Digitalisierung und Privatsphäre im Arbeitsverhältnis

Rechtliche Grundlagen und aktuelle Problemfelder

Christine Kaufmann
Res Schuerch

Bern, 1. September 2021

Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR)
Centre suisse de compétence pour les droits humains (CSDH)
Centro svizzero di competenza per i diritti umani (CSDU)
Swiss Center of Expertise in Human Rights (SCHR)

Schanzeneckstrasse 1, Postfach, 3001 Bern
Telefon +41 31 631 86 51, skmr@skmr.unibe.ch

AUTORENVERZEICHNIS

Christine Kaufmann

Prof. Dr. iur., Professorin für öffentliches Recht, Völker- und Europarecht, Universität Zürich

Res Schuerch

Dr. iur., Geschäftsführer, Kompetenzzentrum für Menschenrechte (MRZ), Universität Zürich

Zitiervorschlag: SCHWEIZERISCHES KOMPETENZZENTRUM FÜR MENSCHENRECHTE (SKMR), Digitalisierung und Privatsphäre im Arbeitsverhältnis. Rechtliche Grundlagen und aktuelle Problemfelder, verfasst von Kaufmann Christine/ Schuerch Res, Bern 2021.

INHALTSVERZEICHNIS

Abkürzungsverzeichnis VI
Zusammenfassung 1
I. Einleitung 5
1. Der Schutz der Privatsphäre am Arbeitsplatz im digitalen Zeitalter 5
2. Ziel der Studie 6
3. Methodik und Aufbau 6
II. Das Recht auf Privatsphäre am Arbeitsplatz im Zeitalter der Digitalisierung 8
1. Das Grundrecht- und Menschenrecht auf Privatsphäre 8
2. Die digitale Transformation am Arbeitsplatz 10
2.1. Industrielle Revolution 4.0 10
2.2. Das digitale Ökosystem – Definitionen 11
2.2.1. Algorithmus 11
2.2.2. Big Data Analysen 11
2.2.3. Cloud-Computing 12
2.2.4. Internet of Things 12
2.2.5. Künstliche Intelligenz 13
3. Internationale Rechtsgrundlagen 15
3.1. Vereinte Nationen (UNO) 15
3.1.1. Allgemeines 15
3.1.2. Art. 17 UNO Pakt II 17
3.1.3. Art. 7 UNO Pakt I 18
3.1.4. Der UNO-Sonderberichterstatter zum Recht auf Privatsphäre 19
3.1.5. Fazit 20
3.2. Europarat 21
3.2.1. Allgemeines 21
3.2.2. Europäische Menschenrechtskonvention (EMRK) 21
3.2.3. Datenschutzkonvention 108 24
3.2.4. Empfehlungen des Ministerkomitees 26
3.2.5. Fazit 29
3.3. Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) 30
3.3.1. Allgemeines 30
3.3.2. OECD-Leitsätze für multinationale Unternehmen 30
3.3.3. Privacy Guidelines 31
3.3.4. Weitere Entwicklungen 32
3.3.5. Fazit 33
3.4. Europäische Union (EU) 34
3.4.1. Allgemeines 34
3.4.2. Art. 7 und Art. 8 Charta der Grundrechte (GRC) 35
3.4.3. Datenschutz-Grundverordnung (DSGVO) 36
3.4.4. Art. 31 Charta der Grundrechte (GRC) 39
3.4.5. Ethik-Leitlinien für eine Vertrauenswürdige KI 40
3.4.6. Fazit 41
4. Rechtsgrundlagen in der Schweiz 41
4.1. Bundesverfassung (BV) 41
4.2. Das Datenschutzrecht 43
4.2.1. Allgemeines 43
4.2.2. Datenschutzgesetz (DSG) und revidiertes Datenschutzgesetz (N-DSG) 44

4.3. Das Arbeitsrecht ... 47
4.3.1. Allgemeines ... 47
4.3.2. Fürsorgepflicht der Arbeitgebenden (Art. 328/328b OR) ... 47
4.4. Fazit ... 49
III. Szenarien – Digitalisierung und Privatsphäre am Arbeitsplatz ... 50
1. Einleitung ... 50
2. Szenario 1: Informationsbeschaffung im Internet/in sozialen Netzwerken während des Bewerbungsverfahrens ... 50
2.1. Sachverhalt ... 50
2.2. Relevanz und Problembereiche ... 51
2.3. Grund- und menschenrechtliche Fragestellungen ... 52
2.4. Rechtliche Beurteilung ... 52
2.4.1. Rechtliche Grundlagen ... 52
2.4.2. Internetrecherche ... 53
2.4.3. Soziale Medien ... 55
A. Freizeitliche Soziale Medien ... 55
B. Berufliche Soziale Medien ... 57
2.5. Fazit ... 57
3. Szenario 2: Verwendung von Algorithmen und KI im Bewerbungsverfahren ... 58
3.1. Sachverhalt ... 58
3.2. Relevanz und Problembereiche ... 59
3.3. Grund- und menschenrechtliche Fragestellungen ... 60
3.3.1. Algorithmen-gestützte Internet-Datenanalysen ... 60
3.3.2. KI-Systeme im Rahmen von Anstellungsinterviews ... 60
3.4. Rechtliche Beurteilung ... 61
3.4.1. Algorithmengestützte Datenanalysen ... 61
3.4.2. Verwendung von KI-Systemen im Rahmen von Anstellungsinterviews ... 62
3.5. Fazit ... 63
4. Szenario 3: Überwachungs- und Kontrollsysteme am Arbeitsplatz ... 63
4.1. Sachverhalt ... 63
4.2. Relevanz und Problembereiche ... 64
4.3. Grund- und menschenrechtliche Fragestellungen ... 64
4.4. Rechtliche Beurteilung: ... 65
4.4.1. Rechtliche Grundlagen ... 65
4.4.2. Internetverhalten und E-Mailverkehr ... 66
4.4.3. Videosysteme ... 69
4.4.4. Geolokalisierung ... 71
4.4.5. Biometrie am Arbeitsplatz ... 73
4.4.6. Fazit 74
5. Szenario 4: Arbeitsplatzspezifische Wearables ... 75
5.1. Sachverhalt ... 75
5.2. Relevanz und Problembereiche ... 76
5.3. Grund- und menschenrechtliche Fragestellungen ... 77
5.4. Rechtliche Beurteilung ... 77
5.5. Fazit ... 79
6. Szenario 5: Die Telearbeit – Emanzipation der Arbeit von Arbeitszeit und Arbeitsort ... 79
6.1. Sachverhalt ... 79
6.2. Relevanz und Problembereiche ... 80

6.3. Grund- und menschenrechtliche Fragestellungen 81
6.4. Rechtliche Beurteilung 81
6.4.1. Rechtliche Grundlagen des Home-Office 81
6.4.2. Entgrenzung zwischen Beruflichem und Privatem 82
6.4.3. Arbeitszeiterfassung 82
6.5. Fazit 83
7. Szenario 6: Bring Your Own Device (BYOD) 84
7.1. Sachverhalt 84
7.2. Relevanz und Problembereiche 84
7.3. Grund- und menschenrechtliche Fragestellungen 85
7.4. Rechtliche Beurteilung 85
7.5. Fazit 87
IV. Schlussbemerkungen 88
Literaturverzeichnis 90
Literatur 90
Amtliche Publikationen 100
Entscheidverzeichnis 108
Normtexte 110

ABKÜRZUNGSVERZEICHNIS

ABl	Amtsblatt der Europäischen Union
Abs.	Absatz
AEMR	Allgemeine Erklärung der Menschenrechte vom 10.12.1948
AEUV	Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung), ABl C 326 vom 26.10.2012, S. 47-388
AI/KI	Artificial Intelligence/Künstliche Intelligenz
AI-HLEG	High Level Expert Group on Artificial Intelligence/Hochrangige Expertengruppe zu Künstlicher Intelligenz
ArG	Bundesgesetz über die Arbeit in Industrie, Gewerbe und Handel vom 13.03.1964, SR 822.11
ArGV1	Verordnung 1 zum Arbeitsgesetz vom 10. Mai 2000, SR 822.111
ArGV3	Verordnung 3 zum Arbeitsgesetz (Gesundheitsschutz) vom 18.08.1993, SR 822.113
Art.	Artikel
ATS	applicant tracking system
BGer	Bundesgericht
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BRK	Übereinkommen über die Rechte von Menschen mit Behinderungen vom 13.12.2006, SR 0.109
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18.04.1999, SR 101
CAHAI	Ad-hoc Ausschuss für künstliche Intelligenz (Ad hoc Committee on Artificial Intelligence)
COVID-19	corona virus disease 2019 (Corona-Virus)
d.h.	das heisst
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
DSG	Bundesgesetz über den Datenschutz vom 19.07.1992, SR 235.1
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, ABl L 119 vom 04.05.2016, S. 1-88 (Datenschutz-Grundverordnung).
ECOSOC	Economic and Social Council (Wirtschafts- und Sozialrat der Vereinten Nationen)
ed./eds.	editor/editors oder Auflage(n)

EDÖB	Eidgenössischer Datenschutzbeauftragter
EDV	elektronische Datenverarbeitung
EGMR/ECtHR	Europäischer Gerichtshof für Menschenrechte/European Court of Human Rights
EK	Europäische Kommission
EMRK/ECHR	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 04.11.1950, SR 0.101/European Convention on Human Rights and Fundamental Freedoms, 04.11.1950, ETS No. 005
ESC	(revidierte) Europäische Sozialcharta vom 03.05.1996, SEV Nr. 163.
et al.	und andere
EU	Europäische Union
EuGH	Europäischer Gerichtshof
f./ff.	folgende/fortfolgende
Fn.	Fussnote
GAV	Gesamtarbeitsvertrag
GCh	Gemeinschaftscharta der Sozialen Grundrechte der Arbeitnehmer vom 09.12.1989, Kom (89) 248 endg.
GRC	Charta der Grundrechte der Europäischen Union, 2000/C 364/01, ABl C 364 vom 18.12.2000, S. 1-22
HArG	Bundesgesetz über die Heimarbeit vom 20.03.1981, SR. 822.31
HRC	Human Rights Council (Menschenrechtsrat)
Hrsg.	Herausgeberinnen und Herausgeber
IERC	European Research Cluster on the Internet of Things
ILO	International Labour Organisation (International Arbeitsorganisation)
insb.	insbesondere
IoT	internet of things (Internet der Dinge)
i.S.v.	im Sinne von
IT	Informationstechnologie
ITU	International Telecommunication Union (Internationale Fernmeldeunion)
i.V.m.	in Verbindung mit
lit.	litera
ML	maschinelles Lernen
MRA	Menschenrechtsausschuss (Human Rights Committee)
m.w.H.	mit weiteren Hinweisen
N-DSG	verabschiedete, totalrevidierte neue Fassung des Datenschutzgesetzes vom 25.09.2020, BBl 2020, S. 7639ff.

NKP/NCP	Nationaler Kontaktpunkt/National Contact Point
N./No./Nr.	number/Nummer
OECD	Organisation for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
OGer	Obergericht
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30.03.1911, SR 220
RBC	responsible business conduct
RFID	radio frequency identification
Rz.	Randziffer
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SBG	Schweizerischer Gewerkschaftsbund
SECO	Staatssekretariat für Wirtschaft
SEV	Sammlung Europäischer Verträge
sog.	sogenannte
SKMR	Schweizerisches Kompetenzzentrum für Menschenrechte
SR	Systematische Sammlung des Bundesrechts
StGB	Schweizerisches Strafgesetzbuch vom 21.12.1937, SR 311
u.a.	unter anderem/und andere
UN/UNO	United Nations Organisation (Vereinte Nationen)
UNGA	United Nations General Assembly (Generalversammlung der Vereinten Nationen)
UNGP	UN Guiding Principles on Business and Human Rights (UN-Leitprinzipien zu Wirtschaft und Menschenrechten)
UNO Pakt I	Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte vom 16.12.1966, SR 0.103.1
UNO Pakt II	Internationaler Pakt über bürgerliche und politische Rechte vom 16.12.1966, SR 0.103.2
VDI	virtual desktop infrastructure (Infrastruktur virtueller Desktops)
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14.06.1993, SR 235.11
Vgl.	vergleiche
VPN	virtual private network
z.B.	zum Beispiel
ZBG	Schweizerisches Zivilgesetzbuch vom 10.12.1907, SR 210

Ziff.	Ziffer

ZUSAMMENFASSUNG

Das (wenig beachtete) Recht auf Privatsphäre am digitalisierten Arbeitsplatz

Das Recht auf Schutz der Privatsphäre eines Menschen ist ein anerkanntes Grund- und Menschenrecht. Es gibt jeder Person ein Mindestmass an Privatheit, damit sie sich in ihrer Persönlichkeit ungestört entwickeln und entfalten kann. Staaten haben zum einen die Pflicht, dieses Recht zu achten und zu gewährleisten. Zum anderen müssen sie Individuen auch vor Menschenrechtsverletzungen durch Dritte schützen. Dies gilt ebenso für das Verhältnis zwischen Arbeitgebenden und Arbeitnehmenden, das durch eine strukturelle Machtasymmetrie charakterisiert ist; Arbeitnehmende bedürfen deshalb eines Schutzes.

Im Kontext der Digitalisierung steht diesem individuellen Schutzbedürfnis das Interesse von Arbeitgebenden gegenüber, digitale Technologien zur Optimierung von Wertschöpfungs- und Kommunikationsprozessen, zum Schutz der Sicherheit der Mitarbeitenden sowie der Produktionsmittel oder zur Kontrolle von Arbeitnehmenden einzusetzen.

Der digitale Wandel bringt zudem eine Diversifizierung von Arbeitsmodellen mit sich, die eine orts- und/oder zeitunabhängige Arbeit ermöglichen und potenziell ebenfalls vielseitige Konsequenzen hinsichtlich der Trennung von Berufs- und Privatleben haben. Beispiele sind das aktuell durch die COVID-19-Pandemie stärker genutzte Home-Office, aber auch die mobile Arbeit und neue Formen der Plattformökonomie.

Obwohl digitale Technologien vielfältige Auswirkungen auf den Schutz der Privatsphäre in einem Arbeitsverhältnis haben können, wird diesem Thema in laufenden Digitalisierungsdiskursen in der Schweiz kaum Beachtung geschenkt. Die vorliegende Studie hat deshalb das Ziel, einen Beitrag zur Schliessung dieser Forschungslücke zu leisten.

Internationale Rechtsgrundlagen

Auf internationaler Ebene ist das Recht auf Privatsphäre in unterschiedlichen, für die Schweiz verbindlichen, Rechtsgrundlagen verankert, u.a. in Art. 8 der Europäischen Menschenrechtskonvention (EMRK) und Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte (UNO Pakt II). Diverse weitere internationale und regionale Institutionen – wie z.B. der UNO-Sonderberichterstatter zum Recht auf Privatsphäre, der Europarat oder die OECD – konkretisieren die datenschutzrechtlichen Erwartungen an einzelne Staaten, wenn es um die Bearbeitung von Personendaten im digitalen Zeitalter allgemein, d.h. nicht nur am Arbeitsplatz, geht. Relevante arbeitsrechtliche Grundlagen sind insbesondere in Art. 7 des Internationalen Pakts über wirtschaftliche, soziale und kulturelle Rechte (UNO Pakt I) enthalten.

Die staatliche Schutzpflicht zum Recht auf Privatsphäre im digitalen Zeitalter beinhaltet, zumindest nach bisheriger Praxis internationaler Überwachungsorgane, keine grundsätzlichen Änderungen gegenüber der Schutzpflicht in der analogen Welt. Demnach haben Staaten mittels gesetzlicher, administrativer, organisatorischer, technischer und anderweitiger Massnahmen für einen genügenden Schutz der Privatsphäre zu sorgen. Eingriffe müssen den üblichen Einschränkungsvoraussetzungen standhalten.

Datenbearbeitungen am Arbeitsplatz in der Schweiz

In der Schweiz beinhaltet Art. 13 der Bundesverfassung (BV) einen grundrechtlichen Anspruch auf Achtung der Privatsphäre einschliesslich des Datenschutzes. Eine Reihe von arbeits- und datenschutzrechtlichen Gesetzen und Verordnungen konkretisiert diesen Schutz im Beschäftigungskontext, allen voran das Arbeitsgesetz (ArG) und das Datenschutzgesetz (DSG).

In allgemeiner Weise wird die Verantwortung von Arbeitgebenden für Arbeitnehmende von der sog. Arbeitgeberfürsorgepflicht (Art. 328 und 328b OR) erfasst. Im Rahmen dieser haben Arbeitgebende die Pflicht, die Privatsphäre und Persönlichkeit von Arbeitnehmenden zu achten und Massnahmen zu deren Schutz zu treffen. Weitere arbeitsrechtlich relevante Bestimmungen für die vorliegende Untersuchung sind Art. 6 ArG (Gesundheitsschutz) sowie Art. 26 ArGV3 (Überwachungs- und Kontrollsysteme).

Darüber hinaus sind die Grundsätze des Datenschutzgesetzes – insbesondere Zweckbindung, Verhältnismässigkeit und Transparenz – im Zusammenhang mit Datenbearbeitungen in Beschäftigungsverhältnissen von Bedeutung. Werden diese Grundsätze verletzt, liegt eine Persönlichkeitsverletzung nach Art. 12 Abs. 2 lit. a DSG vor. Eine solche ist widerrechtlich, wenn die betreffende Datenverarbeitung nicht durch Einwilligung der betroffenen Person, ein überwiegendes privates/öffentliches Interesse oder durch das Gesetz gerechtfertigt ist (Art. 13 DSG). Datenbearbeitungen von personenbezogenen Daten sind in der Schweiz somit grundsätzlich erlaubt, und es bedarf für eine solche keiner vorgängigen Einwilligung der betroffenen Person. Das gilt selbst dann, wenn besonders schützenswerte Personendaten bearbeitet oder Persönlichkeitsprofile erstellt werden.

Divergierende Interessen von Arbeitgebenden und Arbeitnehmenden

Die Verwendung von digitalen Technologien am Arbeitsplatz bringt zum einen die Herausforderung mit sich, dass mit solchen Technologien ein praktisch unbegrenztes Potenzial zur Datenverarbeitung einhergeht. Zum anderen besteht die Gefahr, dass im Rahmen von Datenverarbeitungsprozessen nicht nur geschäftliche Daten erhoben werden, sondern auch personenbezogene private Daten. Art. 328b OR sieht deshalb vor, dass alle Datenbearbeitungen in einem Beschäftigungsverhältnis die Eignung von Arbeitnehmenden betreffen oder für die Durchführung des Arbeitsvertrags erforderlich sein müssen. Je grösser das Risiko für die Privatsphäre der Arbeitnehmenden, desto überzeugender müssen zudem die betrieblichen Interessen sein, um den Einsatz einer Technologie zu rechtfertigen. Höhere Anforderungen gelten, wenn die Datenbearbeitung besonders schützenswerte Personendaten betrifft (wie z.B. Gesundheitsdaten) oder Persönlichkeitsprofile erstellt werden.

