als auch aus der Pflicht zur Erstellung des Geschäftsberichts (Art. 716a Abs. 1 Ziff. 6 OR), der bei grösseren Unternehmen, die von Gesetzes wegen zu einer ordentlichen Revision verpflichtet sind (vgl. Art. 727 Abs. 1 Ziff. 1–3 OR), einen Lagebericht (Art. 961 Ziff. 3 i.V.m. Art. 958 Abs. 2 Satz 3 OR) mit Angaben über die Durchführung

¹⁷³⁹ Gewährleistung der Compliance als Teil der Oberaufsicht: NOBEL, § 9 N 118.

¹⁷⁴⁰ SHOOK *et al.*

¹⁷⁴¹ «Less than 20 [percent] of the companies have a C-level executive in charge of this»: SHOOK *et al.*

¹⁷⁴² Vgl. NISSENBAUM 2011, 35: In der Regel kann nur eine Hand voll Experten die Datenbearbeitungen darstellen.

¹⁷⁴³ Risikomanagement als typische Aufgabe der Exekutive: NOBEL, § 9 N 118. In grösseren Gesellschaften wird das Management von Rechtsrisiken von der Geschäftsleitung wahrgenommen und vom Verwaltungsrat bzw. von seinem Audit Committee überwacht: BSK OR II-PFIFNER/WATTER, Art. 728a OR, N 24. 2008 waren bei den schweizerischen mittelgrossen Unternehmen der Verwaltungsrat in 50,8 Prozent der Fälle und die Geschäftsleitung in 88,3 Prozent der Fälle für das Risikomanagement zuständig: RUUD *et al.*

¹⁷⁴⁴ Die Oberleitung umfasst die Festlegung der Strategie des Unternehmens innerhalb des statutarischen Zweckes: BSK OR II-WATTER/ROTH PELLANDA, Art. 716a OR, N 4. Und das Management von Rechtsrisiken ist eine strategische Aufgabe: KURER, 56.

einer Risikobeurteilung enthält (Art. 961c Abs. 2 Ziff. 2 OR).¹⁷⁴⁵ Die Pflicht zum Rechtsrisiko-Management ergibt sich ferner aus der Organisationspflicht (Art. 716a Abs. 1 Ziff. 2 OR).¹⁷⁴⁶ Somit kann der Verwaltungsrat das Management von Rechtsrisiken nicht an eine Stabsstelle, Compliance Officers oder Anwälte delegieren (vgl. Art. 716b OR).¹⁷⁴⁷

Insgesamt besteht ein reales Risiko einer Haftung der exekutiven Organe der Gesellschaft, vorausgesetzt, dass auch ein entsprechender Schaden, ein Kausalzusammenhang und ein Verschulden nachgewiesen werden können.

6.8 Arbeitsverweigerung, Streik und Kündigung

Kann die Arbeit infolge Verschuldens der Arbeitgeberin nicht geleistet werden oder kommt diese aus anderen Gründen mit der Annahme der Arbeitsleistung in Verzug, so bleibt sie zur Entrichtung des Lohns verpflichtet, ohne dass der Arbeitnehmer zur Nachleistung verpflichtet ist (Art. 324 Abs. 1 OR). Von einem Annahmeverzug und Recht auf Verweigerung der individuellen Arbeitsleistung ist auszugehen, wenn sich die Arbeitgeberin weigert, Massnahmen zum Schutz von Leben und Gesundheit zu treffen und beispielsweise ein unverhältnismässiges Überwachungs- und Kontrollsystem nicht demontiert (Art. 26 Abs. 1 ArGV 3). Grundsätzlich gefährdet erst eine länger andauernde Überwachung die psychische Gesundheit des Arbeitnehmers. Daher darf dieser die Arbeit nicht sofort verweigern, sondern muss alles in seinen Möglichkeiten Stehende unternehmen, um die

¹⁷⁴⁵ Dazu gehören Angaben über den Prozess der Risikobeurteilung und über die Risiken: BSK OR II-NEUHAUS/INAUEN, Art. 961c OR, N 12. BÖCKLI, N 813. Zu besprechen sind alle wesentlichen Risiken, denen das Unternehmen ausgesetzt ist (BSK OR II-PIFFNER/WATTER, Art. 728a OR, N 21; BSK OR II-NEUHAUS/INAUEN, Art. 961c OR, N 12), einschliesslich der Rechtsrisiken (BÖCKLI, N 814).

¹⁷⁴⁶ Im Rahmen der Organisationspflicht kann der Verwaltungsrat ein Risk Committee für das Risikomanagement bestellen: BSK OR II-WATTER/ROTH PELLANDA, Art. 716a OR, N 6. Vgl. MILLER, 483. Möglich ist ebenso ein Corporate Responsibility oder Sustainability Committee für die nachhaltige Entwicklung des Unternehmens, wozu auch die Pflege der Beziehung zu den Mitarbeitern, die bei People Analytics besonders wichtig ist, gehört: BSK OR II-WATTER/ROTH PELLANDA, Art. 716a OR, N 50c.

¹⁷⁴⁷ KURER, 8. Die oberste Leitungsebene muss «tief in den Bereichen verankert» sein: BIEDENKOPF, 148.

Situation zu verbessern (z.B. Vorwarnung der Arbeitgeberin, Verlangen von Abhilfe).¹⁷⁴⁸

Streik und Aussperrung sind zulässig, wenn sie Arbeitsbeziehungen betreffen und wenn keine Verpflichtungen entgegenstehen, den Arbeitsfrieden zu wahren oder Schlichtungsverhandlungen zu führen (Art. 28 Abs. 3 BV). Das verfassungsmässige kollektive Streikrecht entfaltet direkte Horizontalwirkung und ist somit in privatrechtlichen Arbeitsverhältnissen anwendbar.¹⁷⁴⁹ In der Schweiz kommen Streiks zwar selten vor. Aber in den Amazon-Warenlagern in Deutschland und Spanien, in denen Mitarbeiter überwacht werden, gehören sie zur Realität.¹⁷⁵⁰ Bereits 1911 streikten Arbeitnehmer in einer Giesserei bei Boston gegen die früher verbreitete Praxis des «Taylorismus», bei der ein Aufseher mit einer Stoppuhr die Arbeitnehmer bei den Arbeitsvorgängen begleitete.¹⁷⁵¹

Zu bedenken ist das Risiko einer Kündigung durch den Arbeitnehmer, falls People Analytics das Vertrauensverhältnis am Arbeitsplatz zerstören sollte. Der Arbeitnehmer kann unter Einhaltung der Kündigungsfrist (Art. 335b–335c OR) und des zeitlichen Kündigungsschutzes (Art. 336d Abs. 1 OR) ordentlich kündigen (Art. 335 OR). Aus wichtigen Gründen kann der Arbeitnehmer jederzeit das Arbeitsverhältnis fristlos kündigen; als wichtiger Grund gilt namentlich jeder Umstand, bei dessen Vorhandensein dem Kündigenden nach Treu und Glauben die Fortsetzung des Arbeitsverhältnisses nicht mehr zugemutet werden darf (Art. 337 Abs. 1–2 OR).

6.9 Zwischenfazit: mühevoll Rechtsdurchsetzung

Das Datenschutzrecht wird in der Praxis nicht konsequent durchgesetzt.¹⁷⁵² Für die Rechtsdurchsetzung *ex post* sind hauptsächlich die Betroffenen persönlich ver-

¹⁷⁴⁸ WOLFER, N 593.

¹⁷⁴⁹ SGK-SCHWEIZER, Art. 35 BV, N 60.

¹⁷⁵⁰ KECK CATIE, Amazon workers in Spain and Germany announce strikes ahead of Christmas: «Change must come now», 09.12.2018, abrufbar unter <<https://gizmodo.com>> (besucht am 31.05.2020).

¹⁷⁵¹ Siehe S. 70. SPRAGUE 2015, 45.

¹⁷⁵² «There is a huge gap between law on paper and the application»: HIJMANS/KRANENBORG, 5. Vgl. BUCHNER/KÜHLING, 548. Anspruch und Wirklichkeit fallen in keinem Rechtsgebiet so sehr auseinander wie im Datenschutzrecht, was ersichtlich wird, wenn

antwortlich.¹⁷⁵³ Jedoch stehen einer Individualklage zahlreiche materiell- und verfahrensrechtliche Hürden im Wege.¹⁷⁵⁴

Die Hoffnung, der aufwendigen Individualrechtsdurchsetzung mit der Mobilisierung von Gruppeninteressen zu begegnen, zerschlägt sich mehrfach: Der EDÖB kann unverbindliche Empfehlungen, aber keine Verfügungen erlassen, geschweige denn Verwaltungssanktionen, wie z.B. Bussen, aussprechen.¹⁷⁵⁵ Die Arbeitsinspektorate schreiten grundsätzlich erst ein, wenn People Analytics gesundheitsschädliche Auswirkungen zeitigt.¹⁷⁵⁶ Strafverfolgungen wegen People Analytics spielen eine untergeordnete Rolle.¹⁷⁵⁷ Eine mitwirkungsrechtliche Anzeige zieht keine Sanktionen nach sich und eine Klage scheitert in der Regel an prozessrechtlichen Barrieren.¹⁷⁵⁸ Ein solches Verfahren ist auch nicht attraktiv, weil materiell-rechtlich kein Mitentscheidungsrecht in Aussicht steht.¹⁷⁵⁹ Gegebenenfalls wirkt das Risiko einer gesellschaftsrechtlichen Haftung regulierend.¹⁷⁶⁰ Arbeitsverweigerung, Streik und Kündigung verkörpern nur Notlösungen, die wenn immer möglich zu verhindern sind.¹⁷⁶¹

Ein gegensätzlicher Befund ergibt sich bei Sachverhalten, die in den Anwendungsbereich der DSGVO fallen. Die Aufsichtsbehörden der EU-Mitgliedstaaten können Verfügungen erlassen und Bussen bis zu EUR 20 Mio. oder vier Prozent des weltweiten Jahresumsatzes verhängen.¹⁷⁶² Diese wirken abschreckend, sodass das Risiko von Persönlichkeitsverletzungen sinkt.¹⁷⁶³ Auf die Annäherung des schwei-

der Berliner Datenschutzbeauftragte Skype-Interviews zu Einstellungszwecken als unzulässig erachtet: CULIK, 299.

¹⁷⁵³ Siehe S. 251.

¹⁷⁵⁴ Siehe S. 268–273.

¹⁷⁵⁵ Siehe S. 275–278.

¹⁷⁵⁶ Siehe S. 279–281.

¹⁷⁵⁷ Siehe S. 281–282.

¹⁷⁵⁸ Siehe S. 284–288.

¹⁷⁵⁹ Siehe S. 105.

¹⁷⁶⁰ Siehe S. 288–290.

¹⁷⁶¹ Siehe S. 290–291.

¹⁷⁶² Siehe S. 278–279.

¹⁷⁶³ **A.M. HORNUNG**, 90: Es sei zweifelhaft, ob sich die neuen Sanktionsinstrumente gegen den enormen ökonomischen Druck behaupten können, der hinter der Einführung von Big Data-Anwendungen steht.

zerischen Rechts an den europäischen Standard im Rahmen der Totalrevision des DSG ist zu einem späteren Zeitpunkt noch zurückzukommen.¹⁷⁶⁴

Die im schweizerischen Recht gegenwärtig gehemmte Rechtsdurchsetzung bedeutet für die Arbeitgeberin, dass sie geringe Rechtsrisiken bei einem Verstoß gegen die Bestimmungen des DSG und des Diskriminierungsschutzrechts zu befürchten hat. Das Recht lässt somit die durch den technischen Fortschritt angestossene Machtverschiebung im Arbeitsverhältnis tatenlos zu,¹⁷⁶⁵ ohne die Opposition mit wirksamen Kontrollrechten auszustatten. Dies ist, gepaart mit dem fehlenden Fachwissen auf Seiten der Arbeitgeberin,¹⁷⁶⁶ eine gefährliche Mischung, weil das DSG zum toten Buchstaben zu verkümmern droht. Die Glaubwürdigkeit des gesamten Datenschutz-Rechtssystems ist infrage gestellt. Im folgenden Kapitel ist daher ein Konzept zu entwerfen, das dem Datenschutz Leben einhauchen und Systemstabilität verleihen wird.

¹⁷⁶⁴ Siehe S. 348–351.

¹⁷⁶⁵ Siehe zur Machtverschiebung S. 79–82.

¹⁷⁶⁶ Siehe S. 242–247.

7 Neuausrichtung des Datenschutzrechts

7.1 Rekapitulation der gegenwärtigen Probleme

In diesem Kapitel soll aufgezeigt werden, dass das gegenwärtige Datenschutzrecht der Schweiz einer Erneuerung bedarf und wie dieselbe umgesetzt werden könnte. Somit wird die Forschungsfrage beantwortet, die lautet: *Wie könnte eine künftige Neuausrichtung des privatrechtlichen Datenschutzrechts aussehen, bei welcher die Rechtsdurchsetzung ex ante und ex post im Zusammenhang mit People Analytics besser gewährleistet wäre als heute?*¹⁷⁶⁷

Wer aber mit dem Vorschlag einer Neuausrichtung gegen den Strom schwimmen will, muss Atem holen. Deshalb sind die früheren Gedankengänge noch einmal vorzuspielen: In Kapitel 2 wurde festgestellt, dass People Analytics ein neues Phänomen ist, das die arbeitsvertragliche Beziehung beeinflusst.¹⁷⁶⁸ Rechtsrelevant ist dies, weil es zu einer Machtverschiebung im Arbeitsverhältnis und dadurch zu möglichen Einschränkungen der Persönlichkeits-, der Diskriminierungsschutz- und der Mitwirkungsrechte der Arbeitnehmer kommt.¹⁷⁶⁹ Die korrekte Anwendung der datenschutzrechtlichen Bearbeitungsregeln und Rechtfertigungsgründe *ex ante* setzt ein hohes Reflexionsniveau der Arbeitgeberin voraus, das jedoch nicht immer erreicht wird.¹⁷⁷⁰ Gleichzeitig statet das auf People Analytics anwendbare Recht die Gegenseite der Arbeitgeberin weder auf Individual- noch auf Gruppenebene mit hilfreichen Kontrollmechanismen aus, um das Datenschutzrecht *ex post* durchzusetzen.¹⁷⁷¹

Im gegenwärtigen datenschutzrechtlichen Persönlichkeitsschutz, der als Abwehrrecht und Recht zur informationellen Selbstbestimmung aufgebaut ist, sind zudem hauptsächlich die betroffenen Individuen zur Durchsetzung der Rechte an den sie betreffenden Daten verantwortlich.¹⁷⁷² Die einzelnen Arbeitnehmer sind jedoch mit dieser Aufgabe überfordert, weil sie in einer Zeit ubiquitärer Datenbearbeitungen nicht über genügende individuelle Kontrollressourcen verfügen.¹⁷⁷³ Der

¹⁷⁶⁷ Siehe S. 11.

¹⁷⁶⁸ Siehe S. 69–78.

¹⁷⁶⁹ Siehe Kapitel 3, S. 79–106.

¹⁷⁷⁰ Siehe Kapitel 4, insbesondere S. 131–132, und Kapitel 5, insbesondere S. 242–250.

¹⁷⁷¹ Siehe Kapitel 6, insbesondere S. 291–293.

¹⁷⁷² Siehe S. 251–252.

¹⁷⁷³ Siehe S. 267–274.

Mangel an Fachkompetenz bei gleichzeitig ausbleibenden Kontrollen führt zu einer Instabilität des gesamten Datenschutz-Rechtssystems.¹⁷⁷⁴ Zusammenfassend sollte mit dem gegenwärtigen System nicht fortgefahren werden. Es braucht eine neue Konzeption des datenschutzrechtlichen Persönlichkeitsschutzes.

7.2 Neuausrichtung auf das Teilen von Information und die Stärkung des Vertrauens in das Datenschutzrecht

7.2.1 Überblick

Um die beschriebenen Probleme des gegenwärtigen Datenschutzrechts zu überwinden, wird in der Literatur geltend gemacht, dass sich das Datenschutzrecht vermehrt darauf konzentrieren sollte, das Teilen von Information zu fördern (dazu sogleich). Gleichzeitig bestehen Vorschläge, das Vertrauen in das Datenschutzrecht zu stärken (dazu S. 301–313). Diese beiden Ideenstränge gehören nach der vorliegend vertretenen Auffassung zusammen. Sie allein können jedoch nicht zur wirksamen Reformierung des Datenschutzrechts genügen, wie in der anschließenden Kritik aufzuzeigen ist (dazu S. 313–314).

7.2.2 Förderung des Teilens von Information

a) Bedeutung des Teilens für die Informationsgesellschaft

Mit dem Aufkommen eines wirtschaftlichen, soziokulturellen und rechtlichen Gesellschaftssystems auf dem Boden von Datenbearbeitungen und Austausch von Wissen¹⁷⁷⁵ wird das Teilen von Daten mindestens so bedeutsam wie deren Schutz: *«We are a society of sharers.»*¹⁷⁷⁶ Freiheit ist nicht nur die Freiheit von anderen, sondern entsteht auch durch andere.¹⁷⁷⁷

¹⁷⁷⁴ Siehe S. 291–293.

¹⁷⁷⁵ Siehe zum Trend zur Wissensgesellschaft S. 67–68.

¹⁷⁷⁶ WALDMAN, 67.

¹⁷⁷⁷ TALIDOU, 19. Informationen über andere brauchen wir, um uns ihnen gegenüber angemessen zu verhalten: BAUMANN MAX-OTTO, 3. Es kann sein, dass eine Person unter Berufung auf das Recht auf informationelle Selbstbestimmung möchte, dass ihre Daten bearbeitet werden: ROSENTHAL 2012, 82.

Der Gedanke der Selbstentfaltung in der Gemeinschaft reicht historisch weit zurück. Bereits in der Antike beschreibt Aristoteles (384–322 v.Chr.) die Rolle des Subjekts in der staatlichen Gemeinschaft (altgr. πόλις, «*polis*») und der Hausgemeinschaft (altgr. οἶκος, «*oikos*»).

¹⁷⁷⁸ In der römischen Zeit wirkt dieses Begriffspaar fort (lat. *res publica*: Staat, Gemeinwesen; und lat. *domus*: Haus, Hausgenossenschaft).¹⁷⁷⁹ Primär interessiert die Interaktion zwischen der Person und ihrem Umfeld. Bezeichnend für dieses Menschenbild ist beispielsweise die folgende Stelle beim römischen Staatsmann und Rechtsanwalt CICERO (106–43 v.Chr.) zur Rolle des Privatmanns (lat. *privatus*): «Für den Privatmann aber gehört es sich, auf der Grundlage der Rechtsgleichheit mit den Bürgern zu leben [...] und in der Politik friedliche und anständige Ziele zu verfolgen. Denn einen solchen Menschen pflegen wir als guten Bürger zu erleben und zu bezeichnen.»¹⁷⁸⁰ Zwar entsteht bei den Römern die terminologische Unterscheidung zwischen öffentlich (lat. *publicus*) und privat (lat. *privatus*).¹⁷⁸¹ Bis ins Mittelalter bleibt aber die Vorstellung vom Privaten nicht mit Individualität verbunden, sondern wird im Wesentlichen mit dem Familienleben gleichgesetzt.¹⁷⁸² Die Existenz des Menschen definiert sich durch seine Zugehörigkeit zu Gemeinschaften wie etwa Sippen, Zünften, klösterlichen Gemeinschaften oder Vasallenverbindungen.¹⁷⁸³

Der Individualismus und die Vorstellung, dass jeder frei von äusseren Zwängen sein soll, entstammen erst der Renaissance.

¹⁷⁸⁴ Ende des 17. Jh. setzen sich im Bürgertum das Einzelzimmer und das Einzelbett immer mehr durch.¹⁷⁸⁵ Die Privatsphäre erhält ihre heutige Ausprägung im Bürgertum des 18. und 19. Jh., als das Private zum Synonym für Glück wird.¹⁷⁸⁶

Mit der Digitalisierung haben sich die Bedingungen des Privaten gegenüber der Zeit zwischen Renaissance und 19. Jh. grundlegend gewandelt.

¹⁷⁸⁷ Zu hinterfragen

¹⁷⁷⁸ SCHIEDERMAIR, 24; BELSER 2011c, § 2 N 9.

¹⁷⁷⁹ SCHIEDERMAIR, 26.

¹⁷⁸⁰ CICERO, Liber primus/erstes Buch, Ziff. 124.

¹⁷⁸¹ SCHIEDERMAIR, 56.

¹⁷⁸² SCHIEDERMAIR, 29.

¹⁷⁸³ MEIER PHILIPPE, N 2.

¹⁷⁸⁴ HILDEBRANDT/KOOPS, 446; «Entdeckung des Individuums» in der Renaissance: SCHIEDERMAIR, 31.

¹⁷⁸⁵ Auch aus hygienischen Gründen kommt das Einzelzimmer auf: SCHIEDERMAIR, 33.

¹⁷⁸⁶ SCHIEDERMAIR, 35; MEIER PHILIPPE, N 2; BELSER 2011c, § 2 N 9.

¹⁷⁸⁷ SCHIEDERMAIR, 415.

ist daher die prominente Stellung des Persönlichkeitsschutzes als Abwehrrecht und der informationellen Selbstbestimmung in der Form eines Vetorechts. Nach der vorliegend vertretenen Auffassung ist eine Rückbesinnung auf die Antike und das Mittelalter angezeigt. Es braucht (auch) ein Konzept für den Menschen *in* der Informations- und Kommunikationsgesellschaft.¹⁷⁸⁸ Hierbei ist das heutzutage unvermeidliche Teilen von Informationen mit dem Persönlichkeitsschutz in Einklang zu bringen.¹⁷⁸⁹ Diesen Spagat hat die Rechtsordnung bisher nicht geschafft.¹⁷⁹⁰ People Analytics kann den versprochenen Fortschritt nur bringen, wenn auch Daten verfügbar sind, d.h., wenn die Mitarbeiter ihre Daten mit der Arbeitgeberin teilen.¹⁷⁹¹

b) Schranken des Teilens

aa) Richtiges Mass an Teilen

Wenn das erneuerte Datenschutzrecht sich am Teilen orientieren soll, muss das richtige Mass dafür gefunden werden. Sowohl ein Unter- als auch ein Übermass davon sind zu vermeiden, wie sogleich erklärt wird.

bb) Untermass an Teilen

Der Zielwert der Abwehr von Einflüssen auf die Persönlichkeit ist ein Stück weit zu relativieren. Ein Abschottungszustand, in dem keine Informationen geteilt werden, ist nicht erstrebenswert. Ein Individuum kann nicht die informationelle Selbstbestimmung (wieder-)erlangen, indem es den Weg der digitalen Keuschheit beschreitet. Diese Alternative wäre nicht zumutbar. Sich von der Informationsgesellschaft auszuklinken, käme einem kümmerlichen Leben als sozialer Eremit gleich, weil so viele Aspekte des modernen Lebens – von der Kommunikation bis

¹⁷⁸⁸ RUDIN 2007, 25.

¹⁷⁸⁹ Der Bundesrat sieht Handlungsbedarf beim DSG, will aber die Teilhabe der Gesellschaft und Wirtschaft an den Kommunikationstechnologien nicht gefährden: Schweizerischer Bundesrat 2012, 348. Die Informationsgesellschaft brauche Kommunikationsmöglichkeiten: TALIDOU, 19. Vgl. BAUMANN MAX-OTTO, 2: Wegen der zunehmenden Kommunikation und des Teilens von Daten erlange der Schutz der Privatsphäre über den intrinsischen, individuellen hinaus einen gesellschaftlichen Wert.

¹⁷⁹⁰ Die OECD-Leitlinien lassen offen, wie das grundsätzliche Dilemma zwischen dem freien Informationsfluss und dem Datenschutz aufzulösen ist: SCHIEDERMAIR, 149.

¹⁷⁹¹ Siehe zu den versprochenen Chancen von People Analytics S. 2–3. Vgl. RUDIN 2004b, 438: Investitionen in die Technologie lohnen sich nur, wenn das Vertrauen der Konsumenten gewonnen werden kann.

zum Online-Einkauf – digital erfolgen.¹⁷⁹² Vernetzte Technologien sind eine Tatsache des modernen Lebens, und wir sind ein Stück weit von ihnen abhängig geworden.¹⁷⁹³ Werden ganze Infrastrukturen digitalisiert, weil die gesellschaftliche Mehrheit dies begrüsst, beispielsweise durch die Einführung elektronischer Bezahlungssysteme, kann sich ein Einzelner dem nicht mehr entziehen.¹⁷⁹⁴

Am Arbeitsplatz ist es besonders schwierig, sich den Datenbearbeitungen zu entziehen. Wer auf Datenabstinentz beharrt, riskiert, seine Stelle zu verlieren. Der Arbeitnehmer fügt sich in eine fremde Arbeitsorganisation ein. Die Arbeitgeberin diktiert, welche Datenbearbeitungen für die Erledigung der Arbeit erforderlich sind.

Selbst wenn jemand auf die Technik verzichten würde, wäre er nicht vor Datenanalysen gefeit: Tragen Personen aus dem Umfeld intelligente Brillen, so wird auch der Verzichtende digital erfasst. Ferner sind, wie dargelegt,¹⁷⁹⁵ Ableitungen über ihn möglich, wenn genügend viele Personen um ihn herum ihre Daten freiwillig zur Verfügung stellen.¹⁷⁹⁶

Schliesslich führt Isolation nicht notwendig zu mehr Autonomie, wie das Beispiel des schiffbrüchigen Bewohners einer einsamen Insel zeigt: Auch wenn dieser sich völlig aus dem Bewusstsein anderer verabschiedet, geniesst er keine informationelle Selbstbestimmung, da er seine Positionsdaten niemandem kommunizieren kann.¹⁷⁹⁷

cc) Übermass an Teilen

Zu viel Informationsteilung ist nicht förderlich. Man könnte vielleicht meinen, der Arbeitnehmer könne ja die Datenbearbeiter gewähren lassen, denn solange er sich gesetzestreu verhalte, habe er nichts zu verbergen. Diese Haltung würde aber verkennen, dass es bei der durch den liberalen Staat zugesicherten Privatsphäre nicht um etwas Verbotenes oder Unanständiges geht, sondern um etwas, das man für

¹⁷⁹² POLEDNA TOMAS, Vom Ende des Datenschutzrechts, NZZ vom 08.11.2016, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020); SPRAGUE 2015, 28; RICHARDS/HARTZOG 2016, 444–445.

¹⁷⁹³ WALDMAN, 68; PURTOVA 2011, 39.

¹⁷⁹⁴ BAUMANN MAX-OTTO, 5.

¹⁷⁹⁵ Siehe S. 232.

¹⁷⁹⁶ Vgl. zu sozialen Netzwerken: HORVÁT *et al.*, 7; MATZNER, 98.

¹⁷⁹⁷ RULE, 3.

sich behalten oder nur mit einem ausgewählten Kreis teilen möchte.¹⁷⁹⁸ Zudem zeigt die sozialwissenschaftliche Forschung, dass Personen, die unter Beobachtung stehen, weniger produktiv und weniger offen sind.¹⁷⁹⁹ Arbeitnehmer sind eher gewillt, ihre neuen Ideen zu teilen, wenn sie einen gewissen Grad an Privatsphäre am Arbeitsplatz genießen und von den Arbeitskollegen erwarten können, dass sie sich an die anerkannten Normen halten.¹⁸⁰⁰ In einem Experiment stieg die Produktivität eines Betriebs um 10–15 Prozent, als die Arbeitsteams ihre Arbeit hinter Vorhängen, frei von überwachenden Blicken verrichten durften.¹⁸⁰¹

**c) Regulierungsgefäß für die am Teilen
 ausgerichtete Neuordnung**

Der datenschutzrechtliche Persönlichkeitsschutz eignet sich als Regulierungsgefäß für die geplante Ausrichtung am Teilen von Information, weil er (auch) auf eine soziale Kommunikationsordnung abzielt¹⁸⁰² und die dialektische Gegenseitigkeit fördert.¹⁸⁰³ Nach der Rechtsprechung des EGMR umfasst das Recht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) bis zu einem gewissen Grad auch das Recht, Beziehungen zu anderen Menschen zu knüpfen und zu vertiefen, insbesondere Beziehungen im Arbeitsleben.¹⁸⁰⁴ Die mit dem Persönlichkeitsschutz erstrebte Autonomie entsteht nur auf der Basis eines gut informierten und an den gesellschaftlichen Prozessen teilnehmenden Individuums. Dieses schottet sich nicht egozentrisch von den vernetzten sozialen Lebensräumen ab, sondern setzt sich bewusst den neuen Gefahren aus, genießt dafür aber zugleich

¹⁷⁹⁸ RUDIN 2008, 8; RUDIN 2004a, 4.

¹⁷⁹⁹ Vgl. RICHARDS, 186.

¹⁸⁰⁰ WALDMAN, 74.

¹⁸⁰¹ BERNSTEIN, 196; ROSENBLAT/KNEESE/BOYD, 12.

¹⁸⁰² HORNUNG, 90–91. Sozialschädlich sei der Grundsatz der Datenminimierung, weil er eine Kommunikations- und Informationsminimierung bedeute: HÄRTING, N 253.

¹⁸⁰³ TALIDOU, 19. Unser Denken über die Privatsphäre müsse sich «nach aussen» richten: BAUMANN MAX-OTTO, 2, m.w.H. Nicht immer stehen individuelle Privatsphäre und Gesellschaft in einem Konflikt, und der Persönlichkeitsschutz sei integraler Bestandteil der Dynamik aller sozialen Beziehungen: ROESSLER/MOKROSINSKA, 771. Der Persönlichkeitsschutz stehe nicht zwangsläufig in einem Widerspruch zu den Interessen der sozialen Gemeinschaft: JERVIS, 452.

¹⁸⁰⁴ Urteil EGMR vom 16.12.1992, Niemietz vs. Germany, Nr. 13710/88, N 29; Europarat 2016b, 29. A.M. JERVIS, 452: Der gesellschaftliche Wert von Privatsphäre sei bei Interessenabwägungen «häufig unterbewertet» und im Entscheid Urteil EGMR vom 05.09.2017, Bărbulescu vs. Romania, Nr. 61496/08, «nicht anerkannt» worden.

auch die unermesslichen Möglichkeiten.¹⁸⁰⁵ Beispielsweise geht der Arbeitnehmer, der zum Zweck der besprochenen Stimmungsanalyse¹⁸⁰⁶ intime Informationen zu seinen Emotionen an die Arbeitgeberin preisgibt, das Risiko ein, dass die Daten missbraucht werden. Doch bietet sich auch die Chance, dass die Arbeitgeberin dank dem Wissen um die Gefühlslage im Unternehmen Verbesserungsmaßnahmen trifft, etwa Anreizprogramme zur Verhinderung von Personalfluktuationen.¹⁸⁰⁷

7.2.3 Stärkung des Vertrauens in das Datenschutzrecht

a) Datenschutz mit Vertrauenskomponente (*privacy-as-trust*)

Die vorstehend beschriebene Idee, das Teilen von Informationen zu begünstigen, gewinnt nicht nur in Europa an Boden. In der amerikanischen Rechtslehre ist ein ähnlicher Gedanke anzutreffen. Dort verschafft sich eine Meinung Gehör, die den Wert «Vertrauen» in den Persönlichkeitsschutz integrieren will (*privacy-as-trust*). Namentlich WALDMAN sowie RICHARDS und HARTZOG, aber auch BAMBERGER und MULLIGAN vertreten diese These.¹⁸⁰⁸ Aufgabe des Datenschutzes ist es demnach, das Vertrauen zu schützen, welches zur Pflege von Informationsbeziehungen mit anderen Menschen, mit Unternehmen oder mit dem Staat vorausgesetzt wird.¹⁸⁰⁹ Wegzurücken ist von der Einstellung, Persönlichkeitsschutz diene allein Individuen zur Abwehr von Bedrohungen (*privacy pessimism*). Stattdessen ist der Persönlichkeitsschutz auf positive Werte auszurichten, die das System der Datenwirtschaft als Ganzes stärken, wie beispielsweise auf Vertrauen (*privacy in positive terms*).¹⁸¹⁰ Auch das Teilen von Daten soll aktiv geschützt und gefördert werden.¹⁸¹¹ Diese Einstellung dürfte den präventiven Datenschutz begünstigen und den repressiven Rechtsschutz entlasten.

¹⁸⁰⁵ TALIDOU, 19. Siehe zum Begriff der Autonomie S. 84–85.

¹⁸⁰⁶ Siehe S. 57.

¹⁸⁰⁷ Siehe zu den Anreizprogrammen S. 57.

¹⁸⁰⁸ WALDMAN; RICHARDS/HARTZOG 2016; BAMBERGER/MULLIGAN 2015.

¹⁸⁰⁹ RICHARDS/HARTZOG 2017, 1185 und 1187. Bereits in den 1990er-Jahren bestand ein internationaler Konsens über die Bedeutung von Vertrauen in die Informations- und Kommunikationstechnologien im privaten und im öffentlichen Sektor: BAMBERGER/MULLIGAN 2015, 185.