Digitale Technologien am Arbeitsplatz

Um die Relevanz des Rechts auf Privatsphäre am Arbeitsplatz zu untersuchen, werden ausgewählte, mit der Digitalisierung im Zusammenhang stehende Szenarien des Beschäftigungsverhältnisses einer rechtlichen Beurteilung unterzogen:

(1) Informationsbeschaffung im Internet/in sozialen Netzwerken während des Bewerbungsverfahrens

(2) Verwendung von Algorithmen und künstlicher Intelligenz (KI) im Bewerbungsverfahren

(3) Überwachungs- und Kontrollsysteme am Arbeitsplatz

(4) Arbeitsplatzspezifische Wearables

(5) Die Telearbeit – Emanzipation der Arbeit von Arbeitszeit und Arbeitsort

(6) Bring Your Own Device (BYOD)

Bei der Auswahl der Technologien wurde darauf geachtet, sowohl aktuelle als auch zukünftig relevante Technologien in die Szenarien einzubeziehen, einschliesslich Internet, Videosysteme, GPS, auf Biometrie basierte Systeme, Wearables und weitere «intelligente» algorithmische Anwendungen. Bereits «ältere» Technologien, wie z.B. die Telefonüberwachung, wurden hingegen ausgeklammert.

Herstellung des Praxisbezugs

Um den Praxisbezug zu gewährleisten, wurden die Szenarien in Konsultation mit relevanten Beteiligten im Bereich der Beschäftigung – privat- und öffentlich-rechtlichen Arbeitgebenden, Arbeitgebendenverbänden, Gewerkschaften und Datenschutzbeauftragten – erörtert und kritisch hinterfragt. In diesen Befragungen zeigten sich erhebliche Unterschiede, ob, wie und weshalb einzelne Technologien von Arbeitgebenden eingesetzt werden. Die ausgewählten Szenarien werden in der vorliegenden Studie deshalb in einer verallgemeinerten Form wiedergegeben. Die Untersuchung stellt die Beantwortung der mit dem Einsatz von Technologien am Arbeitsplatz verbundenen Rechtsfragen in den Vordergrund, weshalb ein anwendungs- und nicht ein technologiebasierter Ansatz verfolgt wird.

Chancen und menschenrechtliche Risiken

Die Untersuchung zeigt, dass die ausgewählten Technologien am Arbeitsplatz unterschiedliche Chancen und Risiken für die Privatsphäre der Arbeitnehmenden mit sich bringen. Im Vordergrund steht zum einen das damit verbundene Potenzial, praktisch unbegrenzt Daten zu erheben, zu verarbeiten, zueinander in Beziehung zu setzen und auszuwerten. Dabei ist es auch von Bedeutung, dass Technologien nicht, oder nur begrenzt, zwischen privaten und geschäftlichen Daten unterscheiden (können). Von dieser «technologischen Indifferenz» profitieren jene Arbeitgebenden, die mehr Informationen über ihre Arbeitnehmenden erhalten wollen, als dies für die Erfüllung eines Arbeitsverhältnisses notwendig wäre. Zum anderen fördert die Digitalisierung am Arbeitsplatz in indirekter Weise auch die Entgrenzung von Arbeit und Freizeit im Kontext von flexiblen Arbeitserfüllungsformen – z.B. beim Home-Office oder im Zusammenhang mit BYOD.

Nicht zuletzt aufgrund der aktuellen Erfahrungen im Rahmen der COVID-19-Massnahmen zeigt sich, dass jene Technologien, welche die Persönlichkeit und die Privatsphäre Einzelner tangieren können, digitale Arbeitsplätze und flexible Arbeitserfüllungsformen überhaupt erst möglich machen. Aus einer menschenrechtlichen Perspektive stellt sich deshalb die grundsätzliche Frage, wie die Vorteile digitaler Technologien bestmöglich genutzt werden können, ohne die Grund- und Menschenrechte Einzelner zu beeinträchtigen.

Dynamische Entwicklungen im Bereich des Datenschutzes

Trotz bestehenden nationalen und internationalen Rechtsgrundlagen in den Bereichen Privatsphäre, Datenschutz und Arbeitsrecht erschwert die hohe Geschwindigkeit der Technologieentwicklung es den Regulierungsbehörden, Rechtsgrundlagen in Echtzeit den aktuellen Herausforderungen anzupassen. Die rasche Nutzbarmachung neuer Technologien im Alltag und im Arbeitsleben offenbart deshalb immer wieder neue Anwendungsfälle, die noch nicht von bestehenden Normen erfasst sind und deshalb mittels Auslegung beurteilt werden müssen.

Das neue, noch nicht in Kraft getretene, DSG (N-DSG) sowie die für die Schweiz ebenfalls relevante EU-Datenschutz-Grundverordnung (DSGV) versuchen dieser Dynamik gerecht zu werden. Wie bislang beinhalten diese Regelwerke Instrumente, um die Rechtmässigkeit von Datenbearbeitungen *ex post* zu analysieren und die betroffenen Personen bei der Durchsetzung ihrer Rechte zu unterstützen. Zudem gibt es immer mehr Ansätze, die verlangen, den Datenschutz *ex ante* bereits im Rahmen der Technikgestaltung (*privacy by design*) und den Datenschutz-Voreinstellungen angemessen zu berücksichtigen (*privacy by default*). Ergänzt werden diese Instrumente durch eine sog. Datenschutz-Folgenabschätzung (*privacy impact assessment*) für Datenbearbeitungen, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen.

I. EINLEITUNG

1. Der Schutz der Privatsphäre am Arbeitsplatz im digitalen Zeitalter

Künstliche Intelligenz, Big Data, Supercomputer, Internet of Things – die mit der Digitalisierung einhergehenden technologischen Entwicklungen bergen nebst einem unbestritten grossen Potenzial zu positiven Veränderungen unserer Lebensweise auch ernstzunehmende menschenrechtliche Risiken – u.a. für die Unversehrtheit der Privatsphäre einzelner Personen. Das Recht auf Schutz der Privatsphäre gewährt als anerkanntes Grund- und Menschenrecht jeder Person ein Mindestmass an Privatheit, damit sich diese in ihrer Persönlichkeit ungestört entwickeln und entfalten kann.[1]

Staaten haben nicht nur eine Pflicht, dieses Recht zu achten und zu gewährleisten, sondern müssen es auch vor Verletzungen durch Dritte schützen.[2] Das gilt auch für (privatrechtliche) Arbeitsverhältnisse, welche durch eine strukturelle Machtasymmetrie zwischen Arbeitgebenden und Arbeitnehmenden charakterisiert sind, so dass Letztere eines Schutzes bedürfen. Im Kontext der Digitalisierung steht diesem individuellen Schutzbedürfnis das Interesse von Arbeitgebenden gegenüber, digitale Technologien zur Optimierung von Wertschöpfungs- und Kommunikationsprozessen, zum Schutz der Sicherheit der Mitarbeitenden sowie der Produktionsmittel, oder zur Kontrolle von Arbeitnehmenden einzusetzen.

Im Bereich der Arbeit bringt der digitale Wandel zudem eine Diversifizierung von Arbeitsmodellen mit sich, welche eine orts- und/oder zeitunabhängige Arbeit ermöglichen. Flexible Arbeitsformen, welche oftmals auch im Interesse von Arbeitnehmenden liegen, können sich in vielfältiger Weise auf die Trennung von Berufs- und Privatleben auswirken und zu einer sogenannten Entgrenzung zwischen Arbeit und Freizeit führen.

Der Wandel hin zum dezentralen Arbeitsplatz wurde durch die im Zusammenhang mit der COVID-19 Pandemie ergriffenen Massnahmen und Empfehlungen für Home-Office beschleunigt. Gleichzeitig führte uns die Pandemie vor Augen, wie wichtig es ist, mit den digitalen Entwicklungen Schritt zu halten – zum einen um das damit verbundene Potenzial bestmöglich und zum Vorteil der gesamten Gesellschaft auszuschöpfen, zum andern, um den damit verbunden menschenrechtlichen Problemen besser begegnen zu können.

Auf internationaler Ebene ist das Recht auf Privatsphäre in unterschiedlichen für die Schweiz verbindlichen Rechtsgrundlagen, u.a. der Europäischen Menschenrechtskonvention (EMRK)[3] und dem Internationalen Pakt über bürgerliche und politische Rechte (UNO Pakt II)[4], verankert. Zudem konkretisieren weitere internationale und regionale Institutionen – wie z.B. der UNO-Sonderberichterstatter zum Recht auf Privatsphäre, der Europarat oder die OECD – datenschutzrechtliche Erwartungen an einzelne Staaten, wenn es um die Bearbeitung von Personendaten im digitalen Zeitalter (nicht nur am Arbeitsplatz) geht. Relevante arbeitsrechtliche Grundlagen sind z.B. im Internationalen Pakt über wirtschaftliche, soziale und kulturelle Recht (UNO Pakt I) zu finden.

---

1 KIENER/KÄLIN/WYTTENBACH, § 14, Rz. 2.

2 KIENER/KÄLIN/WYTTENBACH, §14, Rz. 10; SKMR, Das Recht auf Privatsphäre im digitalen Zeitalter, Rz. 11.

3 Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 04.11.1950, SR 0.101.

4 Internationaler Pakt über bürgerliche und politische Rechte vom 16.12.1966, SR 0.103.2.

In der Schweiz beinhaltet die Bundesverfassung einen grundrechtlichen Anspruch auf Achtung der Privatsphäre einschliesslich des Datenschutzes. Eine Reihe von arbeits- und datenschutzrechtlichen Gesetzen und Verordnungen konkretisiert diesen Schutz im Beschäftigungskontext. In allgemeiner Weise wird die Verantwortung von Arbeitgebenden Arbeitnehmenden gegenüber von der sog. Arbeitgeberfürsorgepflicht erfasst.[5] Im Rahmen dieser Pflicht müssen Arbeitgebende geeignete Massnahmen zur Achtung und zum Schutz der Privatsphäre und Persönlichkeit von Arbeitnehmenden ergreifen.

Trotz bestehenden nationalen und internationalen Rechtsgrundlagen in den Bereichen Privatsphäre, Datenschutz und Arbeitsrecht erschwert es die hohe Geschwindigkeit der Technologieentwicklung den Regulierungsbehörden, Rechtsgrundlagen in Echtzeit den aktuellen Herausforderungen anzupassen. Die rasche Nutzbarmachung neuer Technologien im Alltag und im Arbeitsleben offenbart deshalb immer wieder neue Anwendungsfälle, welche noch nicht explizit von bestehenden Normen erfasst sind und deshalb mittels Auslegung beurteilt werden müssen.

2. Ziel der Studie

Obwohl neue digitale Technologien beträchtliche Auswirkungen auf den Schutz der Privatsphäre im Verhältnis zwischen Arbeitgebenden und Arbeitnehmenden haben, wird diesem Thema in laufenden Digitalisierungsdiskursen in der Schweiz nur wenig Beachtung geschenkt. Vielmehr steht im Arbeitsmarkt- und Beschäftigungskontext im Vordergrund, wie der digitale Wandel die Beschäftigungsstruktur verändert und ob Arbeitsstellen durch die Digitalisierung verloren gehen oder zusätzlich geschaffen werden.[6] Zudem geht es um die Frage, in welche Richtung sich die Anforderungen an die Arbeitsbedingungen im digitalen Zeitalter verändern und wie der Schweizer Arbeitsmarkt die mit der Digitalisierung verbundenen Herausforderungen meistern und in einen positiven Nutzen umwandeln kann.[7] Ein weiterer Schwerpunkt liegt auf neuen atypischen Arbeitsformen, welche insbesondere im Zusammenhang mit digitalen Marktplätzen (Plattformökonomie oder Gig-Work) eine Rolle spielen.[8]

Da dem Schutz der Privatsphäre *im Arbeitsverhältnis* im Zeitalter der Digitalisierung in der rechtlichen Diskussion bislang vergleichsweise wenig Beachtung geschenkt wurde, will die vorliegende Studie einen Beitrag zur Schliessung dieser Forschungslücke leisten, indem sie für die Privatsphäre relevante und mit der Digitalisierung im Zusammenhang stehende Problemfelder im Kontext von Beschäftigungsverhältnissen einer rechtlichen Beurteilung unterzieht.

3. Methodik und Aufbau

Bestehende Rechtsgrundlagen zum Recht auf Privatsphäre weisen oftmals weder einen expliziten Digitalisierungs- noch Arbeitsplatzbezug auf. Dennoch gibt es eine Vielzahl datenschutz- und arbeitsrechtlicher Erlasse, welche relevante Bestimmungen sowohl zur digitalen Bearbeitung von

---

5 Vgl. Ziff. II.4.3.2.

6 So auch der Bericht des Bundesrates zu den Auswirkungen der Digitalisierung auf Beschäftigung und Arbeitsbedingungen: „Im Kontext der Digitalisierung steht aus arbeitsmarktpolitischer Sicht insbesondere die Frage im Zentrum, wie sich die Beschäftigung in Zukunft entwickeln wird. […] Für den Bundesrat ist es zentral, weiterhin eine möglichst hohe Erwerbsbeteiligung und gute Arbeitsbedingungen zu sichern» (BUNDESRAT, Auswirkungen der Digitalisierung, S. 4, 7).

7 BUNDESRAT, Auswirkungen der Digitalisierung, S. 5f.

8 SECO, Atypische Arbeitsverhältnisse, insb. S. 69ff.

personenbezogenen Daten am Arbeitsplatz als auch zum Schutz der Persönlichkeit und der Gesundheit von Arbeitnehmenden enthalten. Um diese Verflechtung unterschiedlicher Disziplinen den Leserinnen und Lesern möglichst anschaulich näher zu bringen, werden unterschiedliche Szenarien im Umfeld eines Beschäftigungsverhältnisses definiert, in welchen eine Verletzung der Privatsphäre durch die Anwendung digitaler Technologien möglich ist.

Die ausgewählten Szenarien wurden in Konsultation mit relevanten Akteuren im Bereich der Beschäftigung – privat- und öffentlich-rechtliche Arbeitgebende, Arbeitgeberverbände, Gewerkschaften und Datenschutzbeauftragte – erörtert und kritisch hinterfragt. Auf die Rückmeldungen der konsultierten Akteure wird innerhalb der einzelnen Szenarien unter dem Titel «Relevanz und Problembereiche» eingegangen.

Hinsichtlich der verwendeten Technologien haben die Konsultationen ergeben, dass es erhebliche Unterschiede gibt, ob, wie und weshalb spezifische Technologien von Arbeitgebenden eingesetzt werden. Die ausgewählten Szenarien werden in der vorliegenden Studie deshalb in einer verallgemeinerten Form wiedergegeben. Da die Untersuchung primär auf die mit dem Einsatz von Technologien am Arbeitsplatz verbundenen Rechtsfragen fokussiert, hat sich das Projektteam für einen anwendungs- und nicht technologiebasierten Ansatz entschieden. Deshalb wird z.B. bei algorithmischen Systemen, welche am Arbeitsplatz zum Einsatz kommen können, in technischer Hinsicht nicht nach dem «Grad der Intelligenz» unterschieden.[9]

Dennoch ist es für die Vollständigkeit der Analyse unabdingbar, sich mit gewissen technischen Grundlagen von digitalen Entwicklungen auseinanderzusetzen. Nach einer kurzen Einführung in die Thematik der Privatsphäre (Ziff. II.1), werden deshalb die für den Arbeitsplatz wichtigsten Begriffe des digitalen Ökosystems summarisch dargestellt (Ziff. II.2.2). Die Vermittlung dieser Grundbegriffe soll das Verständnis der in den Szenarien in Ziff. III behandelten technischen Methoden erleichtern. Anschliessend werden die für die Beantwortung der Rechtsfragen relevanten Rechtsgrundlagen auf internationaler (Ziff. II.3) und nationaler Ebene (Ziff. II.4) in den Bereichen Schutz der Privatsphäre, Datenschutz und Arbeitsrecht erläutert.

Im dritten Teil werden sechs ausgewählte arbeitsplatzspezifische Szenarien behandelt, in welchen digitale Technologien im Vordergrund stehen, die gegenwärtig, wie auch zukünftig in einem Beschäftigungskontext von Bedeutung sind/sein werden. Diese reichen vom Internet (Ziff. III.2, III.4, III.6, III.7), über unterschiedliche Überwachungs- und Kontrolltechnologien (Ziff. III.4 und III.5) hin zu «intelligenten» algorithmischen Systemen (Ziff. III.3, III.4, III.5). Mit Blick auf die rechtliche Beurteilung der Szenarien bleibt anzumerken, dass die Anwendbarkeit des bestehenden rechtlichen Rahmens *in der Schweiz* im Vordergrund steht; ergänzend erfolgen einzelfallspezifische Verweise auf internationale Normen und relevante Institutionen. Die Szenarien befassen sich zudem nur mit der möglichen Verletzung der Privatsphäre von *Arbeitnehmenden durch Arbeitgebende*. Nicht behandelt werden potenzielle Verletzungen der Privatsphäre von Arbeitnehmenden durch Drittparteien (z.B. Bewertung von Lehrpersonen durch Schulkinder, Bewertung von Uber-Fahrdienst durch Kundschaft etc.) oder von Arbeitgebenden gegenüber Drittparteien (z.B. unbefugte Weitergabe von Kundendaten).

[9] Siehe z.B. Ziff. III.3 und III.5.