¹⁸¹⁰ RICHARDS/HARTZOG 2016, 431; RICHARDS/HARTZOG 2017, 1182.

¹⁸¹¹ Das Teilen von Information wird somit nicht nur als unvermeidbare Nebenerscheinung des Informationszeitalters abgetan: WALDMAN, 67.

Die Lehre vom Datenschutz mit Vertrauenskomponente anerkennt im Ausgangspunkt, dass das Vertrauen in einen robusten Persönlichkeitsschutz und die Bereitschaft zum Teilen von Information in einer funktionalen Beziehung zueinander stehen: Der Schutz der Privatsphäre ermöglicht Vertrauen, und je grösser das Vertrauen ist, desto eher werden Informationen preisgegeben.¹⁸¹² Umgekehrt kommt es zu einem Teufelskreis: Je geringer das Vertrauen ist, desto eher versuchen Arbeitnehmer, sich unsichtbar zu machen. Dies erschwert für Unternehmen das Mitverfolgen der Geschehnisse im Betrieb, weshalb sie eher zu Überwachungsmaßnahmen greifen und dadurch auch Rechtsverletzungen möglich werden.¹⁸¹³

Privacy-as-trust geht zum bisherigen Datenschutzrecht, das sich auf die Individualrechte wie Einwilligung und Verweigerung konzentriert, ein Stück weit auf Distanz. Mit dem Schritt zurück erweitert der Vertrauensansatz den Blick auf die Informationsbeziehungen, die die Datenoffenlegungen veranlassen.¹⁸¹⁴ Informationsbeziehungen sind Beziehungen, in denen Informationen vertraulich geteilt werden. Die dabei geltenden Regeln für den Informationsaustausch schaffen für die Parteien einen Mehrwert, sodass diese Beziehungen im Laufe der Zeit vertieft werden.¹⁸¹⁵ Persönlichkeitsschutz, insbesondere Datenschutz, besteht (auch) aus den Normen, die für Informationsbeziehungen gelten.¹⁸¹⁶ Diese Sichtweise führt eine soziale Dimension in den Persönlichkeitsschutz ein. Ziel des Datenschutzes ist es, nicht mehr bloss Dritte von Informationen auszuschliessen, sondern den Informationsfluss zu regulieren, d.h. zu definieren, wann eine Informationsquelle für jemanden versiegen soll und wann Schleusen für andere Personen geöffnet werden sollen.¹⁸¹⁷

Das Datenschutz-Rechtssystem als Ganzes kann Schaden nehmen, wenn das Vertrauen leidet und dadurch die Informationsflüsse ins Stocken geraten.¹⁸¹⁸ Die Pri-

¹⁸¹² HARTZOG 2018, 17; TAMÒ-LARRIEUX, 36. Steuerpflichtige legen die Angaben zu ihrem Vermögen offen, wenn sie sicher sind, dass die Steuerbehörde die Informationen nicht weitergibt: NISSENBAUM 2011, 40. Der Privatsphäreschutz und das Teilen von Information müssen kompatibel sein: WALDMAN, 61.

¹⁸¹³ KATZ MIRANDA, *The creative ways your boss is spying on you*, 08.12.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020).

¹⁸¹⁴ WALDMAN, 77.

¹⁸¹⁵ RICHARDS/HARTZOG 2017, 1185.

¹⁸¹⁶ RICHARDS/HARTZOG 2017, 1185; WALDMAN, 149.

¹⁸¹⁷ WALDMAN, 6.

¹⁸¹⁸ Z.B. für soziale Netzwerke wie Facebook ist es eine existenzielle Bedrohung, wenn die Mitglieder keine Inhalte mehr generieren: HARTZOG 2018, 197.

vatsphäre wandelt sich somit von einem individuellen Recht zu einem öffentlichen, kollektiven, sozialen Gut.¹⁸¹⁹

Die Vertreter des Datenschutzes mit Vertrauenskomponente beklagen den Zustand, dass das US-amerikanische Recht die Beziehung zwischen Persönlichkeitsschutz und Vertrauen nicht widerspiegle bzw. das Vertrauen sich nicht als zentrale Rechtfertigung dafür entwickelt habe, warum Datenschutz wichtig ist.¹⁸²⁰ Zur rechtlich-theoretischen Umsetzung der Vertrauenskomponente schlägt BALKIN deshalb vor, den Datenbearbeitern, denen Informationen anvertraut werden, dieselben Pflichten wie einem Treuhänder (*fiduciary* des angloamerikanischen Common Law) aufzuerlegen.¹⁸²¹

In der US-amerikanischen Praxis wird, wie die empirische Forschung von BAMBERGER und MULLIGAN zeigt, die Vertrauenskomponente hingegen bereits vielerorts gelebt: Die Arbeitgeber interpretieren den Begriff *privacy* extensiv. Datenschutz wird als Grundwert verstanden, der eng mit Vertrauen, Integrität und Respekt vor dem Menschen verbunden ist.¹⁸²² Die befragten *Chief Privacy Officers* (CPO) geniessen eine unabhängige und einflussreiche, unternehmensweite Rolle, in der sie sowohl als Stimme für den Datenschutz als auch als generelle Vertrauensperson auftreten.¹⁸²³ Die US-amerikanische Bank JPMorgan Chase geht aufgrund der Komplexität der Datenschutz-Sachverhalte so weit, den jeweiligen Projektverantwortlichen mit einer ganzen Gruppe von Führungskräften aus den drei Abteilungen Personal, Risiko und Recht zu unterstützen.¹⁸²⁴ Die Unternehmen orientieren sich an einer Definition von Datenschutz, die über das hinausgeht, was die *Fair Information Practice Principles* (FIPP) des Ministeriums

¹⁸¹⁹ OTTO 2016, 186. Vgl. aus dem europäischen Raum: BAUMANN MAX-OTTO, 1.

¹⁸²⁰ RICHARDS/HARTZOG 2016, 434 und 449. Das Konzept der informierten Einwilligung «ignore» Werte wie die gewohnte Lebenserfahrung und die berechtigten Erwartungen an die Privatsphäre: WALDMAN, 84. Das Vertrauen in die Datenwirtschaft erodiert durch die prädiktiven Analysen von Big Data: WALDMAN, 78.

¹⁸²¹ BALKIN, 1186; WALDMAN, 85–86, m.w.H.

¹⁸²² BAMBERGER/MULLIGAN 2015, 183. Vertrauen spielt eine Schlüsselrolle, ist aber schwierig zu kodifizieren: BAMBERGER/MULLIGAN 2015, 184. Das extensive Verständnis von «*privacy*» ist vergleichbar mit der Konzeption eines umfassenden Persönlichkeitsschutzes gemäss ZGB (dazu S. 82–83). Deshalb ist der Begriff «*privacy*» an manchen Stellen nicht als «Privatsphäre» oder «Datenschutz», sondern treffender als «Persönlichkeitsschutz» zu übersetzen.

¹⁸²³ BAMBERGER/MULLIGAN 2015, 195.

¹⁸²⁴ SHOOK *et al.*

für Innere Sicherheit (*Department of Homeland Security*) der Vereinigten Staaten verlangen.¹⁸²⁵ Die FIPP entsprechen im Wesentlichen den schweizerischen und europäischen Datenbearbeitungsgrundsätzen. Die amerikanische Aufsichtsbehörde FTC sanktioniert heute ganz allgemein unlautere Praktiken (*unfair practices*), was eine Erweiterung des Fokus beim Datenschutzvollzug im Vergleich zu früheren Fällen bedeutet.¹⁸²⁶

b) Begriff des Vertrauens

Um die Vertrauenskomponente zu verstehen, ist der Begriff des Vertrauens zu erklären. Es handelt sich hierbei nicht primär um einen rechtlichen Terminus, auch fehlt es an einer Legaldefinition. Gleichwohl tritt der Begriff des Vertrauens an verschiedenen Orten in der Rechtswissenschaft in Erscheinung. Im Zusammenhang mit People Analytics besteht durch den Arbeitsvertrag eine Verpflichtung beider Parteien zu gegenseitiger Treue (Treuepflicht des Arbeitnehmers, Art. 321a OR; Fürsorgepflicht der Arbeitgeberin, Art. 328 OR). Das DSG bestätigt ausdrücklich die Verpflichtung zu Treu und Glauben beim Bearbeiten von arbeitsbezogenen Personendaten (Art. 4 Abs. 2 DSG bzw. Art. 5 Abs. 2 E-DSG bzw. Art. 6 Abs. 2 rev-DSG i.V.m. Art. 328b Satz 2 OR).

Eine allgemeine Begriffsdefinition lautet: Vertrauen ist der Wille, sich verletzlich zu zeigen.¹⁸²⁷ Ähnlich klingt die folgende Definition: Vertrauen ist die Absicht einer Partei, in einer risikoreichen Situation von der andern Partei abhängig zu sein.¹⁸²⁸

Vertrauen impliziert eine wohlwollende Erwartung an das Handeln und die Absichten anderer Menschen oder den Glauben, dass sich andere in einer vorhersehbaren Weise verhalten werden. Somit beginnt Vertrauen dort, wo der Wissensstand aufhört.¹⁸²⁹ Die wohlwollenden Erwartungen bilden ein gesellschaftliches Kapital, das angemessen zu würdigen ist.¹⁸³⁰ Vertrauen entsteht nicht durch Be-

¹⁸²⁵ BAMBERGER/MULLIGAN 2015, 183.

¹⁸²⁶ So stuft die FTC geschäftliche Tätigkeiten als unlauter ein, wenn sie insgesamt irreführend sind, auch wenn die nach Datenschutzrecht erforderlichen Informationen offengelegt worden sind: BAMBERGER/MULLIGAN 2015, 191.

¹⁸²⁷ OSTERLOH/WEIBEL, 70.

¹⁸²⁸ Verkürzte Fassung von: Europäische Kommission 2019b, 38.

¹⁸²⁹ WALDMAN, 7.

¹⁸³⁰ Art.-29-Datenschutzgruppe 2013, 4; WALDMAN, 51; CAVOUKIAN/DIX/EL EMAM, 8.

schluss; das Heranwachsen von Vertrauen kann Jahrzehnte dauern.¹⁸³¹ Es wird zum Bestandteil der Marke und Reputation eines Unternehmens.¹⁸³² Um etwas plastischer zu werden: Unternehmen riskieren angeblich sechs Prozent Umsatzverlust, wenn sie das Vertrauen ihrer Mitarbeiter verlieren. Umgekehrt führt eine Steigerung von Vertrauen dazu, dass der Umsatz um mehr als sechs Prozent wächst.¹⁸³³

Vertrauen ist auch ein Mechanismus der Reduktion sozialer Komplexität.¹⁸³⁴ Die Komplexität besteht vorliegend darin, dass die Arbeitgeberin zur Implementierung von People Analytics auf die Daten des Arbeitnehmers angewiesen ist, dieser aber grundsätzlich kein Interesse haben kann, Informationen preiszugeben, weil er sich dadurch in eine immer verletzlichere Position hineinmanövrieren würde.¹⁸³⁵ Vertrauen kann das drohende Machtungleichgewicht, das dem Austausch von Daten mit anderen innewohnt, ausgleichen, sodass der Schwächere sich bereit erklärt, Informationen zu teilen.¹⁸³⁶ Die Schaffung einer Vertrauenskultur dürfte (primär) im Interesse der Arbeitgeberin liegen, da Vertrauen es ihren Angestellten ermöglicht, sich auf die Arbeit zu konzentrieren statt die Datenbearbeitungsprozesse zu kontrollieren.¹⁸³⁷ Der grösste Teil des beschriebenen Aufwands zur Prüfung von Datenschutzerklärungen und Informationsflüssen entfällt in einem Klima von Vertrauen.¹⁸³⁸

Je nach Rechtsbeziehung kann Vertrauen zwischen verschiedenen Akteuren entstehen. Denkbar ist neben dem Vertrauen zwischen zwei Einzelpersonen (wie dem Angestellten und dem Vorgesetzten) auch ein solches zwischen Einzelpersonen und Institutionen (etwa zwischen dem Angestellten und der Arbeitgeberin als Unternehmensorganisation) oder zwischen Einzelpersonen und dem Rechtssystem.¹⁸³⁹ Diese letztgenannte Dimension von Vertrauen schliesst auch den Aspekt

¹⁸³¹ NISSENBAUM 2011, 37.

¹⁸³² Der grösste Wert von Privatsphäreschutz ist, dass er Teil der Marke ist: BAMBERGER/MULLIGAN 2015, 184.

¹⁸³³ SHOOK *et al.*

¹⁸³⁴ LUHMANN, 27–38.

¹⁸³⁵ Vgl. RICHARDS/HARTZOG 2016, 451.

¹⁸³⁶ WALDMAN, 47.

¹⁸³⁷ CUSTERS/URSIC, 344.

¹⁸³⁸ Vgl. zum Aufwand für das Lesen von Einwilligungen S. 225–229 und für das Führen von Klagen S. 267–274.

¹⁸³⁹ TAMÒ-LARRIEUX, 37, m.w.H. Die Sozialwissenschaften unterscheiden zwischen besonderem Vertrauen (zwischen bestimmten Personen), institutionellem Vertrauen

der Rechtssicherheit ein. Sie ist besonders wichtig angesichts der Tendenz, dass sich das Datenschutzrecht mit der zunehmenden Informationsbearbeitung zu einer Querschnitt-Rechtsmaterie entwickelt, die alle Sachverhalte des Lebens betrifft. Nur wenn die Betroffenen sich sicher wähnen, dass das «System Datenschutzrecht» ihre Persönlichkeit effektiv schützt, werden sie bereit sein, Daten über sich selbst in allen Lebenssituationen zu teilen, was wiederum Grundvoraussetzung der Digitalisierung der Gesellschaft ist. Dass den Möglichkeiten, gegenüber wem oder was Menschen Vertrauen entwickeln können, keine Grenzen gesetzt sind, verdeutlichen die Geschichten von emotionalen Beziehungen zu sozialen Robotern,¹⁸⁴⁰ Plüschtieren oder gar zu einem Volleyball.¹⁸⁴¹

c) Hohes bestehendes Vertrauen

Gemäss dem Edelman Trust Barometer war im Jahr 2019 die Arbeitgeberin die Institution, die weltweit das höchste Vertrauen genoss. Drei von vier Befragten (75 Prozent) vertrauten ihrer Arbeitgeberin, dass sie das Richtige tut, deutlich mehr als gegenüber Nichtregierungsorganisationen (57 Prozent), der Wirtschaft (56 Prozent), der Regierung (48 Prozent) und den Medien (47 Prozent).¹⁸⁴² Dabei belegt die Schweiz bzgl. des Vertrauens in Unternehmen einen Spitzenplatz.¹⁸⁴³ Einer anderen Umfrage zufolge sollen 88 Prozent der schweizerischen Arbeitnehmer offen sein für die Erhebung von Daten über sie selbst und ihre Arbeit, sofern die Analyse der Steigerung ihrer Leistung oder ihres Wohlbefindens dient oder

(zwischen Individuen und Unternehmen) und allgemeinem Vertrauen (dem Glauben, dass den meisten Menschen vertraut werden kann): WALDMAN, 51. Anders ausgedrückt: Das Teilen von Daten begründet eine Verletzlichkeit nicht nur gegenüber dem Datenbearbeiter, sondern auch gegenüber Drittparteien, die (über den Datenbearbeiter oder anderweitig) in den Besitz von Daten gelangen, sodass in all diesen Beziehungen Vertrauen nötig ist: RICHARDS/HARTZOG 2016, 451.

¹⁸⁴⁰ Mit kommunikationsfähigen und anthropomorphen sozialen Robotern teilen Menschen ihre Emotionen, sodass die Kontakte zum Roboter teilweise echte gesellschaftliche Beziehungen ersetzen können: WALDMAN, 135 und 145.

¹⁸⁴¹ Der Erfolg des Films *Cast away*, in dem Chuck Noland (Tom Hanks) vier Jahre mit seinem stummen Freund Wilson, einem Volleyball, auf einer einsamen Insel verbringt, sei ein Zeichen, dass viele Kinobesucher der Beziehung zum Volleyball nachfühlen konnten: WALDMAN, 140.

¹⁸⁴² Edelman Corporation, 24.

¹⁸⁴³ Edelman Corporation, 48.

andere persönliche Vorteile bietet.¹⁸⁴⁴ Das hohe Vertrauensklima am Arbeitsplatz bzgl. Datenbearbeitungen scheint seit Längerem stabil zu sein: Eine Umfrage von 1993 ergab eine weltweit hohe Zufriedenheit der Arbeitnehmer der Privatwirtschaft im Umgang mit Informationen durch ihre Arbeitgeberin. Nicht einmal jeder Fünfte (weniger als 20 Prozent) vertrat die Meinung, dass die Arbeitgeberin gegen verschiedene, in der Umfrage vorgestellte Rechte zum Schutz der Privatsphäre der Arbeitnehmer verstosse.¹⁸⁴⁵

Das beschriebene hohe und stabile Vertrauensklima könnte der Arbeitgeberin die Tore öffnen, um mit People Analytics zu experimentieren.¹⁸⁴⁶ Jedoch könnte das wertvolle Vertrauen auch schnell zerbröckeln. Über die Hälfte (54 Prozent) der Unternehmen, die das Beratungsunternehmen Accenture befragt hat, hat im Jahr 2018 einen erheblichen Vertrauensverlust erlitten.¹⁸⁴⁷ Im Jahr 2016 glaubten zwei von fünf Arbeitnehmern in Grossbritannien (38 Prozent) nicht, dass ihre Arbeitgeberin die gesammelten Daten in der Weise verwendet, dass die Arbeitnehmer davon profitieren würden.¹⁸⁴⁸ Knapp die Hälfte (48 Prozent) der Arbeitnehmer glaubte gemäss einer Umfrage des HR Metrics & Analytics Summit von 2018 nicht, dass ihre Arbeitgeberin ihre Daten genügend schütze.¹⁸⁴⁹ Verschiedene Datenskandale haben den Beschäftigten vor Augen geführt, dass ihre Daten nur sehr begrenzt gesichert sind.¹⁸⁵⁰ Die Gefahr des Vertrauensverlusts im Arbeitsverhält-

¹⁸⁴⁴ 88 Prozent der Arbeitnehmer in der Schweiz sind offen für Datenbearbeitungen, dies gegenüber 89 Prozent der Arbeitnehmer weltweit: DAVIS PLÜSS JESSICA / REUSSER KAI, Your employer might be watching you. Should you care?, 13.05.2019, abrufbar unter <www.swissinfo.ch> (besucht am 31.05.2020), m.w.H. Mit dem praktisch identischen Ergebnis, nämlich dass weltweit neun von zehn Arbeitnehmern (90 Prozent) ihrer Arbeitgeberin die Datenerhebung gewähren wollen, wenn sie in irgendeiner Weise davon profitieren: SHOOK *et al.*

¹⁸⁴⁵ WESTIN, 445.

¹⁸⁴⁶ DAVIS PLÜSS JESSICA / REUSSER KAI, Your employer might be watching you. Should you care?, 13.05.2019, abrufbar unter <www.swissinfo.ch> (besucht am 31.05.2020).

¹⁸⁴⁷ LONG *et al.*, 3. Accenture hat sowohl Unternehmen mit als auch ohne People Analytics befragt. Die Umfrageresultate spezifizieren nicht die Gründe für den Vertrauensverlust, d.h., People Analytics muss nicht die Ursache sein.

¹⁸⁴⁸ The Economist vom 05.01.2019, The spy who hired me, abrufbar unter <www.economist.com> (besucht am 31.05.2020).

¹⁸⁴⁹ HR Metrics & Analytics Summit, 7.

¹⁸⁵⁰ Vgl. die vorstehend beschriebenen Umsetzungsmängel und öffentlichen Datenskandale auf S. 242–247. «*Between employers and hackers, privacy is disappearing fast*»: COLLIER, 3.

nis lässt sich anhand der Entwicklung im Verhältnis zwischen Konsumenten und Anbietern nachzeichnen: Hier nahmen die öffentlichen Bedenken bzgl. der Privatsphäre in der zweiten Hälfte der 1990er-Jahre mit der Ausbreitung der Internetnutzung dramatisch zu.¹⁸⁵¹ Im Jahr 2010 sorgten sich weltweit fast neun von zehn Konsumenten wegen der Fragen, wer Zugang zu ihren Personendaten hat (88 Prozent) und wo die Daten gespeichert werden (84 Prozent).¹⁸⁵²

d) NFP75-Daten zum Vertrauen

Die empirischen Daten aus der Online-Umfrage des NFP75-Projekts suggerieren insgesamt ein leicht stärkeres Vertrauensklima in Unternehmen mit People Analytics-Anwendungen als in solchen ohne dieselben. Drei Viertel der Antwortenden aus Unternehmen mit People Analytics glauben, dass die Arbeitnehmer ein starkes Vertrauen in die Führungskräfte hätten (siehe Abb. 11: 74 Prozent mit einer Punktzahl von 4 oder 5 auf einer Skala von 1 bis 5, wobei 1 ein schwaches und 5 ein starkes Vertrauen bedeuten), wogegen dies nur drei Fünftel der Antwortenden aus Unternehmen ohne People Analytics glauben (59 Prozent).

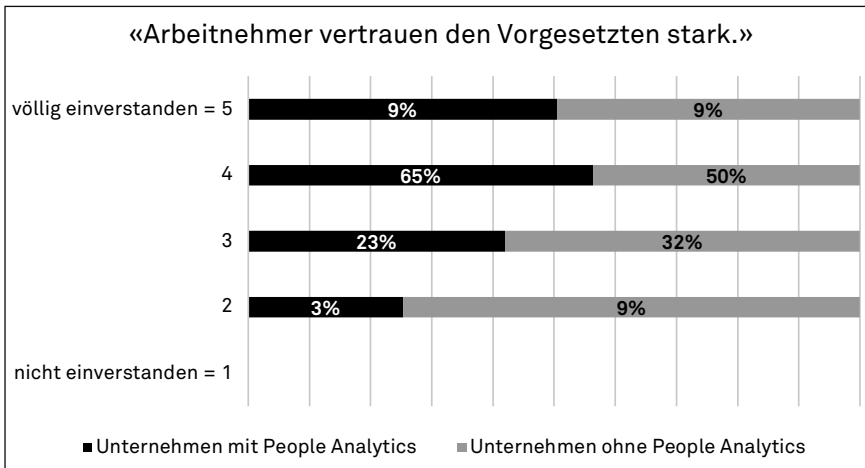


Abb. 11: «Arbeitnehmer vertrauen den Vorgesetzten stark.»

¹⁸⁵¹ WESTIN, 445.

¹⁸⁵² SPIEKERMANN, 323. Der NSA-Skandal, die globale Überwachungs- und Spionageaffäre, die im Jahr 2013 an die Öffentlichkeit gelangte, habe das Vertrauen der Bürger in das Recht nachhaltig beschädigt: HIJMANS/KRANENBORG, 6. Vgl. CUSTERS/VAN DER HOF/SCHERMER, 282: «People tend to express concern about privacy.»

Drei von fünf Antwortenden aus Unternehmen mit People Analytics sagen, dass andersherum die Vorgesetzten den Arbeitnehmern zutrauen, gute Entscheidungen zu treffen (siehe Abb. 12: 60 Prozent mit einer Punktzahl von 4 oder 5 auf einer Skala von 1 bis 5, wobei 1 ein schwaches und 5 ein starkes Vertrauen bedeuten), wogegen es bei den Unternehmen ohne People Analytics etwas weniger als drei Fünftel sind (55 Prozent).

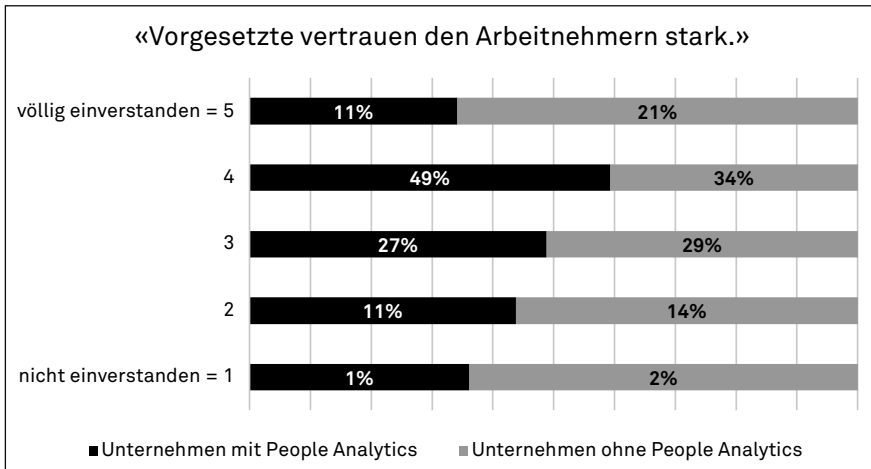


Abb. 12: «Vorgesetzte vertrauen den Arbeitnehmern stark.»

Die Unternehmen wurden gefragt, wie sich die Mitarbeiter verhalten, wenn jemand im Unternehmen etwas verspricht. In drei von vier Unternehmen mit People Analytics ist es so, dass andere im Unternehmen praktisch immer darauf vertrauen, dass die Person ihr Bestes geben werde, um das Versprechen zu halten (73 Prozent mit einer Punktzahl von 4 oder 5 auf einer Skala von 1 bis 5, wobei 1 ein schwaches und 5 ein starkes Vertrauen bedeuten). Dagegen vertrauen auf dieselbe Charaktereigenschaft nur zwei Drittel in den Unternehmen ohne People Analytics (67 Prozent, siehe Abb. 13).

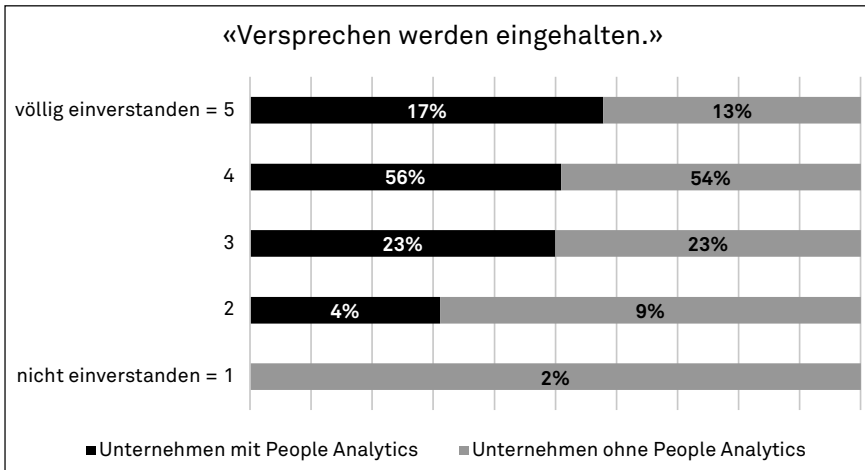


Abb. 13: «Es wird stets darauf vertraut, dass Versprechen eingehalten werden.»

Ausgeglichen fallen die Antworten aus auf die Frage, ob ein sehr hoher Grad an Vertrauen im gesamten Unternehmen herrsche (in Unternehmen mit People Analytics: 65 Prozent mit einer Punktzahl von 4 oder 5 auf einer Skala von 1 bis 5, wobei 1 ein schwaches und 5 ein starkes Vertrauen bedeuten; in Unternehmen ohne People Analytics: 64 Prozent, siehe Abb. 14).

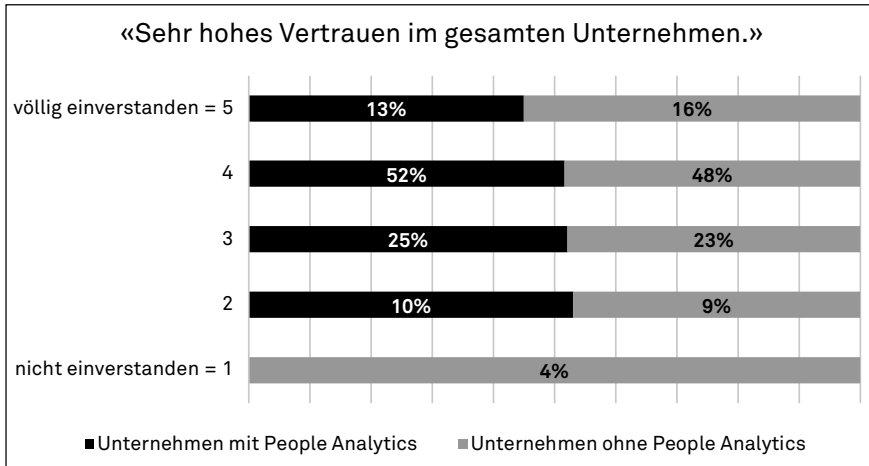


Abb. 14: «Es besteht ein sehr hohes Vertrauen im gesamten Unternehmen.»

Die vorstehenden Zahlen aus der Online-Umfrage des NFP75-Projekts vermögen zu überraschen: Sie besagen, dass ein gutes Vertrauensklima bestehen kann in Unternehmen, die People Analytics betreiben. Teilweise deuten die Antwortwerte sogar auf ein leicht stärkeres Vertrauen in den befragten Betrieben, die People Analytics anwenden, als in denen, die keine Personalanalysen vornehmen (siehe Abb. 11, Abb. 12 und Abb. 13).

Im Kontrast zu den empirischen Resultaten der Online-Umfrage äussert sich die konsultierte Lehre überwiegend kritisch zur zunehmenden Überwachung am Arbeitsplatz.¹⁸⁵³ Skeptiker könnten daher die überraschenden Ergebnisse des NFP75-Projekts auf ein voreingenommenes Design der Online-Umfrage zurückführen: Die befragten Personen gehörten der Personalverwaltung der betreffenden Unternehmen an. Als Personalverantwortliche waren sie in der Regel nicht persönlich

¹⁸⁵³ Es wird gesprochen von «*Post-privacy*»-Zeitalter (HELLER), «*surveillance capitalism*» (ZUBOFF 2015; ZUBOFF 2019) und «*trust crisis*» (STELZER/VELJANOVA, 159), um nur einige Beispiele zu nennen.

von den Aufzeichnungen betroffen. Im Gegenteil, sie dürften eher dazu geneigt haben, vorzugeben, in Personalangelegenheiten stehe alles zum Besten.

Um der potenziellen Kritik von vornherein zu begegnen, wurden die Ergebnisse der quantitativen Online-Umfrage anschliessend in fünf qualitativen Fallstudien hinterfragt.¹⁸⁵⁴ Als Fallstudienpartner wurden fünf Unternehmen auserkoren, die gemäss eigenen Angaben in der Online-Umfrage besonders intensiv People Analytics betreiben. Anders als bei der Online-Umfrage, bei der nur eine Person stellvertretend für das ganze Unternehmen antwortete, wurden bei den Fallstudien pro Unternehmen zwischen 15 und 25 Mitarbeiter zu People Analytics befragt. Unter den Interviewpartnern waren zum grössten Teil (43 Prozent) direkt die überwachten Mitarbeiter (einschliesslich Arbeitnehmervertreter). Die restlichen Interviews (57 Prozent) verteilten sich über verschiedene Funktionen der Führungsebene: Befragt wurden die operativ tätigen Linienvorgesetzten (Teamleiter) und das höhere, strategische Management (Geschäftsleitung und Verantwortliche des betreffenden People Analytics-Projekts), aber auch der jeweilige Datenschutzverantwortliche des Unternehmens, eine Person aus der HR-Abteilung, jemand aus der Rechtsabteilung und schliesslich ein IT-Verantwortlicher.

Die fünf Fallstudien bestätigen den obigen Befund, dass ein gutes Vertrauensklima bestehen kann in Unternehmen, die People Analytics betreiben. Viele Mitarbeiter sagten sogar aus, das People Analytics-System habe kaum einen Einfluss auf ihr Vertrauen in das Unternehmen. In allen fünf Unternehmen bewegt sich das Vertrauen auf einem hohen Niveau (zwischen 8 und 8,5 Punkten auf einer Skala von 1 bis 10, wobei 1 ein tiefes und 10 ein hohes Vertrauen bedeuten; aufgrund der Anzahl der Interviews sind diese Zahlen jedoch nicht repräsentativ für das ganze Unternehmen). Die überwachten, in der Regel subalternen Arbeitnehmer beziffern ihr Vertrauen in das Unternehmen jeweils etwas tiefer als die Angestellten auf der (überwachenden) Führungsebene, doch ist dieser Unterschied vernachlässigbar (zwischen 0,2 und 0,4 Punkten auf der besagten Skala von 1 bis 10).

Es ist jedoch auf die richtige Umsetzung des jeweiligen People Analytics-Projekts zu achten. Gemäss den Eindrücken, die der Autor zusammen mit dem NFP75-Forschungsteam persönlich in den Fallstudieninterviews gewonnen hat, schätzen die Mitarbeiter vor allem die folgenden drei Punkte: Erstens, vertrauensfördernd

¹⁸⁵⁴ Siehe zum Forschungsdesign des NFP75-Projekts S. 14–16. – Eine ausführliche Auswertung und Publikation der Fallstudienresultate im Namen des gesamten Forschungsteams des NFP75-Projekts war im Zeitpunkt der Abgabe der vorliegenden Dissertation noch nicht möglich. Vorliegend werden die Ergebnisse nur kurz skizziert und begründet.

wirkt sich aus, wenn das Unternehmen bestrebt ist, aus den Analysen zu lernen (durch Pflege einer sog. Lernkultur). Es sollte darauf verzichtet werden, einzelne Arbeitnehmer auf schikanöse Weise für Fehler zu sanktionieren. Zweitens, es braucht eine Möglichkeit zur Mitsprache. Verschiedene Unternehmen haben einzelne Mitarbeiter in die Pilotphase des People Analytics-Projekts einbezogen, um bereits dann ihre Einwände in die Gestaltung der Software einfließen zu lassen. Die gleichen Mitarbeiter – sog. «Poweruser» – nahmen später die Rolle eines Sprachrohrs für die restliche Belegschaft ein. Die Arbeitskollegen konnten sich mit Fragen und Anliegen zum System an die Poweruser wenden. Diese kommunizierten die Verbesserungsvorschläge weiter an die IT-Abteilung, die die Vorschläge umsetzte. Drittens ist es ratsam, auf eine sorgfältige Information und Kommunikation zu achten und insbesondere nicht zu viel zu versprechen. Es gab bei allen befragten Unternehmen bei der Einführung der neuen Technologie technische Probleme. Diese lösten bei den einen Arbeitnehmern Frustration aus, während andere, die darauf vorbereitet waren, gelassen reagierten.

Auch wenn die beschriebenen drei Ratschläge zum Gelingen von People Analytics-Projekten beitragen, garantieren sie alleine noch nicht ein stabiles Vertrauensklima im Unternehmen. Wichtig für das Vertrauen waren gemäss den Befragten auch gute Löhne und Sozialleistungen, ehrliche Vorgesetzte, die Rücksichtnahme der Arbeitgeberin auf eine gesunde Work-Life-Balance, ein konstruktiver Umgang mit leistungsschwächeren Arbeitnehmern und interne Aufstiegschancen. Ein Unternehmen muss somit mehrere Ansätze verfolgen, um das Vertrauen der Belegschaft zu gewinnen.

7.2.4 Kritik zur Ausrichtung auf das Teilen und zum Datenschutz mit Vertrauenskomponente

Es hat sich gezeigt, dass eine wichtige Voraussetzung für den Erfolg von People Analytics darin besteht, dass die betroffenen Arbeitnehmer dazu bereit sind, Informationen über sich selbst mit der Arbeitgeberin zu teilen und ihr zu vertrauen.¹⁸⁵⁵ Die Lehre vom Datenschutz mit Vertrauenskomponente verlangt, dass dieses Vertrauen aktiv gefördert werden muss.¹⁸⁵⁶ In der Schweiz besteht generell und auch in den im NFP75-Projekt untersuchten Unternehmen, die besonders intensiv People Analytics betreiben, ein stabiles Vertrauensklima.¹⁸⁵⁷ Eine wesentliche Er-

¹⁸⁵⁵ Siehe S. 296–298.

¹⁸⁵⁶ Siehe S. 301–304.

¹⁸⁵⁷ Siehe S. 306–313.

kenntnis der vorliegenden Arbeit besteht somit darin, dass People Analytics mit den beschriebenen Konzepten des Teilens von Information und des Datenschutzrechts mit Vertrauenskomponente vereinbar ist. People Analytics zerstört nicht per se das Vertrauen der analysierten Arbeitnehmer in das Unternehmen.

Zu kritisieren ist an den zitierten Lehrmeinungen aber zum einen, dass sie recht abstrakt bleiben. Weder eine Auflistung der notwendigen Anreize für das Teilen von Information noch eine konkrete Beschreibung der Vertrauenskomponente sind auffindbar, sodass der Gesetzgeber nicht weiss, wie er diese Forderungen verwirklichen soll. Das Common Law-Institut der *fiduciary relationship*¹⁸⁵⁸ kann nicht ohne Weiteres auf die schweizerische Rechtsordnung, die zum kontinental-europäischen Civil Law gehört, übertragen werden. Das Vertrauen ist, soweit ersichtlich, höchstens als Ideenansatz für die Schweiz vorgeschlagen worden.¹⁸⁵⁹

Zum andern besteht ein Kritikpunkt darin, dass ein Rechtssystem, das nur auf Teilen und Vertrauen setzt, unvollständig ist. Die problematische Machtasymmetrie wird nicht behoben,¹⁸⁶⁰ wenn die schwächere Partei der stärkeren einfach vertraut und in beliebigem Umfang Daten über sich an sie liefert. Blinde Vertrauen kann ausgenutzt werden.

Im Folgenden ist ein Lösungskonzept zu erarbeiten, das eine wirksame Durchsetzung des Datenschutzrechts bei People Analytics gewährleistet. Die Ideen der Förderung des Teilens von Information und der Stärkung des Vertrauens in das Datenschutzrecht sind in das Konzept zu integrieren, weil ja festgestellt wurde, dass People Analytics und der Datenschutz mit Vertrauenskomponente miteinander vereinbar sind. Jedoch ist auch den beiden beschriebenen Kritikpunkten (fehlende Konkretisierung und Fortbestand der Machtasymmetrie) Rechnung zu tragen. Das vorliegend entwickelte Lösungskonzept besteht in einer Professionalisierung und Demokratisierung des Datenschutzrechts (dazu sogleich).

¹⁸⁵⁸ Siehe S. 303.

¹⁸⁵⁹ Vorschlag, zum Schutz von genetischen Daten (Art. 10 E-GUMG) solle die Gewährleistung von Vertraulichkeit in den Fokus gerückt werden: SIGRIST, N 30.

¹⁸⁶⁰ Siehe zur Machtasymmetrie S. 79–82.

7.3 Professionalisierung und Demokratisierung als Mittel zur Umsetzung des neu ausgerichteten Datenschutzrechts

7.3.1 Vorbemerkungen

a) Herleitung der Begriffe «Professionalisierung» und «Demokratisierung»

Der erste Kritikpunkt¹⁸⁶¹ zu den Ideen betreffend die Förderung des Teilens von Information und betreffend den Datenschutz mit Vertrauenskomponente verlangt nach einer konkreten Beantwortung der Frage, wie Vertrauen generiert werden kann. Vorliegend wird vertreten, dass das Vertrauen steigt und Informationen eher geteilt werden, wenn sich die Arbeitgeberin bei der Bearbeitung von Daten professionell verhält. Voraussetzung dafür, dass sich jemand verletzlich zeigen will, ist, dass das Gegenüber imstande und gewillt ist, die Interessen des Verletzlichen zu beschützen. Die Fähigkeit, die Interessen der Betroffenen wahrzunehmen, steigt, wenn das Recht bestimmte Mindestanforderungen an die Professionalität der Verantwortlichen stellt (etwa zur Abwehr von Dritten, die in die Datenbearbeitungssysteme eindringen wollen).

Unter dem Begriff der Professionalisierung wird vorliegend jede Massnahme verstanden, die die Arbeitgeberin dazu veranlasst, das Datenschutzrecht ab Beginn der Datenbearbeitung zu befolgen, sodass die Rechtsdurchsetzung im Zusammenhang mit People Analytics gewährleistet ist. Hierbei ist hauptsächlich nach Mitteln zur Rechtsdurchsetzung *ex ante* zu suchen (z.B. die Pflicht zu datenschutzfreundlichen Voreinstellungen nach Art. 6 E-DSG bzw. Art. 7 rev-DSG). Doch auch im Nachgang einer allfälligen Datenschutzverletzung soll die Arbeitgeberin auf die Rechtsdurchsetzung *ex post* hinwirken (z.B. durch die Meldung von Verletzungen der Datensicherheit, Art. 22 E-DSG, Art. 24 rev-DSG).

Der regulatorische Ansatz, die Arbeitgeberin zu einem professionellen Umgang mit den Daten zu verpflichten, erscheint sachgerecht, weil der Arbeitgeberin bei People Analytics eine wesentlich aktivere Rolle zukommt als dem Arbeitnehmer und sie am meisten Vorteile daraus zieht.¹⁸⁶² Der Prozess der Datenerhebung erfolgt auf einer Einbahn-, nicht aber auf einer Gegenverkehrsstrasse. In der Regel

¹⁸⁶¹ Siehe S. 314.

¹⁸⁶² Datenbearbeiter ziehen am meisten Vorteile aus der Wiederverwertung von Daten und wissen mehr als alle anderen über die Datenbearbeitung: MAYER-SCHÖNBERGER/CUKIER, 174.

läuft die Datenextraktion ohne Dialog ab oder aber nach einer (bestreitbaren) Einwilligung.¹⁸⁶³ Es folgen daher entsprechende Professionalisierungsvorschläge zur Konkretisierung des *Privacy-as-trust*-Ansatzes und der Massnahmen zur Förderung des Teilens von Information.¹⁸⁶⁴

Der zweite Kritikpunkt¹⁸⁶⁵ an der Lehre betreffend die Förderung des Teilens von Information und Datenschutz mit Vertrauenskomponente beinhaltet das Problem, dass der informationelle Schwächezustand der Arbeitnehmer beendet werden muss. Es sind wirksame Kontrollrechte erforderlich, um gegen einen Missbrauch von Daten einzuschreiten. Für die Kontrolle sollte das privatrechtliche Datenschutzrecht seine Hoffnung nicht mehr hauptsächlich auf die Individuen setzen, weil diese mit der Führung von Individualklagen überfordert sind.¹⁸⁶⁶ Stattdessen muss eine breitere Abstützung auf verschiedene Kontrollinstanzen (etwa Arbeitnehmervertretungen und Behörden) der datenschutzrechtlichen Ordnung zu mehr Stabilität verhelfen.¹⁸⁶⁷

Der Einbezug vieler Kontrollstellen führt zur Polykritisierung oder – weniger genau, aber als Begriff vertrauter – zur Demokratisierung des Datenschutzrechts im Arbeitskontext.¹⁸⁶⁸ Der Begriff der Demokratisierung bedeutet vorliegend jede Massnahme, welche den der Arbeitgeberin entgegengesetzten Parteien Kontrollrechte einräumt, um auf die Einhaltung des Datenschutzrechts hinzuwirken, sodass die Rechtsdurchsetzung im Zusammenhang mit People Analytics gewährleistet ist. Es geht hierbei überwiegend um die Rechtsdurchsetzung *ex post* (z.B. durch ein aufsichtsrechtliches Verfahren im Anschluss an eine Datenschutzverletzung), doch ist auch an die Rechtsdurchsetzung *ex ante* zu denken (z.B. durch Stärkung

¹⁸⁶³ Vgl. ZUBOFF 2015, 79. Siehe zur Umstrittenheit der Einwilligung: S. 231–234.

¹⁸⁶⁴ Siehe S. 319–344.

¹⁸⁶⁵ Siehe S. 314.

¹⁸⁶⁶ Siehe S. 267–274. Der Persönlichkeitsschutz sollte im Arbeitskontext nicht «in atomistischer Manier» nur Individuen schützen: JERVIS, 452.

¹⁸⁶⁷ Es brauche einen mehr «präventiven, systemischen» Datenschutz: DIX, 258.

¹⁸⁶⁸ «It's essential [...] to explore the democratic processes available to American workers to reexert control over the capture and use of their personal information by employers»: AJUNWA IFEOMA, Corporate Surveillance Is Turning Human Workers Into Fungible Cogs, The Atlantic vom 19.05.2017, abrufbar unter <www.theatlantic.com> (besucht am 31.05.2020).

der Mitwirkungsrechte schon in der Planungsphase eines People Analytics-Projekts). Es werden somit Demokratisierungsvorschläge ausgearbeitet.¹⁸⁶⁹

Die beiden regulatorischen Stossrichtungen der Professionalisierung und Demokratisierung werden vorliegend nicht von ungefähr zusammen eingeführt. Zwischen ihnen besteht die gleiche Beziehung wie zwischen Vertrauen und Kontrolle. Weder ein Datenschutz-Rechtssystem, in dem allein darauf vertraut wird, dass die Verantwortlichen professionell agieren, noch eines, das unablässige Überprüfungen basierend auf demokratischen Kontrollrechten bedingt, sind sinnvoll. Vertrauen und Kontrolle sind miteinander verbundene Konzepte, die gemeinsam betrachtet werden müssen.¹⁸⁷⁰ Ebenso sind die Professionalisierung und die Demokratisierung gemeinsam in das Datenschutzrecht einzuführen.

b) Regulierungsumfang, Bewahrung der Flexibilität im System

Bei der Prüfung der Professionalisierungs- und Demokratisierungsmöglichkeiten des schweizerischen Datenschutzrechts werden im Folgenden die absehbaren Neuerungen gemäss rev-DSG einbezogen. Die vorliegende Arbeit geht aber bewusst über die dortigen Vorschläge hinaus. Zur Sicherstellung der Einhaltung des Datenschutzrechts in der privatrechtlichen People Analytics-Praxis sind breit angelegte Massnahmen erforderlich. Schon jetzt wird vorweggenommen, dass beispielsweise die folgenden hier vorgeschlagenen Schritte über das Minimum gemäss rev-DSG hinausgehen: Im Bereich der Professionalisierung sind dies die Einführung einer Rechenschaftspflicht, Lösungsvorschläge gegen algorithmische Diskriminierungen und Schulungen.¹⁸⁷¹ Hinsichtlich der Demokratisierung sind es insbesondere die Förderung technologischer «Werkzeuge» zur Befähigung der einzelnen Arbeitnehmer, die Stärkung der Mitwirkungsrechte, die Einführung einer staatlich geführten Diskursmoderation, die Schaffung eines datenschutzrechtlichen ideellen Verbandsklagerechts, sodann Begutachtungsverfahren für Algorithmen und nicht zuletzt Investitionen in die Bildung und Digitalkompetenz der Zivilgesellschaft.¹⁸⁷²

Gleichzeitig ist beim Erlass neuer genereller Rechtsregeln Zurückhaltung geboten. Bei der Gesetzgebungstechnik ist darauf zu achten, dem System eine gewisse Flexibilität zu belassen. Dies ist für den Bereich People Analytics, der auf eine uner-

¹⁸⁶⁹ Siehe S. 344–364.

¹⁸⁷⁰ Vgl. OSTERLOH/WEIBEL, 72–122.

¹⁸⁷¹ Siehe S. 339–344.

¹⁸⁷² Siehe verteilt über die S. 344–364.

schöpflische Vielfalt von Betriebsverhältnissen trifft, offensichtlich.¹⁸⁷³ Es braucht Möglichkeiten, um auf die Besonderheiten von Wirtschaftszweigen oder Unternehmensgrößen Rücksicht zu nehmen.¹⁸⁷⁴ Zudem verändern sich die Geschäftsabläufe dank der adaptiven KI-Techniken stetig.¹⁸⁷⁵ Aus diesem Grund werden Dynamik- und Kontextberücksichtigungen an Bedeutung gewinnen, wogegen generelle Datenschutzregeln immer mehr Ausnahmen erfahren werden.¹⁸⁷⁶

c) Gesundheitssystem als Inspirationsquelle

Auf der Suche nach konkreten Mitteln zur Umsetzung der Professionalisierung und Demokratisierung sind den Möglichkeiten des Gesetzgebers kaum Grenzen gesetzt. Zur Inspiration lohnt sich ein Blick auf andere vertrauensensible soziale Systeme. Zwischen Arzt und Patient besteht eine Vertrauensbeziehung, in der das Teilen von Information sogar lebenswichtig ist.¹⁸⁷⁷ Wir vertrauen, dass die Ärzte «professionell» handeln, weil sie eine langjährige Ausbildung durchlaufen. Es besteht ein einzigartig traditionsreiches Berufsethos, das bis zum Eid des Hippokrates von Kos (460–370 v.Chr.) zurückreicht. Sollte es dennoch zu einer Sorgfaltspflichtverletzung kommen, sind die Schadenersatzansprüche durch die Berufshaftpflichtversicherung des Arztes abgedeckt.

Auch das, was vorliegend unter dem Stichwort «Demokratisierung» gefordert wird, findet sich im Gesundheitssystem wieder: Verschiedene Stakeholder sind an der Aufsicht beteiligt. Zunächst bedürfen Ärzte einer kantonalen Berufsausübungsbewilligung, die bei Wegfall der gesetzlichen Voraussetzungen wieder entzogen werden kann.¹⁸⁷⁸ Die Verletzung des ärztlichen Berufsgeheimnisses kann strafrechtlich verfolgt werden (Art. 321 StGB). Der Berufsverband FMH Verbin-

¹⁸⁷³ «[...] a one-size-fits-all privacy practice is, I don't think, possible»: BAMBERGER/MULLIGAN 2015, 184.

¹⁸⁷⁴ Für eine Vereinfachung der Datenschutzregeln für kleine Unternehmen: Europarat 2011, 8.

¹⁸⁷⁵ WILSON/DAUGHERTY, 5.

¹⁸⁷⁶ World Economic Forum 2013, 11 und 15. «Firms [...] must integrate into their decision making and value structures such collective, contextual, and varied understandings of the ways that corporate use of personal information can intrude on the personal sphere, individual autonomy, and the public good of privacy»: BAMBERGER/MULLIGAN 2015, 27.

¹⁸⁷⁷ WALDMAN, 67.

¹⁸⁷⁸ Bewilligungspflicht: Art. 34 MedBG, Art. 43–44 GesG SG. Entzug der Bewilligung: Art. 38 MedBG, Art. 51 Abs. 2 Satz 2 GesG SG.

dung der Schweizer Ärztinnen und Ärzte kann Verbandsmitglieder sanktionieren, die sich nicht an die Standesordnung halten (Art. 47 SO FMH). Ferner sprechen bei gesetzgeberischen Weichenstellungen die Sozialversicherungen und der Dachverband der Schweizerischen Patientenstellen mit. Nicht zuletzt vertrauen wir uns dem Gesundheitssystem an, weil dieses ein Eigeninteresse an unserer Gesundheit hegt – je gesünder die Bevölkerung, desto weniger Kosten belasten das System.¹⁸⁷⁹ Vergleichbare Vertrauensbeziehungen, in denen sich die schwächere Partei freiwillig in die Hände der stärkeren begibt, bestehen zwischen Anwalt und Klient,¹⁸⁸⁰ Architekt und Auftraggeber oder Autohersteller und Fahrer.

7.3.2 Professionalisierungsvorschläge

a) Professionalisierungstendenzen im Entwurf zum revidierten Datenschutzgesetz

aa) Vorbemerkungen zum Datenschutz durch Technik und zur Datenschutz-Folgenabschätzung

Das rev-DSG statuiert neu die Pflichten sowohl zum Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 6 E-DSG, Art. 7 rev-DSG) als auch zur Datenschutz-Folgenabschätzung (Art. 20 E-DSG, Art. 22 rev-DSG). Beide Pflichten gelten auch im europäischen Datenschutzrecht (*data protection by design and by default*, Art. 25 DSGVO; *data protection impact assessment*, Art. 35 DSGVO). Sie sind in einem inneren Zusammenhang zu sehen. Die Datenschutz-Folgenabschätzung ist die Methode, um die Prinzipien, die für den Datenschutz durch Technik gelten, in einem frühen Projektstadium zu kommunizieren und zu verwirklichen.¹⁸⁸¹ Die Datenschutz-Folgenabschätzung ist ein umfassender Compliance-Prozess, der über die Ausgestaltung der technischen Infrastruktur hinausgeht.¹⁸⁸²

Der Zusatz «durch Technik» bzw. «*by design*» findet sich in verschiedenen Kombinationen. Der Datenschutz durch Technik ist Teil der übergeordneten, umfassenderen Idee eines Persönlichkeitsschutzes durch Technik (*privacy by de-*

¹⁸⁷⁹ Vgl. NISSENBAUM 2011, 36. Positivere Auswirkungen hätten Gesundheitsprogramme am Arbeitsplatz, wenn die Angestellten ein genuines Interesse der Arbeitgeberin an ihrem Wohlergehen spüren würden: The Economist vom 05.01.2019, The spy who hired me, abrufbar unter <www.economist.com> (besucht am 31.05.2020).

¹⁸⁸⁰ Vgl. EDWARDS/VEALE, 43.

¹⁸⁸¹ Vgl. DICKIE/YULE, 101. Vgl. CAVOUKIAN 2011, 15.

¹⁸⁸² Vgl. KROENER/WRIGHT, 356.

sign).¹⁸⁸³ Den Begriff «*privacy by design*» verwenden vor allem Behörden in Kanada, den USA und Australien;¹⁸⁸⁴ gerade im transatlantischen Diskurs darf er nicht mit dem Begriff «*data protection by design*» gleichgesetzt werden.¹⁸⁸⁵ Aus dem Stammkonzept eines allgemeinen Persönlichkeitsschutzes durch Technik spriessen mittlerweile verschiedene Zweige hervor, sodass von einem eigentlichen Trend in Richtung «X durch Technik» bzw. «*X by design*» gesprochen werden kann.¹⁸⁸⁶ WILDHABER, LOHMANN und KASPER fordern einen «Diskriminierungsschutz durch Technikgestaltung».¹⁸⁸⁷ Auch kursieren eine «Ethik durch Technik» (*ethics by design*),¹⁸⁸⁸ eine «Sicherheit durch Technik» (*security by design*)¹⁸⁸⁹ sowie, etwas weiter gegriffen, Technologien zum Privatsphäreschutz (*privacy-enhancing technologies*, PET)¹⁸⁹⁰ und zur Transparenzförderung (*transparency-enhancing technologies*, TET).¹⁸⁹¹

Ähnlich wie im Verhältnis zwischen *privacy by design* und *data protection by design* ist zwischen dem Oberbegriff einer Persönlichkeitsschutz-Folgenabschätzung (*privacy impact assessment*, PIA) und einer Datenschutz-Folgenabschätzung (*data protection impact assessment*, DPIA) zu unterscheiden. Eine Persönlichkeitsschutz-Folgenabschätzung gestaltet sich komplexer als eine Datenschutz-Folgenabschätzung,¹⁸⁹² weil sie neben den Daten auch die übrigen Persönlichkeitsas-

¹⁸⁸³ Der Persönlichkeitsschutz durch Technik umfasse über den Datenschutz hinaus auch die Werte der EU-Grundrechte-Charta und eine ethische Dimension: EDSB 2018, iii. Persönlichkeitsschutz durch Technik als «breites Konzept»: EDSB 2018, N 4; zur Übersetzung von «*privacy*»: FN 1822.

¹⁸⁸⁴ Ebenso verwenden die dortigen Behörden den Begriff «*privacy impact assessment*»: EDSB 2018, E. 52.

¹⁸⁸⁵ BYGRAVE, 116.

¹⁸⁸⁶ GLASS, 103. «*Different <by-design> concepts are already widely used*»: Europäische Kommission 2019b, 21.

¹⁸⁸⁷ WILDHABER *et al.*, 484; «*equal treatment by design*»: HACKER, 1178–1179. Vgl. ALTMAN *et al.*, 43.

¹⁸⁸⁸ ICDPPC, 4.

¹⁸⁸⁹ KROENER/WRIGHT, 358; Europäische Kommission 2019b, 21.

¹⁸⁹⁰ FAIRFIELD, 567.

¹⁸⁹¹ HILDEBRANDT/KOOPS, 449–450.

¹⁸⁹² DE HERT, 34 und 74.

pekte einbezieht.¹⁸⁹³ So wie es verschiedene Konzepte des «X durch Technik» gibt, bilden sich auch verschiedene Konzepte der Folgenabschätzungen heraus.¹⁸⁹⁴

bb) Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

i. Rechtsgrundlage

Die bisherige Verpflichtung zur Gewährleistung der Datensicherheit (Art. 7 DSGVO, Art. 7 E-DSG, Art. 8 rev-DSG) wird künftig erweitert werden.¹⁸⁹⁵ Die Verantwortliche wird verpflichtet sein, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Art. 5 E-DSG bzw. Art. 6 rev-DSG. Sie hat dies ab der Planung zu berücksichtigen (Art. 6 Abs. 1 E-DSG, Art. 7 Abs. 1 rev-DSG). Der Datenschutz durch Technik ist während des gesamten Lebenszyklus des technologischen Systems fortzuführen.¹⁸⁹⁶ Die technischen und organisatorischen Massnahmen müssen insbesondere sowohl dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung als auch den Risiken, welche die Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Personen mit sich bringt, angemessen sein (Art. 6 Abs. 2 E-DSG, Art. 7 Abs. 2 rev-DSG).

Die Verantwortliche ist zudem verpflichtet, mittels geeigneter Voreinstellungen zu gewährleisten, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt (Art. 6 Abs. 3 E-DSG, Art. 7 Abs. 3 rev-DSG).

¹⁸⁹³ Während eine Datenschutz-Folgenabschätzung allein die Folgen für die informationelle Privatheit prüft, geht es bei der Persönlichkeitsschutz-Folgenabschätzung auch um die lokale Privatheit: WRIGHT/DE HERT 2012a, 471. Siehe zur lokalen, dezisionalen und informationellen Privatheit S. 267. Vgl. EDSB 2018, 10–11.

¹⁸⁹⁴ Z.B.: «*algorithmic impact assessment*» für den öffentlich-rechtlichen Einsatz von Algorithmen: REISMAN *et al.*, 1. Vgl. auch «*technological due process*» für den öffentlich-rechtlichen Einsatz von Algorithmen (KEATS CITRON, 1249), «*procedural data due process*» (CRAWFORD/SCHULTZ, 109), «*big data due process*» (EDWARDS/VEALE, 75–76) und, etwas allgemeiner, die sog. «*human rights due diligence*» gemäss Art. 17–21 der Guiding principles on business and human rights der UNO (UNO, 16).

¹⁸⁹⁵ Insbesondere der Datenschutz durch Voreinstellungen (Art. 6 Abs. 3 E-DSG, Art. 7 Abs. 3 rev-DSG) stellt eine Neuerung dar: ROSENTHAL 2017b, N 41. Vgl. BOLLIGER *et al.*, 226.

¹⁸⁹⁶ EDSB 2019a, 25.

ii. *Entstehungsgeschichte*

Erste Vorläufer eines Datenschutzes durch Technik gehen auf die 1950er-Jahre zurück.¹⁸⁹⁷ In den 1970er-Jahren kamen Technologien zum Privatsphäreschutz (PET) auf, die auf einen *Ex-ante*-Datenschutz anstelle der *Ex-post*-Rechtsmittel abzielten.¹⁸⁹⁸ Um die Jahrtausendwende entstand unter dem Terminus «*privacy by design*» das systematische Konzept zur persönlichkeitschutzfreundlichen Gestaltung von jeglichen Technologien.¹⁸⁹⁹ Allen voran hat CAVOUKIAN, damalige Datenschutzbeauftragte der kanadischen Provinz Ontario, den Begriff geprägt.¹⁹⁰⁰ Im Jahr 2010 hat die 32. Internationale Konferenz der Datenschutzbeauftragten in Jerusalem Datenschutz durch Technik einstimmig als internationalen Datenschutzstandard verabschiedet.¹⁹⁰¹

Der EGMR hat in seiner Rechtsprechung von 2008 implizit eine Pflicht zum Datenschutz durch Technik statuiert.¹⁹⁰² In dem betreffenden Fall liess sich eine Arbeitnehmerin eines finnischen Spitals im selbigen Spital auf einer anderen Abteilung behandeln und wurde als HIV-positiv diagnostiziert. Ihr befristeter Arbeitsvertrag wurde danach nicht verlängert, und zwar, wie sie vermutete, weil ihre Arbeitskollegen von ihrer Krankheit erfahren hatten. Damals hatten sämtliche Spitalangestellten freien Zugriff auf die Patientenakten und das System zeichnete nicht auf, wer auf die Akten zugegriffen hatte. Der EGMR erachtete in dieser ungenügenden technischen Infrastruktur eine Verletzung des Rechts auf Achtung der Privatsphäre (Art. 8 EMRK).¹⁹⁰³ Der Grundsatz des Datenschutzes durch Technik

¹⁸⁹⁷ Damals war die Rede von «*preventive law*»: BROWN. ROSSI/HAAPIO, 537, m.w.H.

¹⁸⁹⁸ ROSSI/HAAPIO, 539; GASSER 2016, 65; a.M. HUSTINX, 253: Begriff «PET» erstmals erst 1995 verwendet.

¹⁸⁹⁹ Der Ursprung des Begriffs «*privacy by design*» wird zurückdatiert auf ungefähr das Jahr 2000 (VEALE *et al.*, 106) oder bereits auf die 1990er-Jahre (GASSER 2016, 65).

¹⁹⁰⁰ So behauptet es zumindest CAVOUKIAN selbst: CAVOUKIAN/TAYLOR/ABRAMS, 407. Sie war Informationsfreiheits- und Datenschutzbeauftragte (*Information and Privacy Commissioner*) von Ontario von 1997 bis 2014.

¹⁹⁰¹ Information and Privacy Commissioner of Ontario, 1; CAVOUKIAN 2012, 18.

¹⁹⁰² Laut dem EGMR genügen Datenschutzvorschriften des Gesetzgebers nicht – zusätzlich braucht es «praktische und wirksame» Schutzmassnahmen: Urteil EGMR vom 17.07.2008, I vs. Finland, Nr. 20511/03, N 47; BYGRAVE, 109. Vgl. DIX, 265.

¹⁹⁰³ Urteil EGMR vom 17.07.2008, I vs. Finland, Nr. 20511/03, N 46–49.

ist mittlerweile im Recht des Europarats (vgl. Art. 10 Abs. 3 revidiertes Übereinkommen 108) positiviert.¹⁹⁰⁴

iii. *Normzweck und Norminhalt*

Datenschutz durch Technik bedeutet einen Paradigmenwechsel in dem Sinne, dass die Technologie nicht mehr (nur) als Gefahr für den Persönlichkeitsschutz, sondern als Teil der Lösung betrachtet wird.¹⁹⁰⁵ Der Datenschutz durch Technik bezweckt ein Stück weit eine Abkehr vom rein selbstbestimmten hin zu einem (auch) designbasierten Datenschutz.¹⁹⁰⁶ Ziel dabei ist es, dass die Kontrolle der Einhaltung von Bearbeitungsregeln nicht die permanente persönliche Aufmerksamkeit erfordern soll, was vorliegend als eines der Hauptprobleme des gegenwärtigen Datenschutzes enthüllt worden ist, sondern automatisiert erfolgen muss.¹⁹⁰⁷ Die Architektur eines Systems soll reguliert werden, nicht aber das Verhalten der Systembenutzer.¹⁹⁰⁸ Der Datenschutz ist dadurch zunehmend nicht mehr nur ein rechtliches, sondern wird auch ein technisches Konzept.¹⁹⁰⁹ Menschliche Werte, wie beispielsweise Transparenz, Autonomie, Privatsphäre, Sicherheit, Gerechtigkeit oder Rechenschaftspflicht, finden eine Konkretisierung in der Technologie.¹⁹¹⁰

Die Pflicht, bereits in der Planung den Datenschutz durch Technik umzusetzen, bewirkt einen Wechsel von einem reaktiven zu einem präventiven Rechtsschutz.¹⁹¹¹ Der Datenschutz durch Technik veranlasst somit die Arbeitgeberin, das

¹⁹⁰⁴ Europarat 2018a, N 89; Datenschutz durch Technik auch bei Anlagen erforderlich, die die Tätigkeiten und das Verhalten der Arbeitnehmer indirekt überwachen: Europarat 2015, N 15.2.

¹⁹⁰⁵ GASSER 2016, 65. Auch Immaterialgüter- und Kartellrecht versuchen, die Technologie zu nutzen, um Innovation zu stimulieren: GASSER 2016, 63.

¹⁹⁰⁶ Vgl. GLASS, 103. Die Entscheidungsbefugnis verlagert sich bzgl. Datenbearbeitungen zunehmend in die technische Sphäre: GLASS, 110. Siehe zum Persönlichkeitsschutz durch informationelle Selbstbestimmung S. 258–274.

¹⁹⁰⁷ ROSSNAGEL, 281. Siehe S. 274.

¹⁹⁰⁸ LESSIG, 61–62; HOFFMANN-RIEM, 60–61; CAVOUKIAN 2011, 11–12; HARTZOG 2018, 12; ROSSI/HAAPIO, 542.

¹⁹⁰⁹ NISSIM/WOOD, 2.

¹⁹¹⁰ ROSSI/HAAPIO, 542–543; CAVOUKIAN 2013, 4; HARTZOG 2018, 278.