II. DAS RECHT AUF PRIVATSPHÄRE AM ARBEITSPLATZ IM ZEITALTER DER DIGITALISIERUNG

1. Das Grundrecht- und Menschenrecht auf Privatsphäre

Historisch ist das heute in der Schweiz und in internationalen Rechtsgrundlagen verankerte Grund- und Menschenrecht auf Privatsphäre eng an die Verfügungsmacht über privates Eigentum[10] und das Recht, dass dieser persönliche Bereich frei von staatlichen Interventionen bleibt, gekoppelt.[11] Im Rahmen dieser Konzeption waren das Privateigentum und die Privatsphäre Einzelner von der staatlichen Sphäre sowie der Öffentlichkeit abzugrenzen.[12]

Für den Bereich der Arbeit bedeutete diese eigentumsgeprägte Herleitung, dass die Verfügungsberechtigten über die Produktionsmittel (d.h. die Arbeitgebenden) entscheiden konnten, in welchem Umfang den Arbeitnehmenden (persönliche) Rechte innerhalb des Arbeitsverhältnisses zukamen.[13] Ein Anspruch auf Wahrung der Privatsphäre der Arbeitnehmenden am Arbeitsplatz existierte nur, wenn die Eigentumsberechtigten der Produktionsanlagen dies auch zuliessen.

Dieses historische Verständnis der Privatsphäre hat sich im 20./21. Jahrhundert in kontinentaleuropäischen Rechtssystemen dahingehend gewandelt, dass private Sachverhalte als Teil der Persönlichkeitsrechte einer einzelnen Person unabhängig von Eigentum anerkannt sind.[14] Das Recht auf Privatsphäre entwickelte sich damit zu einem eigenständigen Grund- und Menschenrecht, bei welchem es im Kern um die Autonomie eines jeden Individuums geht, ohne fremde Einwirkung über die eigene Existenz entscheiden zu können.[15]

Dies hat nach heutigem Grundrechtsverständnis zur Folge, dass dem Recht auf Privatsphäre nicht nur eine Abwehrfunktion (gegen staatliche Eingriffe) zukommt; vielmehr besteht auch eine staatliche Pflicht, Individuen vor Menschenrechtsverletzungen durch Dritte zu schützen.[16] Eine Verletzung dieser staatlichen Schutzpflichten liegt vor, «[w]enn der Staat es *unterlässt* seine Rechtsordnung so auszugestalten, dass Übergriffe in grundrechtlich geschützte Rechtsgüter nicht verhindert bzw. sanktioniert werden können oder er solche Übergriffe gar ausdrücklich erlaubt […]».[17] Entsprechend legt Art. 35 Abs. 3 BV fest, dass «[d]ie Behörden [dafür] sorgen […], dass die Grundrechte, soweit sie sich dazu eignen, auch unter Privaten wirksam werden» (sog. horizontale Wirkung oder Drittwirkung der Grundrechte).[18]

---

[10] Vgl. HABERMAS, S. 64, 95f.

[11] Siehe FORD, S. 137, mit Verweis auf ein Zitat von Lord Justice Atkin: «*each house is a domain into which the king's writ does not seek to run and to which his officers do not seek to be admitted*» (Balfour v. Balfour [1919] 2KB 571, 579) und HABERMAS, S. 24. Bereits 1890 hatten Warren und Brandeis in ähnlicher Weise ein «*right to be let alone*» formuliert (WARREN UND BRANDEIS). Für eine detaillierte Herleitung des Rechts auf Privatsphäre im Allgemeinen, SCHIEDERMAIR, S. 23-41; für den amerikanischen Rechtskreis insbesondere, WACKS, S. 50ff.

[12] SCHIEDERMAIR, S. 36f.; zur Trennung zwischen Privatsphäre und öffentlicher Sphäre, Habermas, S. 24.

[13] Vgl. PÄRLI, Schutz der Privatsphäre, S. 50.

[14] WACKS, S. 62ff.; FORD, S. 137f.

[15] SCHABAS, Nowak's CCPR Commentary, S. 459.

[16] KIENER/KÄLIN/WYTTENBACH, § 4, Rz. 17.

[17] KIENER/KÄLIN/WYTTENBACH, § 4, Rz. 21 (Hervorhebung im Original).

[18] Siehe hierzu SCHWEIZER, N. 48ff.; MÜLLER, Art. 35 BV, S. 57ff.

Da private Akteure jedoch nicht die primären Adressaten der Grundrechte sind[19], richten sich die grund- und menschenrechtlichen Schutzpflichten des Staates *zunächst* an den *Gesetzgeber*.[20] In einem ersten Schritt ist der Staat deshalb dazu angehalten, dafür zu sorgen, dass der Schutz der Persönlichkeit und die Achtung der Privatsphäre gesetzlich geregelt werden und somit auch im privatrechtlichen Arbeitsverhältnis garantiert sind.[21] Im Bereich der Arbeit kommt diesen positiven Verpflichtungen des Staates eine grosse Bedeutung zu, da Beeinträchtigungen der Privatsphäre im Arbeitsverhältnis nicht nur, aber oftmals durch private Arbeitgebende erfolgen.

Bei einer Rechtsstreitigkeit unter Privaten können sich diese zwar nicht direkt auf die Grund- und Menschenrechte stützen, sie haben jedoch die Möglichkeit, sich auf die relevanten Gesetzesbestimmungen zu berufen, welche den grundrechtlichen Garantien zwischen Privaten Geltung verleihen. Private, welche Opfer privater Übergriffe geworden sind, haben somit das Recht, staatliche Instanzen aufzurufen. Sofern der (gerichtliche) Schutz durch den Staat *ungerechtfertigt* verweigert wird, ist aus *grundrechtlicher* Sicht der Staat verantwortlich und nicht der/die Private.[22]

Losgelöst vom Digitalisierungskontext stellt sich die Grundsatzfrage, in welchem Umfang das Recht auf Privatsphäre am Arbeitsplatz überhaupt Anwendung findet, da sich der Arbeitsplatz anders als etwa die eigene Wohnung nicht ohne weiteres als typische private Umgebung qualifizieren lässt. Hinzu kommt, dass das Arbeitsverhältnis zwar nicht mehr dieselbe eigentumsrechtliche Prägung wie früher aufweist, aber immer noch durch ein Subordinations- und Abhängigkeitsverhältnis zwischen Arbeitgebenden und Arbeitnehmenden und die damit verbundenen (vertraglichen) Weisungs- und Kontrollbefugnisse charakterisiert ist.[23]

Um den Schutzbereich des Rechts auf Privatsphäre im digitalen Zeitalter mit Blick auf das Arbeitsverhältnis bestimmen zu können, werden nachfolgend zunächst die internationalen und nationalen Rechtsgrundlagen zum Schutz der Privatsphäre und des Datenschutzes analysiert und es wird abgeklärt, inwieweit arbeitsrechtliche Bestimmungen ergänzend zur Anwendung kommen können (*infra* Ziff. 3 und 4). Zusätzlich werden Entwicklungen im Bereich des Soft Law und die Praxis/Empfehlungen relevanter Institutionen der UNO/EU/ILO/OECD in die Untersuchung miteinbezogen.

Vor dieser rechtlichen Analyse wird dargelegt, was die digitale Transformation am Arbeitsplatz als Teil der sog. «industriellen Revolution 4.0» überhaupt beinhaltet (*infra* Ziff. 2.1). Danach werden summarisch die relevanten Begriffe des digitalen Ökosystems erläutert, um den Leserinnen und Lesern ein Grundverständnis für jene Technologien zu vermitteln, welche in den vom Projektteam ausgewählten Szenarien unter Ziff. III eine Rolle spielen (*infra* Ziff. 2.2).

---

[19] Eine Ausnahme liegt in jenen Fällen vor, in welchen private Akteure staatliche Aufgaben wahrnehmen (Art. 35 Abs. 2 BV).

[20] KIENER/KÄLIN/WYTTENBACH, § 4, Rz. 17ff. und § 14, Rz. 10; MÜLLER, Art. 35 BV, S. 71f.

[21] KIENER/KÄLIN/WYTTENBACH, § 14, Rz. 10. Im EGMR-Verfahren ***Bărbulescu v. Romania***, worin es um die Überwachung von privater Korrespondenz eines Arbeitnehmenden durch einen privatrechtlichen Arbeitgebenden ging, hat der EGMR auf diese positive Verpflichtung des Staates in folgender Weise Bezug genommen: „*The Court observes that [the] State's positive obligations under Article 8 of the Convention are not adequately fulfilled unless it secures respect for private life in the relations between individuals by setting up a legislative framework taking into consideration the various interests to be protected in a particular context*» (Bărbulescu v Romania, 61496/08 (2017), Rz. 115).

[22] Ausführlich, KIENER/KÄLIN/WYTTENBACH, § 4, Rz. 77; siehe auch WEBER, Grundrechtskonzeption, S. 27f.

[23] HENDRICKX UND VAN BEVER, S. 185.

2. Die digitale Transformation am Arbeitsplatz

2.1. Industrielle Revolution 4.0

Digitale Technologien entwickeln sich in rasantem Tempo; Big Data, Blockchain, Supercomputer, künstliche Intelligenz (KI) und virtuelle Realität sind nur einige Schlagworte, welche den heutigen digitalen Wandel versinnbildlichen. Dieser Wandel findet weltweit statt und betrifft praktisch alle Lebensbereiche.

In einem wirtschaftlichen Kontext wird die umfassende Digitalisierung der Produktion unter dem Begriff *industrielle Revolution 4.0*[24] zusammengefasst. Im Gegensatz zur dritten industriellen Revolution, welche bereits durch eine Automatisierung von Produktionsprozessen mittels dem Einsatz von Elektronik und IT charakterisiert war, kommen jetzt die «Entwicklung intelligenterer Überwachungs- und autonomer Entscheidungsprozesse neu hinzu, um Unternehmen und ganze Wertschöpfungsnetzwerke in nahezu Echtzeit steuern und optimieren zu können».[25] Wichtige Treiber dieser fortgeschrittenen digitalen Transformation sind u.a.:[26]

- umfangreiche Datenmengen (Big Data – *infra* Ziff. 2.2.2)
- immer effizientere Datenverarbeitungsressourcen (*computing power* – *infra* Ziff. 2.2.3)
- die zunehmende Vernetzung von Informationen und physischen und virtuellen Objekten mit dem Internet und untereinander (*Internet of Things* – *infra* Ziff. 2.2.4)
- Fortschritte in der Robotik und Sensorik (*infra* Ziff. 2.2.4)
- die zunehmende Lernfähigkeit von auf Algorithmen basierten Systemen (*infra* Ziff. 2.2.1 und Ziff. 2.2.5)

Insbesondere aufgrund der grossen Geschwindigkeit, Reichweite sowie den damit verbundenen systemischen Auswirkungen sieht SCHWAB in der industriellen Revolution 4.0 nicht nur die blosse Fortsetzung der dritten industriellen Revolution, sondern assoziiert damit einen beispiellosen wirtschaftlichen Wandel.[27] Diese Transformation hat weitreichende Auswirkungen auf die Art der Produktion und unternehmensinterne Wertschöpfungsprozesse und bringt tiefgreifende Veränderungen für den Arbeitsmarkt und das gesamte Wirtschafts- und Sozialversicherungssystem mit sich.[28]

Bestehende Herausforderungen und Lösungsansätze für die Schweiz wurden vom Bund im Rahmen der Strategie «Digitale Schweiz» zusammengefasst.[29] Darin sind mit Blick auf den Beschäftigungskontext die Bedeutung der Innovationsförderung im Bereich der Forschung zu digitalen Technologien[30], die Flexibilität des Arbeitsmarktes, eine hochwertige Infrastruktur sowie eine exzellente Ausbildung[31] und der verantwortungsvolle Umgang mit Daten und KI[32] hervorgehoben. Im

---

[24] Vgl. KAGERMANN/LUKAS/WAHLSTER sowie SCHWAB.

[25] KAGERMANN/LUKAS/WAHLSTER.

[26] Vgl. BUNDESRAT, Auswirkungen der Digitalisierung, S. 11f.

[27] SCHWAB.

[28] Für einen Überblick über die Vielseitigkeit der Fragestellungen, welche sich im Zusammenhang mit der industriellen Revolution 4.0. ergeben, DUNAND/MAHON/WITZIG.

[29] BAKOM. Basierend auf diesen Erkenntnissen hat der Bund einen Aktionsplan mit Umsetzungsaktivitäten publiziert, abrufbar unter: https://www.digitaldialog.swiss/de/aktionsplan (zuletzt besucht am 20.04.2021).

[30] BAKOM, S. 6ff., 21.

[31] BAKOM, S. 21.

[32] BAKOM, S. 25ff.

Bereich KI hat der Bund zudem eine bundesinterne Arbeitsgruppe eingesetzt, welche «strategische Leitlinien für den Umgang mit den Herausforderungen der Künstlichen Intelligenz (KI) auf Ebene des Bundes» ausgearbeitet hat (weiterführend zu KI, *infra* Ziff. 2.2.5).[33] In seinem Bericht «Auswirkungen der Digitalisierung auf Beschäftigung und Arbeitsbedingungen – Chancen und Risiken» vom 8. November 2017[34], kommt der Bundesrat zum Schluss, «dass die Digitalisierung für den Schweizer Arbeitsmarkt sowohl mit Chancen als auch mit Risiken verbunden ist» und dass für die positive Bewältigung eines von der Digitalisierung getriebenen strukturellen Wandels die Rahmenbedingungen weiter optimiert werden müssen.[35]

2.2. Das digitale Ökosystem – Definitionen

2.2.1. Algorithmus

Ein Algorithmus basiert auf einer «Abfolge elementarer Schritte, die zur Erfüllung einer Aufgabe abgearbeitet werden müssen».[36] Solche Handlungsanweisungen können in unterschiedlicher Weise dargestellt werden, z.B. durch Sprache, Diagramme, Codes oder Programme.[37] In der Informatik wurden Algorithmen entwickelt, um repetitive und komplexe Berechnungen und Datenverarbeitungsaufgaben durchzuführen.[38] Unter Verwendung algorithmischer Anwendungen können Daten erhoben, kombiniert, bereinigt und eingeordnet werden.[39] Algorithmische Systeme können so in effizienter Weise Muster in grossen Datensätzen erkennen und durch Transformation von Daten(sätzen) in Informationen einen Mehrwert aus Daten generieren.[40] Basierend auf diesen Informationen nehmen Algorithmen je nach Programmierung eine Auswahl vor, formulieren Empfehlungen oder treffen Entscheidungen.[41]

⇨ Im Rahmen der vorliegenden Untersuchung spielen Algorithmen eine Rolle im Zusammenhang mit Big Data Analysen (*infra* Ziff. 2.2.2) sowie bei Anwendungen der künstlichen Intelligenz (sog. Algorithmen des maschinellen Lernens – *infra* Ziff. 2.2.5). Im Bereich von Beschäftigungsverhältnissen kommen algorithmische Systeme vor allem dort vor, wo automatisierte Vorgänge eine manuelle Tätigkeit ersetzen oder unterstützen – u.a. beim Profiling (Ziff. III.3), bei der Überwachung (Ziff. III.4) oder der Verwendung von Wearables (Ziff. III.5).

2.2.2. Big Data Analysen

Der Begriff «Big Data» bezieht sich auf Daten(sätze), welche sich durch ein hohes Volumen, eine hohe Geschwindigkeit und eine grosse Vielfalt auszeichnen sowie auf die Fähigkeit, diese Daten

---

33 BUNDESRAT, Leitlinien KI. Diese Arbeitsgruppe wurde Ende 2020 aufgelöst und soll von einem Kompetenznetzwerk Künstliche Intelligenz abgelöst werden (siehe BUNDESRAT, Medienmitteilung KI); weiterführend, SBFI, Herausforderungen der künstlichen Intelligenz.

34 BUNDESRAT, Auswirkungen der Digitalisierung.

35 BUNDESRAT, Auswirkungen der Digitalisierung, S. 6.

36 HÖFER, Rz. 2.

37 OECD, Algorithms and Collusion, S. 9.

38 OECD, Algorithms and Collusion, S. 9.

39 MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Appendix A., Ziff.2.

40 BITKOM/DFKI, S. 17.

41 MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Appendix A., Ziff.2.

zu analysieren.[42] Während bereits einzelne Daten einen (kommerziellen) Wert haben können, basiert der Wert von Big Data v.a. auf jenen Informationen, welche mithilfe einer leistungsfähigen IT-Infrastruktur und Algorithmen aus Daten(sätzen) extrahiert werden.[43] Bei Big Data *Analysen* geht es somit weniger um die Daten an und für sich, als um den Prozess, grosse Datensätze zu durchsuchen, Daten zu sammeln, diese zueinander in Bezug zu setzen und Erkenntnisse daraus abzuleiten.[44] Big Data kann sich sowohl auf personenbezogene als auch auf nicht personenbezogene Daten beziehen.[45]

⇨ Big Data profitiert u.a. vom *Internet of Things* (IoT – *infra* Ziff. 2.2.4) als Datenquelle und vom Cloud-Computing (*infra* Ziff. 2.2.3) im Zusammenhang mit Datenverarbeitungsprozessen. Eingesetzt werden Big Data Analysen am Arbeitsplatzes u.a. bei Prozessen des maschinellen Lernens (*infra* Ziff. 2.2.5), z.B. bei der Evaluation von potenziellen Kandidaten für eine neue Stelle (Ziff. III.3) oder im Kontext von Wearables (Ziff. III.5).[46]

2.2.3. Cloud-Computing

Cloud-Computing beschreibt ein Dienstleistungsmodell für Computer Dienstleistungen, welches Nutzerinnen und Nutzern Datenverarbeitungsressourcen (*computing power* – z.B. Netzwerke, Server, Speicher, Software-Anwendungen) in flexibler und bedarfsgerechter Form zugänglich macht.[47] Bereits bestehende IT-Infrastrukturen und Informations- und Kommunikationstechnologien können so von Unternehmen/Privatpersonen genutzt werden, ohne dass der/die Anwendende diese selber beschaffen oder einrichten muss.[48]

⇨ Cloud-Computing erhöht die Erschwinglichkeit, Verfügbarkeit, Kapazität und Vielfalt von Computerressourcen für Arbeitgebende und begünstigt die Anwendung von Big Data Analysen (*supra* Ziff. 2.2.2) oder «intelligenten» Technologien (*infra* Ziff. 2.2.5) am Arbeitsplatz. Überdies spielt Cloud-Computing eine Rolle im Kontext des Home-Office (Ziff. III.6) und bei der Nutzung eigener Geräte zur Arbeitserfüllung (BYOD – Ziff. III.7).[49]

2.2.4. Internet of Things

Das Internet der Dinge (*Internet of Things* – IoT) umschreibt eine auf dem Internet basierte globale Informations- und Kommunikationsarchitektur und ein Netzwerk untereinander verbundener Geräte/Gegenstände.[50] In technischer Hinsicht geht es darum, Gegenstände – z.B. mittels *Radio Fre-*

---

42 OECD, Going Digital, S. 20.

43 OECD, Going Digital, S. 20; BOYD UND CRAWFORD, S. 664; EPINEY, Rz. 6.

44 BOYD UND CRAWFORD, S. 663; EPINEY, Rz. 6.

45 EPINEY, Rz. 8.

46 Vgl. auch OECD, Going Digital, S. 20.

47 OECD, Cloud-Computing, S. 8.

48 OECD, Going Digital, S. 19.

49 OECD, Going Digital, S. 19.

50 Das European Research Cluster on the Internet of Things (IERC) bezieht sich auf folgende Definition: «*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual «things» have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network*.» (abrufbar unter: www.internet-of-things-research.eu/about_iot.htm (zuletzt besucht am 20.04.2021). Siehe auch EK, IoT, S. 5f. und WEBER, Internet of Things (2009), S. 522.

quency Identification (RFID) – zu identifizieren, mithilfe von Sensortechnologie Zustandsinformationen von Objekten zu sammeln und um die Fähigkeit smarter Geräte, untereinander zu kommunizieren (*machine-to-machine communication*).[51] Durch das Sammeln und Generieren von Daten und der Vernetzung von Informationen und Gegenständen mit dem Internet und untereinander ermöglicht das IoT eine Reihe neuer Geschäftsmodelle, Anwendungen und Dienstleistungen.[52]

⇨ Das IoT profitiert von Big Data als Datenquelle (*supra* Ziff. 2.2.2) und wird u.a. durch *Cloud-Computing* (*supra* Ziff. 2.2.3) ermöglicht. Am Arbeitsplatz ist es z.B. bei der systematischen Überwachung von Mitarbeitenden (Ziff. III.4.4.6) oder im Zusammenhang mit arbeitsplatzspezifischen Wearables (Ziff. III.5) relevant.