¹⁹¹¹ «*The door should be locked before the horse bolts*»: DIX, 265. Reaktionen und Sanktionen genügen nicht: DIX, 257. Vgl. EDWARDS/VEALE, 77: *Privacy by design* führe zu «*privacy-friendly systems, starting from the beginning of the process of design rather than tacking privacy on at the end*». Vgl. HARTZOG 2018, 12: «*[...] privacy by design to mean a proactive ex ante approach.*»

Datenschutzrecht ab Beginn der Datenbearbeitung zu befolgen, was zur Professionalisierung im vorliegend verstandenen Sinne beiträgt.¹⁹¹²

iv. *Norminhalt und Umsetzungsmassnahmen*

CAVOUKIAN definiert den Normgehalt des Datenschutzes durch Technik über sieben Prinzipien.¹⁹¹³ Datenschutz durch Technik bedeutet demnach (1) ein proaktives Konzept (*proactive not reactive; preventative not remedial*). Dieses Konzept folgt (2) dem Leitmotiv der datenschutzfreundlichen Voreinstellungen (*privacy by default*) und (3) ist in Informationssysteme eingebaut (*embedded into design*). (4) Sowohl für Betroffene als auch für Verantwortliche muss der Datenschutz durch Technik einen Mehrwert bringen (*full functionality – positive-sum, not zero-sum*). (5) Der Datenschutz durch Technik muss über den gesamten Lebenszyklus von Information wirksam sein (*end-to-end security – full lifecycle protection*), (6) für alle Beteiligten transparent erfolgen (*visibility and transparency*) und (7) stets nutzerzentriert umgesetzt werden (*user-centric*).¹⁹¹⁴

Es gibt unzählige kreative Möglichkeiten, um die sieben Prinzipien in die Datenbearbeitungsabläufe und -produkte zu integrieren.¹⁹¹⁵ Der Kontext der Datenbearbeitung beeinflusst massgeblich die Antwort auf die Frage, welche technischen Massnahmen angezeigt sind.¹⁹¹⁶ Beispielhaft seien ein paar Umsetzungsmöglichkeiten aufgeführt: Hierzu zählen die Pseudonymisierung (vgl. Art. 25 Abs. 1 DSGVO) und Reduzierung der Menge der erhobenen personenbezogenen Daten, des Umfangs ihrer Bearbeitung, ihrer Speicherfrist und ihrer Zugänglichkeit (vgl. Art. 25 Abs. 2 DSGVO).¹⁹¹⁷ Eine Markierung der Daten mittels Metadaten (*tagging*) kann zur Einhaltung des Zweckbindungsgebots den ursprünglichen Bearbeitungszweck festhalten und zur Befolgung des Verhältnismässigkeitsprinzips Sperr- oder Löschrufen vorsehen.¹⁹¹⁸ Als datenschutzfreundliche Voreinstellung

¹⁹¹² Siehe zum Begriff der Professionalisierung S. 315.

¹⁹¹³ CAVOUKIAN bezieht sich auf die *privacy by design*; jedoch können die sieben Prinzipien auch auf den Datenschutz durch Technik (*data protection by design*) appliziert werden. Siehe zur Unterscheidung der Begriffe S. 319–321.

¹⁹¹⁴ CAVOUKIAN 2010; CAVOUKIAN/DIX/EL EMAM, 19–20; GLASS, 106. Ein anderes Konzept mit sechs *Privacy by design*-Prinzipien beschreibt SCHAAR 2010, 269.

¹⁹¹⁵ CAVOUKIAN/TAYLOR/ABRAMS, 413.

¹⁹¹⁶ CAVOUKIAN 2011, 11.

¹⁹¹⁷ Vgl. Europarat 2015, N 14.2, HARTZOG/STUTZMAN 2013, 388, und TA, 5.

¹⁹¹⁸ Siehe bereits S. 179 und 211–212. Festhaltung des Zwecks: KK-WEDDE, Art. 25 DSGVO, N 24; CALDAROLA/SCHREY, N 189; Sperr- und Löschrufen: HOFFMANN-RIEM, 58. Ziel müsse es sein, sog. «SmartData», die selbständig die Einhaltung der Nutzerpräferenzen

ist zu fordern, dass Einwilligungen durch positive Zustimmungen eingeholt werden (*Opt-in*-Modell) und nicht durch bereits angekreuzte Kästchen, die zur Verhinderung der Datenbearbeitung angeklickt werden müssen (*Opt-out*-Modell).¹⁹¹⁹ Zu den systemischen Schutzvorkehrungen gehören sowohl die Reduktion globaler Vernetzung als auch, für besonders sensible Daten, die Einrichtung dezentraler und in sich geschlossener Clouds.¹⁹²⁰ Diverse weitere technische Massnahmen sind realisierbar.¹⁹²¹

Bezeichnend für das Bemühen, mit mathematischer Sprache den Beweis zu erbringen, dass die Persönlichkeit angemessen geschützt wird,¹⁹²² ist zudem der sog. Differenzial-Persönlichkeitsschutz (*differential privacy*). Dies ist ein auf das mathematische Teilgebiet der Analysis bezugnehmender Ansatz, um Risiken für den Persönlichkeitsschutz zu quantifizieren und zu kontrollieren.¹⁹²³ Es besteht jedoch Uneinigkeit darüber, wie bestimmte Werte oder Rechtsbegriffe in eine mathematische Formel übersetzt werden sollen.¹⁹²⁴

Der Datenschutz durch Technik erfordert auch organisatorische Massnahmen (vgl. Art. 6 Abs. 1 E-DSG, Art. 7 Abs. 1 rev-DSG), etwa eine organisatorische Priori-

kontrollieren, zu entwickeln: CAVOUKIAN 2013, 6. Vgl. SCHAAR 2010, 267–268. Siehe zum Begriff der Metadaten FN 213.

¹⁹¹⁹ BOLLIGER *et al.*, 226; CAVOUKIAN/DIX/EL EMAM, 14. Vgl. HERMSTRÜWER, 101.

¹⁹²⁰ HOFFMANN-RIEM, 61.

¹⁹²¹ Z.B. Unterdrückung von Identifikationsdaten (*suppression*), Vertauschen von Daten (*data swapping*), Hinzufügen von Störsignalen (*noise addition*) und anonymisierten Produktionsdaten (*synthetic data*), Aggregation (*aggregation via statistical and machine learning tools*) sowie Dokumentation von Suchanfragen (*query logging*): NISSIM/WOOD, 2 und 7. Verunmöglichung des Zusammenführens verschiedener Datensätze (*unlinkability*) und die Möglichkeit, dass ein Mensch in die Datenbearbeitung eingreifen kann (*intervenability*): EDSB 2018, E. 64; zur LINDDUN-Methodologie (*linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness, non-compliance*): EDSB 2018, E. 70–71.

¹⁹²² «*Mathematical proof*»: NISSIM *et al.*, 702; «*precise mathematical language*»: NISSIM *et al.*, 772; «*mathematical proofs*»: TA, 2.

¹⁹²³ WOOD *et al.*, 209–210. Der Differenzial-Persönlichkeitsschutz ist eine technische Definition des Persönlichkeitsschutzes: NISSIM *et al.*, 763. Vgl. NISSIM/WOOD, 13.

¹⁹²⁴ Uneinigkeit über die Bedeutung von Datenschutz durch Technik: BYGRAVE, 117; RUBINSTEIN, 1421. Siehe zu den unterschiedlichen Definitionen von Diskriminierung: S. 96–99. Schwierigkeit, eine offen formulierte Zweckbestimmung mathematisch zu übersetzen: KOOPS/LEENES, 166.

sierung des Datenschutzes.¹⁹²⁵ Es braucht eine datenschutzfreundliche Mentalität.¹⁹²⁶ Eine Dokumentation aller Bearbeitungsschritte steigert die Reflexion und das Verantwortungsbewusstsein der bearbeitenden Person.¹⁹²⁷ Beispielsweise ist auch ein Prozess einzuspielen, damit die Arbeitgeberin erforderliche Daten vom E-Mail-Konto eines austretenden Arbeitnehmers noch in dessen Gegenwart bezieht und das Konto nach seinem Austritt umgehend sperrt.¹⁹²⁸

v. Grenzen des Datenschutzes durch Technik

Der Datenschutz durch Technik ist kein Allerheilmittel.¹⁹²⁹ Er versagt in Situationen, in denen sämtliche Umstände zu berücksichtigen sind. Zahlreiche rechtliche Normen sind in einer flexiblen, abstrakten Sprache formuliert.¹⁹³⁰ Die Entscheidungsfindung bei der Anwendung solcher Normen erfordert die Anwendung von Ermessen und situativen Werturteilen.¹⁹³¹ Algorithmen beschränken sich aber in der Regel auf die Analysen von Daten, für die sie programmiert sind.¹⁹³² Der Datenschutz durch Technik kann kaum bei der Anwendung des Verhältnismäßigkeitsprinzips helfen, weil dieses eine Interessenabwägung vorschreibt, für welche ein Ermessensentscheid erforderlich ist.¹⁹³³ Der Datenschutz durch Technik stösst auch an Grenzen bei der Beurteilung, ob eine Einwilligung freiwillig erfolgt ist, weil hier alle situativen Umstände einzubeziehen sind.¹⁹³⁴

¹⁹²⁵ HARTZOG/STUTZMAN 2013, 387–388. Vgl. BYGRAVE, 115.

¹⁹²⁶ *«Internalise the data protection framework as part of their mindset»*: KOOPS/LEENES, 168. Art. 25 DSGVO ist *«a catalyst for the mental hardwiring of privacy-related interests»*: BYGRAVE, 120. Erforderlich sei eine optimale Kombination zwischen KI und Menschen: GUIHOT *et al.*, 409.

¹⁹²⁷ KROENER/WRIGHT, 360. Vgl. HOFFMANN-RIEM, 58, und KOOPS/LEENES, 167.

¹⁹²⁸ Europarat 2015, N 14.5.

¹⁹²⁹ HARTZOG 2018, 78 und 277; DIX, 265.

¹⁹³⁰ Der EGMR betont das zeitliche Element in einer Interessenabwägung, indem er feststellt, dass konkurrierende Interessen in Zukunft ein anderes Gewicht erhalten könnten, wenn man bedenkt, welche Eingriffe in das Privatleben durch neue, immer ausgefeiltere Technologien ermöglicht werden: Urteil EGMR vom 05.10.2010, Köpke vs. Germany, Nr. 420/07, 13. KOOPS/LEENES, 166.

¹⁹³¹ *«Human discretion cannot be automated»*: KEATS CITRON, 1304. GUIHOT *et al.*, 408–409.

¹⁹³² Die Programmierung definiert (positiv), welche Daten in die Berechnungen einzubeziehen sind. Es kann aber auch entscheidend sein, sich zu vergegenwärtigen, welche Daten fehlen bzw. was die Daten nicht sagen: CUKIER/MAYER-SCHÖNBERGER, 40.

¹⁹³³ KEATS CITRON/PASQUALE, 7.

¹⁹³⁴ Vgl. zur Freiwilligkeit der Einwilligung S. 221–224.

Datenschutz durch Technik kann gesellschaftliche Probleme, deren Ursachen nicht in der Technik liegen, nur begrenzt zu beseitigen helfen.¹⁹³⁵ Beispielsweise wird eine Arbeitsstelle, die flexible Verfügbarkeit und Arbeit in den Abendstunden voraussetzt, alleinerziehende Eltern systematisch benachteiligen, unabhängig davon, wie die Datenbearbeitungen am Arbeitsplatz technisch ausgestaltet sind.¹⁹³⁶ Jedoch kann der Datenschutz durch Technik beispielsweise helfen, Mobbing von Arbeitskollegen im Netz einzudämmen, indem das Teilen von Beiträgen in Foren limitiert wird.¹⁹³⁷

cc) Datenschutz-Folgenabschätzung

i. Rechtsgrundlage und Normzweck

Die Pflicht zur Datenschutz-Folgenabschätzung sehen sowohl das künftige Datenschutzrecht (Art. 20 E-DSG, Art. 22 rev-DSG) als auch der Europarat (Art. 10 Abs. 2 revidiertes Übereinkommen 108) und die EU vor (Art. 35 DSGVO).¹⁹³⁸ Zahlreiche europäische Rechtsordnungen waren bereits vor Inkrafttreten der DSGVO mit der Idee einer (zumeist freiwilligen) Persönlichkeitsschutz-Folgenabschätzung vertraut.¹⁹³⁹ Im Madrider Übereinkommen von 2009 (Art. 22 lit. h)

¹⁹³⁵ KIM 2017, 191. Um einen Algorithmus zu verstehen, muss auch den sozialen Konstrukten, die um ihn herum existieren, Beachtung geschenkt werden: Europarat 2016a, 6.

¹⁹³⁶ KIM 2017, 871. Siehe auch S. 98.

¹⁹³⁷ Vgl. HARTZOG 2018, 198.

¹⁹³⁸ EU/Europarat, 179.

¹⁹³⁹ Siehe zur Unterscheidung zwischen der Datenschutz- (DPIA) und der Persönlichkeitsschutz-Folgenabschätzung (PIA) S. 320–321. – Nur in Nordmazedonien und Norwegen war ein PIA für Datenbearbeiter im Jahr 2012 obligatorisch: LE GRAND/BARRAU, 112–113. Ein *privacy and data protection impact assessment* empfiehlt die EU seit 2009 hinsichtlich RFID-Anwendungen: Art. 4 Empfehlung der Kommission vom 12.05.2009 zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen (bekanntgegeben unter dem Aktenzeichen K(2009) 3200) (2009/387/EG) [sic]. BYGRAVE, 116; WRIGHT/DE HERT 2012b, 4. Vgl. SPIEKERMANN, 345. Für EU-Mitgliedstaaten war eine staatliche Vorabkontrolle (*prior checking*) für Datenbearbeitungen mit spezifischen Risiken für die Rechte und Freiheiten der Personen vorgesehen (vgl. Art. 20 DSRL), die jedoch nicht mit dem durch den Verantwortlichen durchzuführenden PIA zu verwechseln ist: LE GRAND/BARRAU, 114.

wurde diese Idee erstmals global festgehalten.¹⁹⁴⁰ International propagiert besonders Kanada das Konzept der Persönlichkeitsschutz-Folgenabschätzung.¹⁹⁴¹

Die Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden (Art. 20 Abs. 1 E-DSG). Dabei muss die Arbeitgeberin systematisch die möglichen Risiken eines Projekts für die Persönlichkeit des Betroffenen evaluieren und Massnahmen finden, um die Auswirkungen auf ihn zu mildern.¹⁹⁴² Es handelt sich bei der Pflicht zur Datenschutz-Folgenabschätzung um eine Professionalisierungsmassnahme, weil sie die Arbeitgeberin dazu veranlasst, den Datenschutz schon ab Beginn der Datenbearbeitung umzusetzen. Zudem trägt die Norm zufolge ihrer expliziten Bezugnahme auf ein allfällig «hohes Risiko» einer Datenbearbeitung dazu bei, die vorliegend geäusserte Forderung nach mehr Risikoorientierung zu erfüllen.¹⁹⁴³

ii. Voraussetzungen

Eine Datenschutz-Folgenabschätzung muss vorgenommen werden, «wenn eine Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann» (Art. 20 Abs. 1 Satz 1 E-DSG, Art. 22 Abs. 1 Satz 1 rev-DSG),¹⁹⁴⁴ dies im Unterschied zum Datenschutz durch Technik und zu den datenschutzfreundlichen Voreinstellungen, die jederzeit einzuhalten sind. Das hohe Risiko ergibt sich aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung (Art. 20 Abs. 2 Satz 1 E-DSG, Art. 22 Abs. 2 Satz 1 rev-DSG). Wann die Relevanzschwelle des hohen Risikos erreicht ist, definiert

¹⁹⁴⁰ RALLO LOMBARTE, 390.

¹⁹⁴¹ STODDART, 419.

¹⁹⁴² Europarat 2015, N 20.1; SPIEKERMANN, 323–324. Vgl. HARTZOG 2018, 181. Umstritten ist, ob es sich bei einer Datenschutz-Folgenabschätzung um eine reine Überprüfung der Compliance handelt (so WRIGHT/DE HERT 2012b, 8, und DE HERT, 34) oder um mehr (so KROENER/WRIGHT, 360).

¹⁹⁴³ Siehe S. 140. Vgl. zum risikobasierten Ansatz der DSGVO: Art.-29-Datenschutzgruppe 2017a, 5.

¹⁹⁴⁴ Vgl. Art. 35 Abs. 1 DSGVO. Zum europäischen Recht: BYGRAVE, 115. Vgl. das Prüfschema der Art.-29-Datenschutzgruppe zur Erforderlichkeit einer Datenschutz-Folgenabschätzung: Art.-29-Datenschutzgruppe 2017a, 7.

das Gesetz nicht.¹⁹⁴⁵ Es empfiehlt sich daher, für die Abschätzung des Risikos die vorliegend erarbeiteten Parameter auf den Einzelfall anzuwenden.¹⁹⁴⁶

Die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung besteht nicht nur, wenn eine Einzelfallprüfung ergibt, dass hohe Risiken voraussehbar sind, sondern namentlich auch, wenn eines der beiden Regelbeispiele (vgl. Art. 20 Abs. 2 lit. a–c E-DSG, Art. 22 Abs. 2 lit. a–b rev-DSG) verwirklicht ist. Hierzu zählt, erstens, die umfangreiche Bearbeitung besonders schützenswerter Personendaten (Art. 20 Abs. 2 lit. a E-DSG, Art. 22 Abs. 2 lit. a rev-DSG). Für die Bedeutung des Merkmals «umfangreich» kann auf die bereits gemachten Ausführungen verwiesen werden.¹⁹⁴⁷

Zweitens, eine systematische umfangreiche Überwachung öffentlicher Bereiche birgt ebenfalls ein hohes Risiko (Art. 20 Abs. 2 lit. c E-DSG, Art. 22 Abs. 2 lit. b rev-DSG). Hierzu zählt beispielsweise die Videoüberwachung des Empfangsraums in einer Arztpraxis.¹⁹⁴⁸ Offen ist, ob im Umkehrschluss die Videoüberwachung in nicht öffentlich zugänglichen Bereichen oder eine Videoüberwachung öffentlich zugänglicher Bereiche, die nur einen begrenzten Bereich erfasst (z.B. eine Kamera, die nur bei Nutzung einer Türklingel aktiviert wird), keiner Folgenabschätzung bedarf.¹⁹⁴⁹ Nach der hier vertretenen Ansicht, die von einer risikoorientierten Auslegung des DSG ausgeht, besteht in solchen Fällen oft ein geringeres Verletzungsrisiko, weshalb eine Datenschutz-Folgenabschätzung in der Regel nicht notwendig ist.

iii. Umsetzung

Die Datenschutz-Folgenabschätzung muss zum frühestmöglichen Zeitpunkt bereits in der Entwicklungsphase der Bearbeitungstätigkeiten beginnen, selbst wenn

¹⁹⁴⁵ Ebenso wenig die DSGVO: DSGVO-BDSG-K-MARTINI, Art. 35 DSGVO, N 13.

¹⁹⁴⁶ Siehe zu den Risikoparametern S. 141–148.

¹⁹⁴⁷ Siehe S. 147.

¹⁹⁴⁸ Vgl. zur Parallelbestimmung in Art. 35 Abs. 3 lit. c DSGVO: DOCHOW, 53.

¹⁹⁴⁹ DSGVO-BDSG-K-MARTINI, Art. 35 DSGVO, N 31.

einige der Bearbeitungsvorgänge noch nicht bekannt sind.¹⁹⁵⁰ Während des folgenden Projektablaufs muss sie kontinuierlich aktualisiert werden.¹⁹⁵¹

In persönlicher Hinsicht sollte die jeweilige Projektverantwortliche darüber entscheiden, ob, in welchem Umfang und mit welchen Beteiligten eine Datenschutz-Folgenabschätzung durchgeführt wird.¹⁹⁵² Damit sich die Datenschutz-Folgenabschätzung in der Praxis erfolgreich durchsetzt, ist zudem erforderlich, dass sie von der Führungsebene unterstützt wird und ein hochrangiger Datenschutzexperte im Unternehmen existiert.¹⁹⁵³

Der Prozess einer Datenschutz-Folgenabschätzung gliedert sich entsprechend der allgemeinen Doktrin zum Risikomanagement in die folgenden fünf Schritte: Definition einer Risikopolitik, Identifizierung und Analyse der Risiken, Risikobewertung, Ergreifung von Massnahmen zur Risikosteuerung sowie Risikoüberwachung und Reporting (vgl. Art. 20 Abs. 3 E-DSG, Art. 22 Abs. 3 rev-DSG).¹⁹⁵⁴ Die Resultate sind in einem Bericht festzuhalten.¹⁹⁵⁵

Der Prüfradius der Datenschutz-Folgenabschätzung ist – entsprechend dem Gesetzeszweck (Art. 1 E-DSG, Art. 1 rev-DSG) – grundsätzlich auf den Schutz personenbezogener Daten der jeweils betroffenen Person beschränkt. Jedoch wäre es erstrebenswert, in der Datenschutz-Folgenabschätzung auch die Folgeerscheinun-

¹⁹⁵⁰ Vgl. zur DSGVO: Art.-29-Datenschutzgruppe 2017a, 17. Vgl. WRIGHT/DE HERT 2012b, 6.

¹⁹⁵¹ Gegebenenfalls müssen einzelne Schritte der Datenschutz-Folgenabschätzung wiederholt werden, da sich die Schwere oder Eintrittswahrscheinlichkeit der Risiken ändern können: Art.-29-Datenschutzgruppe 2017a, 17.

¹⁹⁵² WRIGHT/DE HERT 2012b, 25.

¹⁹⁵³ WRIGHT/DE HERT 2012a, 447.

¹⁹⁵⁴ STAUB, 705. Vgl. ROMEIKE, 24–31. Zum *privacy impact assessment*: CAVOUKIAN 2011, 15.

¹⁹⁵⁵ Musterbericht einer Datenschutz-Folgenabschätzung gemäss DSGVO: SCHULZ, 97.

gen einer Persönlichkeitsverletzung für Gruppen und die Gesellschaft¹⁹⁵⁶ sowie für das Gesamtunternehmen¹⁹⁵⁷ zu beurteilen.

iv. *Konsultationen des EDÖB und der Arbeitnehmer*

Ergibt sich aus der Datenschutz-Folgenabschätzung, dass die geplante Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person zur Folge hätte, wenn die Verantwortliche keine Massnahmen trafe, so holt sie vorgängig die Stellungnahme des EDÖB ein (Art. 21 Abs. 1 E-DSG, Art. 23 Abs. 1 rev-DSG). Auch die EU sieht eine entsprechende obligatorische vorherige Konsultation der Aufsichtsbehörde vor (Art. 36 Abs. 1 DSGVO), und der Europarat empfiehlt eine solche Konsultation.¹⁹⁵⁸

Die private Verantwortliche kann von der Konsultation des EDÖB absehen, wenn sie den Datenschutzberater konsultiert hat (Art. 21 Abs. 4 E-DSG, Art. 23 Abs. 4 rev-DSG).¹⁹⁵⁹ Es gibt somit keine Pflicht, den Datenschutzberater bei einer Datenschutz-Folgenabschätzung zu konsultieren. Im Gegensatz dazu verpflichtet die DSGVO die Verantwortliche bei der Durchführung der Datenschutz-Folgenabschätzung zum Einholen des Rates des Datenschutzbeauftragten, sofern ein solcher vorgängig benannt wurde (Art. 35 Abs. 2 DSGVO).¹⁹⁶⁰

Die DSGVO statuiert zudem eine Pflicht, gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Datenbearbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Bearbeitungsvorgänge einzuholen (Art. 35 Abs. 9 DSGVO). Der Einbezug der Individuen bedeutet, dass sich nicht nur Experten, wie die Aufsichtsbehörde und der interne Datenschutzbeauftragte, mit der Datenbearbeitung aus-

¹⁹⁵⁶ Eine Berücksichtigung der Gemeinwohlbelange in der Datenschutz-Folgenabschätzung sei «dringend empfehlenswert»: HOFFMANN-RIEM, 65. Art. 35 DSGVO habe auch betroffene Gruppen und Verbraucherverbände im Auge: DSGVO-BDSG-K-MARTINI, Art. 35 DSGVO, N 60. Vgl. zum *privacy impact assessment* RAAB/WRIGHT, 382: «The most important shortcoming would be the restriction [...] to assessing the impact on individuals, even if its recognition that categories and groups might be at risk takes a step into the field of considering wider impacts, and ultimately impacts on society as a whole.»

¹⁹⁵⁷ WRIGHT/DE HERT 2012b, 14.

¹⁹⁵⁸ Europarat 2015, N 21.d.

¹⁹⁵⁹ Siehe zum Datenschutzberater später, S. 333–335.

¹⁹⁶⁰ Der Verantwortliche muss den Datenschutzbeauftragten aktiv anfragen: BeckOK DS-HANSEN, Art. 35 DSGVO, N 22.

einandersetzen.¹⁹⁶¹ Im vorliegenden Kontext bedeutet dies, dass die Arbeitnehmervertretung und/oder die Gewerkschaft zu Rate zu ziehen ist.¹⁹⁶² Eine derartige Konsultationspflicht verordnet der E-DSG nicht. Jedoch verleiht das Mitwirkungsrecht der Belegschaft ein Mitspracherecht.¹⁹⁶³ Dieses gilt umfassend bzgl. aller Fragen des Arbeitnehmer-Gesundheitsschutzes; es dürfte tendenziell grosszügiger sein als das unter europäischem Datenschutzrecht vorgesehene Mitspracherecht, das nur bei Datenbearbeitungen mit hohen Risiken gilt.

Die Verantwortliche wird nicht ausdrücklich verpflichtet, die eingeholten Vorschläge umzusetzen.¹⁹⁶⁴ Soweit jedoch den Empfehlungen des betrieblichen Datenschutzberaters nicht gefolgt wird, ist davon auszugehen, dass allfällige Datenschutzverletzungen vorsätzlich begangen werden.¹⁹⁶⁵ Deshalb empfiehlt es sich, zumindest die Gründe für die Handlungen oder Unterlassungen der Verantwortlichen zu dokumentieren, dies in Anlehnung an das Arbeitsrecht, das eine Begründungspflicht statuiert, falls die Ratschläge der Arbeitnehmer ignoriert werden.¹⁹⁶⁶

Die verschiedenen mit der Datenschutz-Folgenabschätzung verbundenen Konsultationspflichten vermitteln den konsultierten Parteien die Informationen, die sie benötigen, um die Einhaltung des DSG zu kontrollieren. Dies ist auch für die vorliegend verlangte Demokratisierung förderlich.

v. *Fehlende Publizität des Berichts zur Datenschutz-Folgenabschätzung*

Der E-DSG enthält keine Anweisung, den Bericht über die Datenschutz-Folgenabschätzung zu veröffentlichen. Zwar bringt der Umstand, dass die Verantwortliche selbst oder von ihr beauftragte Personen die Folgenabschätzung durchführen,

¹⁹⁶¹ DE HERT, 75.

¹⁹⁶² Europarat 2015, N 21.c; BeckOK DS-HANSEN, Art. 35 DSGVO, N 61. Gar mit der Forderung nach einer «Zustimmung» der Arbeitnehmervertretung zur Datenbearbeitung, was einem unter Schweizer Recht nicht vorgesehenen Mitentscheidungsrecht gleichkäme: Europarat 2015, N 20.2. Siehe S. 105.

¹⁹⁶³ Siehe S. 103–105.

¹⁹⁶⁴ Eine Befolgungspflicht findet sich weder im rev-DSG (Art. 20 E-DSG bzw. Art. 22 rev-DSG betreffend Konsultation des Datenschutzberaters) noch im Mitwirkungsrecht (Art. 10 lit. a MitwG i.V.m. Art. 48 Abs. 2 ArG i.V.m. Art. 6 ArGV 3 betreffend Mitsprache der Arbeitnehmer). Ebenso wenig verpflichtet die DSGVO zur Umsetzung der Vorschläge: DSGVO-BDSG-K-MARTINI, Art. 35 DSGVO, N 61.

¹⁹⁶⁵ EDÖB 2010, 141; BSK DSG-EHRENSPERGER/BELSER, Art. 11a DSG, N 16d.

¹⁹⁶⁶ Vgl. Art. 48 Abs. 2 ArG. Siehe S. 104. Zur DSGVO: BeckOK DS-HANSEN, Art. 35 DSGVO, N 23.

den Vorteil mit sich, dass Geschäftsgeheimnisse geschützt bleiben.¹⁹⁶⁷ Doch sollte die Folgenabschätzung in einem «Geist der Offenheit» angegangen werden.¹⁹⁶⁸ Ideal wäre es daher, auch mit Blick auf den Transparenzgrundsatz, die wesentlichen Teile der Folgenabschätzung den interessierten Parteien zugänglich zu machen.¹⁹⁶⁹

dd) Datenschutzberater

Private Verantwortliche können einen Datenschutzberater ernennen (Art. 9 Abs. 1 E-DSG, Art. 10 rev-DSG). Bereits unter dem bisherigen Recht besteht die Möglichkeit, einen sog. «Datenschutzverantwortlichen» zu bezeichnen, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt (Art. 11a Abs. 5 lit. e DSGVO). Die Begriffe des Datenschutzberaters gemäss E-DSG und des Datenschutzverantwortlichen gemäss DSGVO werden vorliegend gleichbedeutend verwendet.

Die Ernennung des Datenschutzberaters ist in der Schweiz freiwillig. Dabei wird kritisiert, dass Unternehmen rechtlich keinen Vorteil davon tragen, wenn sie eine Stelle für einen betrieblichen Datenschutzberater schaffen.¹⁹⁷⁰ Es bräuchte mehr Anreize, beispielsweise könnten im öffentlich-rechtlichen Beschaffungswesen Bearbeiterinnen bevorzugt werden, die über einen unabhängigen Datenschutzberater verfügen.¹⁹⁷¹ Auch könnten Unternehmen mit einem Datenschutzberater von gewissen Berichts- oder Registrierungspflichten befreit werden.¹⁹⁷² Beispielsweise ist es zu begrüßen, dass künftig Unternehmen mit einem Datenschutzberater von der Pflicht befreit werden, den EDÖB zu konsultieren, wenn eine Datenschutz-Folgenabschätzung auf ein hohes persönlichkeitsrechtliches Risiko hindeutet (vgl. Art. 21 Abs. 4 i.V.m. Art. 9 E-DSG; Art. 23 Abs. 3 i.V.m. Art. 10 rev-DSG).

¹⁹⁶⁷ Vgl. MAYER-SCHÖNBERGER/CUKIER, 174.

¹⁹⁶⁸ DE HERT, 76.

¹⁹⁶⁹ Zur DSGVO: BeckOK DS-HANSEN, Art. 35 DSGVO, N 50. Vgl. zum *privacy impact assessment*: DE HERT, 75.

¹⁹⁷⁰ RUDIN 2002, 394.

¹⁹⁷¹ BOLLIGER *et al.*, 225. Dieselbe Quelle verlangt aber auch, zu prüfen, inwieweit das WTO-Recht solche Anreize zulässt. Zu denken ist an die Schranken des WTO-Übereinkommens zum Beschaffungswesen.

¹⁹⁷² RUDIN 2002, 415, schlägt dies auch als Anreiz für mehr Zertifizierungen (Art. 11 DSGVO, Art. 12 E-DSG, Art. 13 rev-DSG) vor.

Der hauptsächliche Unterschied des europäischen zum Schweizer Recht bzgl. des Datenschutzberaters besteht in der Verbindlichkeit.¹⁹⁷³ Im Rahmen der DSGVO ist ein sog. «Datenschutzbeauftragter», das Pendant zum schweizerischen Datenschutzberater, unter gewissen Voraussetzungen «auf jeden Fall» zu benennen (vgl. Art. 37 Abs. 1 DSGVO). 2002 beschäftigte erst jedes fünfte Schweizer Unternehmen (21 Prozent) einen eigenen Datenschutzberater.¹⁹⁷⁴ Durch die DSGVO sind indessen 3'682 zusätzliche Datenschutzberater für Schweizer Unternehmen erforderlich geworden.¹⁹⁷⁵

Im Übrigen sind die Anforderungen an den Datenschutzberater gemäss rev-DSG und an den Datenschutzbeauftragten gemäss DSGVO ähnlich:¹⁹⁷⁶ Erstens, er muss seine Funktion fachlich unabhängig ausüben können und darf gegenüber der Verantwortlichen nicht weisungsgebunden sein (Art. 9 Abs. 2 lit. a E-DSG, Art. 10 Abs. 3 lit. a rev-DSG, Art. 38 Abs. 3 DSGVO). Es ist nach vorliegender Auffassung zu konkretisieren, dass die Weisungsfreiheit in Bezug auf Fragen des Datenschutzes und der Datensicherheit beschränkt ist. Ist der Datenschutzberater ein interner Mitarbeiter, sollte das Unternehmen ihn direkt der Geschäftsleitung unterstellen, um ihm die unabhängige Ausübung seiner Beratungs- und Kontrollfunktion zu ermöglichen.¹⁹⁷⁷ Nicht vorgesehen ist ein Sonderkündigungsschutz, wie ihn etwa der betriebliche Datenschutzbeauftragte unter deutschem Recht genießt.¹⁹⁷⁸ Zweitens, der Datenschutzberater darf keine Tätigkeit ausüben, die mit seinen Aufgaben als Datenschutzberater unvereinbar sind (Art. 9 Abs. 2 lit. b E-DSG, Art. 10 Abs. 3 lit. b rev-DSG, Art. 38 Abs. 6 DSGVO). Es darf somit nicht zu Interessenkonflikten kommen.¹⁹⁷⁹ Drittens, der Datenschutzberater muss über die erforderlichen Fachkenntnisse verfügen (Art. 9 Abs. 2 lit. c E-DSG, Art. 10 Abs. 3 lit. c rev-DSG, Art. 37 Abs. 5 DSGVO) – eine Tugend, die vorliegend bereits mehrfach inständig reklamiert wurde.¹⁹⁸⁰ Bei der Fachkenntnis han-

¹⁹⁷³ CHARLET, N 107.