2.2.5. Künstliche Intelligenz

Obwohl es sich nicht um einen neuen Begriff[53] handelt, gibt es noch keine universell anerkannte Definition von «Künstliche Intelligenz» (KI).[54] Allgemein umschrieben umfassen Systeme der KI «Informatik-Anwendungen, deren Ziel es ist, intelligentes Verhalten zu zeigen. Dazu sind bestimmte Kernfähigkeiten notwendig: Wahrnehmen, *Verstehen*, Handeln und *Lernen*».[55] Insbesondere die Elemente *Verstehen* und *Lernen* sind charakteristisch für KI-Systeme im Vergleich zu herkömmlichen EDV-Anwendungen.

Die erfolgreiche Entwicklung gegenwärtiger KI-Anwendungen basiert primär auf Algorithmen (*supra* Ziff. 2.2.1) und maschinellem Lernen (ML).[56] Dabei handelt es sich um eine weit verbreitete *Methode* der KI – wobei es hier unterschiedliche Ausprägungen gibt[57] – welche dazu eingesetzt wird, «Systeme zu entwickeln, welche in neuen Situationen Vorhersagen/Prognosen […] erstellen, indem sie aus vergangenen Erfahrungen *lernen*».[58] Im Unterschied zu einer konventionellen Software oder einem gewöhnlichen Algorithmus, welche immer nach dem gleichen Schema funktionieren, werden auf ML basierte Entscheidungen durch Optimierung, d.h. «Lernen» über die Zeit, getroffen (z.B. durch einen «*trial-and-error*» Ansatz).[59] Der Begriff KI-*Systeme* umfasst jedoch nicht nur ML, sondern bezieht sich auch auf die weitergehende Fähigkeit eines Systems, komplexere und für einen *bestimmten Anwendungskontext* bestehende Probleme, deren Bewältigung bislang dem Menschen vorbehalten waren, zu lösen.[60]

---

51 Vgl. ITU, Internet of Things, S. 3; OECD, Going Digital, S. 19.

52 OECD, Going Digital, S. 19.

53 Der Begriff KI wird nachweislich seit 1956 und dem *Dartmouth Project on Artificial Intelligence* (auch *Dartmouth Conference*) verwendet (McCarthy et. al.).

54 SBFI, Herausforderungen der künstlichen Intelligenz, S. 7, 19f.

55 BITKOM/DFKI, S. 29 (Hervorhebung hinzugefügt).

56 SBFI, Herausforderungen der künstlichen Intelligenz, S. 7.

57 Zu den unterschiedlichen Kategorien des maschinellen Lernens, SBFI, Herausforderungen der künstlichen Intelligenz, S. 103ff. (Anhang 2).

58 SBFI, Herausforderungen der künstlichen Intelligenz, S. 20, mit Verweis auf OECD, AI in society (Hervorhebung hinzugefügt).

59 SBFI, Herausforderungen der künstlichen Intelligenz, S. 20. Ein «*trial-and-error*» Problemlösungsansatz impliziert, dass durch wiederholende Versuche immer wieder neue Lösungsansätze angewendet werden, bis schliesslich das gewünschte Resultat vorliegt.

60 SBFI, Herausforderungen der künstlichen Intelligenz, S. 7/21.

Die vom Bund eingesetzte KI-Arbeitsgruppe[61] beschränkte sich mangels einer vorhandenen allgemeingültigen Definition von KI auf einen anwendungs- und nicht technologiebasierten Erklärungsansatz. Demnach sind auf KI basierte Systeme in der Lage: (1) Daten in Komplexität und Menge in einer Form auszuwerten (insbesondere durch selbstständig lernende Algorithmen), die mit anderen Technologien nach heutigem Stand nicht möglich wäre; (2) Vorhersagen zu erstellen, welche als Grundlage für (automatisierte) Entscheidungen dienen; (3) dadurch Fähigkeiten zu erlangen, die mit der menschlichen Kognition und Intelligenz in Verbindung gebracht werden und (4) auf dieser Basis weitgehend autonom, d.h. ohne menschliche Einwirkung, agieren zu können.[62] Einzelne dieser Elemente können je nach KI-Anwendung unterschiedlich stark zum Tragen kommen und auch in Nicht-KI-Anwendungen vorhanden sein.[63]

In der vorliegenden Untersuchung wird ebenfalls ein anwendungsorientierter Ansatz von KI-Systemen verfolgt. Deshalb wird bei den Einzelnen, später untersuchten KI-Systemen nicht auf den Grad der Intelligenz der dahinterstehenden Technologie abgestellt, sondern auf die (rechtlichen) Folgen der damit verbundenen automatisierten Datenverarbeitung. Im Einzelfall wird somit *keine* Unterscheidung zwischen nur auf Algorithmen basierten Systemen und komplexeren ML- und KI-Systemen vorgenommen.

⇨ Im Kontext von Beschäftigungsverhältnissen können Systeme der KI u.a. im Rahmen von automatisierten Bewerbungsverfahren, bei der Evaluation von Bewerbenden/Mitarbeitenden (Ziff. III.3), im Zusammenhang mit dem Einsatz von Überwachungs- und Kontrollsystemen (Ziff. III.4) sowie bei der Verwendung von Wearables (Ziff.III.5) zur Anwendung kommen.

[61] SBFI, Herausforderungen der künstlichen Intelligenz.

[62] SBFI, Herausforderungen der künstlichen Intelligenz, S. 7. In ähnlicher Weise wurden KI-Systeme auch in der OECD-Empfehlung des Rates zu künstlicher Intelligenz beschrieben: «*An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy*» (OECD, Recommendation AI, Ziff. I).

[63] SBFI, Herausforderungen der künstlichen Intelligenz, S. 7.

3. Internationale Rechtsgrundlagen

3.1. Vereinte Nationen (UNO)

3.1.1. Allgemeines

Das Recht auf Privatsphäre ist auf der Ebene der UNO seit 1948 in Art. 12 AEMR[64] verbürgt und seit 1966 in rechtlich verbindlicher Form in Art. 17 UNO Pakt II[65] verankert.[66] Beide Artikel beziehen sich in allgemeiner Weise darauf, dass niemand ungerechtfertigten Eingriffen in das Privatleben ausgesetzt werden darf, beinhalten jedoch weder einen direkten Bezug zum Arbeitsplatz noch zu Digitalisierungssachverhalten (*infra* Ziff. 3.1.2).

Bereits in den 1960er Jahren wuchs bei den zuständigen Organen der UNO das Bewusstsein, dass technologische Fortschritte nicht nur ein grosses Potenzial für die wirtschaftliche, soziale und kulturelle Entwicklung mit sich bringen, sondern auch eine Gefahr für die Menschenrechte und damit verbundene Freiheiten darstellen können.[67] 1990 verabschiedete die Generalversammlung der Vereinten Nationen (UNGA) schliesslich die rechtlich nicht bindenden Richtlinien betreffend personenbezogener Daten in automatisierten Dateien.[68] Diese Richtlinien enthalten eine Reihe von Grundsätzen zur Datenverarbeitung im öffentlichen und privaten Bereich und formulieren Mindeststandards für die Rechtsetzung in den Mitgliedsstaaten der UNO.[69]

In der Folgezeit hat sich die UNO während längerer Zeit nicht mehr aktiv in Diskussionen über Privatsphäre und Datenschutz eingebracht. Erst durch die Snowden-Enthüllungen und den internationalen Überwachungsskandal 2013[70] hat das Recht auf Privatsphäre in jüngerer Vergangenheit international wieder vermehrt Beachtung erhalten. Viele daraufhin lancierte Initiativen beschäftigten sich mit der durch digitale Technologien ermöglichten, umfassenden Überwachung von Individuen durch staatliche und nichtstaatliche Akteure. Diese Arbeiten haben massgeblich dazu beigetragen, den Schutzbereich der Privatsphäre im Hinblick auf Sachverhalte der Digitalisierung und des Datenschutzes zu präzisieren.

---

64 Art. 12 Allgemeine Erklärung der Menschenrechte vom 10.12.1948 (AEMR):
Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

65 Art. 17 Internationaler Pakt über bürgerliche und politische Rechte vom 16.12.1966, SR 0.103.2 (UNO Pakt II):
(1) Niemand darf willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden.
(2) Jedermann hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen.

66 Vgl. auch Art. 22 Übereinkommen vom 13.12.2006 über die Rechte von Menschen mit Behinderungen, SR 0.109 (BRK), welcher ebenfalls ein Recht auf Privatsphäre für Personen mit Behinderung vorsieht.

67 Vgl. UN, Final Act of the International Conference on Human Rights, S. 12, XI. Siehe auch UNGA, Human Rights and Scientific and Technological Developments 1981; ECOSOC, Human Rights and Scientific and Technological Developments 1976; ECOSOC, Human Rights and Scientific and Technological Developments 1970; UNGA, Human Rights and Scientific and Technological Developments 1968.

68 UNGA, Guidelines for the Regulation of Computerized Personal Data Files 1990; ausführlich, SCHIEDERMAIR, S. 118ff.

69 UNGA, Guidelines for the Regulation of Computerized Personal Data Files 1990, Teil A.

70 HRC, Special Rapporteur Right to Privacy 2016, Ziff. 10.

U.a. hielt die UNO-Generalversammlung 2014 in Resolution 68/167 zum Recht auf Privatsphäre im digitalen Zeitalter fest, dass die rasanten technologischen Entwicklungen und die Nutzung neuer Informations- und Kommunikationstechnologien eine Gefahr für die Privatsphäre darstellen. Alle Rechte, welche in der analogen Welt (offline) gelten, müssten in gleichem Umfang auch in einem digitalen Umfeld (online) geschützt werden. Überdies forderte die UNO-Generalversammlung darin die Staaten auf, das Recht auf Privatsphäre zu respektieren und Massnahmen zu ergreifen, um zukünftig ungerechtfertigte Eingriffe in die Privatsphäre Einzelner zu verhindern.[71] Ende März 2015 setzte der UNO-Menschenrechtsrat zudem einen Sonderberichterstatter für das Recht auf Privatsphäre ein.[72] Dessen Arbeiten sind für die nachfolgende Untersuchung besonders relevant, da er sich nicht nur mit Fragen der staatlichen Überwachung beschäftigt hat, sondern darüber hinaus auch mit arbeitsplatzrelevanten datenschutzrechtlichen Fragen (*infra* Ziff. 3.1.4).

Neben den Bestimmungen des Rechts auf Privatsphäre finden sich auf Ebene der UNO verschiedene Menschenrechte im Bereich der Arbeit.[73] Für die vorliegende Untersuchung ist insbesondere Art. 7 UNO Pakt I relevant , welcher das Recht auf gerechte und günstige Arbeitsbedingungen postuliert (*infra* Ziff. 3.1.3).[74] Im Bereich der Arbeit ist zudem die Internationale Arbeitsorganisation (*International Labour Organisation*, ILO), eine Sonderorganisation der UNO, zuständig für die Erarbeitung und Einhaltung internationaler Arbeits- und Sozialstandards. Im Lauf der Jahre hat die ILO im Bereich der Arbeit grundlegende menschenrechtliche Standards (sog. Kernarbeitsnormen[75]) definiert, u.a. zur Vereinigungsfreiheit, dem Diskriminierungsverbot und der Beseitigung von Kinder- und Zwangsarbeit. Mit diesen Standards hat die ILO weltweit einen wichtigen Beitrag zur Umsetzung der Menschenrechte im Beschäftigungskontext geleistet.[76] Ergänzend gibt es eine Vielzahl von sektorspezifischen Abkommen, wobei sich keines schwergewichtig mit dem Schutz der Privatsphäre befasst. Lediglich ein bereits 1997 verfasster, nicht verbindlicher Leitfaden (*Code of Practice*) thematisiert den Schutz von persönlichen Daten am Arbeitsplatz.[77] In ihrer erst kürzlich angenommenen Deklaration zum hundertjährigen Bestehen der ILO wurden die Mitglieder zudem

---

71 UNGA, Right to privacy in the digital age 2014, ausführlich zum Inhalt der Resolution, JOYCE, S. 271ff.

72 HRC, Right to privacy in the digital age 2015.

73 Vgl. Art. 23 AEMR; Art. 6-8 Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte vom 16.12.1966, SR 0.103.1 (UNO Pakt I).

74 Siehe auch Art. 27 Abs. 1 lit. b BRK. Diese Bestimmung fordert analog zu Art. 7 UNO Pakt I die Verwirklichung von gerechten und günstigen Arbeitsbedingungen, einschliesslich sicherer und gesunder Arbeitsbedingungen, für Personen mit Behinderung.

75 Übereinkommen Nr. 29 über Zwangs- oder Pflichtarbeit vom 28.06.1930, SR 0.822.713.9; Übereinkommen Nr. 87 über die Vereinigungsfreiheit und den Schutz des Vereinigungsrechtes vom 09.07.1948, SR 0.822.719.7; Übereinkommen Nr. 98 über die Anwendung der Grundsätze des Vereinigungsrechtes und des Rechtes zu Kollektivverhandlungen vom 01.07.1949, SR 0.822.719.9; Übereinkommen Nr. 100 über die Gleichheit des Entgelts männlicher und weiblicher Arbeitskräfte für gleichwertige Arbeit vom 29.06.1951, SR 0.822.720.0; Übereinkommen Nr. 105 über die Abschaffung der Zwangsarbeit vom 25.06.1957, SR 0.822.720.5; Übereinkommen Nr. 111 über die Diskriminierung in Beschäftigung und Beruf vom 25.06.1958, SR 0.822.721.1; Übereinkommen Nr. 138 über das Mindestalter für die Zulassung zur Beschäftigung vom 26.06.1973, SR 0.822.723.8; Übereinkommen Nr. 182 über das Verbot und unverzügliche Massnahmen zur Beseitigung der schlimmsten Formen der Kinderarbeit vom 17.06.1999, SR 0.822.728.2.

76 Die Kernarbeitsabkommen haben im Juni 1998 eine politische Aufwertung erfahren, als die sog. «Erklärung über die grundlegenden Prinzipien und Rechte bei der Arbeit» ohne Gegenstimme an der 86. Internationalen Arbeitskonferenz angenommen wurden (ILO, Erklärung 1998).

77 Abrufbar unter: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf (zuletzt besucht am 20.04.2021). Seit 2013 liegt ein Schwerpunkt der ILO überdies auf dem Thema „die Zukunft der Arbeit» («*The future of work*») – mehr Informationen zu dieser Initiative, welche sich mit der Entwicklung und Implementierung neuer Technologien im Bereich der Arbeit beschäftigt, sind abrufbar unter: https://www.ilo.org/global/topics/future-of-work/lang--en/index.htm (zuletzt besucht am 20.04.2021).

aufgefordert, angesichts der fortschreitenden digitalen Transformation angemessene Massnahmen zu ergreifen, um den Schutz der Privatsphäre im Berufsleben zu gewährleisten.[78]

Ein weiteres Instrument, welches sich mit der Beeinträchtigung von Menschenrechten im Zusammenhang mit wirtschaftlichen Aktivitäten von Staaten und Unternehmen beschäftigt, sind die 2011 vom UNO-Menschenrechtsrat angenommenen UNO-Leitprinzipien für Wirtschaft und Menschenrechte (UNGP).[79] Diese rechtlich nicht verbindlichen Leitprinzipien fordern zum einen Staaten auf, ihren menschenrechtlichen Schutzpflichten im Bereich von wirtschaftlichen Aktivitäten nachzukommen (*duty to protect*); zum andern konkretisieren sie die unternehmerische Verantwortung zur Achtung der Menschenrechte (*responsibility to respect*).[80] Sie sehen vor, dass Unternehmen die international anerkannten Menschenrechte achten und «es vermeiden, durch ihre eigene Tätigkeit nachteilige Auswirkungen auf die Menschenrechte zu verursachen oder dazu beizutragen […]».[81] Trotz ihrer formellen Unverbindlichkeit für Unternehmen haben diese Prinzipien dazu beigetragen, das Grund- und Menschenrechtsbewusstsein von vielen Unternehmen zu stärken und Ansätze der Selbstregulierung zu fördern.[82]

3.1.2. Art. 17 UNO Pakt II

Nach Art. 17 Abs. 1 UNO Pakt II 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». Nach Abs. 2 haben alle Menschen Anspruch auf rechtlichen Schutz gegen solche Eingriffe.

Analog zur schweizerischen Grundrechtslehre (siehe *supra* Ziff. 1) wird den international anerkannten Menschenrechten und somit auch Art. 17 UNO Pakt II nicht nur eine Abwehrfunktion vor Einschränkungen durch den Staat zugeschrieben; vielmehr leiten sich für die Vertragsstaaten daraus positive Pflichten ab, dem Recht auf Privatsphäre auch unter Privaten Geltung zu verleihen.[83] In General Comment Nr. 16 von 1988 hat der Menschenrechtsausschuss (MRA) mit Blick auf den Schutz der Privatsphäre eine solche horizontale Wirkung der Menschenrechte bejaht: «*In the view of the Committee this right is required to be guaranteed against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons*».[84]

Der sachliche Schutzbereich von Art. 17 Abs. 1 UNO Pakt II ist sehr offen formuliert, und es werden immer wieder neue Entwicklungen und Lebensbereiche darunter subsumiert. Der Begriff Pri-

---

78 ILO, Centenary Declaration, III.C.v.

79 HRC, UN-Leitprinzipien zu Wirtschaft und Menschenrechten.

80 Ausführlich zu den Prinzipien, SKMR, Grundlagenstudie, Rz. 19ff.

81 HRC, UN-Leitprinzipien zu Wirtschaft und Menschenrechten, Prinzip 13 (a).

82 Zur Selbstregulierung von Unternehmen, SKMR, Das Recht auf Privatsphäre im digitalen Zeitalter, Rz. 183ff.

83 U.a. KÄLIN UND KÜNZLI, Rz. 3.70 und 3.94 und SCHABAS**,** Nowak's CCPR Commentary, N. 5f.

84 MRA, General Comment No. 16, Ziff. 1. In General Comment No. 31 (zu den rechtlichen Pflichten der Vertragsstaaten) bestätigt der MRA mit Blick auf Art. 17 UNO Pakt II, dass Staaten auch Aktivitäten von privaten Personen und Entitäten regeln müssen: «*the positive obligations on States Parties to ensure Covenant rights will only be fully discharged if individuals are protected by the State […] also against acts committed by private persons or entities that would impair the enjoyment of Covenant rights in so far as they are amenable to application between private persons or entities*» (MRA, General Comment No. 31, Ziff. 8). Weiterführend zu den staatlichen Schutzpflichten unter Art. 17 UNO Pakt II, SCHIEDERMAIR, S. 74ff.

vatleben fungiert als «Auffangtatbestand», welcher zur Anwendung kommt, wenn sich ein Sachverhalt nicht einem der weiteren spezifischen Menschenrechte zuordnen lässt.[85] Neben dem Begriff Privatleben spielt vorliegend der Begriff Schriftverkehr («*Correspondence*») eine Rolle. Dieser umfasst auch die *elektronische* Kommunikation und deren Überwachung.[86] Vor dem Hintergrund fortschreitender technologischer Entwicklungen hielt der MRA in General Comment Nr. 16 zudem fest, dass der Staat auf Grundlage von Art. 17 UNO Pakt II das Sammeln und Speichern persönlicher Daten auf Computern und anderen Geräten sowie in Datenbanken gesetzlich regeln muss, unabhängig davon, ob die Bearbeitung der Personendaten durch den Staat oder *durch Private* erfolgt. Ein Vertragsstaat muss deshalb effektive Massnahmen ergreifen, um sicherzustellen, dass personenbezogene Daten nicht in unbefugter Weise erhoben, gesammelt, verarbeitet, aufbewahrt oder weitergegeben werden. Dazu müssen Privatpersonen – und somit auch Arbeitnehmende – die Möglichkeit erhalten, sich über eine Datenspeicherung sowie deren Umfang und Verwendungszweck informieren zu können und einen Anspruch auf Korrektur oder Löschung von falschen oder unrechtmässig gesammelten Personendaten haben.[87]

Während sich der MRA wiederholt mit Fragen betreffend die positiven Schutzpflichten der Vertragsstaaten im digitalen Zeitalter und mit dem Schutz der Privatsphäre im Kontext von staatlichen Überwachungsmassnahmen[88] beschäftigt hat, gibt es soweit ersichtlich keine einschlägigen Ausführungen zum Schutz der Privatsphäre *von Arbeitnehmenden*.

3.1.3. Art. 7 UNO Pakt I

Art. 7 UNO Pakt I ist das Äquivalent zu Art. 23 Abs. 1 AEMR und dem darin enthaltenen Anspruch auf «gerechte und befriedigende Arbeitsbedingungen». Die Bestimmung sieht vor, dass die Vertragsstaaten das Recht auf «gerechte und günstige Arbeitsbedingungen» anerkennen und diesem innerstaatlich effektiv Geltung verleihen.[89] Dies beinhaltet die Gewährleistung von «sichere[n] und gesunde[n] Arbeitsbedingungen»[90] sowie «Arbeitspausen, Freizeit, [und] eine angemessene Begrenzung der Arbeitszeit […]»[91].

Wie in UNO Pakt II sind die Vertragsstaaten des UNO Pakt I verpflichtet, die Konventionsbestimmungen durch geeignete gesetzgeberische und weitere Massnahmen innerstaatlich effektiv umzusetzen, auch um diesen Rechten unter Privaten Geltung zu verleihen.[92] Im Zusammenhang mit der Forderung nach «gerechten und günstigen Arbeitsbedingungen» bedeutet dies, dass innerstaatliche Massnahmen sicherstellen müssen, dass private Arbeitgebende die in Art. 7 UNO Pakt I geforderten Arbeitsstandards einhalten.

In General Comment Nr. 23 zu Art. 7 UNO Pakt I geht der Ausschuss für wirtschaftliche, soziale und kulturelle Rechte auf die Teilgehalte dieser Arbeitgeberfürsorgepflicht (*infra* Ziff. 4.3.2) ein. Zum einen wird mit Blick auf «sichere und gesunde Arbeitsbedingungen» hervorgehoben, dass der

---

85 SCHABAS, Nowak's CCPR Commentary, N. 15.

86 SCHABAS, Nowak's CCPR Commentary, N. 53ff. Siehe auch MRA, General Comment No. 16, Ziff. 8.

87 MRA, General Comment No. 16, Ziff. 10. Vgl. auch SCHABAS, Nowak's CCPR Commentary, N. 23, N. 54f.

88 Vgl. SCHABAS, Nowak's CCPR Commentary, N. 54ff. und SKMR, Das Recht auf Privatsphäre im digitalen Zeitalter, Rz. 28ff.

89 ECOSOC, General Comment No. 23, Ziff. 50ff.

90 Art. 7 lit. b UNO Pakt I.

91 Art. 7 lit. d UNO Pakt I.

92 Zu den staatlichen Pflichten im Zusammenhang mit den Konventionsrechten, ECOSOC, General Comment No. 24.

Umgang mit Daten durch Arbeitgebende menschenrechtskonform erfolgen muss.[93] Zum andern wird mit Bezug auf die Arbeitszeit darauf hingewiesen, dass Arbeitspausen, Freizeit und eine angemessene Begrenzung der Arbeitszeit dazu beitragen, ein gesundes Gleichgewicht zwischen Beruf und Privatleben zu schaffen.[94] Diese beiden Teilbestimmungen von Art. 7 UNO Pakt I konkretisieren somit ebenfalls einen Teilgehalt des Rechts auf Privatsphäre im Kontext von Arbeitsverhältnissen.

Der Anspruch auf angemessene Arbeitsbedingungen tangiert alle Arbeitsverhältnisse und ist insbesondere auch im Kontext von flexiblen Arbeitsformen (z.B. Home-Office, mobiles Büro) relevant, welche in zeitlicher, räumlicher und sachlicher Hinsicht eine Vermischung von Privat- und Berufsleben mit sich bringen können (sog. Entgrenzung, Ziff. III.6 und Ziff. III.7).

Aufgrund der Tatsache, dass die Mehrheit der Arbeitsverhältnisse in der Schweiz privatrechtlicher Natur sind, hängt die Wirksamkeit der Umsetzung von Art. 7 UNO Pakt I primär davon ab, wie private Unternehmen die darin enthaltenen menschenrechtlichen Anforderungen erfüllen (horizontale Wirkung der Menschenrechte).[95] In Ergänzung zur staatlichen Schutzpflicht bestätigt deshalb General Comment Nr. 24 unter Bezugnahme auf die UNO-Leitprinzipien für Wirtschaft und Menschenrechte die Erwartung, dass Unternehmen ihren menschenrechtlichen Verpflichtungen *unabhängig davon* nachkommen, ob und wie diese in der innerstaatlichen Gesetzgebung umgesetzt sind.[96]

3.1.4. Der UNO-Sonderberichterstatter zum Recht auf Privatsphäre

Mit Resolution 28/16[97] setzte der UNO-Menschenrechtsrat Ende März 2015 Prof. Joseph Cannataci als Sonderberichterstatter für das Recht auf Privatsphäre ein. Mit der Schaffung dieses Mandats reagierte der UNO-Menschenrechtsrat auf die mit der fortschreitenden Entwicklung neuer (Überwachungs-)Technologien im Zusammenhang stehenden Gefahren für das Recht auf Privatsphäre.[98]

Nachdem er sich anfangs überwiegend mit der staatlichen Überwachung[99] und der Kommerzialisierung persönlicher Daten durch grosse Unternehmen beschäftigt hat[100], dehnte er sein Mandat im Laufe der Zeit auf weitere Themenbereiche aus und beschäftigte sich u.a. auch mit dem «Gebrauch persönlicher Daten durch Unternehmen» und der «Privatsphäre und Persönlichkeit».[101] Gestützt auf diese Arbeiten hat er in seinem Bericht 2020 eine Reihe von detaillierten Empfehlungen für die Bereiche Arbeit und Beschäftigung formuliert. Insbesondere fordert er staatliche und

93 ECOSOC, General Comment No. 23, Ziff. 28.

94 ECOSOC, General Comment No. 23, Ziff. 34.

95 Vgl. CRAVEN, S. 246.

96 ECOSOC, General Comment No. 24, Ziff. 5.

97 HRC, Right to privacy in the digital age 2015.

98 UNGA, Right to privacy in the digital age 2014, Ziff. 4 lit. b. Am 14.7.2021 wurde Ms. Ana Brian Nougreres zur Nachfolgerin von Prof. Cannataci ernannt.

99 Vgl. HRC, Special Rapporteur Right to Privacy 2016, Ziff. 9f.; HRC, Special Rapporteur Right to Privacy 2017; HRC, Special Rapporteur Right to Privacy 2018, Ziff. 102ff.; HRC, Special Rapporteur Right to Privacy 2019, Ziff. 26ff.

100 Vgl. HRC, Special Rapporteur Right to Privacy 2016, Ziff. 8; HRC, Special Rapporteur Right to Privacy 2018, Ziff. 22f. Weiterführend, SKMR, Das Recht auf Privatsphäre im digitalen Zeitalter, Rz. 69ff.

101 HRC, Special Rapporteur Right to Privacy 2019, Ziff 3 (a).

nicht-staatliche Akteure dazu auf, einen umfassenden Schutz der Privatsphäre in der Bearbeitung von persönlichen Daten zu Beschäftigungszwecken zu gewährleisten und verlangt u.a.[102]

- Transparenz darüber, welche Daten über Arbeitnehmende erhoben und bearbeitet werden;
- die Aufklärung der Arbeitnehmenden über deren Rechte hinsichtlich der über sie erhobenen und bearbeiteten Daten, inkl. Aufbewahrungsfristen;
- die Berichtigung und Löschung von nicht arbeitsplatzrelevanten Daten;
- eine rechtzeitige und umfassende Kommunikation von Seiten des Unternehmens über bestehende Datenbearbeitungsprozesse und ihre Zwecke;
- dass Arbeitgebende Arbeitnehmende vor Einführung von neuen Informationssystemen klar und umfassend informieren;
- dass Datenanalysesysteme und prädiktive Technologien den gesetzlichen Anforderungen entsprechen und diese nur zum Schutz von Arbeitnehmenden eingesetzt werden und nicht zu Überwachungszwecken;
- dass biometrische Daten nur bearbeitet werden, wenn es wirklich nötig ist und unter Einhaltung von geeigneten Schutzvorkehrungen;
- die Entwicklung von unternehmensinternen Datenschutzrichtlinien und -Prinzipien (Datenminimierung, Zweckbezogenheit, Datenschutz-Folgenabschätzungen, Konsultation der Arbeitnehmenden, Vertraulichkeit, Beschwerdemechanismen).

Dieser umfangreiche Katalog illustriert, dass der sachliche Schutzbereich der Privatsphäre nach Art. 17 UNO Pakt II nicht abschliessend verstanden, sondern im Rahmen einer zweckorientierten Auslegung laufend weiterentwickelt wird, um den wachsenden Anforderungen in einem digitalen Umfeld zu entsprechen.

3.1.5. Fazit

Die UNO hat mit Art. 12 AEMR und Art. 17 UNO Pakt II bereits früh einen normativen Rahmen geschaffen, um dem Recht auf Privatsphäre national und international Geltung zu verleihen. Trotz dieser frühzeitigen Anerkennung als grundlegendes Menschenrecht hat das Recht auf Privatsphäre international erst in den letzten Jahren eine grosse Beachtung erfahren, u.a. als Reaktion auf den weltweiten Überwachungsskandal 2013 und die rasanten technologischen Entwicklungen im Bereich von Datenverarbeitungsprozessen seither.

Im Zuge dieser Entwicklungen haben sich unterschiedliche Organe der UNO eingehend mit dem Recht auf Privatsphäre im Kontext der Digitalisierung auseinandergesetzt. Ein zentrales Thema ist die Gewährleistung des Schutzes von persönlichen Daten, welche staatliche und private Akteure in unterschiedlichen von der Digitalisierung betroffenen Lebensbereichen erheben, bearbeiten und (weiter-)verwenden. Besonders instruktiv für die vorliegende Studie sind die Empfehlungen des Sonderberichterstatters für das Recht auf Privatsphäre zu «*Work and Employment*» in seinem Bericht von 2020, wie der Schutz der Privatsphäre im digitalen Zeitalter am Arbeitsplatz umgesetzt werden sollte.

In normativer Hinsicht wird das in Art. 17 UNO Pakt II verankerte Recht auf Privatsphäre durch Art. 7 UNO Pakt I ergänzt. Die darin enthaltenen Bestimmungen setzen sich in allgemeiner Weise mit der Ausgestaltung des Rechts auf Arbeit und gerechten und günstigen Arbeitsbedingungen

[102] HRC, Special Rapporteur Right to Privacy 2020, Ziff. 48f.

auseinander und tangieren im Kontext der Privatsphäre auch Fragen über die Entgrenzung zwischen Beruf und Freizeit.

Auf Grundlage der genannten Bestimmungen muss der Staat wirksame Massnahmen ergreifen, um sicherzustellen, dass persönliche Daten weder durch staatliche, noch private Arbeitgebende in unbefugter Weise erhoben, gesammelt, verarbeitet, aufbewahrt oder weitergegeben werden. Betroffene Personen müssen zudem die Möglichkeit erhalten, sich über eine Datenspeicherung sowie deren Umfang und Verwendungszweck erkunden zu können, und sie haben ein Anrecht darauf, dass falsche oder unrechtmässig gesammelte Personendaten korrigiert oder gelöscht werden. Überdies muss der Staat Massnahmen ergreifen, um einer zeitlichen Entgrenzung zwischen Arbeit und Freizeit vorzubeugen.

Die relevanten Organe der UNO haben zudem die Erwartung geäussert, dass private Unternehmen (und somit auch Arbeitgebende) aufgrund ihrer bedeutenden Rolle im Bereich der Entwicklung und Anwendung von Datenverarbeitungstechnologien den Konventionsrechten *eigenständig* Geltung verleihen.

3.2. Europarat

3.2.1. Allgemeines

Der Europarat zählt zu den weltweit führenden Institutionen, wenn es um die Entwicklung des Rechts auf Privatsphäre im digitalen Zeitalter geht.[103] Bereits 1950 wurde das Recht in Art. 8 EMRK verankert. Vor der Hintergrund der fortschreitenden Digitalisierung und einer progressiven Rechtsprechung durch den Europäischen Gerichtshof für Menschenrechte (EGMR) hat der Europarat 1981 eine Konvention erlassen, welche sich mit der automatischen Verarbeitung personenbezogener Daten und dessen Auswirkungen auf den Schutz der Privatsphäre auseinandersetzt.[104] Diese Datenschutzkonvention hat die Ausgestaltung späterer nationaler (*infra* Ziff. 4.2.1) und regionaler (*infra* Ziff. 3.4.3) Datenschutzgesetzgebungen massgeblich beeinflusst. Um den technologischen Entwicklungen Rechnung zu tragen, hat er 2018 ein Änderungsprotokoll zur Datenschutzkonvention verabschiedet.[105]

Aufgrund der grossen Bedeutung der Rechtsprechung des EGMR für die Schweiz wird nachfolgend zunächst aufgezeigt, wie der Gerichtshof das Recht auf Privatsphäre mit Blick auf digitale Sachverhalte (in Beschäftigungsverhältnissen) über die Jahre entwickelt hat (*infra* Ziff. 3.2.2). Danach werden die 1981/2018 Datenschutzkonventionen (*infra* Ziff. 3.2.3) sowie zwei Empfehlungen des Ministerkomitees des Europarates im Bereich von Beschäftigungsverhältnissen und algorithmischen Systemen beleuchtet (*infra* Ziff. 3.2.4).

3.2.2. Europäische Menschenrechtskonvention (EMRK)

Das Recht auf Privatsphäre wird durch Art. 8 EMRK garantiert:

---

[103] Ausführlich, SIMITIS, N. 154ff. und SKMR, Das Recht auf Privatsphäre im digitalen Zeitalter, Rz. 80ff.

[104] Übereinkommen vom 28.01.1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, SR 0.235.1 (Datenschutzkonvention).

[105] Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 10.10.2018, SEV Nr. 223 (noch nicht in Kraft getreten – Änderungsprotokoll).

> «(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
>
> (2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.»