¹⁹⁷⁴ RIESELMANN-SAXER, 45.

¹⁹⁷⁵ ALIYEV SAMIR, Why do Swiss companies need a data protection officer?, 16.04.2019, abrufbar unter <www.vista.blog> (besucht am 31.05.2020).

¹⁹⁷⁶ CHARLET, N 107.

¹⁹⁷⁷ BBI 2017, 7033. Vgl. zum deutschen Recht: WYBITUL/SCHULTZE-MELLING, N 370.

¹⁹⁷⁸ Unzulässige Kündigung innerhalb eines Jahrs nach Beendigung der Bestellung unter deutschem Recht: WEDDE 2016a, 259; WYBITUL/SCHULTZE-MELLING, N 370.

¹⁹⁷⁹ Vgl. zur DSGVO: DOMENIG/MITSCHERLICH, N 387–388.

¹⁹⁸⁰ Siehe S. 131–132 und 247–250.

delt es sich um einen unbestimmten Rechtsbegriff.¹⁹⁸¹ Einerseits wird rechtliche Kenntnis der Datenschutzgesetzgebung erwartet, andererseits technische Kenntnisse, welche dazu befähigen, die Umsetzung des Datenschutzrechts wirksam zu begleiten und zu überwachen.¹⁹⁸² Viertens, die Kontaktdaten des Datenschutzberaters sind zu veröffentlichen und dem EDÖB mitzuteilen (Art. 9 Abs. 2 lit. d E-DSG, Art. 10 Abs. 3 lit. d rev-DSG, Art. 37 Abs. 7 DSGVO).

Ein Unternehmen, das einen Datenschutzberater anstellt, unternimmt einen Schritt in Richtung Professionalisierung, da der Datenschutzberater mit seiner Fachkenntnis darauf hinwirken kann, dass die Arbeitgeberin das Datenschutzrecht laufend einhält. Es wäre deswegen zu begrüßen, wenn die Zusammenarbeit mit einem Datenschutzberater in gewissen Fällen für verbindlich erklärt würde oder wenn wenigstens konkretere Anreize zur freiwilligen Ernennung eines Datenschutzberaters gesetzt würden.

ee) Förderung der regulierten Selbstregulierung

Die regulierte Selbstregulierung muss gefördert werden.¹⁹⁸³ Bei der regulierten Selbstregulierung stellt der Staat den Privaten einen strukturierten regulativen Rahmen bereit, der die spezifischen Regulierungsziele, -instrumente und -instanzen festlegt. Durch diesen Rahmen steht den selbstregulierenden Privaten zwar ein Spielraum für die Optionenkonkretisierung und -wahl zur Verfügung, doch dieser wird zugleich dadurch eingeeengt, dass der Staat selbst die verfügbaren Optionen strukturiert.¹⁹⁸⁴ Der grösste Vorteil der Selbstregulierung besteht darin, dass die Datenschutz-Expertise direkt in den Unternehmen wächst.¹⁹⁸⁵ Die Arbeitgeberin setzt sich dank der Möglichkeit zur legislatorischen Mitgestaltung proaktiv mit dem Datenschutzrecht auseinander, wodurch die vorliegend verlangte Professionalisierung zunimmt. Zudem entstehen kontextrelevante, branchenspezifische

¹⁹⁸¹ Vgl. zur deutschen Parallelbestimmung: WEDDE 2016a, 256.

¹⁹⁸² DOMENIG/MITSCHERLICH, N 387.

¹⁹⁸³ Vgl. die Forderung nach Selbstregulierung unter Vorgabe von Zertifizierungsstandards: RUDIN 2004b, 437.

¹⁹⁸⁴ TALIDOU, 27. Im Gegensatz zur regulierten Selbstregulierung steht die reine Selbstregulierung. Ein Beispiel hierfür ist die Netiquette: Sie legt die Sitten und Gebräuche im Internet fest, welchen sich ein grosser Teil der Internet-Benutzer ohne staatlichen Zwang unterworfen hat: TALIDOU, 212–213.

¹⁹⁸⁵ BAMBERGER/MULLIGAN 2015, 35. Vgl. die Bezeichnung der betrieblichen Datenschutzverantwortlichen als «*norm entrepreneurs*», d.h. als Personen, die die Sorgen bzgl. Privatsphäre in die unternehmerischen Entscheidungsprozesse integrieren: BAMBERGER/MULLIGAN 2011, 314.

Präzisierungen, die Rechtssicherheit schaffen.¹⁹⁸⁶ Diese Vorteile sind für eine sektorspezifische Datenschutzregulierung charakteristisch, wie sie etwa in den USA existiert.¹⁹⁸⁷ Sie könnten aber auf dem Wege der regulierten Selbstregulierung auch unter dem schweizerischen DSG und der europäischen DSGVO genutzt werden. Das DSG und die DSGVO stellen Omnibus-Erlasse dar, die auf alle Datenbearbeitungen anwendbar und daher abstrakter formuliert sind.¹⁹⁸⁸ Selbstregulierungsnormen, die die Branchenvertreter persönlich ausgehandelt haben, dürften ferner in der Branche auf höhere Akzeptanz stossen.¹⁹⁸⁹ Ein weiterer Vorteil der Selbstregulierung besteht in einem flexiblen Normsetzungsverfahren.¹⁹⁹⁰ Anreize wie diese sind erforderlich, um das Datenschutzrecht zu beleben.¹⁹⁹¹

Eine Möglichkeit zur regulierten Selbstregulierung sind Verhaltenskodizes.¹⁹⁹² Berufs- und Wirtschaftsverbände, die nach ihren Statuten zur Wahrung der wirtschaftlichen Interessen ihrer Mitglieder befugt sind, sowie Bundesorgane können dem EDÖB einen Verhaltenskodex zur Stellungnahme vorlegen (Art. 10 Abs. 1 E-DSG, Art. 11 Abs. 1 rev-DSG). Da der Verhaltenskodex vom Berufs- oder Wirtschaftsverband ausgearbeitet wird, reicht seine Geltung weiter als unterneh-

¹⁹⁸⁶ RITZER, 504. Vgl. World Economic Forum 2013, 17.

¹⁹⁸⁷ «One notable advantage is that certification standards could be set on a per-sector basis»: EDWARDS/VEALE, 80. Vgl. die Forderung nach einem Datenrecht als Rahmengesetz und präzisierenden, schutzmotivierten Spezialerlassen: EGGIMANN, 213. Anzustreben sei ein auf den jeweiligen Problembereich zugeschnittenes, dessen Kontextbedingungen beachtendes, responsives und lernfähiges Recht: HOFFMANN-RIEM, 73. Es «scheint, abweichend vom Omnibus-Ansatz der DSGVO [...] eine sektoral differenzierte Regulierung [...] sinnvoll»: HERMSTRÜWER, 114. Die Tatsache, dass die DSGVO ein Omnibus-Gesetz ist, schliesst sektorspezifische Gesetze auf nationaler Ebene nicht aus, wie sich am Beispiel von Belgien zeigt: CALLAGHAN/WIGMAN, 16–23. Zur sektorspezifischen Regulierung auf Bundesstaatsebene in den USA: White House, Executive Office of the President 2014, 18, WOOD *et al.*, 215, GILBERT, 335, OTTO 2016, 4, SOLOVE/HARTZOG, 587, und CAVOUKIAN 2011, 22. Selbst die US-Verfassung schützt nicht explizit das Recht auf Privatsphäre: GILBERT, 335, und OTTO 2016, 8.

¹⁹⁸⁸ Vgl. zur DSGVO: WRIGLEY, 189. Vgl. zum Übereinkommen 108: Europarat 2016b, 24.

¹⁹⁸⁹ A.M. MARTINI, 1023: Selbstverpflichtungen seien in der Digitalwirtschaft bislang nicht zum wirkmächtigen Erfolgsmodell aufgestiegen.

¹⁹⁹⁰ Der demokratische Gesetzgebungsprozess hinke der Geschwindigkeit des technologischen Fortschritts hinterher: HJUMANS/KRANENBORG, 5.

¹⁹⁹¹ Vgl. DREYER/SCHULZ, 37: «Es kommt für die tatsächliche Umsetzung auf ein wirksames Anreizsystem an.» – «Nudging»: GUIHOT *et al.*, 386. Es brauche eine «win-win solution»: CAVOUKIAN 2012, 19.

¹⁹⁹² Schweizerischer Bundesrat 2017b, 72.

mensinterne Datenschutzrichtlinien, die bereits eine deutliche Mehrheit der Schweizer Unternehmen besitzt.¹⁹⁹³ Es gibt bereits erste Beispiele von Verhaltenskodizes betreffend das Datenschutzrecht.¹⁹⁹⁴

Ebenfalls in die Richtung einer Selbstregulierung zielt die Möglichkeit, dass die Hersteller von Datenbearbeitungssystemen oder -programmen sowie die Verantwortlichen und Auftragsbearbeiter ihre Systeme, Produkte und Dienstleistungen einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen können (Art. 12 Abs. 1 E-DSG, Art. 13 Abs. 1 rev-DSG, vgl. Art. 11 Abs. 1 DSG). Die Zertifizierung ist freiwillig.¹⁹⁹⁵ Der Bundesrat erlässt Vorschriften über die Anerkennung von Zertifizierungsverfahren und die Einführung eines Datenschutzes-Qualitätszeichens. Er berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen (Art. 12 Abs. 2 E-DSG, Art. 13 Abs. 2 rev-DSG). Wegweisend können dabei die Empfehlungen der ENISA für Zertifizierungen gemäss Art. 42 DSGVO sein.¹⁹⁹⁶ Des Weiteren können private, nicht offiziell anerkannte Standards konsultiert werden, wie beispielsweise die Normen des schweizerischen Vereins ISO,¹⁹⁹⁷ das deutsche EuroPriSe (*European Privacy Seal*), die nordamerikanischen *TRUSTe*, *BBBOnLine* des Better Business Bureau und *WebTrust* oder das *PrivacyMark* aus Japan.¹⁹⁹⁸ Im EU-Raum gibt es, soweit ersichtlich, noch keine DSGVO-konformen Zertifizierungen.¹⁹⁹⁹ Zertifizierungen könnten stärker gefördert werden mit Anreizen, wie vorstehend bzgl. der

¹⁹⁹³ Zwei Drittel (67 Prozent) der Schweizer Unternehmen besaßen 2002 Datenschutz-Richtlinien: RIESELMANN-SAXER, 45.

¹⁹⁹⁴ Als erster deutscher Verband hat der Gesamtverband der Deutschen Versicherungswirtschaft eigene Verhaltensregeln zum Datenschutz aufgestellt und mit der zuständigen Behörde abgestimmt: RITZER, 501.

¹⁹⁹⁵ So auch Art. 42 Abs. 3 DSGVO. Vgl. EDWARDS/VEALE, 79.

¹⁹⁹⁶ ENISA.

¹⁹⁹⁷ Z.B. ISO/IEC 27001 zur Zertifizierung der «Sicherheit der Bearbeitung» (vgl. Art. 32 DSGVO): RESCH, 215; z.B. ISO 9000 ff. und ISO/IEC 27000 zur Zertifizierung eines Datenschutz-Management-Systems: FASCHING *et al.*, N 18. Vgl. zu weiteren ISO-Normen: MASEBERG SÖNKE, ISO/IEC 27552 ist keine DSGVO-konforme Zertifizierung!, 04.03.2019, abrufbar unter <www.datenschutz-notizen.de> (besucht am 31.05.2020).

¹⁹⁹⁸ CAVOUKIAN 2011, 16; TAMÒ-LARRIEUX, 182.

¹⁹⁹⁹ Stand am 31.05.2020. Siehe bereits zum Stand am 04.03.2019: MASEBERG SÖNKE, ISO/IEC 27552 ist keine DSGVO-konforme Zertifizierung!, 04.03.2019, abrufbar unter <www.datenschutz-notizen.de> (besucht am 31.05.2020), und zum Stand in Österreich per 01.01.2019: RESCH, 215.

Förderung der Datenschutzberaterstellen diskutiert wurde.²⁰⁰⁰ Einen solchen Anreiz wird es gemäss rev-DSG bald geben: Unternehmen, die über ein Zertifikat verfügen oder einen Verhaltenskodex befolgen, werden unter gewissen Bedingungen von der Erstellung einer Datenschutz-Folgenabschätzung befreit sein (vgl. Art. 20 Abs. 5 E-DSG, Art. 22 Abs. 5 rev-DSG).

ff) Verzeichnis-, Informations- und Meldepflicht

Die Verantwortlichen und Auftragsbearbeiter führen ein Verzeichnis ihrer Bearbeitungstätigkeiten (Art. 11 Abs. 1 E-DSG, Art. 12 Abs. 1 rev-DSG). Diese Pflicht statuiert auch das europäische Datenschutzrecht (vgl. Art. 30 DSGVO). Der Bundesrat sieht jedoch Ausnahmen für Unternehmen vor (Art. 11 Abs. 5 E-DSG, Art. 12 Abs. 5 rev-DSG). Das Parlament hat beschlossen, dass die Ausnahmen für Unternehmen mit weniger als 250 Mitarbeitern gelten sollen,²⁰⁰¹ d.h. für 99,73 Prozent der Schweizer Unternehmen.²⁰⁰² Es ist daher davon auszugehen, dass die Verzeichnispflicht selten anwendbar sein wird. Immerhin gilt die Verzeichnispflicht auch bei kleinen Unternehmen, sofern ihre Datenbearbeitung mehr als ein geringes Risiko von Persönlichkeitsverletzungen mit sich bringt (Art. 11 Abs. 5 E-DSG bzw. Art. 12 Abs. 5 rev-DSG *e contrario*).

Die Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden (Art. 17 Abs. 1 E-DSG, Art. 19 Abs. 1 rev-DSG). Die Arbeitgeberin sollte in einem internen, für alle Arbeitnehmer zugänglichen Reglement offenlegen, welche Daten sie bei People Analytics verwendet.²⁰⁰³ Transparenz, Erklärungen und Verzeichnisse der Bearbeitungstätigkeiten können das Vertrauen der Arbeitnehmer in das Unternehmen erhöhen.²⁰⁰⁴ Da die Vermittlung der komplexen Sachverhalte von People Analytics aber nicht immer

²⁰⁰⁰ Siehe S. 333. BOLLIGER *et al.*, 224–225.

²⁰⁰¹ Beschluss Nationalrat: AB NR 2019, 1808–1809; Bestätigung durch Ständerat: AB SR 2019, 1243. Die Botschaft setzte die De-Minimis-Schwelle bei 50 Mitarbeitern an: Art. 11 Abs. 5 E-DSG.

²⁰⁰² AB NR 2019, 1806.

²⁰⁰³ RIEDY/WEN, 95.

²⁰⁰⁴ Vgl. THELISSON *et al.*, 55–56. Vgl. BIRAN/COTTON, 8: Empirische Studien belegen den Nutzen von Erklärungen zur Steigerung des Vertrauens in KI und maschinelles Lernen.

sinnvoll ist, sollte die Informationspflicht im vorstehend beschriebenen Sinn restriktiv ausgelegt werden.²⁰⁰⁵

Die Verantwortliche meldet eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, dem EDÖB so rasch als möglich (Art. 22 Abs. 1 E-DSG, Art. 24 Abs. 1 rev-DSG). Die Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt (Art. 22 Abs. 4 E-DSG, Art. 24 Abs. 4 rev-DSG). Eine entsprechende Meldung (*data breach notification*, Art. 33 DSGVO) und eine Benachrichtigung (Art. 34 DSGVO) sieht auch die DSGVO vor.

Die Verzeichnis-, Informations- und Meldepflicht stellen Professionalisierungsmassnahmen dar: Sie verpflichten die Arbeitgeberin, von Anfang an den Überblick über die eigenen Datenbearbeitungstätigkeiten und die Datensicherheit zu behalten, sowie dazu, gegebenenfalls die Betroffenen oder den EDÖB zu benachrichtigen. Die Pflichten dienen indirekt aber auch der Demokratisierung, weil beispielsweise die Meldung dem EDÖB die nötigen Grundlagen verschafft, um gegebenenfalls gegen die Datenbearbeitung einzuschreiten.

b) Weitere Professionalisierungsvorschläge

aa) Rechenschaftspflicht

Die europäische Datenschutzordnung sieht neu explizit eine sog. Rechenschaftspflicht (*accountability*) vor, sodass die Arbeitgeberin für die Einhaltung der Datenschutz-Grundsätze verantwortlich ist und deren Einhaltung nachweisen können muss (vgl. Art. 5 Abs. 2 DSGVO). Die systematische Stellung der Rechenschaftspflicht in einem gesonderten Absatz (Art. 5 Abs. 2 DSGVO) verdeutlicht, dass es sich dabei um ein übergeordnetes Prinzip von besonderer Wichtigkeit handelt, das gleichermassen in Bezug auf alle restlichen sechs Grundsätze der DSGVO (vgl. Art. 5 Abs. 1 DSGVO) gilt.²⁰⁰⁶

Es fällt schwer, den Begriff «*accountability*» in einem Wort ins Deutsche zu übersetzen.²⁰⁰⁷ Die in der deutschsprachigen DSGVO-Version bezeichnete «Rechenschaftspflicht» ist ganz allgemein die Pflicht zur Rechnungslegung. Diese wieder-

²⁰⁰⁵ Siehe S. 202–205.

²⁰⁰⁶ KELLEHER/MURRAY, N 6.22; DEBEER, 411.

²⁰⁰⁷ Ungewiss, ob «Verantwortlichkeit» oder «Verantwortung» den Begriffskern besser treffe: HÄRTING, N 277.

rum ist eine Auskunft über die näheren Umstände oder Gründe eines Sachverhalts, wofür man verantwortlich ist.²⁰⁰⁸

Im rechtlichen Sinn ist unter der Rechenschaft zunächst die Verantwortlichkeit bzw. die Haftung (*liability*) zu verstehen.²⁰⁰⁹ Sie ist bereits Bestandteil des geltenden Datenschutzrechts (vgl. Art. 82 DSGVO, vgl. aber auch Art. 15 DSGVO bzw. Art. 28 E-DSG bzw. Art. 32 rev-DSG i.V.m. Art. 28a Abs. 3 ZGB).

Zusätzlich aber impliziert die Rechenschaftslegung eine Dokumentationspflicht²⁰¹⁰ und einen Prozess der transparenten Interaktion mit jemandem, der die Datenbearbeitung überprüfen will.²⁰¹¹ Es genügt somit nicht, die Regeln einzuhalten; Unternehmen müssen die Einhaltung des Gesetzes jederzeit nachweisen können.²⁰¹² Dies veranlasst die Arbeitgeberin dazu, das Datenschutzrecht ab Beginn der Bearbeitung zu befolgen, und ist somit als Professionalisierungsmassnahme zu begrüssen. Die Dokumentationspflicht führt letztlich dazu, dass die Verantwortliche bzw. im Fall von People Analytics die Arbeitgeberin die Beweislast für die Einhaltung der datenschutzrechtlichen Pflichten trägt.²⁰¹³ Dies gilt sowohl gegenüber der Aufsichtsbehörde als auch im Zivilverfahren.²⁰¹⁴ Folgerichtig wird für Schadenersatzklagen eine Verschuldensvermutung statuiert (siehe Art. 82 Abs. 3 DSGVO). Der Kläger bleibt aber für den Eintritt des Schadens und den Kausalzusammenhang beweispflichtig.²⁰¹⁵ Die explizite Verankerung des Grundsatzes der Rechenschaftspflicht und damit einer Beweislastumkehr ist eine der wichtigsten

²⁰⁰⁸ Duden, Rechenschaft, die, abrufbar unter <www.duden.de> (besucht am 31.05.2020).

²⁰⁰⁹ «Accountability» stehe synonym zu «liability»: KROENER/WRIGHT, 359–360. Die Arbeitgeberin hafte z.B. für diskriminierende Wirkungen eines Algorithmus: GAY/KAGAN.

²⁰¹⁰ DÄUBLER, N 583–583i.

²⁰¹¹ Algo:aware [sic], 27. An einen Gerichtssaal erinnert die Definition der Rechenschaftspflicht als «*a relationship between an actor and a forum, in which the actor has an obligation to explain and to justify his or her conduct, the forum can pose questions and pass judgement, and the actor may face consequences*»: algo:aware [sic], 27. Vgl. ZWEIG/KRAFFT, 112, WEBER/OERTLY, N 32–33, und EDWARDS/VEALE, 41.

²⁰¹² EDSB 2019c; DICKIE/YULE, 101; KROENER/WRIGHT, 360; THOMAS, 139. Vgl. CAVOUKIAN/TAYLOR/ABRAMS, 408.

²⁰¹³ Dass die Verantwortliche die Beweislast trägt, ist ein generelles Prinzip der DSGVO. Z.B. muss sie beweisen, dass eine Einwilligung freiwillig erfolgt ist (vgl. Art. 7 Abs. 4 DSGVO): Art.-29-Datenschutzgruppe 2017d, 9. TAMÒ-LARRIEUX, 171.

²⁰¹⁴ Vgl. Europarat 2011, 7, zur Rechenschaftspflicht unter der Empfehlung No. R (89) 2 (Europarat 1989).

²⁰¹⁵ Urteil Oberster Gerichtshof [Österreich] OGH 6Ob217/19h vom 27.11.2019 E. 4.2–4.3.

Neuerungen des EU-Rechts gegenüber der Vorgängerrichtlinie 95/46/EG.²⁰¹⁶ Die Rechenschaftspflicht verlagert die Verantwortung für den Schutz der Privatsphäre vom informationell selbstbestimmt handelnden Betroffenen auf die Datenbearbeiterin.²⁰¹⁷

Eine vorstellbare Umsetzungsform der Rechenschaftspflicht besteht in einem personalisierten Übersichtsfenster (*dashboard*), das für den Anfragenden grafisch aufarbeitet, welche Daten über ihn das Unternehmen wie lange speichert.²⁰¹⁸ Zusätzlich braucht es eine Verpflichtung der Organisation zur Rechenschaftslegung mittels eines internen Reglements und Schulungen.²⁰¹⁹

Das rev-DSG sieht nicht explizit eine Rechenschaftspflicht mit genereller Beweislastumkehr vor. Dies ist zu bedauern, da sich Persönlichkeitsschutz- und Diskriminierungsklagen erheblichen Beweisschwierigkeiten ausgesetzt sehen.²⁰²⁰ Im Bereich der Grundrechte ist die Beweislastumkehr aber international vorgegeben: Die EGMR-Rechtsprechung zum Recht auf Achtung des Privat- und Familienlebens (Art. 8 EMRK) anerkennt eine Beweislast der Arbeitgeberin.²⁰²¹ Da sich die Schweiz zur Einhaltung der EMRK verpflichtet hat, muss in der Konsequenz in der Schweiz zumindest in öffentlich-rechtlichen Arbeitsverhältnissen die Arbeitgeberin die Beweislast für die Einhaltung des Grundrechts auf Achtung des Privat- und Familienlebens tragen. Nach der hier vertretenen Meinung sollte auch die privatrechtliche Arbeitgeberin die Einhaltung des Datenschutzgesetzes beweisen müssen, da sie als Datenbearbeiterin über die notwendigen Informationen verfügt.²⁰²² Zudem wirkt es professionell und vertrauensfördernd, wenn sie imstande ist, darzulegen, wie sie bei der Datenbearbeitung vorgeht, und dass sie dabei das Gesetz einhält.

²⁰¹⁶ EDÖB 2018b, 8; KELLEHER/MURRAY, N 6.22.

²⁰¹⁷ Vgl. HÄRTING, N 279, und THOMAS, 147.

²⁰¹⁸ WEBER 2018, 104–105.

²⁰¹⁹ Zusätzlich interne Prozessüberprüfungen, Mechanismen zur individuellen Teilhabe und externe Rechtsdurchsetzung: THOMAS, 140–141.

²⁰²⁰ Siehe S. 268–273. Forderung nach einer Beweislastumkehr im schweizerischen Rechtsraum: MEIER REGINA, N 19.

²⁰²¹ Die EGMR-Rechtsprechung hat im Fall I gegen Finnland festgehalten, dass die Arbeitgeberin die Einhaltung der Datensicherheit beweisen müsse: TAMÒ-LARRIEUX, 171. Vgl. Urteil EGMR vom 17.07.2008, I vs. Finland, Nr. 20511/03, N 44–46. Siehe FN 1903.

²⁰²² Vgl. S. 315.

bb) Lösungen gegen algorithmische Diskriminierungen

Zur Professionalisierung gehört auch, dass sich die Arbeitgeberin der beschriebenen komplexen diskriminierungsrechtlichen Probleme annimmt.²⁰²³ Vorab ist klarzustellen, dass es keine taugliche Lösung ist, einfach alle diskriminierungssensiblen Variablen (z.B. Geschlecht, Alter, Religion) zu löschen. Denn durch das Weglassen dieser Einzelheiten kann es zu einer ungerechtfertigten Gleichbehandlung von Ungleichem kommen. So kann es beispielsweise für die gerechte Beurteilung der Arbeitsleistung angezeigt sein, das Lebensalter zu berücksichtigen und zwischen Jung und Alt zu unterscheiden.²⁰²⁴ Zudem wird der Datensatz selbst bei einer Löschung der Daten über die verpönten Merkmale noch Informationen enthalten, die mit den geschützten Attributen korrelieren, wodurch die Gefahr einer Proxy-Diskriminierung nicht gebannt ist.²⁰²⁵ Ein Analysesystem muss die Daten zu den diskriminierungssensiblen Persönlichkeitsmerkmalen somit erfassen und speichern, um darauf Rücksicht nehmen zu können.²⁰²⁶ Denkbar ist jedoch, dass, nachdem ein Modell unter Einbezug der diskriminierungssensiblen Daten erstellt worden ist, die Information zum geschützten Merkmal nicht mehr als Eingabe für die Entscheidungsfindung erforderlich ist.²⁰²⁷

Technische Lösungen zur Behebung von Diskriminierungsrisiken bestehen etwa in der Aufnahme bestimmter Quotierungsziele in die Algorithmenprogrammierung (z.B. bevorzugte Einstellung von Angehörigen einer Minderheit bei gleicher Qualifikation, vorausgesetzt es liegt kein atypischer Fall vor).²⁰²⁸ Auch weitere Techniken zur Abwendung von Diskriminierungen stehen bereit.²⁰²⁹

Technische Lösungen allein genügen aber nicht zur Bekämpfung von Diskriminierungen.²⁰³⁰ Ein rechtliches Mittel gegen Diskriminierungen wäre die Einfüh-

²⁰²³ Siehe S. 91–99 und 115–126.

²⁰²⁴ Eine ungerechtfertigte Gleichbehandlung könnte auch entstehen, wenn ein System Protestanten und Katholiken zu Christen oder Schiiten und Sunniten zu Muslimen aggregieren würde: VEALE/BINNS, 2.

²⁰²⁵ Siehe zur Proxy-Diskriminierung S. 95. VEALE/BINNS, 4.

²⁰²⁶ Algo:aware [sic], 19. Vgl. VEALE/BINNS, 6.

²⁰²⁷ ŽLIOBAITĖ/CUSTERS, 199. Siehe zum Konzept «Eingabe – Analysemodell – Ausgabe» bei Algorithmen S. 91.

²⁰²⁸ Bevorzugte Anstellung von Frauen: DZIDA/GROH, 1922.

²⁰²⁹ Z.B. *data repair* gegen indirekte Diskriminierungen: WILDHABER 2017, 215; *discrimination-aware data mining* (DADM) und *fairness, accountability and transparency machine learning* (FATML): VEALE/BINNS, 1.

²⁰³⁰ Vgl. bzgl. Proxy-Diskriminierungen: HURLEY/ADEBAYO, 199.

ung eines arbeitsrechtlichen Diskriminierungsverbots, das auch vor Lifestyle-Diskriminierungen schützt, welches jedoch wie erwähnt kaum politische Chancen hat.²⁰³¹ Das Recht könnte zur Minimierung von Diskriminierungsrisiken zudem rassistisch motivierte Absagen bei Bewerbungen als Straftat behandeln (vgl. Art. 261^{bis} Abs. 5 StGB), wie von PÄRLI vorgeschlagen.²⁰³² Ferner könnte der Urheberrechtsschutz für die Analytik-Industrie gelockert werden, sodass die Verzerrungen wegfallen, welche dadurch entstehen, dass ein Algorithmus urheberrechtlich geschützte Daten nicht bearbeiten darf.²⁰³³

cc) Schulungen

People Analytics bringt neue Probleme hervor, die aufgrund der verschiedenen betroffenen Rechtsgebiete, des technischen Hintergrunds und möglicherweise zwischenmenschlicher Reibungen äusserst komplex sein können. Zu fordern ist daher, dass alle Angestellten, die Daten auf risikoreiche Art bearbeiten, insbesondere die Führungskräfte, Schulungen durchlaufen.²⁰³⁴ Nur wenn die mit den Daten umgehenden Menschen das nötige Wissen mitbringen, kann ein Unternehmen das Datenschutzrecht im Sinne der Professionalisierung schon ab Beginn der Bearbeitungstätigkeiten einhalten. Es bräuchte entweder eine gesetzliche Pflicht zur Schulung oder aber genügend Anreize, damit Schulungen freiwillig besucht werden.

Ein wesentliches Ziel einer Schulung sollte darin bestehen, dass die Verantwortlichen die Hoheit über die Technik behalten, sodass ein Algorithmus Personalentscheide nicht über Gebühr beeinflusst. Zu einem sorgfältigen Umgang mit Algorithmen gehört es, dass die Selektionskriterien wie in einem Polizeiverhör möglichst eng gehalten werden; man kann einen Algorithmus nicht wie einen fachkundigen Unternehmensberater einfach befragen: «Was sollen wir in unserer Organisation besser machen?»²⁰³⁵ Die Arbeitgeberin wird nützliche Resultate nur erhalten, wenn sie spezifische Fragen stellt, die sich in eine Programmiersprache übersetzen lassen.²⁰³⁶

²⁰³¹ Siehe S. 117–118 und FN 684.

²⁰³² Es handle sich bei einer Stellenausschreibung (nicht aber bei Spontanbewerbungen) um eine tatbestandsmässige «Leistung»: PÄRLI 2009, N 1592. Vgl. aber FN 657.

²⁰³³ LEVENDOWSKI, 579 und 630.

²⁰³⁴ AKHTAR/MOORE, 123.

²⁰³⁵ Vgl. die Beispiele zur Selektionsbefugnis und -pflicht bei DRUEY 1995, 119.

²⁰³⁶ GAY/KAGAN.

Schulungs-, Seminar- und Weiterbildungsangebote finden sich zuhauf im Internet. Besonders praxisorientierte (Fach-)Hochschulen sind in diesem Bereich aktiv. Beispielhaft sei es gestattet, an die Tagung «Big Data am Arbeitsplatz – Arbeits- und datenschutzrechtliche Fragen rund um Workforce Analytics» vom 16.10.2018 in Zürich zu erinnern, die der Autor zusammen mit seiner Doktormutter organisieren und durchführen durfte. Die Tagung zog Personen an, die die Weiterbildung zum Fachanwalt Arbeitsrecht absolvierten, sowie Datenschutz- und Compliance-Verantwortliche, Unternehmensjuristen, die mit Personalfragen konfrontiert sind, und HR-Verantwortliche.