Diese Bestimmung ist historisch eng an Art. 12 AEMR angelehnt und ähnlich offen formuliert.[106] Mit Blick auf das Berufsleben hat sich der EGMR bereits 1992 in *Niemietz gegen Deutschland*[107] – es ging um die Durchsuchung einer Anwaltskanzlei im Zusammenhang mit einem Strafverfahren – ausführlich dahingehend geäussert, dass eine strikte Trennung zwischen Privat- und Berufsleben im Kontext von Art. 8 EMRK nicht möglich ist:

> *«[…] it would be too restrictive to limit the notion [of private life] to an «inner circle» in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of «private life» should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not».*[108]

Der EGMR begründet die Anwendbarkeit des Rechts auf Privatsphäre am Arbeitsplatz mit der Fülle von sozialen Beziehungen, welche eine Person im Rahmen ihrer beruflichen Tätigkeiten pflegt. Gleichzeitig verweist der EGMR darauf, dass sich die Aktivitäten von einzelnen Personen nicht immer eindeutig dem Privat- oder Berufsleben zuordnen lassen und die Grenzen dieser beiden Bereiche oftmals fliessend verlaufen. Diese Entgrenzung hat im Zeitalter der Digitalisierung an Bedeutung gewonnen, da heutige Technologien in vielen Bereichen eine örtlich und zeitlich flexible Arbeitserfüllung begünstigen (insbesondere Ziff. III.6). Der EGMR hat über die Jahre die Anwendbarkeit von Art. 8 EMRK auf berufliche Sachverhalte unter Verweis auf dieses Urteil mehrmals bestätigt.[109] Überdies hat er den Schutzbereich des Privatlebens auch auf den *Zugang* zum Arbeitsverhältnis und somit das Bewerbungsverfahren ausgedehnt, obwohl die EMRK kein Recht auf Anstellung vorsieht.[110]

Der Schutz von persönlichen Daten – allgemein wie auch am Arbeitsplatz – ist nach langjähriger Rechtsprechung des EGMR ebenfalls ein wesentliches Element des Rechts auf Privatleben.[111]

---

[106] Siehe, SCHABAS, ECHR Commentary, S. 359ff. und DIGGELMANN UND CLEIS, S. 452ff.

[107] EGMR, Niemietz v. Germany, 13710/88 (1992).

[108] EGMR, Niemietz v. Germany, 13710/88 (1992), Ziff. 29.

[109] Z.B. EGMR, Taliadorou and Stylianou v. Cyprus, 39627/05 and 39631/05 (2008), Ziff. 53 und Fernández Martínez v. Spain, 56030/07 (2014), Ziff. 108f. Für weitere Beispiele, PÄRLI, Gutachten EMRK, Ziff. 31ff.

[110] Sidabras and Džiautas v. Lithuania, 55480/00 and 59330/00 (2004), Ziff. 42ff.; vgl. auch PÄRLI, Gutachten EMRK, Rz. 28.

[111] Zur Herleitung, wie die Erweiterung des Schutzbereiches der Privatsphäre auf den Schutz von persönlichen Daten durch den EGMR vollzogen wurde, MARSCH, S.8ff. (u.a. auch mit Verweis auf EGMR, Amman gegen die Schweiz, 27798/95 (2000)) und BOEHM, S. 25ff. und S. 75ff.

Erfasst werden namentlich die Sammlung, Speicherung, Verarbeitung, Verwertung und Zurückhaltung von persönlichen Daten sowie die Achtung der Korrespondenz, unabhängig davon, ob die entsprechenden Kommunikations- und Speichersysteme staatlich oder privat betrieben werden.[112]

Mit Blick auf datenschutzrechtlich relevante Sachverhalte am Arbeitsplatz hat sich der EGMR einerseits wiederholt mit Beschwerden befasst, welche Übergriffe *durch den Staat* gegenüber Angestellten betrafen. So wurde im Fall *Halford gegen Vereinigtes Königreich*[113] festgestellt, dass die Überwachung des Diensttelefons einer Polizistin durch die Polizeibehörde eine Verletzung des Privatlebens wie auch der Korrespondenz im Sinne von Art. 8 EMRK darstellte. In *Copland gegen das Vereinigte Königreich*[114] wurde eine Verletzung von Art. 8 EMRK bejaht, nachdem eine staatliche Bildungsanstalt das Telefon, E-Mail und die Internetnutzung einer Angestellten überwachen liess, um herauszufinden, ob sie während der Arbeitszeit private Geschäfte tätigte.

Anderseits hat der EGMR bereits früh anerkannt, «dass die Grundrechte der Konvention auch für die Rechtsbeziehungen zwischen Privatrechtssubjekten Rechtswirkungen» und somit eine Horizontalwirkung entfalten.[115] Daraus leitet der Gerichtshof – analog zur schweizerischen Grundrechtskonzeption[116] – ab, dass der Staat nicht nur Unterlassungspflichten, sondern auch positive Handlungs- und Schutzpflichten hat, damit die Grundrechte der EMRK auch im Verhältnis zwischen Privaten Geltung erlangen.[117] Wie MARSCH zurecht festhält, ist diese Schutzpflicht angesichts der allgegenwärtigen Rolle von privaten Akteuren im Zusammenhang mit Datenverarbeitungsvorgängen im Kontext des Datenschutzes von besonderer Bedeutung.[118]

Hinsichtlich der Wahrung der Privatsphäre in einem *privatrechtlichen* Beschäftigungskontext sind insbesondere die Ausführungen des EGMR zu zwei Fällen interessant.[119] In ***Bărbulescu gegen Rumänien*** ging es um die Überwachung eines Instant-Messaging-Dienstes, welchen die Arbeitnehmenden eines privaten Unternehmens zu geschäftlichen Zwecken einrichten mussten. Ein Angestellter missachtete die internen Regeln, wonach das Internet während der Arbeitszeit nicht für private Zwecke gebraucht werden durfte.[120] Seine darauffolgende Entlassung focht er mit der Begründung der Verletzung seiner Privatsphäre gerichtlich an. Der Gerichtshof verneinte zunächst im Ergebnis eine Verletzung von Art. 8 EMRK, die Grosse Kammer kam aber 2017 zum gegenteiligen Schluss. In ihrer Argumentation führte sie aus, dass es sich beim Verhältnis zwischen Arbeitgebenden und Arbeitnehmenden um ein vertragliches Subordinationsverhältnis mit rechtlichen Pflichten *für beide Seiten* handelt.[121] Trotz der vertraglichen Subordination bestehe somit grundsätzlich Spielraum für die bilaterale Regelung der vertraglichen Pflichten zwischen den Vertragsparteien.[122] Da auf europäischer Ebene ein Konsens fehlt, wie dieser Spielraum bei der Ausgestaltung des Rechts auf Privatsphäre am Arbeitsplatz auf nationaler Ebene einzubeziehen

---

[112] PÄTZOLD, Art. 8 N. 28ff., N. 36f., N. 59f. m. w. H. auf die Rechtsprechung (u.a. EGMR, Uzun v. Germany, 35623/05 (2010); EGMR, Copland v. the United Kingdom, 62617/00 (2007); EGMR, Rotaru v. Romania, 28341/95 (2000); EGMR, Halford v. The United Kingdom, 20605/92 (1997)). Weiterführend MARSCH, S. 11ff.

[113] EGMR, Halford v. The United Kingdom, 20605/92 (1997).

[114] EGMR, Copland v. the United Kingdom, 62617/00 (2007).

[115] SEIFERT, S. 698.

[116] Vgl. Ziff. II.1.

[117] Vgl. SEIFERT, S. 698f.

[118] MARSCH, S. 247ff.

[119] EGMR, Bărbulescu v Romania, 61496/08 (2017).

[120] EGMR, Bărbulescu v Romania, 61496/08 (2017), Ziff. 10ff.

[121] EGMR, Bărbulescu v Romania, 61496/08 (2017), Ziff. 117.

[122] EGMR, Bărbulescu v Romania, 61496/08 (2017), Ziff. 118.

sei, gewährt der Gerichtshof den Mitgliedstaaten bei der Umsetzung grundsätzlich ein weites Ermessen. In jedem Fall müssten die Staaten jedoch dafür sorgen, dass Arbeitgebende angemessene Schutzmassnahmen ergreifen um zu verhindern, dass Arbeitnehmende in missbräuchlicher Weise überwacht werden. Im Rahmen der Abwägung zwischen Arbeitgebenden- und Arbeitnehmendeninteressen hätten innerstaatliche Behörden deshalb u.a. folgende Faktoren zu berücksichtigen:[123]

- ob Arbeitnehmende vorgängig über die Möglichkeit einer Überwachung informiert wurden;
- den Umfang der Überwachung und die Schwere des Eingriffes in die Privatsphäre von Arbeitnehmenden;
- das Vorliegen von legitimen Gründen;
- das Vorhandensein einer milderen Massnahme;
- die Konsequenzen des Eingriffs für die Arbeitnehmenden und ob die Überwachung zweckgebunden war;
- das Bestehen von angemessenen Schutzvorkehrungen zugunsten von Arbeitnehmenden.

Die Grosse Kammer kam zum Ergebnis, dass die innerstaatlichen Gerichte verschiedene dieser Faktoren nicht angemessen zugunsten des Angestellten berücksichtigt und somit dem Recht auf Achtung der Privatsphäre des Angestellten nicht genügend Beachtung geschenkt hatten und bejahte deshalb eine Verletzung von Art. 8 EMRK.[124]

Im kürzlich ergangenen Urteil *López Ribalda and Others v. Spain*[125] ging es um die Videoüberwachung von Mitarbeitenden in einem Supermarkt. Nachdem es zu Fehlbeständen gekommen war, installierte der Supermarktbetreiber sowohl sichtbare als auch verdeckte Kameras, um die Mitarbeitenden zu überwachen. Er informierte das Personal jedoch lediglich über die Installation der sichtbaren Kameras.[126] Insgesamt 14 Personen wurden daraufhin wegen Diebstahls entlassen, woraufhin fünf ihre Entlassung mit Verweis auf die Verletzung ihrer Privatsphäre anfochten. Die Grosse Kammer des EGMR verneinte eine Verletzung von Art. 8 EMRK nach Prüfung der im *Bărbulescu*-Urteil genannten Voraussetzungen.[127] Trotz der fehlenden vorgängigen Information der Mitarbeitenden über die Installation der verdeckten Kameras, akzeptierte der Gerichtshof die Argumentation der innerstaatlichen Gerichte, dass ein überwiegendes finanzielles Interesse des Supermarktbetreibers vorlag und die Überwachung der Angestellten verhältnismässig und im Einklang mit Art. 8 EMRK war.[128]

3.2.3. Datenschutzkonvention 108

Das zentrale Instrument zum Datenschutz im Europarat ist das Übereinkommen Nr. 108 *zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom*

[123] EGMR, Bărbulescu v Romania, 61496/08 (2017), Ziff. 118-121.

[124] EGMR, Bărbulescu v Romania, 61496/08 (2017), Ziff. 139ff.

[125] EGMR, López Ribalda and Others v. Spain, 1874/13 and 8567/13 (2019).

[126] EGMR, López Ribalda and Others v. Spain, 1874/13 and 8567/13 (2019), Ziff. 10ff.

[127] EGMR, López Ribalda and Others v. Spain, 1874/13 and 8567/13 (2019), Ziff. 115f.

[128] EGMR, López Ribalda and Others v. Spain, 1874/13 and 8567/13 (2019), Ziff. 133f.; für eine kritische Auseinandersetzung mit dem Urteil, BREGIANNIS.

28. Januar 1981 (Datenschutzkonvention), welches die Schweiz 1997 ratifizierte.[129] Die Konvention ist *non-self-executing*, d.h. die Mitgliedsstaaten müssen die erforderlichen Massnahmen treffen, um den im Übereinkommen festgelegten Grundsätzen Wirkung zu verleihen.[130] Die Datenschutzkonvention beinhaltet Grundprinzipien über den Datenschutz, regelt den grenzüberschreitenden Datenverkehr und enthält Bestimmungen zur Zusammenarbeit zwischen den Mitgliedsstaaten bei der Durchführung der Konvention.[131] Ihr Anwendungsbereich erstreckt sich auf personenbezogene, automatisiert verarbeitete Daten natürlicher Personen im öffentlichen und im privaten Sektor.[132] Der EGMR zieht die Datenschutzkonvention regelmässig zur Auslegung von Art. 8 EMRK bei.[133]

Um den aktuellen Herausforderungen für den Schutz der Privatsphäre in den Bereichen der Datenverarbeitung und des Datenverkehrs begegnen zu können, hat das Ministerkomitee des Europarats 2018 ein Änderungsprotokoll zur bestehenden Konvention verabschiedet.[134] Dieses wurde bislang von elf Staaten ratifiziert und mehr als 30, darunter auch die Schweiz[135], haben es unterzeichnet.[136] Es tritt in Kraft, sobald alle Vertragsstaaten der Datenschutzkonvention das Änderungsprotokoll ratifiziert haben, oder am 11. Oktober 2023, sofern bis dahin mindestens 38 Ratifikationen vorliegen.[137] In der Schweiz hat der Bundesrat im Dezember 2019 die Botschaft zur Genehmigung des Änderungsprotokolls verabschiedet,[138] die Bundesversammlung genehmigte den Beitritt im Juni 2020. Die Umsetzung des Änderungsprotokolls erfolgt auf Ebene des Bundes im Rahmen der Totalrevision des Datenschutzgesetzes (N-DSG, *infra* Ziff. 4.2.2). Eine Ratifikation ist allerdings erst möglich, wenn die im Änderungsprotokoll vorgesehenen Massnahmen im Rahmen des N-DSG in Kraft getreten sind.[139] Das Änderungsprotokoll ist vollständig kompatibel mit dem neuen Datenschutzrecht der EU (*infra* Ziff. 3.4.4).[140]

Im Vergleich zur Datenschutzkonvention legt das Änderungsprotokoll einen grösseren Fokus auf die Selbstbestimmung und das Recht des Individuums, Kontrolle über seine eigenen Daten und die damit verbundene Datenverarbeitung ausüben zu können.[141] So beinhaltet Art. 11 Änderungsprotokoll (neu Art. 9) auch eine Aufzählung der Rechte, welche einer natürlichen Person im Zusammenhang mit der Verarbeitung von persönlichen Daten zustehen, u.a.:

---

[129] Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.01.1981, SR 0.235.1 (Datenschutzkonvention).

[130] Art. 4 Datenschutzkonvention.

[131] 2001 verabschiedete der Europarat zudem ein Zusatzprotokoll, welches von den Staaten u.a. verlangt, Aufsichtsbehörden einzusetzen, welche die Durchsetzung und Kontrolle der Datenschutzkonvention verbessern (Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 08.11.2001, SR 0.235.11 (Zusatzprotokoll – für die Schweiz seit April 2008 in Kraft)).

[132] Art. 3 Abs. 1 Datenschutzkonvention.

[133] Vgl. z.B. EGRM, López Ribalda and Others v. Spain, 1874/13 and 8567/13 (2019), Ziff. 60; EGMR, Bărbulescu v Romania, 61496/08 (2017), Ziff. 42.

[134] Der Inhalt des Änderungsprotokolls ist abrufbar unter https://rm.coe.int/16808ac918 (zuletzt besucht am 20.04.2021).

[135] Siehe hierzu: BUNDESRAT, Botschaft Änderungsprotokoll.

[136] Der Status der Ratifikation/Unterzeichnungen ist ersichtlich unter: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures (Stand 22.04.2021).

[137] Art. 37 Abs. 1 und 2 Änderungsprotokoll.

[138] BUNDESRAT, Botschaft Änderungsprotokoll.

[139] Vgl. Art. 6 Abs. 2 Änderungsprotokoll (neu Art. 4 Abs. 2) und BUNDESRAT, Konventionen Europarat, S. 8105.

[140] BAERISWYL, Entwicklungen im Datenschutzrecht 2018, S. 451.

[141] Siehe Art. 1 Abs. 2 und Abs. 5 Änderungsprotokoll (neu Präambel).

- dass keine Entscheidung, welche sich erheblich auf eine Person auswirkt, auf Grundlage einer automatischen Datenverarbeitung getroffen wird, ohne dass sich diese Person dazu äussern konnte (lit. a);
- dass betroffene Personen Zugang zu Informationen über die Datenverarbeitung von persönlichen Daten erhalten, einschliesslich Informationen zu Aufbewahrungsfristen und zur Sicherstellung der Transparenz der Datenverarbeitung (lit. b);
- das Recht, auf Antrag die Gründe einer personenbezogenen Datenbearbeitung zu erfahren, sofern die Ergebnisse dieser Datenverarbeitung im Zusammenhang mit dieser Person verwendet werden (lit. c);
- das Recht sich zu wehren, dass persönliche Daten verarbeitet werden; eine Weiterverarbeitung ist in diesen Fällen nur gerechtfertigt, wenn berechtigte Gründe für die Datenverarbeitung vorliegen, welche die Interessen, Rechte oder die Grundfreiheiten der betroffenen Person überwiegen (lit. d);
- das Recht, unentgeltlich und ohne übermässige Verzögerung die Berichtigung/Löschung von persönlichen Daten zu beantragen, wenn die Datenverarbeitung nicht im Einklang mit den Bestimmungen dieser Konvention erfolgt (lit. e);
- das Recht auf ein Rechtsmittel gem. Art. 12 der Konvention, wenn die Rechte im Sinne dieser Konvention verletzt worden sind (lit. f);
- das Recht zur Inanspruchnahme einer Aufsichtsbehörde i.S.v. Art. 15 der Konvention (lit. g).

Zusätzlich wurden die Begriffsdefinitionen wie auch die grundlegenden Prinzipien, welche im Rahmen der Datenverarbeitung eingehalten werden müssen, konkretisiert und ergänzt. So betont das Änderungsprotokoll insbesondere die Bedeutung der Zweckbindung, der Transparenz und des Verhältnismässigkeitsgrundsatzes in der Datenerhebung und -verarbeitung.[142] Zudem werden die Pflichten für sämtliche Entscheidungsträger über Datenverarbeitungen («*controller*») sowie für die Datenverarbeiter («*processor*») präzisiert.[143] Das Änderungsprotokoll trägt weiter dem Umstand Rechnung, dass es gewisse Kategorien von Daten gibt, welche aufgrund ihrer Sensibilität ein besonders grosses Missbrauchspotenzial aufweisen, darunter auch genetische und biometrische Daten (vgl. Ziff. III.4.4.5) sowie weitere höchstpersönliche Daten, welche über die Herkunft, religiöse Gesinnung, Gesundheit, etc. einer Person Aufschluss geben.[144] Im Zusammenhang mit höchstpersönlichen Daten sind die Staaten verpflichtet, gesetzliche Vorkehrungen zu treffen, um den Missbrauch dieser Daten zu verhindern.[145]

3.2.4. Empfehlungen des Ministerkomitees

Zusätzlich zur Datenschutzkonvention und dem Änderungsprotokoll wurden vom Ministerkomitee des Europarats diverse Empfehlungen erlassen, welche sich mit unterschiedlichen Themen zum Recht auf Privatsphäre im digitalen Zeitalter beschäftigen.[146] Diese richten sich an die Mitgliedstaaten des Europarates, sind jedoch völkerrechtlich nicht verbindlich. Gleichwohl können sie im

[142] Vgl. Art. 7 (neu Art. 5), Art. 10 (neu Art. 8) und Art. 14 (neu Art. 11) Änderungsprotokoll.

[143] Siehe Art. 9 (neu Art. 7), Art. 10 (neu Art. 8) und Art. 12 (neu Art. 10) Änderungsprotokoll.

[144] Art. 8 (neu Art. 6) Änderungsprotokoll.

[145] Vgl. Art. 8 Abs. 1 (neu Art. 6 Abs. 1) Änderungsprotokoll.

[146] Für eine Übersicht, SKMR, Das Recht auf Privatsphäre im digitalen Zeitalter, Rz. 103 m.w.H. in Fn. 171.

Rahmen der nationalen Rechtssetzungs- und Gerichtspraxis eine Rolle spielen, da sie eine gemeinsame Rechtsüberzeugung der Mitgliedstaaten zum Ausdruck bringen.[147] Für die vorliegende Untersuchung sind zwei Empfehlungen zum Gebrauch persönlicher Daten in Beschäftigungsverhältnissen wie auch eine kürzlich erlassene Empfehlung zu den menschenrechtlichen Risiken algorithmischer Systeme relevant.

Im Zusammenhang mit der Verwendung persönlicher Daten in Beschäftigungsverhältnissen hat das Ministerkomitee bereits 1989[148] eine Empfehlung erlassen, die 2015[149] überarbeitet wurde. Beide Empfehlungen richten sich sowohl an den öffentlichen, als auch den privaten Sektor.[150] Es wird hervorgehoben, dass der Respekt für die Menschenwürde, die Privatsphäre und der Schutz von personenbezogenen Daten im Kontext von Datenverarbeitungsprozessen für die Entwicklung der Persönlichkeit von Arbeitnehmenden zentral sind.[151] Die Erhebung, Bearbeitung und Speicherung von Daten muss im Beschäftigungsverhältnis wie auch im Bewerbungsprozess zudem den Grundsätzen der Zweckbindung, Rechtmässigkeit, Verhältnismässigkeit, Transparenz und der vorherigen Einwilligung entsprechen. Zudem besteht ein Anspruch auf Löschung und Berichtigung von unrichtigen oder unrechtmässig erhobenen Daten.[152] Arbeitgebende haben zudem die Pflicht, angemessene Massnahmen zum Schutz von persönlichen Daten zu ergreifen, menschenrechtliche Risiken zu analysieren und Eingriffe in die Grund- und Menschenrechte der Mitarbeitenden zu verhindern oder zumindest zu minimieren.[153] Die Empfehlung von 2015 befasst sich weiterführend mit spezifischen Datenverarbeitungsprozessen im Beschäftigungsverhältnis, wobei mit Blick auf die unter Ziff. III behandelten Szenarien folgende Empfehlungen relevant sind:

- Arbeitgebende sollten davon absehen, von Arbeitnehmenden oder Bewerbenden Zugang zu online, insbesondere auf sozialen Netzwerken geteilten Informationen zu verlangen[154];
- bei der Verarbeitung von persönlichen Daten im Zusammenhang mit Intra- und Internetaktivitäten von Arbeitnehmenden sollten präventive Lösungen wie Internet-Filter und anonymisierte Kontrollen gegenüber einer personalisierten Überwachung bevorzugt werden[155];
- die Überwachung der beruflichen Kommunikation ist nur in sehr engen Grenzen und die der privaten Kommunikation von Arbeitnehmenden unter keinen Umständen erlaubt[156];

[147] Vgl. BGE 118 Ia 64 E. 2a, S. 69f.

[148] MINISTERKOMITEE, The protection of personal data used for employment purposes.

[149] MINISTERKOMITEE, The processing of personal data in the context of employment; weiterführend, MINISTERKOMITEE, Explanatory Memorandum to «The processing of personal data in the context of employment».

[150] MINISTERKOMITEE, The protection of personal data used for employment purposes, Ziff. 1.1; MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 1.1.

[151] MINISTERKOMITEE, The protection of personal data used for employment purposes, Ziff. 2; MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 3.

[152] MINISTERKOMITEE, The protection of personal data used for employment purposes, Ziff. 3-14; MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 4-13.

[153] MINISTERKOMITEE, The protection of personal data used for employment purposes, Ziff. 13; MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 12, 20, 21.

[154] MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 5.3.

[155] MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 14.2.

[156] MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 14.3, 14.4.

- eine Überwachung der Aktivitäten von Mitarbeitenden ist zu vermeiden; sie ist nur bei Vorliegen von legitimen Gründen – Wirtschaftlichkeit, Gesundheit, Sicherheit, organisatorische Effizienz – erlaubt und bedarf Schutzmassnahmen wie der Vorabinformation der Arbeitnehmenden/Konsultation von Arbeitnehmendenvertretungen[157];
- Überwachungssysteme, welche nur indirekt die Aktivitäten der Mitarbeitenden überwachen, dürfen die Grund- und Menschenrechte der Mitarbeitenden nicht verletzten; die Videoüberwachung persönlicher Bereiche ist unter keinen Umständen erlaubt[158];
- die Verwendung von Geräten, welche den Standort von Mitarbeitenden offenlegen, muss einem legitimen Ziel – Wirtschaftlichkeit, Gesundheit, Sicherheit, organisatorische Effizienz – entsprechen und sollte nicht zu einer dauerhaften Überwachung von Mitarbeitenden führen; der Einsatz solcher Systeme muss verhältnismässig sein und Mitarbeitende müssen vorgängig über deren Einsatz informiert werden[159];
- die Erhebung/Bearbeitung von biometrischen Daten muss legitime Interessen von Arbeitgebenden/Arbeitnehmenden/Drittparteien verfolgen und verhältnismässig sein; es dürfen keine mildere Mittel zur Verfügung stehen, und die Mitarbeitenden müssen vorab über die Installation/den Einsatz der Systeme informiert werden.[160]

Im April 2020 hat das Ministerkomitee des Europarates zudem eine Empfehlung und dazugehörige Richtlinien über die menschenrechtlichen Auswirkungen von algorithmischen Systemen erlassen (zum Begriff Algorithmus, *supra* Ziff. 2.2.1).[161] In dieser Empfehlung werden Staaten und private Akteure zu einem menschenrechtskonformen Umgang mit algorithmischen Systemen aufgefordert.[162] Der Anhang zur Empfehlung enthält Leitlinien für den Umgang mit den menschenrechtlichen Auswirkungen algorithmischer Systeme (*Guidelines on addressing the human rights impacts of algorithmic systems*). Diese halten in einem ersten allgemeinen Teil (Abschnitt A) zunächst fest, dass algorithmische Systeme nicht nur einen positiven Nutzen haben können, sondern auch menschenrechtliche Herausforderungen mit sich bringen, u.a. für das Recht auf Privatsphäre und den Datenschutz.[163] Gleichzeitig wird hervorgehoben, dass die grosse Komplexität algorithmischer (Entscheidungs-)Prozesse es erschwert, negative menschenrechtliche Auswirkungen einzelnen Akteuren zuzuordnen.[164] Der zweite Teil (Abschnitt B) befasst sich mit den menschenrechtlichen Schutzpflichten von Staaten.[165] Mit Blick auf das Berufsleben sollen Staaten Anreize schaffen, um technologische Entwicklungen in Einklang mit den international anerkannten Arbeits- und Beschäftigungsstandards zu bringen.[166] Für die vorliegende Untersuchung interessant sind vor allem jene Prinzipien, welche die Verantwortlichkeit des privaten Sektors betreffen (Abschnitt C). Diese sehen u.a. eine menschenrechtliche Sorgfaltsprüfungspflicht für private Akteure vor, welche in der Konzeption, der Entwicklung, dem Verkauf, der Bereitstellung, der Implementierung oder der Wartung

---

157 MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 15.1, 21.

158 MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 15.2.

159 MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 16.1, 21.

160 MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 17.1, 21.

161 MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems; siehe ergänzend, MINISTERKOMITEE, The manipulative capabilities of algorithmic processes.

162 MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Ziff. 1.

163 MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang A Ziff. 3; zu den menschenrechtlichen Risiken, Anhang A Ziff. 4-9.

164 MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang A, Ziff. 12-14.

165 MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang B.

166 MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang B, Ziff. 6.3.

von algorithmischen Systemen tätig sind.[167] Weitere relevante Prinzipien betreffen die Informations- und Zustimmungspflicht von betroffenen Individuen[168], das Einsetzen von datenschutzfreundlichen Voreinstellungen (*privacy by default*)[169], Sicherheitsanforderungen[170], Transparenzbestimmungen[171], das Bereitstellen von Beschwerde- und Abhilfemechanismen[172], die Durchführung von menschenrechtlichen Folgenabschätzungen (*human rights impact assessment*) und zu ergreifende Massnahmen, wenn menschenrechtliche Risiken festgestellt wurden[173].

Es bleibt darauf hinzuweisen, dass das Ministerkomitee des Europarates im Herbst 2019 zudem einen ad-hoc Ausschuss für künstliche Intelligenz (CAHAI) eingesetzt hat[174], welcher die Grundlage für die Schaffung eines Rechtsrahmens im Bereich KI abklären soll[175] – zum Zeitpunkt des Verfassens der Studie (April 2021) ist eine Multistakeholder-Konsultation hierzu im Gange.[176]

3.2.5. Fazit

Der EGMR anerkennt, dass Art. 8 EMRK auch in Arbeitsverhältnissen anwendbar ist und datenschutzrechtliche Sachverhalte sowie die elektronische Korrespondenz einer Person einschliesst. Staaten sind deshalb verpflichtet, den Schutz der Privatsphäre von Arbeitnehmenden im Beschäftigungsverhältnis sicherzustellen und dafür zu sorgen, dass mögliche Eingriffe im Rahmen von innerstaatlichen Verfahren überprüft werden können. Einschränkungen sind nur innerhalb der von der EMRK festgelegten Schranken möglich und müssen insbesondere verhältnismässig sein.

Des Weiteren sind in einem Digitalisierungskontext die Datenschutzkonvention des Europarates von 1981 sowie das Änderungsprotokoll von 2018 von Bedeutung, welche die betroffenen Personen und ihre Verfügungshoheit über die eigenen Daten in den Mittelpunkt von personenbezogenen Datenverarbeitungsvorgängen stellt.

Während sich die Datenschutzkonvention/das Änderungsprotokoll überwiegend an Staaten richten, hat sich das Ministerkomitee des Europarats in seinen Empfehlungen zu Arbeitsverhältnissen/algorithmischen Systemen klar – und unter Verweis auf die UNGP[177] – dahingehend geäussert, dass auch privatrechtlichen Arbeitgebenden bei (algorithmischen) Datenbearbeitungen eine menschenrechtliche Verantwortung zukommt. Auch wenn diese Empfehlungen nicht verbindlich sind, zeigen sie, dass die Rolle von privaten Akteuren in zukünftigen (regulatorischen) Initiativen des Europarates im Kontext der Digitalisierung zunehmend im Vordergrund stehen dürfte.

---

[167] MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang C, Ziff. 1.1.

[168] MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang C, Ziff. 2.1.

[169] MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang C, Ziff. 2.2.

[170] MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang C, Ziff. 3.3.

[171] MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang C, Ziff. 4.3.

[172] MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang C, Ziff. 4.4.

[173] MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Anhang C, Ziff. 5.3 und 5.4.

[174] MINISTERKOMITEE, CAHAI.

[175] Ein erster Zwischenbericht ist im Dezember 2020 erschienen, MINISTERKOMITTEE, CAHAI Feasibility Study.

[176] Siehe https://www.coe.int/en/web/artificial-intelligence/cahai-multi-stakeholder-consultation (zuletzt besucht am 20.04.2021).

[177] MINISTERKOMITEE, The Human Rights Impacts of Algorithmic Systems, Preamble.

3.3. Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

3.3.1. Allgemeines

Im Kontext der verantwortungsvollen Unternehmensführung (*responsible business conduct* – Ziff. 3.3.2) hat die OECD die digitale Transformation als eines ihrer Schwerpunktthemen identifiziert. Dabei verweist sie sowohl auf das mit der Digitalisierung verbundene Potenzial, eine verantwortungsvolle Unternehmensführung zu fördern, als auch auf die mit neuen digitalen Technologien zusammenhängenden menschenrechtlichen Risiken – u.a. auch für den Schutz der Privatsphäre.[178]

Im Bereich des Datenschutzes hat die OECD zudem die *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (*Privacy Guidelines*, *infra* Ziff. 3.3.3) erlassen. Im Gegensatz zum Europarat, dessen Bemühungen zum Recht auf Privatsphäre darauf ausgerichtet sind, den Schutz des Individuums bei automatisierten Datenverarbeitungen zu gewährleisten, sieht die OECD die Notwendigkeit internationaler Regeln vorrangig in der Harmonisierung von nationalen Datenschutzgesetzgebungen, um unter Wahrung der Menschenrechte Handelshemmnisse zu verhindern und den freien globalen Datenaustausch und Informationsfluss zu gewährleisten.[179]

3.3.2. OECD-Leitsätze für multinationale Unternehmen

Die Leitsätze für multinationale Unternahmen (OECD-Leitsätze) sind das zentrale Instrument zur Förderung von verantwortungsvoller Unternehmensführung der OECD. Sie sind Bestandteil der OECD-Erklärung über internationale Investitionen und multinationale Unternehmen, welche vom OECD-Ministerrat 1976 verabschiedet wurde.[180] Bei den OECD-Leitsätzen handelt es sich um gemeinsame Empfehlungen der Regierungen der Teilnehmerstaaten an multinationale Unternehmen. Sie sind in Teilen für die Regierungen verbindlich[181]; für Unternehmen werden sie erst verpflichtend, wenn sie im nationalen oder internationalen Recht umgesetzt worden sind. Sie enthalten Grundsätze und Massstäbe für gute unternehmerische Praktiken im Einklang mit dem geltenden Recht der Gastländer und international anerkannten Standards.[182] Seit 2011 beinhalten die Leitsätze auch ein eigenes Menschenrechtskapitel.[183]

Die Teilnehmerstaaten trifft die Pflicht, die auf ihrem Staatsgebiet tätigen oder von dort aus operierenden Unternehmen dazu anzuhalten, die OECD-Leitsätze und damit auch die Menschenrechte überall dort zu beachten, wo sie ihre Geschäftstätigkeit ausüben.[184] Wie die Teilnehmerstaaten ihrer Förderungs- bzw. Mainstreaming-Pflicht nachkommen, steht ihnen weitgehend frei, z.B. durch

---

[178] OECD, Digitalisation and RBC, S. 5f. Mit Blick auf die Herausforderungen im Zusammenhang mit der künstlichen Intelligenz, OECD, AI & RBC.

[179] OECD, Privacy-Guidelines 1980, Vorwort; die Leitsätze wurden 2013 überarbeitet (OECD, Privacy-Guidelines 2013). Weiterführend, SCHIEDERMAIR, S. 144f.; SIMITIS, N. 184ff.

[180] OECD, Leitsätze 1976.

[181] Das Umsetzungsverfahren der OECD-Leitsätze ist Gegenstand eines OECD-Ratsbeschlusses (OECD, Ratsbeschluss), der gemäss Art. 5 lit. a i. V. m. Art. 7 OECD-Konvention (Übereinkommen über die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung vom 14.12.1960, SR 0.970.4) alle Regierungen der Mitgliedsstaaten bindet.

[182] OECD, Leitsätze 2011, Teil I, I, Ziff. 1.

[183] OECD, Leitsätze 2011, Kapitel IV.

[184] OECD, Leitsätze 2011, Teil I, I, Ziff. 3 und IV, Ziff. 37.

entsprechende Politiken, gesetzgeberische Massnahmen oder andere Durchsetzungsmassnahmen.[185] Gestützt auf einen Beschluss des OECD-Ministerrates sind die Teilnehmerstaaten aber in jedem Fall rechtlich verpflichtet, sog. Nationale Kontaktpunkte (NKP) einzurichten.[186] NKPs fungieren als nichtgerichtliche Vermittlungs- und Schlichtungsplattformen, die Eingaben wegen potenzieller Verstösse gegen die OECD-Leitsätze durch Unternehmen entgegennehmen und bei Konflikten vermitteln.[187]

Im 2011 eingefügten Kapitel IV über Menschenrechte, das massgeblich von den UN-Leitprinzipien zu Wirtschaft und Menschenrechten geprägt ist (*supra* Ziff. 3.1.1), werden Unternehmen dazu angehalten unabhängig von ihrer Grösse, ihrem Sektor, ihrem operativen Umfeld und ihren Eigentumsverhältnissen, die Menschenrechte zu achten und im Kontext ihrer Aktivitäten negativen Auswirkungen auf die Menschenrechte vorzubeugen.[188] Unternehmen sollten deshalb Verfahren einrichten, um tatsächliche oder potenzielle Menschenrechtsbeeinträchtigungen zu ermitteln. Die aus dieser Sorgfaltsprüfung resultierenden Erkenntnisse sind in der Folge zu berücksichtigen und Massnahmen zu ergreifen, um Verstösse gegen die Menschenrechte zu verhindern oder zumindest zu mildern. Unternehmen haben zudem Rechenschaft darüber abzulegen, wie sie negativen menschenrechtlichen Auswirkungen, die sie selbst verursachen oder im Rahmen ihrer Geschäftsbeziehungen dazu beitragen, begegnen wollen.[189]

Die Gesamtheit der international anerkannten Menschenrechte dient als Massstab für die unternehmerische Verantwortung, die Menschenrechte zu achten. Diese umfassen die AEMR sowie die UNO-Pakte I und II (*supra* Ziff. 3.1). Ferner wird in den OECD-Leitsätzen auf die ILO-Erklärung von 1998 über grundlegende Prinzipien und Rechte bei der Arbeit verwiesen.[190] Somit fällt auch der menschenrechtliche Schutz der Privatsphäre am Arbeitsplatz in deren Geltungsbereich. Die OECD-Leitsätze sind überdies technologieneutral formuliert und sowohl auf analoge, wie auch digitale Sachverhalte anwendbar. Dies wurde auch in diversen Verfahren vor NKP's bestätigt, welche sich mit der Bereitstellung und Bearbeitung von personenbezogenen Daten durch Unternehmen beschäftigen.[191]

3.3.3. Privacy Guidelines

Der Fortschritt der Informations- und Kommunikationstechnologien und die damit verbundenen Gefahren für die Menschenrechte bewog einige Staaten – einschliesslich der Schweiz – bereits in den 1970er Jahren zur Ausarbeitung von nationalen Datenschutzgesetzen (*infra* Ziff. 4.2).[192] Diese nationalen Entwicklungen veranlassten auch die OECD, sich mit der Thematik auseinanderzusetzen und im Jahr 1980 die *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Privacy-Guidelines)* zu verabschieden.[193]