7.3.3 Demokratisierungsvorschläge

a) Befähigung der einzelnen Arbeitnehmer

aa) Technologische «Werkzeuge»

Nach der Diskussion der Professionalisierungsmassnahmen ist nun zu prüfen, welche Kontrollrechte die der Arbeitgeberin entgegengesetzte Seite benötigt, um effektiv auf die Einhaltung des Datenschutzrechts bei People Analytics hinzuwirken. Auf der Ebene der einzelnen betroffenen Arbeitnehmer ist hier ganz praktisch zu beginnen: Gemäss Apple-CEO Tim Cook genügen Gesetze allein nicht, damit die Individuen von ihrer Privatsphäre im digitalen Zeitalter Gebrauch machen können: *«We also need to give people tools that they can use to take action.»*²⁰³⁷ Jeder braucht einfache (nicht rechtliche, sondern technologische) «Werkzeuge», um die eigenen Datenbearbeitungspräferenzen ohne Zeitverlust zu kommunizieren und durchzusetzen. Die beschriebenen, simplen Menüs zur Steuerung der Cookies sind ein erster Ansatz hierfür.²⁰³⁸ Einen Schritt weiter gehen Lösungen, bei denen der Benutzer durch einmaliges Setzen genereller Einstellungen steuern kann, von wem er wie «getrackt» werden darf. Beispielsweise können solche Einstellungen im

²⁰³⁷ COOK TIM, You deserve privacy online. Here's how you could actually get it, abrufbar unter <<https://time.com>> (besucht am 31.05.2020).

²⁰³⁸ Siehe S. 226. Zumindest der Autor der vorliegenden Arbeit nutzt einfach handhabbare Mittel, um die Cookies zu blockieren. A.M. ROSENTHAL 2012, 86–87: Die meisten Internetbenutzer würden ohne nähere Gedanken das Setzen von Cookies erlauben. Es habe sich eine «Wegklick-Mentalität» entwickelt: ROSENTHAL DAVID, Cookies: comment la CJUE lutte-t-elle contre la mentalité du «cliquer et fermer sans regarder», abrufbar unter <www.lawinside.ch> (besucht am 31.05.2020).

Browser²⁰³⁹ oder über eine dafür spezialisierte Plattform vorgenommen werden.²⁰⁴⁰ Die Entwicklung weiterer solcher Werkzeuge sollte durch die Technologieunternehmen vorangetrieben und durch den Staat mittels geeigneter Rahmenbedingungen gefördert werden.

bb) Rechtliche Verbesserungen für Individuen

Die rechtliche Stellung der Individuen soll gemäss rev-DSG verbessert werden. Mit der Umsetzung des rev-DSG ist eine Änderung der ZPO verbunden, um die zivilrechtlich klagende Partei bei Streitigkeiten nach dem DSG von der Leistung einer Sicherheit für die Parteientschädigung und von den Gerichtskosten zu befreien.²⁰⁴¹ Ferner wäre es eine Überlegung wert, ob für Auskunftsbeghen (Art. 8 DSG, Art. 23 E-DSG, Art. 25 rev-DSG) das summarische Verfahren (Art. 248 ZPO) an die Stelle des derzeit vorgesehenen vereinfachten Verfahrens (Art. 243 Abs. 2 lit. d ZPO) treten könnte, weil es einen einfacheren und schnelleren Rechtsschutz bietet.²⁰⁴² Wenn man der hier vertretenen Auffassung folgt, dass die Arbeitgeberin jederzeit nachweisen können muss, dass sie das Datenschutzrecht einhält,²⁰⁴³ müssten in der Regel auch die Beweismittel liquide sein, sodass ein summarisches Verfahren möglich wird. Insgesamt aber gelten für die vorliegend interessierenden Streitigkeiten im Schnittbereich zwischen Datenschutz- und Arbeitsrecht bereits bislang erleichterte Bedingungen,²⁰⁴⁴ und trotzdem kommt es selten zu Individualklagen. Deshalb dürfte den genannten rechtlichen Verbesserungsvorschlägen ein geringes Potenzial innewohnen.

²⁰³⁹ ROSENTHAL DAVID, Cookies: comment la CJUE lutte-t-elle contre la mentalité du «cliquer et fermer sans regarder», abrufbar unter <www.lawinside.ch> (besucht am 31.05.2020).

²⁰⁴⁰ Eine solche Plattformlösung bietet etwa das schweizerische Unternehmen One.Thing.Less AG [sic] an. Der Autor dankt Herrn Dr. iur. Lukas Morscher, Rechtsanwalt, für den wertvollen Hinweis.

²⁰⁴¹ Siehe Art. 99 Abs. 3 lit. d, Art. 113 Abs. 2 lit. g und Art. 114 lit. f ZPO in: BBl 2017, 7247.

²⁰⁴² GNEHM, 103. A.M. BOLLIGER *et al.*, 218: Das Auskunftsrecht nach Art. 8 DSG habe sich insgesamt bewährt, so dass es sich nicht aufdränge, die diesbezüglichen Rechtsgrundlagen zu modifizieren.

²⁰⁴³ Siehe S. 341.

²⁰⁴⁴ Z.B. Befreiung von den Prozesskosten, siehe S. 273.

b) Stärkung der Arbeitnehmervertretungen und -verbände

aa) Stärkung der Mitwirkung

Unter der Berücksichtigung, dass die Arbeitnehmer die wesentlichen Datenlieferanten von People Analytics sind,²⁰⁴⁵ ist im Rahmen der hier vorgeschlagenen Demokratisierung eine Stärkung der Rechte der Arbeitnehmervertretungen und -verbände naheliegend. Dies wird auch im nationalrätlichen Postulat «Mitbestimmung und Mitarbeitendenrechte bei der Digitalisierung der Arbeitswelt» vorgeschlagen.²⁰⁴⁶

Zunächst könnte die institutionelle Stellung der Arbeitnehmervertretungen und -verbände verbessert werden. Erinnert sei an die möglichen Schwierigkeiten bei der Konstitution der Arbeitnehmervertretung.²⁰⁴⁷ Eine obligatorische Arbeitnehmervertretung für Betriebe ab hundert Angestellten könnte dieses Problem abdämpfen.²⁰⁴⁸ In grösseren Betrieben könnte die Zusammenarbeit zwischen der Arbeitgeberin und der Belegschaft institutionalisiert werden in Form einer aus Mitgliedern der Arbeitnehmervertretung und der Unternehmensleitung paritätisch zusammengesetzten Kommission für Arbeitssicherheit und Gesundheitsschutz.²⁰⁴⁹ Zudem gäbe es die Option, dem Personal eine angemessene Vertretung im Verwaltungsrat zu gewähren. Bei der Schweizerischen Post haben zwei Gewerkschaften, die auch GAV-Parteien der Post sind, je einen Sitz im Verwaltungsrat (vgl. Art. 8 Abs. 3 POG).²⁰⁵⁰

Sodann ist eine Verbesserung der eigentlichen Mitwirkung möglich. Es könnte ein Anspruch festgehalten werden, dass die Arbeitgeberin nur im Beisein eines Ar-

²⁰⁴⁵ Vgl. S. 42–59.

²⁰⁴⁶ GYSI BARBARA, Postulat 20.3569: Mitbestimmung und Mitarbeitendenrechte bei der Digitalisierung der Arbeitswelt, 10.06.2020, abrufbar unter <www.parlament.ch> (besucht am 20.10.2020). Der Bundesrat beantragt in seiner Stellungnahme vom 26.08.2020 die Ablehnung des Postulats mit der Begründung, dass entsprechende Regelungen nicht im MitwG festgeschrieben werden sollten, sondern in Gesamtarbeitsverträgen. Das Postulat steht zum Zeitpunkt der Publikation dieser Dissertation im Nationalrat zur Behandlung an.

²⁰⁴⁷ Siehe S. 287.

²⁰⁴⁸ FURER 2009a, 156. Nur knapp die Hälfte (49 Prozent) aller Gesamtarbeitsverträge sah im Jahr 1990 eine Pflicht zur Schaffung von Arbeitnehmervertretungen vor: MÜLLER, 336.

²⁰⁴⁹ MÜLLER, 262.

²⁰⁵⁰ MUGGLIN, 122.

beitehmervertreter auf die Überwachungsdaten zugreift.²⁰⁵¹ Des Weiteren kann die wirksame Vertretung der Interessen aufgrund der komplexen Sachverhalte von People Analytics erhöhte Fachkenntnis voraussetzen, die die Arbeitnehmervertretung nicht immer hat. Deshalb ist ein Recht der Arbeitnehmervertretung auf Beizug eines internen oder externen Sachverständigen, wie dies das deutsche Recht vorsieht, prüfenswert.²⁰⁵² Sind diese beiden Vorschläge umgesetzt, ist zu reflektieren, ob die Einführung eines Mitentscheidungsrechts sachgerecht wäre.²⁰⁵³

Schliesslich ist zu überlegen, ob ein Verstoss gegen die Mitwirkungsrechte sanktioniert werden sollte. Als Sanktionen könnten verwaltungsstrafrechtliche Bussen gesetzlich vorgesehen werden. Dies würde einen rechtssystematischen Wandel weg von einem privatrechtlich, hin zu einem öffentlich-rechtlich konzipierten MitwG bedeuten.²⁰⁵⁴

Es handelt sich bei der Stärkung der Mitwirkungsrechte der Arbeitnehmervertretungen und -verbände um eine Demokratisierungsmassnahme, da eine der Arbeitgeberin entgegengesetzte Partei Kontrollinstrumente erhält, um indirekt via Mitwirkungsrecht auf die Einhaltung des Datenschutzrechts hinzuwirken. Das Mitwirkungsrecht erscheint besonders vielversprechend, weil es den Arbeitnehmern ermöglicht, schon in der Planungsphase eines People Analytics-Projekts, d.h. *ex ante*, das Datenschutzrecht durchzusetzen.

bb) Finanzielle Mitarbeiterbeteiligung

People Analytics kann die Betriebseffizienz und den Unternehmensgewinn steigern. Dies kann bei den Mitarbeitern die Begehrlichkeit nach einem Anteil am gesteigerten Gewinn wecken, da sie neu neben Arbeit auch ihre Daten beitragen. Ein Interesse an einer solchen Bezahlung könnten insbesondere schlecht bezahlte Arbeitnehmer haben. In einem kreativen Gedankenspiel setzen sich POSNER und WEYL dafür ein, das Gewähren der Datenerhebung als Arbeit zu entschädigen

²⁰⁵¹ Vgl., jedoch ohne spezifischen Bezug zur Schweiz: AKHTAR/MOORE, 122.

²⁰⁵² Beratung des Betriebsrats durch einen sachkundigen Arbeitnehmer als Auskunftsperson (§ 80 Abs. 2 Satz 3 BetrVG) oder durch einen externen Sachverständigen nach näherer Vereinbarung mit dem Arbeitgeber (§ 80 Abs. 3 BetrVG): WEDDE 2016c, 13; BMAS 2017, 159.

²⁰⁵³ Siehe S. 105.

²⁰⁵⁴ DERRER BALLADORE, 191–192.

(*data as labor*).²⁰⁵⁵ Erfolgsabhängige Mitarbeiterbeteiligungen, beispielsweise ein Anteil am Geschäftsergebnis (Art. 322a OR), eine Provision (Art. 322b–c OR) oder eine Gratifikation (Art. 322d OR), sind dem schweizerischen Arbeitsrecht bereits vertraut. Sie werden vor allem mit leitenden Arbeitnehmenden vereinbart, welche aufgrund ihrer Position in der Gesellschaft einen unmittelbaren Einfluss auf das Geschäftsergebnis ausüben können und damit ein eigenes Interesse am Erfolg haben.²⁰⁵⁶ Die Idee einer Entlohnung ist jedoch aus den gleichen Gründen zu verwerfen, aus denen auch Eigentums- und andere Herrschaftsrechte an Daten abzulehnen sind.²⁰⁵⁷ Ein kalifornisches Gericht hat eine Klage abgewiesen, in der eine Nutzerin von Google eine Entschädigung mit der Begründung forderte, der Identifizierungsdienst reCAPTCHA zwingt sie zu unbezahlter Arbeit.²⁰⁵⁸ Das Bedürfnis nach einer finanziellen Abgeltung relativiert sich insofern weiter, als der Bundesrat ohnehin mit steigenden Einkommen infolge höherer Arbeitsproduktivität als Folge der Digitalisierung rechnet.²⁰⁵⁹ Eine Entschädigung überlässt den Mitarbeitern zudem eine passive Rolle; zum Schutz der Persönlichkeit ist es für die Arbeitnehmer nach hier vertretener Einschätzung wertvoller, sich aktiv an der Datenbearbeitungspolitik des Unternehmens beteiligen zu können. Eine finanzielle Mitarbeiterbeteiligung kann somit kaum auf das hier verfolgte Ziel der Demokratisierung, d.h. der wirksamen Durchsetzung des Datenschutzrechts durch die der Arbeitgeberin entgegengesetzten Parteien, hinwirken.

c) **Stärkung des Staats**

aa) **Stärkung der Datenschutzaufsicht**

Damit der EDÖB im Sinne der Demokratisierung auf die Einhaltung des Datenschutzrechts hinwirken kann, müssen seine gegenwärtig beschränkten Möglich-

²⁰⁵⁵ «Datenarbeit» (*«data labour»*) würde somit zu einer zusätzlichen Einkommensquelle werden: POSNER/WEYL, 246. Die Autoren rechnen mit einem Zusatzeinkommen von USD 20'000 pro vierköpfigem Haushalt: POSNER/WEYL, 247.

²⁰⁵⁶ KASPER, N 39.

²⁰⁵⁷ Siehe S. 265–266.

²⁰⁵⁸ Urteil Rojas-Lozano vs. Google, Inc., Case No. 15-cv-03751-JSC, United States District Court, N.D. California, 03.02.2016, zu finden bei: Leagle, Rojas-Lozano vs. Google, Inc., abrufbar unter <www.leagle.com> (besucht am 31.05.2020), m.w.H.; Urteil Rojas-Lozano vs. Google, Inc., Case No. 15-10160-MGM, United States District Court, District of Massachusetts, 12.08.2015, zu finden bei: Casetext, Rojas-Lozano vs. Google, Inc., abrufbar unter <<https://casetext.com>> (besucht am 31.05.2020), m.w.H.; POSNER/WEYL, 235–236, m.w.H.

²⁰⁵⁹ Schweizerischer Bundesrat 2017b, 105.

keiten²⁰⁶⁰ verbessert werden. Der Rat der EU hat im Jahr 2018 die Anwendung des Schengen-Besitzstands in der Schweiz im Bereich des Datenschutzes evaluiert und Defizite festgestellt. Er empfahl darum der Schweiz, die Datenschützer mit mehr Personal und Kompetenzen zu versehen.²⁰⁶¹ Auch in der Schweiz ist verschiedentlich der Ruf nach einer besseren personellen und finanziellen Ausstattung des EDÖB und der kantonalen Datenschutz- und Öffentlichkeitsbeauftragten zu vernehmen.²⁰⁶² Der Bereich «Arbeit» verursacht gegenwärtig rund vier Prozent des Aufwands des EDÖB.²⁰⁶³ Angesichts der steigenden Verbreitung von People Analytics könnte dieser Anteil künftig zunehmen.²⁰⁶⁴ Das Problem akzentuiert sich angesichts der Tatsache, dass die meisten EU- und EWR-Mitgliedstaaten die Mittel ihrer jeweiligen Datenschutz-Aufsichtsbehörden zwischen 2018 und 2019 angesichts des Inkrafttretens der DSGVO erhöht haben.²⁰⁶⁵ Eine starke finanzielle Basis ist aber erforderlich, weil der EDÖB sowohl von den Privaten als auch vom Staat unabhängig sein muss.²⁰⁶⁶

Nach der vorgesehenen Totalrevision des DSG werden die Kompetenzen des EDÖB gestärkt. Zwar entspricht die Kompetenz zur Führung von Untersuchungen (Art. 43 E-DSG, Art. 49 rev-DSG) noch weitgehend dem bisherigen Recht (vgl. Art. 29 DSG). Doch wenn das Bundesorgan oder die private Person den Mitwirkungspflichten nicht nachkommt, kann der EDÖB im Rahmen der Untersuchung Anordnungen treffen, die über das bisher Mögliche (vgl. Art. 29 Abs. 2 DSG) hinausgehen, nämlich insbesondere: Verschaffung des Zugangs zu allen Auskünften, Unterlagen, Verzeichnissen der Bearbeitungstätigkeiten und Personendaten, die für die Untersuchung erforderlich sind; Verschaffung des Zugangs zu den Räumlichkeiten und Anlagen; Zeugeneinvernahmen; sowie Begutachtungen durch Sachverständige (Art. 44 Abs. 1 lit. a–d E-DSG, Art. 50 Abs. 1 lit. a–d rev-DSG).

²⁰⁶⁰ Siehe S. 275–278.

²⁰⁶¹ Rat der Europäischen Union, 4.

²⁰⁶² RUDIN 2002, 396; BOLLIGER *et al.*, 222; Aussage von Dr. iur. Reto Fanger, Rechtsanwalt und Datenschutzbeauftragter des Kantons Luzern von 2011 bis 2018, im Bericht von KUNZ YASMIN, Neuer Luzerner Datenschützer steht vor einer happigen Aufgabe, Luzerner Zeitung vom 14.11.2018, abrufbar unter <www.luzernerzeitung.ch> (besucht am 31.05.2020); ZINKE, 170.

²⁰⁶³ EDÖB 2018a, 56.

²⁰⁶⁴ Siehe zur steigenden Verbreitung von People Analytics S. 66–69.

²⁰⁶⁵ Vgl. EDSA 2019, 7. Aufwertung des Europäischen Datenschutzbeauftragten: DE HERT/PAPAKONSTANTINOU, 250.

²⁰⁶⁶ Vgl. zu den europäischen Aufsichtsbehörden EDWARDS/VEALE, 75.

Der EDÖB kann für die Dauer der Untersuchung zudem vorsorgliche Massnahmen anordnen und sie durch eine Bundesbehörde oder die kantonalen oder kommunalen Polizeiorgane vollstrecken lassen (Art. 44 Abs. 2 E-DSG, Art. 50 Abs. 3 rev-DSG).

Liegt eine Verletzung von Datenschutzvorschriften vor, so kann der EDÖB verfügen, dass die Bearbeitung ganz oder teilweise angepasst, unterbrochen oder abgebrochen wird und die Personendaten ganz oder teilweise gelöscht oder vernichtet werden (Art. 45 Abs. 1 E-DSG, Art. 51 Abs. 1 rev-DSG). Eine nicht abschliessende («namentliche») Aufzählung von möglichen Anordnungen findet sich in Art. 45 Abs. 3 E-DSG bzw. Art. 51 Abs. 3 rev-DSG. Mit der Kompetenz, Verfügungen zu erlassen (Art. 46 Abs. 1 E-DSG bzw. Art. 52 Abs. 1 rev-DSG i.V.m. Art. 5 VwVG), ist der EDÖB nicht mehr auf ein Gericht angewiesen, das an seiner Stelle entscheidet, dass einer Empfehlung des EDÖB Folge geleistet werden muss (vgl. Art. 29 Abs. 4 DSG).²⁰⁶⁷

Hat das Bundesorgan oder die private Person während der Untersuchung die erforderlichen Massnahmen getroffen, um die Einhaltung der Datenschutzvorschriften wiederherzustellen, so kann der EDÖB sich darauf beschränken, eine Verwarnung auszusprechen (Art. 45 Abs. 4 E-DSG, Art. 51 Abs. 5 rev-DSG).

Die Position des EDÖB wird auch dadurch gestärkt, dass er zwingend konsultiert werden muss, wenn sich aus einer Datenschutz-Folgenabschätzung ergibt, dass die geplante Bearbeitung ein hohes Risiko birgt (Art. 21 Abs. 1 E-DSG, Art. 23 Abs. 1 rev-DSG) und kein Datenschutzberater konsultiert wird (Art. 21 Abs. 4 E-DSG, Art. 23 Abs. 4 rev-DSG).

bb) Stärkung der Strafbehörden

Die Tatbestände der Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten (Art. 54 E-DSG, Art. 60 rev-DSG) sowie der beruflichen Schweigepflicht (Art. 56 E-DSG, Art. 62 rev-DSG) sind bereits bisher unter Strafe gestellt. Neu werden auch die Verletzung der Sorgfaltspflicht (Art. 55 E-DSG, Art. 61 rev-DSG), das Missachten von Verfügungen (Art. 57 E-DSG, Art. 63 rev-DSG) und Widerhandlungen in Geschäftsbetrieben (Art. 58 E-DSG, Art. 64 rev-DSG) strafbar sein.

²⁰⁶⁷ Vgl. bzgl. vorsorglicher Massnahmen: BBl 2017, 7092.

Der Strafraum wird um das 25-Fache erweitert. Die maximale Busse beträgt neu CHF 250'000 (Art. 54–57 E-DSG, Art. 60–63 rev-DSG).²⁰⁶⁸

Zuständig für die Verfolgung und Beurteilung strafbarer Handlungen in der Schweiz sind die kantonalen Strafverfolgungsbehörden (Art. 59 Abs. 1 E-DSG, Art. 65 Abs. 1 rev-DSG). Der EDÖB kann (lediglich) Strafanzeige erstatten und im Verfahren die Rechte einer Privatkülerschaft wahrnehmen (Art. 59 Abs. 2 E-DSG, Art. 65 Abs. 2 rev-DSG). Diese Kompetenzaufteilung widerspricht zwar der Grundregel der DSGVO, wonach für die Verhängung von Geldbussen die jeweiligen Aufsichtsbehörden der EU-Mitgliedstaaten zuständig sind (Art. 83 Abs. 1 i.V.m. Art. 4 Nr. 21 DSGVO). Jedoch ist eine Umsetzung der DSGVO dahingehend möglich, dass die Geldbusse von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird (Art. 83 Abs. 9 Satz 1 DSGVO). Damit ist die schweizerische Kompetenzzuweisung DSGVO-konform.

Insgesamt können die Strafbehörden vor allem *ex post* auf die Einhaltung des DSG hinwirken, da ein Strafverfahren erst eröffnet wird, wenn es bereits zur Datenschutzverletzung gekommen ist. Die höheren, abschreckenden Bussen dürften zudem eine gewisse präventive Wirkung zeigen. Nach der Meinung des Autors muss sich der Vorteil der schweizerischen Zerteilung der Kompetenzen zwischen dem EDÖB und den Strafbehörden aber erst noch beweisen. Da die Sachverhalte und die rechtliche Beurteilung bei Datenschutzverletzungen oft komplex sind, erscheint es aufwendig, mit dem EDÖB in Bern und den jeweiligen Strafbehörden in den Kantonen zahlreiche Kompetenzzentren parallel zu betreiben. Im Kartellrecht, das sich ebenfalls durch vielschichtige Sachverhalte auszeichnet, verfügt die Wettbewerbskommission über die Kompetenz zur Verhängung von Verwaltungsbusen (Art. 18 Abs. 3 Satz 1 i.V.m. Art. 49a ff. KG). Eine solche Konzentration der Aufsichtstätigkeit wäre auch für das Datenschutzrecht prüfenswert.

cc) Staat als Diskursmoderator

Angesichts der tiefgreifenden Neuerungen, die People Analytics ins Arbeitsleben bringen wird, ist eine Aufklärung der Gesellschaft erforderlich.²⁰⁶⁹ Besonders wertvoll wäre die Entwicklung einer rechtsstaatlich begleiteten Dialogkultur zwi-

²⁰⁶⁸ Siehe zum gegenwärtigen Strafraum S. 281–282.

²⁰⁶⁹ Vgl. ZWEIG/KRAFFT, 115.

schen den Verantwortlichen, Betroffenen und übrigen Anspruchsgruppen bzw. Stakeholdern, einschliesslich der breiten Öffentlichkeit.²⁰⁷⁰

Einen lebhaften Austausch zwischen Experten fördert die US-amerikanische Behörde FTC: Sie engagiert sich nicht nur in der Rechtsdurchsetzung, sondern schart um sich herum mittels Workshops ein soziales Netzwerk, in dem hochrangige privatwirtschaftliche Datenschutzberater verkehren. Dadurch gelingt es der FTC, sowohl die Schwächen einer rein staatlichen *Top-down*-Regulierung als auch einer reinen *Bottom-up*-Selbstregulierung auszumerzen.²⁰⁷¹ Das Zusammenspiel der Interessenvertreter ist auch für die Formulierung neuer Datenschutzregeln wichtig, weil in der Analytik nichtstaatliche Hersteller und Anwender sowie die Wissenschaft oft einen Informationsvorsprung vor der Politik und der Aufsicht haben.²⁰⁷² Die vielseitige Tätigkeit der FTC kann als Inspiration dienen, um die Rolle des EDÖB zu überdenken. Es ist allerdings festzuhalten, dass die FTC keine eigentliche Datenschutz-Aufsichtsbehörde, sondern die Wettbewerbs- und Verbraucherschutzbehörde der USA ist. Insofern kann das «Modell FTC» nicht telquel auf die Schweiz übertragen werden.

Vorab sind die drei Hauptaufgaben des EDÖB zu vergegenwärtigen: Aufsicht (Art. 27 und Art. 29 DSG, Art. 43–47 E-DSG, Art. 49–53 rev-DSG), Beratung (Art. 28 DSG, Art. 52 Abs. 1 lit. a und g E-DSG, Art. 58 Abs. 1 lit. a und g rev-DSG) und Information respektive Sensibilisierung (Art. 30 DSG; Art. 51 und Art. 52 Abs. 1 lit. c–d E-DSG; Art. 57 und Art. 58 Abs. 1 lit. c–d rev-DSG).²⁰⁷³ Würde nun der EDÖB als staatlicher Diskursmoderator auftreten, so müsste er verstärkt in den beiden Aufgabenbereichen der Beratung und Information aktiv werden. Bereits heute stehen die Beratung bzw. die fachliche Unterstützung bei der Umsetzung der gesetzlichen Vorschriften im vorliegend gegenständlichen privatrechtlichen Umfeld im Vordergrund.²⁰⁷⁴ Die beratende Funktion des EDÖB verträgt sich aber nicht gut mit seinen Aufsichtskompetenzen, die nach der Totalrevision des

²⁰⁷⁰ GLASS, 110; «*stakeholder participation and social dialogue*»: Europäische Kommission 2019b, 23; «*multi-stakeholders' discussion*»: POULLET 2010, 30; «*social conversation*»: RICHARDS/KING, 432.

²⁰⁷¹ BAMBERGER/MULLIGAN 2011, 313.

²⁰⁷² GUIHOT *et al.*, 417. Am meisten investieren private Unternehmen, wie z.B. Google, Facebook, Microsoft, Apple und Amazon: GUIHOT *et al.*, 420. Vgl. Datenschutzkonferenz, 5.

²⁰⁷³ BOLLIGER *et al.*, III.

²⁰⁷⁴ RUDIN 2002, 381; BOLLIGER *et al.*, V.

DSG zunehmen werden.²⁰⁷⁵ Es wird gegargwöhnt, dass der EDÖB wegen dieser Doppelrolle als Ratgeber gemieden werden könnte.²⁰⁷⁶

Der (potenzielle) Interessenkonflikt des EDÖB veranlasst dazu, über eine verstärkte organisatorische Trennung der Aufsichtsfunktion einerseits sowie der Beratungs- und Informationstätigkeit andererseits nachzudenken.²⁰⁷⁷ RUDIN schlägt vor, eine zentrale Behörde für die Kontrolle und Überwachung zu behalten, während regionale Kompetenzzentren, die vorgeschrieben oder durch ein Anreizsystem gefördert werden, die Beratungsfunktion übernehmen sollten.²⁰⁷⁸ Statt regionaler könnten auch branchenspezifische Kompetenzzentren geschaffen werden. Jedenfalls hätte die Dezentralisierung im Beratungsbereich das Potenzial, mehr Personen näher und gezielter anzusprechen und somit zu einer Demokratisierung beizutragen.

d) Einbezug der Zivilgesellschaft

aa) Ideelle Verbandsklage

i. Übersicht

Vereinigungen der Zivilgesellschaft könnten sich mittels ideeller Verbandsklage an der demokratischen Durchsetzung des Datenschutzrechts beteiligen. Vorliegend ist zunächst zu prüfen, ob es sinnvoll wäre, im DSG eine spezialgesetzliche Grundlage für die ideelle Verbandsklage zu schaffen (dazu sogleich). Sodann ist auf die Möglichkeiten der allgemeinen zivilprozessualen Verbandsklage einzugehen (dazu anschliessend, S. 359–361).

ii. Datenschutzrechtliche Verbandsklage

Die Einführung einer Verbandsklage im privatrechtlichen Datenschutzrecht ist in der Lehre mehrfach erwogen worden.²⁰⁷⁹ Auch der Gesetzgeber hat bei der Erschaffung des DSG ein Verbandsklagerecht diskutiert; dies als Kompensationsmassnahme, nachdem er zuvor die Funktion des EDÖB im privatrechtlichen Bereich «auf jene eines reinen Ombudsmanns gestützt» hatte und dieser daher

²⁰⁷⁵ Siehe zur Stärkung der Datenschutzaufsicht S. 348–350.

²⁰⁷⁶ BOLLIGER *et al.*, IV und 223.

²⁰⁷⁷ RUDIN 2002, 414; BOLLIGER *et al.*, 223.

²⁰⁷⁸ RUDIN 2002, 417, lehnt sich dabei an die Umweltschutzgesetzgebung, die ein Bundesgesetz und eine dezentrale Aufsichtsorganisation kennt.

²⁰⁷⁹ SIEGENTHALER, 113; BOLLIGER *et al.*, 219. Vgl. zum deutschen Recht: HERMSTRÜWER, 113.

«nichts mehr zu sagen» hatte.²⁰⁸⁰ Die Idee der Verbandsklage war im Parlament jedoch umstritten und wurde relativ knapp abgelehnt.²⁰⁸¹ In der Vorbereitung zur Totalrevision des DSG hat der Bundesrat im Jahr 2017 erneut festgehalten, dass ein Verbandsklagerecht im DSG «nicht opportun» sei.²⁰⁸²

Nach der hier vertretenen Ansicht sprechen indes wichtige Gründe für die Einführung eines Verbandsklagerechts im DSG. Verbandsklagerechte sind für Querschnittsthemen, die zahlreiche Personen betreffen, geeignet.²⁰⁸³ Dies trifft auf das Datenschutzrecht zu, denn die Digitalisierung geht jedermann an.²⁰⁸⁴ Zudem bezwecken Verbandsklagerechte die Prävention in Bereichen, in denen Streuschäden vorkommen.²⁰⁸⁵ Das Datenschutzrecht ist ein solcher Bereich: Denn einerseits ist der Schaden aus Datenschutzverletzungen oft über eine Vielzahl von nur minimal betroffenen Personen verstreut.²⁰⁸⁶ Andererseits ist der Vorsorgegedanke im DSG präsent, was sich darin äussert, dass die Datenbearbeitungsregeln unabhängig davon gelten, ob es zu einer eigentlichen Persönlichkeitsverletzung kommt.²⁰⁸⁷ Schliesslich ist das Datenschutzrecht ein äusserst abstraktes Gebiet: Das DSG ist im Vergleich zur europäischen Datenschutz-Gesetzgebung sehr dicht gehalten und beschränkt sich auf die Formulierung von Grundsätzen.²⁰⁸⁸ Deshalb bedarf es der

²⁰⁸⁰ AB SR 1990, 127; AB SR 1990, 147. Der Entwurf des Bundesrats hatte ein Verfügungsrecht des EDÖB vorgesehen, was der Ständerat gestrichen hat: AB SR 1990, 146.

²⁰⁸¹ Ein Verbandsklagerecht war im Vorentwurf zum DSG noch vorgesehen, wurde später aber verworfen: BBl 1988 II, 465. Ablehnung mit 19 zu 15 Stimmen im Ständerat: AB SR 1990, 148; Ablehnung mit 58 zu 44 Stimmen im Nationalrat: AB NR 1991, 968.

²⁰⁸² BBl 2017, 6984.

²⁰⁸³ MEIER REGINA, N 14. Querschnittsaufgaben und Verbandsbeschwerderechte bestehen insbesondere bei der Durchsetzung von umwelt- und sozialpolitischen Interessen: HÄNER, N 1063.

²⁰⁸⁴ MEIER REGINA, N 15.

²⁰⁸⁵ Ebenso wird mit der Verbandsklage die Justizgewährleistung gefördert, da die individuelle Geltendmachung eines Streuschadens unrealistisch wäre: KUKO ZPO-WEBER, Art. 89 ZPO, N 5a, BSK ZPO-KLAUS, Art. 89 ZPO, N 7.

²⁰⁸⁶ Siehe S. 271.

²⁰⁸⁷ Die Idee der Prophylaxe wird künftig zusätzliches Gewicht erhalten. Dies zeigen die neuen Pflichten, die mit der Totalrevision des DSG eingeführt werden, wie z.B. die Pflicht zum Datenschutz durch Technik bereits ab der Planung (Art. 6 Abs. 1 E-DSG, Art. 7 Abs. 1 rev-DSG), die Pflicht zu datenschutzfreundlichen Voreinstellungen (Art. 6 Abs. 3 E-DSG, Art. 7 Abs. 3 rev-DSG) und die Pflicht zur vorgängigen Erstellung einer Datenschutz-Folgenabschätzung (Art. 20 E-DSG, Art. 22 rev-DSG).

²⁰⁸⁸ Das DSG umfasst 24 Seiten. Zum Vergleich: Die DSGVO umfasst 88 wesentlich dichter beschriebene Seiten. Zusätzlich zur DSGVO kommt die jeweilige nationale Um-

gerichtlichen Auslegung, um den wahren Gesetzesgehalt auszuloten.²⁰⁸⁹ Dies gilt umso mehr, als es sich um eine vergleichsweise junge Rechtsmaterie handelt.²⁰⁹⁰ Wenn keine Verbandsklagen und nur selten Individualklagen möglich sind, kann das Datenschutzgesetz von der Praxis kaum richtig ausgearbeitet werden. Es gibt in der Schweiz «viel zu wenige» Gerichtsentscheide zum DSG.²⁰⁹¹ Insgesamt würden also die Rahmenbedingungen für die Einführung eines Verbandsklagerechts im DSG stimmen.

Im Folgenden ist daher darauf einzugehen, wie eine Verbandsklage im DSG ausgestaltet werden könnte. Vorwegzunehmen ist, dass das Bundesgericht das privatrechtliche Verbandsklagerecht ursprünglich aus dem öffentlich-rechtlichen Verbandsbeschwerderecht abgeleitet hat.²⁰⁹² Dort wird zwischen der egoistischen und der ideellen Verbandsbeschwerde unterschieden.²⁰⁹³ Bei Ersterer geht der Verband im Interesse seiner eigenen Mitglieder vor.²⁰⁹⁴ Letztere dient dagegen der Wahrung bestimmter öffentlicher Interessen der Allgemeinheit;²⁰⁹⁵ die zu schützenden Personen müssen nicht Mitglieder des Verbands sein.²⁰⁹⁶ Das durch die Rechtsprechung anerkannte privatrechtliche Verbandsklagerecht lehnt sich an die egoistische Verbandsbeschwerde an.²⁰⁹⁷ Es kann sich jedoch der ideellen Verbandsbeschwerde annähern, wenn etwa das Gesetz vom Erfordernis der Betroffenheit und selbständigen Klageberechtigung der Mitglieder absieht²⁰⁹⁸ oder wenn mit der

setzungsgesetzgebung hinzu. Diese umfasst z.B. in Österreich nochmals 331 Seiten: FORGÓ, 27–32.

²⁰⁸⁹ AB NR 1991, 967; Gerichtspraxis zum DSG wünschenswert: BACHER/DUBOIS, 144.

²⁰⁹⁰ Siehe S. 5.

²⁰⁹¹ ROSENTHAL 2012, 72.

²⁰⁹² Siehe BGE 73 II 65 E. 2–3.

²⁰⁹³ Siehe die Gegenüberstellung der ideellen und der egoistischen Verbandsbeschwerde bei: HÄNER, N 777.

²⁰⁹⁴ Vergleich zwischen der privatrechtlichen Verbandsklage und den öffentlich-rechtlichen Verbandsbeschwerden bei KUKO ZPO-WEBER, Art. 89 ZPO, N 3, und bei BSK ZPO-KLAUS, Art. 89 ZPO, N 15. Vgl. auch STEINAUER.

²⁰⁹⁵ Vergleich zwischen der privatrechtlichen Verbandsklage und den öffentlich-rechtlichen Verbandsbeschwerden bei KUKO ZPO-WEBER, Art. 89 ZPO, N 3, und bei BSK ZPO-KLAUS, Art. 89 ZPO, N 15.

²⁰⁹⁶ HÄNER, N 1053.

²⁰⁹⁷ KUKO ZPO-WEBER, Art. 89 ZPO, N 3; BSK ZPO-KLAUS, Art. 89 ZPO, N 15.

²⁰⁹⁸ HÄNER, N 777. Z.B. für die wettbewerbsrechtliche Verbandsklage (Art. 10 Abs. 2 lit. a–b UWG) ist eine selbständige Klageberechtigung der Verbandsmitglieder nicht erforderlich: BGE 121 III 168 E. 4a.

Verbandsklage nicht zwingend die Wahrung der Interessen von Mitgliedern, sondern auch ideelle Interessen verfolgt werden können.²⁰⁹⁹ Vorliegend ist eine Verbandsklage mit ideeller Zwecksetzung zu prüfen. Einerseits könnte diese auch dem grossen Teil der schweizerischen Arbeitnehmer dienen, der nicht einem (Personal-)Verband angeschlossen ist.^{2100, 2101} Andererseits würde sie zur Wahrung der erwähnten öffentlichen Interessen beitragen.²¹⁰²

Somit sind die allgemeinen rechtlichen Voraussetzungen einer ideellen Verbandsklage zu beschreiben. Die erste Voraussetzung ist eine explizite Rechtsgrundlage in einem Spezialgesetz.²¹⁰³ Ein ideelles Verbandsklagerecht existiert beispielsweise in Fragen der Mitwirkung (Art. 15 Abs. 2 MitwG), der Gleichstellung von Mann und Frau (Art. 7 GlG) sowie von Behinderten (Art. 9 BehiG), der Schwarzarbeit (Art. 15 BGSA) oder der Entsendung von Arbeitnehmern (Art. 11 EntsG). Gegen Verfügungen der Arbeitsaufsichtsbehörden steht die Verbandsbeschwerde offen (Art. 58 ArG). Doch weder das DSG noch das rev-DSG sehen ein spezialgesetzliches Verbandsklagerecht vor. Eine solche Norm müsste erst geschaffen werden. Zum Vergleich: Die DSGVO lässt den EU-Mitgliedstaaten Raum für die Einführung einer ideellen Verbandsklage (vgl. Art. 80 Abs. 2 DSGVO).²¹⁰⁴

²⁰⁹⁹ Z.B. die zivilverfahrensrechtliche Verbandsklage (Art. 89 ZPO) dient sowohl dem Schutz wirtschaftlicher als auch ideeller Interessen: BBl 2006, 7289; BSK ZPO-KLAUS, Art. 89 ZPO, N 15.

²¹⁰⁰ Siehe die Mitgliederzahlen der Gewerkschaften und anderer Arbeitnehmerorganisationen bei: SGB. Über 80 Prozent der Arbeitnehmer sind nicht gewerkschaftlich organisiert: SCHÖCHLI HANSUELI, Wer vertritt die Schweizer Arbeitnehmer?, NZZ vom 14.05.2019, abrufbar unter <www.nzz.ch> (besucht am 31.05.2020); Statista Research Department, Gewerkschaftlicher Organisationsgrad in der Schweiz bis 2018, 04.03.2020, abrufbar unter <<https://de.statista.com>> (besucht am 31.05.2020).

²¹⁰¹ Ganz allgemein sind die von Datenschutzverletzungen Betroffenen selten als Verband formiert. Wird z.B. der Kundendatensatz eines Unternehmens gestohlen, so definiert sich die Gruppe der Betroffenen über die Kundenbeziehung zu dem Unternehmen, nicht über eine Verbandszugehörigkeit. Somit wäre nach vorliegend vertretener Meinung eine ideelle Verbandsklage im DSG auch für Kontexte ausserhalb von People Analytics geeignet.

²¹⁰² Siehe S. 235–237: z.B. Meinungspluralismus, Schutz vor Manipulation und Diskriminierungsschutz.

²¹⁰³ Gegebenenfalls kann sich ein Verbandsbeschwerderecht auch aus einem qualifizierten Schweigen des Gesetzes ergeben: HÄNER, N 1031.

²¹⁰⁴ Vgl. HOFFMANN-RIEM, 63, und OTTO 2016, 117.

Zweitens bedarf die auftretende Organisation zur Führung einer ideellen Verbandsklage der juristischen Persönlichkeit. Diese Voraussetzung geht einher mit derjenigen der Parteifähigkeit.²¹⁰⁵ In der Regel klagen Vereine, aber auch Stiftungen und Genossenschaften sind zugelassen.²¹⁰⁶ Das DSG könnte somit Vereine, Stiftungen und Genossenschaften als Kläger zulassen.

Die dritte Voraussetzung einer ideellen Verbandsklage besteht darin, dass sich der Verband statutengemäss dem Rechtsbereich widmet, um den es im Verbandsklageprozess geht.²¹⁰⁷ Gemäss HÄNER mangelte es noch um die Jahrtausendwende an geeigneten Organisationen, die die Wahrung von Datenschutzinteressen explizit in ihren Statuten führten.²¹⁰⁸ Seither haben sich jedoch einige solche Verbände gebildet.²¹⁰⁹ Zudem können in der kleinräumigen Schweiz relativ schnell Leute zusammenfinden und Vereine gründen, wie sich bei andern durch die Digitalisierung aktuell gewordenen Gesellschaftsthemen gezeigt hat.²¹¹⁰ Im Entstehungsprozess des DSG wurde die Befürchtung laut, dass sich zu viele Ad-hoc-Gruppierungen als Verbände formieren könnten, um in querulatorischer Absicht Verbandsklagen zu führen.²¹¹¹ Dieser Sorge könnte der Gesetzgeber begegnen, indem er nur jene Organisationen zur Führung einer Verbandsklage berechtigt, die schon seit einer bestimmten Zeit bestehen²¹¹² und sich geografisch weit herum etabliert haben.²¹¹³ Zudem sollte die klagelegitimierte Organisation mit ihrer statuten- oder satzungsmässigen Tätigkeit keinen Gewinn anstreben,²¹¹⁴ d.h., ein all-

²¹⁰⁵ HÄNER, N 787.

²¹⁰⁶ HÄNER, N 787.

²¹⁰⁷ MEIER REGINA, N 9.

²¹⁰⁸ Aus damaliger Sicht sei daher eher eine Verstärkung der Behörden- und nicht der Verbandsbeschwerde zu prüfen gewesen: HÄNER, N 1066.

²¹⁰⁹ Z.B. die Vereine «Digitale Gesellschaft», «grundrechte.ch» und «Swiss Privacy Foundation». MEIER REGINA, N 10, m.w.H.

²¹¹⁰ Z.B. ist 2016 der Verein «#NetzCourage» entstanden, der sich gegen Hassreden im Internet einsetzt: #NetzCourage, <www.netzcourage.ch> (besucht am 31.05.2020). Der Verein «elternet.ch» (gegründet 2006) unterstützt Eltern in Erziehungsfragen betreffend die Nutzung digitaler Medien durch Kinder und Jugendliche: elternet.ch, <www.elternet.ch> (besucht am 31.05.2020).

²¹¹¹ AB NR 1991, 966; AB SR 1990, 129.

²¹¹² Z.B. Existenz des Verbands seit mindestens zwei Jahren (Art. 7 Abs. 1 GlG) oder seit zehn Jahren (Art. 9 Abs. 1 BehiG).

²¹¹³ Z.B. Organisationen von regionaler (Art. 89 Abs. 1 ZPO) oder gesamtschweizerischer Bedeutung (Art. 9 Abs. 1 BehiG).

²¹¹⁴ Vgl. zum Entwurf eines revidierten Art. 89 ZPO: Bundesamt für Justiz 2018, 40.

fälliger Prozessgewinn sollte entweder überwiegend derjenigen Personengruppe zukommen, für die die klagende Organisation tätig wird, oder von der klagenden Organisation ausschliesslich im Interesse dieser Personengruppe verwendet werden.²¹¹⁵ Eine weitere sinnvolle Hürde bestünde darin, vorauszusetzen, dass der Verbandskläger zur Interessenwahrung geeignet ist, d.h., dass er sowohl über die fachlichen Kenntnisse als auch die organisatorischen und finanziellen Möglichkeiten und Ressourcen verfügt, welche die angemessene Interessenwahrung zugunsten der betroffenen Personengruppe im konkreten Einzelfall objektiv erfordert.²¹¹⁶

Für eine ideelle Verbandsklage wird nicht vorausgesetzt, dass die klagende Organisation in ihren eigenen Interessen betroffen ist.²¹¹⁷ Ihre Legitimation ergibt sich daraus, dass die individuelle Rechtsdurchsetzung nicht funktioniert; ein Mangel, der sich bei Datenschutzverletzungen bewahrheitet hat.²¹¹⁸ Es genügt somit, dass Personen, für die sich die Organisation gemäss ihrem statutarischen Zweck einsetzt, betroffen sind. Die Personen müssen nicht aktuell betroffen sein, aber zumindest muss eine virtuelle Betroffenheit dargetan werden, die besteht, wenn mögliche künftige Rechtsnachteile drohen.²¹¹⁹ Das Verbandsklagerecht kann per Gesetz derart eingeschränkt werden, dass die Betroffenheit einer grösseren Zahl von Personen verlangt wird.²¹²⁰ Mit der Aufnahme dieser zusätzlichen Voraussetzung kann sichergestellt werden, dass die Verbandsklage nicht allein zugunsten eines einzelnen Arbeitnehmers geführt wird.²¹²¹

Der Ständerat hat im Jahr 1990 das Verbandsklagerecht auch mit dem Argument abgelehnt, dass Dritte (d.h. die Verbände) sich nicht in eine private Arbeitsbeziehung einmischen und bestehende Vertrauensverhältnisse stören sollten.²¹²² Das ideelle Verbandsklagerecht könnte aber in einer Weise ausgestaltet werden, dass der Dispositionsfreiheit der betroffenen Person der Vorrang zukommt, soweit diese auf den Vorteil, welcher der Verband für sie erkämpfen soll, verzichten

²¹¹⁵ Vgl. zum Entwurf eines revidierten Art. 89 ZPO: Bundesamt für Justiz 2018, 44.

²¹¹⁶ Vgl. zum Entwurf eines revidierten Art. 89 ZPO: Bundesamt für Justiz 2018, 41.

²¹¹⁷ Vgl. MEIER REGINA, N 11.

²¹¹⁸ Siehe S. 274.

²¹¹⁹ HÄNER, N 1049.

²¹²⁰ Siehe z.B. Art. 7 Abs. 1 GlG und Art. 9 Abs. 1 BehiG. Vgl. auch Art. 89 Abs. 1 ZPO.

²¹²¹ HÄNER, N 1049.

²¹²² AB SR 1990, 146.

will.²¹²³ Beispielsweise könnte der Verband verpflichtet werden, von den einzelnen Angehörigen der betroffenen Personengruppe eine Klagebeitrittserklärung einzuholen, sei es schriftlich oder auf eine andere Art, die den Nachweis durch Text erlaubt (sog. *opt in*).²¹²⁴ Alternativ könnte die Dispositionsfreiheit durch die Statuierung eines Vetorechts für direkt Betroffene sichergestellt werden (sog. *opt out*), d.h., die Ermächtigung des Verbands zur Prozessführung würde so lange vermutet, als der Betroffene nicht aktiv widerspricht.²¹²⁵ Eine dritte Variante wäre, eine Behörde dazwischenzuschalten; beispielsweise könnte festgelegt werden, dass die Empfehlung oder Verfügung des EDÖB das Anfechtungsobjekt einer Verbandsbeschwerde bildet und nicht unmittelbar das vertragliche Verhältnis.²¹²⁶ Diese dritte Option brächte jedoch kaum nennenswerte Vorteile für die betroffenen Arbeitnehmer, da der EDÖB ohnehin in ihrem Interesse tätig wird (vgl. Art. 29 Abs. 1 lit. a DSG) und sich somit die Tätigkeiten der Verbände und des EDÖB überschneiden würden.

iii. *Zivilprozessrechtliche Verbandsklage*

Alternativ zur vorstehend beschriebenen spezialgesetzlichen Verbandsklagebestimmung könnte eine wirksame allgemeine zivilprozessrechtliche Verbandsklagemöglichkeit in der ZPO vorgesehen werden. Eine solche Norm existiert in Art. 89 ZPO. Dieses Verbandsklagerecht ist jedoch praktisch irrelevant, was in der starken Einschränkung auf Verletzungen von Persönlichkeitsrechten und auf bloss negatorische und nichtmonetäre reparatorische Ansprüche begründet liegt (vgl. Art. 89 Abs. 2 ZPO).²¹²⁷ Zudem bestehen hohe formelle Anforderungen: Ein Verband kann die Widerrechtlichkeit einer Verletzung nur feststellen lassen, wenn sich diese weiterhin störend auswirkt (Art. 89 Abs. 2 lit. c ZPO). Zur Auslegung dieser Bestimmung kann auf die Rechtsprechung zum Persönlichkeitsschutz und zum unlauteren Wettbewerb gegriffen werden, weil dort Normen mit dem identischen Wortlaut bestehen (siehe Art. 28a Abs. 1 Ziff. 3 ZGB und Art. 9 Abs. 1 lit. c UWG). Eine auf das UWG gestützte Verbandsklage der Stiftung für Konsumenten-

²¹²³ HÄNER, 514 Ziff. 55.

²¹²⁴ Vgl. zum Entwurf eines revidierten Art. 89 ZPO: Bundesamt für Justiz 2018, 45.

²¹²⁵ Die Opt-out-Möglichkeit hat der Bundesrat für Art. 89 VE-ZPO jedoch verworfen: Bundesamt für Justiz 2018, 45.

²¹²⁶ Z.B. bei der arbeitsgesetzlichen Verbandsbeschwerde (Art. 58 ArG) bildet die Verfügung des Bundes- oder der kantonalen Behörde den Gegenstand des Verfahrens: HÄNER, N 1054.

²¹²⁷ BSK ZPO-KLAUS, Art. 89 ZPO, N 9. Seit Inkrafttreten der ZPO wurde keine einzige Verbandsklage erhoben: Bundesamt für Justiz 2018, 38.

tenschutz betraf den VW-Abgasskandal. Das Handelsgericht des Kantons Zürich ist auf diese Klage nicht eingetreten, weil im Zeitpunkt der Urteilsfällung kein täuschendes Verhalten der Autohersteller und Autohändler mehr bestand.²¹²⁸ Das Bundesgericht hat diesen Entscheid bestätigt.²¹²⁹ Aus demselben Grund dürften allfällige Verbandsklagen scheitern, die sich gestützt auf Art. 89 Abs. 2 lit. c ZPO gegen eine People Analytics-Praxis wenden: Die potenziell beklagte Arbeitgeberin könnte die störende Datenbearbeitung ändern, sobald sich ein Gerichtsverfahren abzeichnet. Damit liefe die Verbandsklage ins Leere.

Die beschriebenen Probleme haben den Bundesrat dazu bewogen, eine Verbesserung der ZPO im Bereich des kollektiven Rechtsschutzes und in anderen Punkten auszuarbeiten.²¹³⁰ Am 02.03.2018 schickte er den Vorentwurf der geänderten ZPO in die Vernehmlassung. Dieser sah eine Stärkung des kollektiven Rechtsschutzes in dreierlei Hinsicht vor. Erstens sollte die Verbandsklage nicht mehr nur auf Persönlichkeitsverletzungen beschränkt sein, sondern für das gesamte Privatrecht geöffnet werden (z.B. auch für arbeitsrechtliche Ansprüche, Art. 89 Abs. 1 VE-ZPO).²¹³¹ Zweitens war neu eine reparatorische Verbandsklage vorgesehen, die es dem Verband ermöglicht hätte, finanzielle Ansprüche (Schadenersatz, Gewinnherausgabe, Herausgabe einer ungerechtfertigten Bereicherung) geltend zu machen (Art. 89 Abs. 2 lit. d i.V.m. Art. 89a VE-ZPO).²¹³² Der Unterschied zwischen diesen beiden Klagen bestand darin, dass die klagende Organisation im ersteren Fall einen eigenen Anspruch des Verbands geltend machen sollte (Art. 89 VE-ZPO), wohingegen sie im letzteren Fall als Prozessstandschafterin handeln sollte, d.h., sie sollte als Partei auftreten und in eigenem Namen finanzielle Ansprüche geltend machen, die materiell-rechtlich den einzelnen Angehörigen der repräsentierten Personengruppe zugestanden hätten.²¹³³ Die dritte Neuerung be-

²¹²⁸ Urteil HGer ZH HG170181-O vom 12.07.2018 E. 3.3–3.4. Die betreffende Verletzungshandlung war seit dem 18.09.2015 beendet: Urteil HGer ZH HG170181-O vom 12.07.2018 E. 3.2.3.

²¹²⁹ Urteil BGer 4A_483/2018 vom 08.02.2019 E. 4 und Urteil BGer 4A_43/2020 vom 16.07.2020 E. 4.

²¹³⁰ Den ersten Meilenstein bildete die Bestandesaufnahme des Bundesrats von 2013 zum kollektiven Rechtsschutz: Schweizerischer Bundesrat 2013a.

²¹³¹ Bundesamt für Justiz 2018, 17 und 38–39. Siehe bereits: Schweizerischer Bundesrat 2013a, 27.

²¹³² Bundesamt für Justiz 2018, 17 und 42.

²¹³³ Bundesamt für Justiz 2018, 43.

stand in der Schaffung eines allgemeinen Gruppenvergleichsverfahrens zur Geltendmachung von Massenschäden (Art. 352a ff. VE-ZPO).²¹³⁴

Die Verbesserungsvorschläge des Bundesrats bzgl. des kollektiven Rechtsschutzes waren in der Vernehmlassung jedoch umstritten.²¹³⁵ Deshalb hat der Bundesrat die entsprechenden Ideen nicht in die Botschaft zur Revision der ZPO und den entsprechenden ZPO-Entwurf aufgenommen.²¹³⁶ Sie sollen stattdessen zu einem späteren Zeitpunkt separat behandelt werden, wie in der Medienmitteilung vom 26.02.2020 bekanntgegeben worden ist.²¹³⁷ Somit kann das zivilprozessrechtliche Verbandsklagerecht bis auf Weiteres nicht wirksam zur Durchsetzung des Datenschutzrechts beitragen. Möglicherweise ist es politisch ohnehin einfacher, ein spezialgesetzliches Verbandsklagerecht für den privatrechtlichen Teil des DSG zu schaffen, das auf die konkreten Umstände im Datenschutzrecht zugeschnitten ist. Eine Aufwertung des allgemeinen zivilprozessrechtlichen Verbandsklagerechts in der ZPO dürfte auf höheren politischen Widerstand stossen, weil dies Auswirkungen auf das gesamte Privatrecht hätte. Aus diesem praktischen Grund ist die im vorhergehenden Unterkapitel²¹³⁸ vorgeschlagene datenschutzrechtliche ideelle Verbandsklage gegenüber einer Revision von Art. 89 ZPO vorzuziehen.

bb) Begutachtung von Algorithmen

Es ist nach vorliegend vertretener Meinung ein freiwilliges oder gesetzlich vorgeschriebenes Kontrollverfahren für private Softwareanwendungen vorzuschlagen, die in besonders persönlichkeits- und diskriminierungssensiblen Bereichen zum Einsatz kommen sollen oder schwere Schäden verursachen können.²¹³⁹ Ziel dabei ist es, dass eine neutrale Drittpartei das Modell, das der Entwickler entworfen hat, auf die Rechtsprobleme der Persönlichkeitsverletzungen und Diskriminierungen

²¹³⁴ Bundesamt für Justiz 2018, 17. Unter einem Massenschaden ist ein Schaden zu verstehen, bei dem eine Vielzahl von Personen in gleicher oder gleichartiger Weise betroffen ist und jede einzelne in einer für sie erheblichen Weise geschädigt wird. Der Begriff ist von Streuschäden abzugrenzen, bei welchen eine Vielzahl von Personen lediglich einen wertmässigen kleinen Schaden erleidet: BBI 2020, 25.

²¹³⁵ Insbesondere wurde vertreten, dass der kollektive Rechtsschutz beim Erlass der ZPO abgelehnt worden sei und es nicht gerechtfertigt sei, auf diesen Entscheid zurückzukommen: Bundesamt für Justiz 2020, 12.

²¹³⁶ BBI 2020, 26.

²¹³⁷ Schweizerischer Bundesrat 2020.

²¹³⁸ Siehe S. 353–359.

²¹³⁹ Ebenso bereits RUDIN 2002, 415.

hin testet.²¹⁴⁰ Zum Prüfradius müsste einerseits die Validität der algorithmischen Ergebnisse, andererseits aber auch der Trainingsprozess der lernfähigen Systeme gehören.²¹⁴¹ Als Methode wäre beispielsweise eine explorative²¹⁴² oder kontrafaktische²¹⁴³ Analyse der algorithmischen Modelle auf Gerechtigkeit hin geeignet. Nach bestandem Test bekommt der Algorithmus ein Gütesiegel.

Das Kontrollverfahren müsste kontinuierlich stattfinden; eine einmalige Zulassungskontrolle genügt nicht, da sich Algorithmen im Laufe ihres Einsatzes wie ein Chamäleon verändern – sei es durch Updates oder aufgrund eines maschinellen Lernverfahrens.²¹⁴⁴ Einer Regelmässigkeit bedarf die Prüfung auch, um dem Wandel der gesellschaftlichen Normen Rechnung zu tragen: Ein Datensatz zur Geschlechterverteilung am Arbeitsplatz kann beispielsweise das früher akzeptierte Rollenbild des Ehemanns als Alleinverdiener abbilden; jedoch haben sich die Formen des Zusammenlebens und der Arbeitsverteilung inzwischen vervielfältigt. Demzufolge müssen die Annahmen, die dem Modell zugrunde liegen, aufs Neue begründet werden.²¹⁴⁵

Die Prüfung kann durch verschiedene Kontrollinstanzen erfolgen. Denkbar ist ein externes Audit durch eine privatrechtliche Organisation nach dem Vorbild des

²¹⁴⁰ Beim *«trusted third party approach»* hat der Entwickler keinen Zugriff auf Informationen zu diskriminierungsrechtlich geschützten Merkmalen, der Dritte hingegen schon: VEALE/BINNS, 6. Dieser Ansatz empfehle sich vor allem für Unternehmen, die ein geringes Vertrauen geniessen oder ein hohes Reputationsrisiko tragen: VEALE/BINNS, 12.

²¹⁴¹ Ungenügende bisherige Überprüfung der Validität in den USA: ANGWIN JULIA / LARSON JEFF / MATTU SURYA / KIRCHNER LAUREN, Machine bias, 23.06.2016, abrufbar unter <www.propublica.org> (besucht am 31.05.2020).

²¹⁴² *«Exploratory fairness analysis»*: VEALE/BINNS, 5. Dieser Ansatz erfordert geringen organisatorischen Aufwand, garantiert aber begriffsimmanent keine systematische Behebung aller Risiken: VEALE/BINNS, 12.

²¹⁴³ ALTMAN *et al.*, 43. Die kontrafaktische Analyse stellt verschiedene Hypothesen einander gegenüber. Z.B. fragt sie: «Welches Resultat hätte der Algorithmus ausgegeben, wenn das Datum B statt A eingegeben worden wäre?» Siehe zum Begriff «kontrafaktische Erklärung» S. 204.

²¹⁴⁴ MARTINI, 1021. Vgl. AJUNWA/FRIEDLER *et al.*, 25.

²¹⁴⁵ Vgl. S. 93–94. Zum Wandel ethischer Normen: algo:aware [sic], 17. Vgl. REINSCH/GOLTZ, 42. Einer rechtstheoretischen Begründung bedarf es, wenn der COMPAS-Algorithmus der Firma Northpointe Inc. zur Vorhersage der Rückfälligkeit eines Straftäters Daten über Straftaten von dessen engen Verwandten einbezieht: ZWEIF/KRAFFT, 112.

deutschen TÜV (eingetragener Technischer Überwachungsverein)²¹⁴⁶ oder des amerikanischen Unternehmens ORCAA (O'Neil Risk Consulting and Algorithmic Auditing).²¹⁴⁷ Unabhängiger Auditor könnte auch der Staat sein.²¹⁴⁸ Auch eine Mischform ist nicht ausgeschlossen, bei der die Behörde nicht selbst Auditierungen durchführt, sich aber daran beteiligt, etwa durch die Akkreditierung eines Auditors.²¹⁴⁹ In den Fällen, in denen sich eine zusätzliche externe Kontrollinstanz einschaltet, trägt die Begutachtung zur Demokratisierung der Datenbearbeitungsprozesse bei. Möglich ist aber auch ein internes Audit, wie es beispielsweise im Unternehmen Pymetrics institutionalisiert ist, welches Persönlichkeitstests zur Rekrutierung entwickelt.²¹⁵⁰ Im letzteren Fall führt die Massnahme mehr zu einer Professionalisierung, weil die Arbeitgeberin ihre eigenen Ressourcen verstärkt, aber keine aussenstehenden natürlichen oder juristischen Personen in die Kontrolle der Datenbearbeitung einbezogen werden.

Denkbar ist, die Prüfergebnisse zu veröffentlichen.²¹⁵¹ Die Prüfungsgrundlagen, insbesondere der Algorithmus selbst, sollten jedoch als privatwirtschaftliche Geschäftsgeheimnisse geschützt bleiben.²¹⁵² Hierfür braucht es prüfverfahrensrechtliche Geheimhaltungspflichten, die gesetzlich oder vertraglich geregelt werden müssen, je nachdem, ob die Prüfinstanz eine staatliche Behörde oder eine privatrechtliche Institution ist.²¹⁵³

²¹⁴⁶ MARTINI, 1021; «*external and independent auditing [...] separately from regulatory requirements*»: UNO Generalversammlung, 21–22. Eine neue Berufsgattung von «*external algorithmists*» solle sich mit einem Verhaltenskodex selbst regulieren: MAYER-SCHÖNBERGER/CUKIER, 181.

²¹⁴⁷ HEMPEL JESSI, Want to prove your business is fair? Audit your algorithm, 05.09.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020).

²¹⁴⁸ ZWEIG/KRAFFT, 115; MARTINI, 1021.

²¹⁴⁹ RUDIN 2002, 415.

²¹⁵⁰ HEMPEL JESSI, Want to prove your business is fair? Audit your algorithm, 05.09.2018, abrufbar unter <www.wired.com> (besucht am 31.05.2020).

²¹⁵¹ UNO Generalversammlung, 22.

²¹⁵² Vgl. UNO Generalversammlung, 19. Hingegen ist bei Algorithmen in öffentlich-rechtlichen Anwendungsfeldern eine Offenlegung des Quellcodes zu verlangen: KEATS CITRON, 1308.

²¹⁵³ Vgl. DREYER/SCHULZ, 10, und HÄNOLD, 151.

cc) Bildung

Bildung, Aufklärung und die Entwicklung einer Digitalkompetenz (*digital literacy*) müssen im politischen Programm zur Verbesserung des Datenschutzes eine zentrale Rolle einnehmen.²¹⁵⁴ Die Bildung dient dem Zweck, Ungleichheiten, die durch den technologischen Fortschritt entstehen können, zu beseitigen.²¹⁵⁵ Nicht nur die Arbeitnehmer benötigen Digitalkompetenzen, sondern auch die Politiker und Rechtsanwälte²¹⁵⁶ sowie bereits die Kinder.²¹⁵⁷ Beim Vorantreiben der Sensibilisierung für den Datenschutz spielen Schulen und Medien eine wichtige Rolle, weil sie als Multiplikatoren wirken.²¹⁵⁸ Die Bildung der breiten Bevölkerung stellt die «Demokratisierungsmassnahme» schlechthin dar, weil dadurch das ganze «Volk» (altgr. δῆμος, «dēmos») am Diskurs über die Datenbearbeitungen und an deren Kontrolle partizipieren kann.

7.4 Zwischenfazit: effektiverer Datenschutz basierend auf Professionalisierung und Demokratisierung

Das vorliegende Kapitel hat sich der Beantwortung der Forschungsfrage gewidmet, die lautet: *Wie könnte eine künftige Neuausrichtung des privatrechtlichen Datenschutzrechts aussehen, bei welcher die Rechtsdurchsetzung ex ante und ex post im Zusammenhang mit People Analytics besser gewährleistet wäre als heute?*²¹⁵⁹

Die Ausgangslage ist diejenige, dass People Analytics grosse Chancen bietet, dass es aber immer wieder zu Datenskandalen kommt, weil das Datenschutzrecht von

²¹⁵⁴ Auch «Medienkompetenz»: RUDIN 2004b, 437; RUDIN 2010, 139; TAMÒ-LARRIEUX, 237. Vgl. TALIDOU, 213. Bildung im Bereich Big Data als eines der obersten Ziele der EU: Europäisches Parlament 2017, 7; Digitalkompetenz-Initiativen der US-Regierung: White House, Executive Office of the President 2015, 6; CRAWFORD/SCHULTZ, 123. Vgl. THIERER, 437, und HARTZOG 2018, 159. Zur Bildung gehört ein Verständnis für den Wert der Daten: World Economic Forum 2013, 4.

²¹⁵⁵ BRYNJOLFSSON/MCAFEE, 208–209.

²¹⁵⁶ HILDEBRANDT/KOOPS, 460.

²¹⁵⁷ Insbesondere die Eltern stehen in der Verantwortung für die Erziehung der Kinder im Umgang mit digitalen Medien: PALFREY/GASSER 2008, xvi. Vgl. auch GASSER/CORTESI, m.w.H. UNICEF, 17; THIERER, 439.

²¹⁵⁸ BOLLIGER *et al.*, 228.

²¹⁵⁹ Siehe S. 11.

der Arbeitgeberin nicht korrekt angewendet wird. Da die Gegenseite das Recht nicht effektiv durchsetzen kann, droht deren Vertrauen in die Rechtsordnung zu zerbröckeln. Das Schrifttum äussert Ideen, das Datenschutzrecht vermehrt auf das Teilen von Information auszurichten und das Vertrauen in das Datenschutzrecht zu stärken.²¹⁶⁰ Arbeitnehmer, die auf den Schutz ihrer Daten vertrauen können, sind eher gewillt, Informationen über sich preiszugeben, was wiederum für den Erfolg von People Analytics förderlich ist. Doch die bestehenden Ideenansätze sind abstrakt und unvollständig.²¹⁶¹

Deshalb präsentiert die vorliegende Arbeit ein eigenes Konzept für einen effektiven Datenschutz. Aufbauend auf der Erkenntnis, dass das Vertrauen der Arbeitnehmer gewonnen werden muss, wird einerseits eine Professionalisierung des Datenschutzes vorgeschlagen. Komplementär dazu müssen andererseits die Kontrollrechte gestärkt werden, was mittels einer Demokratisierung gelingen kann.²¹⁶² Die vom Autor ausgearbeiteten Vorschläge gehen deutlich über die Reformen gemäss rev-DSG hinaus.

Unter dem Begriff der Professionalisierung wird vorliegend jede Massnahme verstanden, die die Arbeitgeberin dazu veranlasst, das Datenschutzrecht ab Beginn der Datenbearbeitung zu befolgen, sodass die Rechtsdurchsetzung im Zusammenhang mit People Analytics gewährleistet ist. Es kommen hauptsächlich Mittel zur Rechtsdurchsetzung *ex ante* infrage, aber auch Mittel zur Einwirkung *ex post* sind nicht ausgeschlossen. Professionalisierend wirken etwa die im rev-DSG vorgesehenen Pflichten zum Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 6 E-DSG, Art. 7 rev-DSG) sowie zur Datenschutz-Folgenabschätzung (Art. 20 E-DSG, Art. 22 rev-DSG), ebenso die Pflichten sowohl zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten (Art. 11 E-DSG, Art. 12 rev-DSG) als auch zur Information bei der Beschaffung von Personendaten (Art. 17 E-DSG, Art. 19 rev-DSG) und zur Meldung von Verletzungen der Datensicherheit (Art. 22 E-DSG, Art. 24 rev-DSG). Die Ernennung eines Datenschutzberaters (Art. 9 E-DSG, Art. 10 rev-DSG) sowie die Schaffung von anerkannten Verhaltenskodizes (Art. 10 E-DSG, Art. 11 rev-DSG) und anerkannten Zertifizierungsstellen (Art. 12 E-DSG, Art. 13 rev-DSG) erfolgen auf freiwilliger Basis. Diese drei freiwilligen Massnahmen könnten dazu beitragen, dass die Arbeitgeberin ihre personellen Ressourcen betreffend Datenschutz aufstockt und sich proak-

²¹⁶⁰ Siehe S. 296–304.

²¹⁶¹ Siehe die Kritik auf S. 313–314.

²¹⁶² Siehe S. 315–317.

tiver mit dem Datenschutz auseinandersetzt. Im schweizerischen Recht sollten die nötigen Anreize geschaffen werden, damit die Arbeitgeberin diesen Zusatzaufwand freiwillig auf sich nimmt.²¹⁶³

Das vorliegend erarbeitete Teilkonzept der Professionalisierung bedeutet aber mehr als bloss die Neuerungen gemäss rev-DSG: Erstens könnte eine zusätzliche Rechenschaftspflicht, wonach die Arbeitgeberin jederzeit die Einhaltung des Gesetzes nachweisen können muss (vgl. Art. 5 Abs. 2 DSGVO), bewirken, dass sich die Arbeitgeberin bewusster mit den Datenbearbeitungen und deren Folgen auseinandersetzt. Die Rechenschaftspflicht würde zudem zu einer Beweislastumkehr führen, sodass die Durchsetzung des Datenschutzrechts auf dem Gerichtsweg einfacher werden würde. Zweitens könnte die Aufnahme bestimmter Quotierungsziele in die Algorithmenprogrammierung der algorithmischen Diskriminierungsgefahr entgegenwirken. Drittens sollten Schulungen des Personals dazu beitragen, dass sich die Angestellten aller Stufen von Anfang an Gedanken darüber machen, wie das Datenschutzrecht bei People Analytics eingehalten werden kann.²¹⁶⁴

Der Begriff der Demokratisierung bedeutet vorliegend jede Massnahme, welche den der Arbeitgeberin entgegengesetzten Parteien Kontrollrechte einräumt, um auf die Einhaltung des Datenschutzrechts hinzuwirken, sodass die Rechtsdurchsetzung im Zusammenhang mit People Analytics gewährleistet ist. Hier geht es primär um die Rechtsdurchsetzung *ex post*, doch auch Mittel zur präventiven Kontrolle sind zu erwägen. Das rev-DSG sieht eine Stärkung der Datenschutzaufsicht (etwa durch das Verfügungsrecht des EDÖB, Art. 45 Abs. 1 E-DSG, Art. 51 Abs. 1 rev-DSG) und der Strafbehörden (etwa durch die Erhöhung des Strafrahmens, Art. 54–57 E-DSG, Art. 60–63 rev-DSG) vor.²¹⁶⁵

Das vorliegend ausgefertigte Teilkonzept der Demokratisierung schliesst zusätzlich zu den im rev-DSG vorgesehenen eine Reihe weiterer Massnahmen mit ein. Das Ziel der Demokratisierung besteht darin, das Wissen und die Eingriffskompetenzen im Zusammenhang mit People Analytics möglichst breit zu verteilen, denn je mehr Kontrollakteure auf Fehler in der Rechtspraxis hinweisen, desto eher kann gewährleistet werden, dass diese Fehler korrigiert werden. Zur Befähigung der einzelnen Arbeitnehmer sind unkomplizierte technologische «Werkzeuge» erforderlich, mit denen sie ihre Datenbearbeitungspräferenzen ohne Zeitverlust kom-

²¹⁶³ Siehe zu den Neuerungen gemäss rev-DSG S. 319–339.

²¹⁶⁴ Siehe die über das rev-DSG hinausgehenden Professionalisierungsvorschläge auf S. 339–344.

²¹⁶⁵ Siehe S. 348–351.

munizieren und durchsetzen können (z.B. einfache Browsereinstellungen; oder ein simpler «*Do not sell my personal information*»-Button, wie unter kalifornischem Recht verlangt, 1798.135 (a) (1) CCPA). Die Arbeitnehmervertretung kann gestärkt werden (z.B. durch Sanktionierung von Verstößen gegen das MitwG). Würde der Staat vermehrt als Diskursmoderator auftreten, könnte er zahlreiche Arbeitgeberinnen und Arbeitnehmer für die rechtlichen Aspekte von People Analytics sensibilisieren. Für diese Aufgabe ist über eine Reorganisation des EDÖB nachzudenken (z.B. Aufteilung in eine zentrale Aufsichtsbehörde sowie dezentrale Beratungs- und Informationsstellen). Schliesslich sollte die Zivilgesellschaft stärker einbezogen werden durch die Schaffung eines datenschutzrechtlichen ideellen Verbandsklagerechts, durch Begutachtungsverfahren für Algorithmen (wobei als Begutachtungsinstanz neben zivilrechtlichen Vereinen auch Unternehmen oder staatliche Stellen infrage kommen) und nicht zuletzt durch Investitionen in die Bildung und Digitalkompetenz der Zivilgesellschaft.²¹⁶⁶

Die aufgezeigten Vorschläge gehen teilweise über das Rechtliche hinaus und beinhalten auch eine technische und eine soziale Seite, die etwa beim Datenschutz durch Technik und bei den technologischen «Werkzeugen» für die Individuen einerseits oder aber bei den Schulungen und der Bildung andererseits herausstechen. Insgesamt ist mit dem Konzept der Professionalisierung und Demokratisierung, wie es sich der Autor vorstellt, auch ein allgemeiner Mentalitätswandel verbunden. Zur wirksamen Durchsetzung des Datenschutzes muss diesem in den Köpfen der Verantwortlichen und Betroffenen eine höhere Priorität zukommen als bislang. Nur auf diese Weise werden die Arbeitgeberinnen ihre Sorgfaltspflichten erfüllen und die Gegenseite ihre Kontrollrechte ausüben.

Der Mehrwert des vorgeschlagenen Konstrukts der Professionalisierung und Demokratisierung liegt schliesslich darin, dass es auf das gesamte Datenschutzrecht angewendet werden kann. Sein möglicher Anwendungsbereich ist nicht auf den vorliegend untersuchten arbeitsrechtlichen Kontext beschränkt. Es handelt sich um ein gedankliches Gerüst, das stets weiterentwickelt werden kann. Das theoretische Konzept ist offen dafür, neue praktische Ideen zur Verbesserung der Durchsetzung des Datenschutzrechts aufzunehmen, auch wenn diese andere Bereiche als das Arbeitsrecht betreffen.

²¹⁶⁶ Siehe die über das rev-DSG hinausgehenden Demokratisierungsvorschläge auf S. 344–348 und 351–364.

8 Ergebnisse

Es gilt nun, die eingangs gestellten acht Vorfragen und anschliessend die Forschungsfrage zu beantworten.²¹⁶⁷

(1) Was ist People Analytics und was ist daran neu im Vergleich zu früheren Überwachungspraktiken an den Arbeitsplätzen?

People Analytics bezeichnet die Personalentwicklungspraxis, bei der digitale Daten aus unternehmensinternen und -externen Quellen, die sich auf das Humankapital beziehen, mit Informationstechnologie systematisch ausgewertet werden, um Entscheidungen zur Steigerung des Unternehmenswerts zu treffen. Dabei kontrolliert die Arbeitgeberin den gesamten Daten-Lebenszyklus, angefangen bei der Beschaffung, über die Analyse und Nutzung bis hin zur allfälligen Wiederverwertung der Daten. Sie greift auf eine umfangreiche Apparatur zurück bestehend aus Hardware (z.B. Sensoren, Wearables, Roboter) und Software (Algorithmen). Die Datenbearbeitungen finden im Verlauf des gesamten Arbeitnehmer-Lebenszyklus statt, insbesondere zu den Zwecken der Rekrutierung, der Leistungssteuerung, des Compliance-Managements, der Arbeits- und Arbeitsplatzgestaltung sowie der Mitarbeiterbindung. People Analytics wird bereits grossflächig angewendet und wird sich künftig weiter ausbreiten. Im Unterschied zu älteren Überwachungsformen am Arbeitsplatz zeichnet sich People Analytics durch Ubiquität, Interoperabilität und steigende KI aus. Ubiquität meint, dass die Datenbearbeitungen überall und immer stattfinden. Interoperabilität bedeutet, dass die Datenquellen zusammengeführt und daraus Erkenntnisse von neuer Qualität gewonnen werden können. Die steigende KI weist auf den Umstand hin, dass eine zunehmend autonom handelnde, intelligente Infrastruktur im Interesse der Arbeitgeberin das Arbeitsverhältnis beeinflusst.

(2) Welche Rechtsprobleme ergeben sich aus People Analytics?

Das Grundproblem von People Analytics ist ein Informations- und Machtgefälle zugunsten der Arbeitgeberin und zulasten des Arbeitnehmers, welches die ohnehin bestehende Asymmetrie im Arbeitsverhältnis verschärft. Daraus leiten sich die Rechtsprobleme ab: People Analytics kann zu Persönlichkeitsverletzungen führen, wenn Eingriffe sowohl in die Privatsphäre und psychische Integrität als auch in das Recht am eigenen Wort und Bild stattfinden. Zudem drohen Diskriminie-

²¹⁶⁷ Siehe S. 11.

rungen sowie Verletzungen der mitwirkungsrechtlichen Ansprüche auf Information und Mitsprache.

(3) Welche Rechtsgebiete sind für People Analytics relevant?

People Analytics ist eine Querschnittsmaterie. Einzuhalten sind insbesondere der arbeitsrechtliche Persönlichkeitsschutz (Art. 328 OR und Art. 28 ZGB), der datenschutzrechtliche Persönlichkeitsschutz (Art. 328b OR und das DSG), der öffentlich-rechtliche Arbeitnehmer-Gesundheitsschutz (Art. 26 ArGV 3 i.V.m. Art. 342 OR), verschiedene Bestimmungen zum Diskriminierungsschutz,²¹⁶⁸ das Mitwirkungsrecht (nach dem MitwG, gegebenenfalls auch Kollektivregelungen in Gesamtarbeitsverträgen und Betriebsvereinbarungen) und strafrechtliche Bestimmungen.²¹⁶⁹ Auch verfassungsrechtliche und internationale Normen können anwendbar sein (insbesondere Art. 13 BV, Art. 8 EMRK und gegebenenfalls die DSGVO). Erst durch die Wechselwirkung all dieser Bestimmungen kann ein Auffangnetz entstehen, das die Arbeitnehmer vor Rechtsverletzungen weitgehend zu schützen vermag.

(4) Welchen Zweck verfolgt das DSG im Hinblick auf People Analytics?

Das DSG bezweckt im privatrechtlichen Bereich den Schutz der Persönlichkeit von Personen, über die Daten bearbeitet werden (Art. 1 DSG, Art. 1 E-DSG, Art. 1 rev-DSG). Dabei bildet der Persönlichkeitsschutz das Endziel, während als Mittel zur Zielerreichung die zulässigen Bearbeitungsprozesse definiert werden. Das DSG enthält deshalb einerseits risikoorientierte Normen, die den privatrechtlichen Persönlichkeitsschutz statuieren. Andererseits existieren prozessorientierte Normen, die den Persönlichkeitsschutz in Bezug auf Datenbearbeitungen konkretisieren. Beide Normtypen sind erforderlich, haben aber ihre Defizite, weil sie entweder zu abstrakt (die risikoorientierten) oder zu starr und formalistisch (die prozessorientierten) sind. Die prozessbezogenen Normen müssen nach der vorliegend vertretenen Meinung risikoorientiert ausgelegt werden, damit die *ratio* des DSG erfüllt werden kann. Diese Interpretationsweise bringt mehr Flexibilität ins

²¹⁶⁸ Auf Verfassungsebene: Art. 8 Abs. 2 i.V.m. Art. 35 Abs. 3 BV sowie Art. 8 Abs. 3 Satz 3 BV. Auf Staatsvertragebene: Art. 2, Art. 7 lit. a FZA sowie Anhang I Art. 9 Abs. 1 und 4 FZA. Auf Gesetzesebene: Art. 22 AIG, Art. 3 GlG, Art. 4 GUMG und Art. 4 Abs. 1 HarG.

²¹⁶⁹ Aus dem Strafgesetzbuch: Art. 179 ff. StGB und Art. 292 StGB i.V.m. Art. 51 Abs. 2 ArG. Aus dem Nebenstrafrecht: Art. 34–35 DSG (bzw. Art. 54–60 E-DSG bzw. Art. 60–66 rev-DSG), Art. 59 Abs. 1 lit. a ArG i.V.m. Art. 26 ArGV 3, Art. 60 ArG, Art. 36–37 sowie Art. 39 i.V.m. Art. 21 GUMG.

Datenschutzrecht in dem Sinne, dass die Prozessnormen strikter oder lockerer angewendet werden können, je nachdem, welche konkreten Risiken einer fraglichen Datenbearbeitung innewohnen. Die vorgeschlagene Auslegungsart wird auch durch die Rechtsprechung getragen. So achtet das Bundesgericht zur Prüfung der Zulässigkeit von Überwachungssystemen am Arbeitsplatz (Art. 26 ArGV 3) darauf, ob von diesen eine gesundheitsschädigende Wirkung ausgeht, und nicht etwa darauf, welchem formalen Zweck die Systeme dienen.

(5) *Welche People Analytics-Anwendungen erfasst das DSG und welche Datenbearbeitungsregeln stellt es für People Analytics in privatrechtlichen Arbeitsverhältnissen auf?*

Das DSG erfasst diejenigen People Analytics-Anwendungen, bei denen Personen-daten bearbeitet werden. Hingegen unterstehen Bearbeitungen anonymisierter Daten nicht dem DSG. Noch nicht höchststrichterlich entschieden ist, ob das Typisieren (auch Aussondern oder Singularisieren) datenschutzrechtlich relevant ist. Im Sinne einer risikoorientierten Auslegung sollten Typisierungen nach dem vorliegend vertretenen Standpunkt in den Anwendungsbereich des DSG fallen, wenn von ihnen ein hohes Risiko für die Persönlichkeit der Betroffenen ausgeht. Dies ist beispielsweise der Fall sowohl bei Typisierungen, durch die ein Mensch auf ein Profil reduziert wird, das als Grundlage für einschneidende Entscheidungen über ihn dient, obwohl es seiner Identität nicht entspricht, als auch bei Typisierungen, die das arbeitsrechtliche Frageverbot verletzen, sowie bei Typisierungen, bei denen genetische Daten bearbeitet werden.

Wird die Anwendbarkeit des DSG auf People Analytics bejaht, gelten zunächst die allgemeinen Rechtsgrundsätze der Rechtmässigkeit (Art. 4 Abs. 1 DSG, Art. 5 Abs. 1 E-DSG, Art. 6 Abs. 1 rev-DSG), des Handelns nach Treu und Glauben und der Verhältnismässigkeit (Art. 4 Abs. 2 DSG, Art. 5 Abs. 2 E-DSG, Art. 6 Abs. 2 rev-DSG). Sodann muss sich People Analytics an die spezifischen Datenbearbeitungsregeln halten. Von diesen wurden die Zweckbindung (Art. 4 Abs. 3 DSG, Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG), die Erkennbarkeit (Art. 4 Abs. 4 DSG, Art. 5 Abs. 3 E-DSG, Art. 6 Abs. 3 rev-DSG), die Richtigkeit (Art. 5 DSG, Art. 5 Abs. 5 E-DSG, Art. 6 Abs. 5 rev-DSG), die Datensicherheit (Art. 7 DSG, Art. 7 E-DSG, Art. 8 rev-DSG) sowie die Datenminimierung, die Speicherbegrenzung und die Löschpflicht näher behandelt. Es hat sich gezeigt, dass die Bearbeitungsregeln oft nicht absolut gelten können, da sie einen bestimmten Auslegungsspielraum lassen oder einander zu einem gewissen Grad widersprechen. Die Arbeitgeberin bedarf somit eines hohen Masses an Fachwissen und Reflexionskompetenz, um das DSG bei People Analytics korrekt anzuwenden.

(6) Welche Rechtfertigungsmöglichkeiten bestehen für allfällige Datenschutzverletzungen?

Verstöße gegen das DSG kommen in der People Analytics-Betriebspraxis gehäuft vor. Eine Rechtfertigung ist aber nicht ausgeschlossen. Zunächst ist festzuhalten, dass – entgegen dem Gesetzeswortlaut von Art. 12 Abs. 2 lit. a DSG (bzw. Art. 26 Abs. 2 lit. a E-DSG bzw. Art. 30 Abs. 2 lit. a rev-DSG) – Verstöße gegen die Datenschutz-Grundsätze gerechtfertigt werden können. Als Rechtfertigungsgründe kommen die Einwilligung, ein überwiegendes privates oder öffentliches Interesse sowie eine gesetzliche Bearbeitungspflicht infrage (Art. 13 Abs. 1 DSG, Art. 27 Abs. 1 E-DSG, Art. 31 Abs. 1 rev-DSG). Die Einwilligung sollte im arbeitsrechtlichen Kontext nur im Notfall als Rechtfertigungsgrund hinhalten müssen. Es ist kritisch zu hinterfragen, ob sie freiwillig und informiert erfolgt; zudem droht jederzeit der Widerruf der Einwilligung.

(7) Warum hat die zivilrechtliche Individualklage ihre Rolle bei der Durchsetzung des Datenschutzrechts bis heute nicht erfüllen können?

Für die Durchsetzung des privatrechtlichen Datenschutzes *ex post* sind hauptsächlich die individuell betroffenen Arbeitnehmer verantwortlich, die eine zivilrechtliche Persönlichkeitsschutzklage führen müssen (vgl. Art. 15 DSG, Art. 28 E-DSG, Art. 32 rev-DSG). Dies ist darauf zurückzuführen, dass die Vorstellungen des Persönlichkeitsschutzes als Abwehrrecht und der informationellen Selbstbestimmung tief im (datenschutzrechtlichen) Persönlichkeitsschutz verankert sind. Für eine zivilrechtliche Klage bestehen jedoch zu wenig Anreize. Die potenziellen Verfahrenskosten übertreffen die möglichen finanziellen Ersatzansprüche, und verfahrensrechtliche Hindernisse stehen einem kollektiven Vorgehen mehrerer Arbeitnehmer zusammen im Wege. Angesichts der oft komplexen datenschutzrechtlichen Sachverhalte und der fehlenden Transparenz können sich Einzelpersonen auch überfordert fühlen, was sie davon abhält, ihre Rechte selbstbestimmt wahrzunehmen.

(8) Wie können Gruppen und/oder Behörden ihre Interessen beim Datenschutz wirksam einbringen, um zur Rechtsdurchsetzung beizutragen?

Verschiedene Akteure könnten auf die Realisierung der datenschutzrechtlichen Ziele hinwirken, doch ist ihr Einfluss aus je unterschiedlichen Gründen begrenzt. Dem EDÖB sind die Hände gebunden, weil er nur unverbindliche Empfehlungen, aber keine Verfügungen erlassen, geschweige denn Verwaltungssanktionen aussprechen kann. Die Arbeitsinspektorate schreiten erst ein, wenn People Analytics die Gesundheit beeinträchtigt. Strafverfolgungen wegen People Analytics spielen

eine untergeordnete Rolle. Die Arbeitnehmervertretung kann aktiv werden, aber ihre allfälligen Klagen scheitern am Verfahrensrecht und selbst bei Obsiegen drohen weder mitwirkungsrechtliche Sanktionen für die Arbeitgeberin noch steht ein materiell-rechtliches Mitentscheidungsrecht für die Arbeitnehmer in Aussicht. Allenfalls wirken die Risiken der gesellschaftsrechtlichen Haftung, der Arbeitsverweigerung, des Streiks und der Kündigung regulierend. Insgesamt können Gruppen und Behörden ihre Interessen unter der aktuellen Rechtslage nicht genügend einbringen, um den Datenschutz wirksam zu stärken.

Ein gegensätzlicher Befund ergibt sich bei Sachverhalten, die in den Anwendungsbereich der DSGVO fallen, da die Aufsichtsbehörden der EU-Mitgliedstaaten Verfügungen erlassen und hohe Bussen verhängen können. Auch für das künftige totalrevidierte schweizerische Datenschutzrecht sind eine entsprechende Verfügungskompetenz des EDÖB (Art. 45 E-DSG, Art. 51 rev-DSG) und ein erweiterter Strafraum geplant (Art. 54–57 E-DSG, Art. 60–63 rev-DSG), womit sich die Rechtsdurchsetzung ein Stück weit verbessern wird.

FORSCHUNGSFRAGE: Wie könnte eine künftige Neuausrichtung des privatrechtlichen Datenschutzrechts aussehen, bei welcher die Rechtsdurchsetzung ex ante und ex post im Zusammenhang mit People Analytics besser gewährleistet wäre als heute?

Die Defizite in der gegenwärtigen Rechtsdurchsetzung machen eine Neuausrichtung des Datenschutzrechts notwendig. Vorliegend wird vorgeschlagen, die Durchsetzung des Datenschutzes mittels einer Professionalisierung und Demokratisierung zu gewährleisten. Es handelt sich hierbei um ein umfassendes Konzept, das auch einen Mentalitätswandel in dem Sinne einschliesst, dass dem Datenschutzrecht allgemein ein höherer Stellenwert zugesprochen werden muss.

Unter dem Begriff der Professionalisierung wird jede Massnahme verstanden, die die Arbeitgeberin dazu veranlasst, das Datenschutzrecht ab Beginn der Datenbearbeitung zu befolgen, sodass die Rechtsdurchsetzung im Zusammenhang mit People Analytics gewährleistet ist. Hauptsächlich geht es um die Rechtsbefolgung *ex ante*, aber auch Mittel zur Durchsetzung des Rechts im Anschluss an eine Datenschutzverletzung (*ex post*) werden im Rahmen der Professionalisierung vorgeschlagen. Mit der Professionalisierung wird das Vertrauen in die Datenwirtschaft und das Datenschutz-Rechtssystem gewonnen.

Im Sinne einer Professionalisierung kommt eine stärkere Inpflichtnahme der Arbeitgeberin als Datenbearbeiterin infrage. Im rev-DSG sind gewisse professionalisierende Schritte vorgezeichnet, etwa die Pflicht zum Datenschutz sowohl durch

Technik als auch durch datenschutzfreundliche Voreinstellungen (Art. 6 E-DSG, Art. 7 rev-DSG), die Pflicht zur Datenschutz-Folgenabschätzung (Art. 20 E-DSG, Art. 22 rev-DSG) und die freiwillige Ernennung eines Datenschutzberaters (Art. 9 E-DSG, Art. 10 rev-DSG). Auch die Förderung von Verhaltenskodizes (Art. 10 E-DSG, Art. 11 rev-DSG) und Zertifizierungen (Art. 11 DSG, Art. 12 E-DSG, Art. 13 rev-DSG) wirkt sich professionalisierend aus. Zudem sind die Pflicht zur Führung eines Verzeichnisses der Bearbeitungstätigkeiten (Art. 11 E-DSG, Art. 12 rev-DSG), eine Informationspflicht (Art. 17 E-DSG, Art. 19 rev-DSG) und die Pflicht zur Meldung von Verletzungen der Datensicherheit vorgesehen (Art. 22 E-DSG, Art. 24 rev-DSG).

Nach vorliegend vertretener Ansicht sind aber noch weitere Professionalisierungsmassnahmen geboten, die über das Minimum gemäss rev-DSG hinausgehen: Hierzu zählen die Einführung einer Rechenschaftspflicht, eine konkretere Diskriminierungsbekämpfung (z.B. durch Aufnahme von Quotierungszielen in der Algorithmenprogrammierung) und entweder verpflichtende oder gezielt geförderte freiwillige Schulungen.

Neben dem Vertrauen in das Rechtssystem ist auch eine stärkere Kontrolle der Rechtmässigkeit der Datenflüsse erforderlich, welche über eine Demokratisierung des Datenschutzrechts erreicht werden kann. Der Begriff der Demokratisierung bedeutet jede Massnahme, welche den der Arbeitgeberin entgegengesetzten Parteien Kontrollrechte einräumt, um auf die Einhaltung des Datenschutzrechts hinzuwirken, sodass die Rechtsdurchsetzung im Zusammenhang mit People Analytics gewährleistet ist. Demokratische Kontrollrechte betreffen vorwiegend die Rechtsdurchsetzung *ex post*, doch ist auch an die Rechtsdurchsetzung *ex ante* zu denken.

Hinsichtlich einer Demokratisierung könnten neben dem einzelnen Arbeitnehmer weitere Parteien, namentlich die Arbeitnehmervertretung, verschiedene Behörden und die Zivilgesellschaft, an der Rechtsdurchsetzung beteiligt werden. Damit könnte der Durchsetzungsmechanismus des Datenschutzrechts auf mehrere Säulen abgestützt werden, was dem System als Ganzem Stabilität verleihen würde. Es ist zu begrüessen, dass mit der Totalrevision des DSG die Kompetenzen des EDÖB (Art. 43 ff. E-DSG, Art. 49 ff. rev-DSG) und der Strafbehörden ausgeweitet werden (Art. 54 ff. E-DSG, Art. 60 ff. rev-DSG).

Doch Demokratisierung bedeutet mehr als das, was das rev-DSG vorsieht: Eine Stärkung der Mitwirkungsrechte der Arbeitnehmervertretung durch den Gesetzgeber und durch Gesamtarbeitsverträge sind erforderlich. Der Staat könnte seine Rolle noch aktiver ausgestalten, wenn er als Diskursmoderator die Interessenver-

treter zusammenführen und die Gesellschaft über die Risiken der Datenbearbeitungen aufklären würde. Jedoch ist zu hinterfragen, ob der EDÖB für diese beratend-moderierende Tätigkeit die geeignete Behörde wäre oder ob hierfür nicht dezentralere Organisationen geschaffen werden sollten. Die Zivilgesellschaft könnte ins Boot geholt werden durch die Einführung einer ideellen Verbandsklage im Datenschutzrecht und durch Investitionen in die Bildung und die Digitalkompetenz der breiten Bevölkerung. Ferner sind Verfahren zur Begutachtung von Algorithmen denkbar, wobei als begutachtende Instanzen sowohl privatrechtliche Organisationen als auch eine staatliche Stelle infrage kommen.

Abschliessend ist festzuhalten, dass People Analytics nicht nur rechtlich, sondern wegen der vielen involvierten Personen auch zwischenmenschlich ein hochkomplexes Thema ist. Die Unternehmen, die People Analytics anwenden, sollten daher eine ganzheitliche Sicht einnehmen. Etwas, das rechtlich erlaubt ist, kann sozial inakzeptabel sein. Um abschätzen zu können, wie eine neue Datenbearbeitungspraxis bei den Arbeitnehmern ankommt, muss die Arbeitgeberin in regem Austausch mit der Belegschaft stehen. Es ist daher eminent wichtig, dass die Mitwirkungsrechte im Unternehmen aktiv gelebt werden. Von den Programmierern bis hinauf zu den Verwaltungsräten sollten alle darauf achten, verschiedene, auch kritische Meinungen zu People Analytics zuzulassen. Es muss sichergestellt werden, dass die Rechte der Arbeitnehmer nicht nur formell gewahrt werden, sondern dass sich die Menschen auch als vollberechtigte, autonom handelnde Subjekte fühlen. Nur auf diese Weise wird ein People Analytics-Projekt von allen im Unternehmen Unterstützung erfahren und letztlich Erfolg haben.

Schriften zum Recht der neuen Technologien
Etudes du droit des nouvelles technologies
Legal Studies on New Technologies

Band 1 Joel Drittenbass

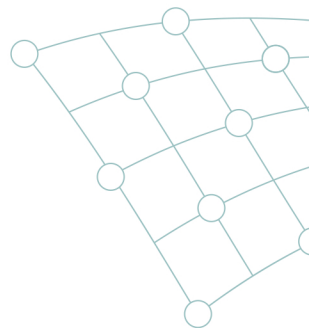
Regulierung von autonomen Robotern

Angewendet auf den Einsatz von autonomen Medizinrobotern: Eine datenschutzrechtliche und medizinproduktrechtliche Untersuchung

2021. 526 Seiten, gebunden, CHF 110.—

SCHRIFTEN ZUM RECHT DER NEUEN TECHNOLOGIEN ETUDES DU DROIT DES NOUVELLES TECHNOLOGIES LEGAL STUDIES ON NEW TECHNOLOGIES

Das Recht der neuen Technologien ist das Recht der nächsten Gesellschaft. Es reflektiert die wachsenden Verbindungen von Informations- und Kommunikationstechnologien mit weiteren Anwendungsfeldern der Lebens-, Medizin-, Gesundheits- und Kognitionswissenschaften. Diese Konvergenzen bilden die Grundlage dafür, die Rechtsgebiete des Informations- und Medienrechts, des Gesundheits- und Medizinrechts sowie des Umwelt- und Technikrechts einem eigenständigen Themenbereich zuzuordnen. Das Recht der neuen Technologien soll die rechtswissenschaftliche Grundlagenforschung einbeziehen und den interdisziplinären Austausch mit technologischer Innovationsorientierung verknüpfen. Mit den «Schriften zum Recht der neuen Technologien» werden zukunftsgestaltende Forschungsergebnisse der Wissenschaft, Praxis und Gesellschaft zugänglich gemacht.



People Analytics in privatrechtlichen Arbeitsverhältnissen

Mit People Analytics werten Arbeitgeber systematisch ihr Humankapital aus, um den Unternehmenswert zu steigern. Dabei begegnen sie datenschutz- und arbeitsrechtlichen Herausforderungen: Sie müssen etwa das Gesetz risikoorientiert anwenden; ferner bilden Einwilligungen des Arbeitnehmers ein fragiles Rechtfertigungsfundament für Datenbearbeitungen.

Rechtspraktiker, Personal- und IT-Verantwortliche finden in diesem Buch neben Antworten auf ihre Fragen zum Thema auch empirische Daten aus einer branchenübergreifenden Studie. Auf einer übergeordneten Ebene plädiert die Dissertation für eine Professionalisierung und Demokratisierung des Datenschutzrechts – mit dem Ziel einer besseren Rechtsdurchsetzung in der Praxis. Das topaktuelle Werk berücksichtigt neben dem geltenden auch das künftige, totalrevidierte Datenschutzgesetz, die EU-Datenschutz-Grundverordnung und Aspekte des US-Datenschutzrechts.

Die Dissertation hat den Stefano Rodotà-Award des Europarats und den Professor Walther Hug-Preis gewonnen.

Dike Verlag, Zürich/St. Gallen
ISBN 978-3-03891-273-6



Nomos Verlag, Baden-Baden
ISBN 978-3-8487-8262-8



dike.ch