---

185 SKMR, Extraterritorialität im Bereich Wirtschaft und Menschenrechte, Rz. 115ff.

186 OECD, Ratsbeschluss, Ziff. I.

187 OECD, Leitsätze 2011, S. 3 und S. 78; SKMR, Grundlagenstudie, Rz. 49.

188 OECD, Leitsätze 2011, Teil I, IV, Ziff. 1 und Ziff. 37.

189 OECD, Leitsätze 2011, Teil I, IV, Ziff. 5 und Ziff. 45.

190 OECD, Leitsätze 2011, Teil I, IV, Ziff. 39.

191 Vgl. UK NCP, Rz. 44ff. und AU NCP, Rz. 26.

192 OECD, Privacy-Guidelines 1980, Vorwort.

193 OECD, Privacy-Guidelines 1980, Annex.

Den *Privacy-Guidelines* kommt Empfehlungscharakter zu, d.h. sie sind im Gegensatz zu den Datenschutzkonventionen des Europarates (*supra* Ziff. 3.2.3) rechtlich nicht verbindlich. Dennoch ist es der OECD damit gelungen, die Entwicklung des Datenschutzrechts auf nationaler und internationaler Ebene mitzugestalten.[194] U.a. fanden die *Privacy-Guidelines* Erwähnung in beiden Botschaften des Bundesrates zu den Datenschutzgesetzen[195] und auch diverse wirtschaftlich wichtige nicht-europäische Staaten (u.a. die USA, Kanada, Japan und Australien) haben diesen Richtlinien zugestimmt.[196]

Die *Privacy-Guidelines* wurden 2013 überarbeitet.[197] Trotz der erheblichen technischen Veränderungen im Bereich der Informations- und Kommunikationstechnologien entschied sich die federführende Expertengruppe nicht für eine Totalrevision, was verschiedentlich zu Kritik führte.[198] In beiden Versionen gelten als personenbezogene Daten alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.[199] Der Anwendungsbereich erstreckt sich auf alle Daten aus dem öffentlichen und privaten Sektor, die aufgrund der Art ihrer Verarbeitung, ihrer Natur oder den Umständen, unter welchen sie genutzt werden, eine Gefahr für die Privatsphäre und andere individuellen Freiheiten bedeuten.[200] Auch das Herzstück von 1980, die acht datenschutzrechtlichen Grundprinzipien – begrenzte und rechtmässige Datenerhebung, Datenqualität, Zweckbestimmung, Nutzungsbegrenzung, Datensicherheit, Transparenz, Mitspracherecht der Betroffenen und Verantwortlichkeit – blieben unverändert.[201]

Eine für die vorliegende Untersuchung relevante Neuerung in den *Privacy-Guidelines* 2013 besteht darin, dass die Pflichten des Datenhauptverantwortlichen konkretisiert wurden.[202] Diese sollen neu sog. *privacy management programmes* einrichten.[203] Diese beinhalten u.a. die Durchführung von Datenschutz-Folgenabschätzungen (*privacy impact assessments*), d.h. Datenhauptverantwortliche müssen bei der Einführung neuer Programme/Dienstleistungen überprüfen, welche Risiken für das Recht auf Privatsphäre bestehen.[204]

3.3.4. Weitere Entwicklungen

In der jüngeren Vergangenheit hat die OECD weitere Initiativen lanciert, welche sich mit der digitalen Transformation und der Entwicklung neuer Technologien in unterschiedlichen

---

[194] Siehe SCHIEDERMAIR, S. 145f. und S. 150f.; EPINEY/CIVITELLA/ZBINDEN, S. 9f.; HUSI-STÄMPFLI, N. 4; CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 2 und S. 5.

[195] BUNDESRAT, Botschaft DSG, S. 424; BUNDESRAT, Botschaft E-DSG, S. 6968f.

[196] BUNDESRAT, Botschaft DSG, S. 424.

[197] OECD, Privacy-Guidelines 2013, Annex.

[198] OECD, Privacy Expert Group Report 2013. Kritisch hierzu, CATE/CULLEN/MAYER-SCHÖNEBERGER; GREENLEAF/CLARKE/WATERS, S. 2.

[199] OECD, Privacy-Guidelines 1980/2013, Annex, Ziff. 1 lit. b.

[200] OECD, Privacy-Guidelines 1980/2013, Ziff. 2; zum Anwendungsbereich, siehe SCHIEDERMAIR, S. 145f.

[201] OECD, Privacy-Guidelines 1980/2013, Annex, Ziff. 7-14; siehe auch OECD, Privacy Framework 2013, S. 22 sowie CATE/CULLEN/MAYER-SCHÖNEBERGER, S. 10. Die unveränderte Beibehaltung der Grundsätze wurde von GREENLEAF/CLARKE/WATERS in den folgenden Worten kritisiert: «*The OECD's 2013 decision to leave the OECD's 'Basic Principles of National Application' unchanged is a missed opportunity to respond to the developments of the last 35 years. The only significant positive addition is a new Part on 'Implementing Accountability,' which introduces additional obligations on data controllers, including breach notification requirements*» (S. 2).

[202] OECD, Privacy-Guidelines 2013, Grundsatz 15; bezüglich weiterer Neuerungen, SKMR, Das Recht auf Privatsphäre im digitalen Zeitalter, Rz. 133f.

[203] OECD, Privacy Framework 2013, S. 23ff.

[204] Allgemein zu *Privacy Impact Assessment*s, WEBER, Privacy Impact Assessments.

Lebensbereichen beschäftigen, u.a. das *Going Digital* Projekt.[205] Ziel dieses Projektes ist es, einen kohärenten und gesamtheitlichen Ansatz zu entwickeln, um mithilfe der digitalen Transformation ein integratives und nachhaltiges Wachstum zu fördern und sicherzustellen, dass den damit verbundenen Gefahren erfolgreich begegnet werden kann.

Begleitend zu diesem Projekt wurde 2019 eine Empfehlung über Künstliche Intelligenz vom OECD-Ministerrat verabschiedet.[206] Diese formuliert Prinzipien zum verantwortungsvollen Umgang aller mit KI befassten Akteure und verlangt

- die Achtung von grundlegenden Menschenrechten – u.a. der Menschenwürde, Selbstbestimmung, Schutz Privatsphäre und des Datenschutzes[207];
- die Ergreifung von angemessenen Schutzmassnahmen (z.B. der Einbezug menschlicher Entscheidungen)[208];
- einen transparenten Umgang mit KI[209];
- die Implementierung von systematischen Risiko-Analysen[210];
- die Sicherstellung, dass alle mit KI befassten Akteure für die Einhaltung dieser Prinzipien zur Verantwortung gezogen werden können[211].

Obwohl diese Empfehlung rechtlich nicht verbindlich ist, zeigt sich ihre politische Bedeutung darin, dass die Prinzipien in der von den G 20-Wirtschafts- und Handelsministern im Juni 2019 verabschiedeten Ministererklärung übernommen wurden.[212]

3.3.5. Fazit

Die OECD schuf 1980 mit den *Privacy-Guidelines* das erste (nicht verbindliche) internationale Dokument zum Datenschutz und hat sich seither als wichtiger Akteur im Bereich der Digitalisierung und den damit verbundenen menschenrechtlichen Herausforderungen im Rahmen der verantwortungsvollen Unternehmensführung etabliert.

Insbesondere das in Anlehnung an die UNGP 2011 neu eingefügte Kapitel IV der OECD-Leitsätze zu den Menschenrechten und die damit verbundene Konkretisierung der Sorgfaltspflicht ist hinsichtlich der Verantwortung von Unternehmen in einem digitalen Kontext relevant. In diesem Zusammenhang sind auch die Aktivitäten der NKPs hervorzuheben, welche sich im Rahmen des von den Leitsätzen geschaffenen Beschwerdemechanismus verschiedentlich mit Fragen im Schnittbereich Digitalisierung und Privatsphäre befasst haben.

Durch ihre jüngsten, langfristig angelegten Initiativen im Bereich Digitalisierung wird die OECD auch zukünftig eine wichtige Rolle spielen, wenn es darum geht, länderübergreifende Standards zu neuen Technologien zu definieren.

---

[205] OECD, Going Digital (Informationen zu diesem Projekt sind abrufbar unter: https://www.oecd.org/going-digital/ (zuletzt besucht am 20.04.2021)). Weiterführend, OECD, Economic and Social Implications of AI; OECD, Digital Security and Risk Management; OECD, Managing Digital Security and Privacy und OECD, Protecting Privacy.

[206] OECD, AI in society, S. 3 (mehr Informationen sind abrufbar unter: https://www.oecd.org/going-digital/ai/ und https://oecd.ai/ (beides zuletzt besucht am 20.04.2021)).

[207] OECD, Recommendation AI, Ziff.1.2 lit. a.

[208] OECD, Recommendation AI, Ziff.1.2 lit. b.

[209] OECD, Recommendation AI, Ziff.1.3.

[210] OECD, Recommendation AI, Ziff.1.4 lit. c.

[211] OECD, Recommendation AI, Ziff.1.5.

[212] Siehe G20, Ziff. 19.

3.4. Europäische Union (EU)

3.4.1. Allgemeines

Das Recht auf Privatsphäre und Datenschutz findet sich in der EU in einer Vielzahl von Regulierungen. Für den vorliegenden Kontext sind zunächst Art. 7 und Art. 8 der Charta der Grundrechte der Europäischen Union (Charta der Grundrechte; GRC) hervorzuheben (*infra* Ziff. 3.4.2).[213] Sie schützen das Recht jeder Person auf Achtung ihres Privatlebens, ihrer Kommunikation und ihrer personenbezogenen Daten.

Die wichtigsten datenschutzrechtlichen Regelungen im europäischen Sekundärrecht sind in der Datenschutz-Grundverordnung (DSGVO)[214] sowie in der Datenschutzrichtlinie für elektronische Kommunikation[215] zu finden.[216] Das Datenschutz-Regelwerk der EU basiert inhaltlich grundsätzlich auf denselben Prinzipien wie die Datenschutzkonventionen des Europarats und die *Privacy-Guidelines* der OECD.[217] Durch ihren teils weit gefassten räumlichen Anwendungsbereich haben diese Erlasse einen erheblichen Einfluss auf Drittstaaten und damit auch auf die Schweiz (*infra*. Ziff. 4.2.2). Aufgrund dessen Umfangs und seiner Anwendbarkeit in unterschiedlichen Rechtsbereichen ist es allerdings nicht möglich, das Datenschutzrecht der EU an dieser Stelle umfassend abzubilden. Deshalb beschränkt sich die vorliegende Untersuchung auf jene Bestimmungen, welche für den Schutz der Privatsphäre am Arbeitsplatz im digitalen Zeitalter von Bedeutung sind und beleuchtet die Rechtsprechung des Europäischen Gerichtshofes (EuGH) ausschliesslich in diesem Kontext (*infra* Ziff. 3.4.3.).

Für die Wahrung der Privatsphäre von Arbeitnehmenden im Beschäftigungsverhältnis ist überdies Art. 31 GRC zu gerechten und angemessenen Arbeitsbedingungen relevant (*infra* Ziff. 3.4.4). Neben den wichtigsten Bestimmungen im europäischen Primär- und Sekundärrecht wird abschliessend auf die im Auftrag der EU-Kommission erarbeiteten *Ethik-Leitlinien für eine Vertrauenswürdige KI* eingegangen (*infra* Ziff. 3.4.5).

---

213 Charta der Grundrechte der Europäischen Union, 2000/C 364/01, ABl C 364 vom 18.12.2000, S. 1-22 (GRC); zum Ganzen, BERNSDORFF, Art. 7 GRC und Art. 8 GRC.

214 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, ABl L 119 vom 04.05.2016, S. 1-88 (Datenschutz-Grundverordnung; DSGVO).

215 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, ABl L 201 vom 31.07.2002, S. 37-47 (Datenschutzrichtlinie für elektronische Kommunikation).

216 Zum Verhältnis zwischen der Datenschutz-Grundverordnung und Richtlinie 2002/58/EG siehe Art. 95 DSGVO und PILZ, Art. 95 DSGVO, N. 15. Die Richtlinie 2002/58/EG wurde am 25.11.2009 durch Richtlinie 2009/136/EG zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz ergänzt. Zu den Bestrebungen, Richtlinie 2002/58/EG durch eine E-Privacy Verordnung zu ersetzen, siehe: https://eur-lex.europa.eu/procedure/DE/2017_3 (zuletzt besucht am 20.04.2021).

217 Vgl. BERNSDORFF, Art. 8 GRC, N. 37; KÜHLING UND SACKMANN S. 681.

3.4.2. Art. 7 und Art. 8 Charta der Grundrechte (GRC)

Nach Art. 7 GRC hat «Jede Person […] das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation».[218] Diese Vorschrift ist Art. 8 EMRK (*supra* Ziff. 3.2.2) nachgebildet und soll in ihrem Schutzbereich auch nicht über diese Bestimmung hinausgehen, sondern dieselbe Bedeutung und Tragweite haben.[219] Sie unterscheidet sich von Art. 8 EMRK lediglich dadurch, dass der traditionellere Begriff der «Korrespondenz» durch den weitergehenden und zeitgemässeren Begriff der «Kommunikation» ersetzt wurde.[220] Mit Blick auf die Entstehungsgeschichte von Art. 7 GRC ist erwähnenswert, dass bei den Beratungen zur Grundrechtscharta – unter explizitem Verweis auf *Niemietz gegen Deutschland*[221] – diskutiert wurde, neben dem Begriff der «Wohnung» auch «Betriebs- und Geschäftsräume» in die Bestimmung aufzunehmen.[222] Auch wenn dieser Vorschlag letztendlich nicht angenommen wurde, wird dadurch die bisherige Rechtsprechung des EGMR bestätigt, dass Sachverhalte des Privatlebens am Arbeitsplatz unter den Schutzbereich des Rechts auf Privatsphäre fallen.[223] Auch der EuGH hat diese Auslegung in seiner Rechtsprechung zu Art. 7 GRC wiederholt bestätigt.[224]

Im Unterschied zur EMRK wurde der Schutz von personenbezogenen Daten in der Charta der Grundrechte nicht unter das Recht auf Privatsphäre (Art. 7 GRC) subsumiert, sondern in einer separaten Bestimmung festgehalten (Art. 8 GRC).[225] Art. 8 GRC fungiert als *lex specialis* zu Art. 7 GRC.[226] Trotz der Verankerung als eigenes Grundrecht geht der Schutz von personenbezogenen Daten nach Art. 8 GRC nicht über Art. 8 EMRK hinaus*;* die separate Auflistung unterstreicht jedoch den hohen Stellenwert des Datenschutzes innerhalb der EU.[227] Nach Art. 8 Abs. 1 GRC sind personenbezogene Daten alle auf eine (bestimmte oder bestimmbare) Person bezogenen Informationen.[228] Diese dürfen nach Abs. 2 nur «nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden». Der Begriff «Verarbeitung» umfasst die gesamte Verwendung solcher Daten, beginnend mit deren Erhebung.[229] Die Bestimmung verankert weiter ein Recht der betroffenen Person, «Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken».

Obwohl der Schutz der Privatsphäre aus menschenrechtlicher Sicht primär Aufgabe des Staates ist, hatte sich der EuGH in den letzten Jahren vermehrt mit Fällen auseinanderzusetzen, welche

---

218 Ausführlich, BERNSDORFF, Art. 7 GRC.

219 Siehe Art. 52 Abs. 3 Satz 1 GRC.

220 BERNSDORFF, Art. 7 GRC, N. 20.

221 EGMR, Niemietz v. Germany, 13710/88 (1992); siehe Ziff. II.3.2.2.

222 BERNSDORFF, Art. 7 GRC, N. 8; weiterführend siehe FRENZ, Rz. 1203ff.

223 Siehe auch SCHIEDERMAIR, S. 344f.

224 EuGH, In den verbundenen Rechtssachen C-465/00, C-138/01 und C/139/01, Rechnungshof und Christa Neukomm und Joseph Lauermann gegen Österreichischer Rundfunk u.a., Urteil vom 20.05.2003, Ziff. 73; EuGH, In den verbundenen Rechtssachen C-92/09 und C-93/09, Volker und Markus Schecke und Hartmut Eifert gegen Land Hessen, Urteil vom 09.11.2010, Ziff. 59; EuGH, C-450/06, Varec SA gegen Belgischer Staat, Urteil vom 14.02.2008, Ziff. 48.

225 Vgl. auch Art. 16 Vertrag über die Arbeitsweise der Europäischen Union (Konsolidierte Fassung), ABl C 326 vom 26.10.2012, S. 47-388 (AEUV), welcher eine datenschutzrechtliche Gesetzgebungskompetenz für die Europäische Union schafft.

226 BERNSDORFF, Art. 8 GRC, N. 13.

227 BERNSDORFF, Art. 8 GRC, N. 12; vgl. auch SCHWEIZER UND RECHSTEINER, N. 2.81ff. und HUSI-STÄMPFLI, N. 6; SCHIEDERMAIR, S. 348.

228 BERNSDORFF, Art. 8 GRC, N. 20.

229 BERNSDORFF, Art. 8 GRC, N. 22.

die Datenverarbeitung von grossen (privaten) Unternehmen und die kommerzielle Nutzung von Daten durch diese Unternehmen für den Eigen- und Fremdgebrauch betrafen.[230] Mit seiner Rechtsprechung hat der Gerichtshof Standards gesetzt, welche auch im Rahmen der DSGVO (*infra* Ziff. 3.4.3) kodifiziert wurden, u.a. hinsichtlich des Rechts auf Vergessen[231], der Vorratsdatenspeicherung[232], sowie den Schutzvorkehrungen im Rahmen des grenzüberschreitenden Datenverkehrs[233]. Zudem hat er wiederholt bestätigt, dass Staaten die Pflicht haben, Private vor Verletzungen der Privatsphäre und des Datenschutzes durch Unternehmen zu schützen und dass das datenschutzrechtliche Regelwerk der EU

> «nicht nur einen wirksamen und umfassenden Schutz der Grundfreiheiten und Grundrechte natürlicher Personen, insbesondere des Grundrechts auf Achtung der Privatsphäre, bei der Verarbeitung personenbezogener Daten gewährleiste[t], sondern auch ein *hohes Niveau* des Schutzes dieser Grundrechte und Grundfreiheiten.»[234]

Ausnahmen und Einschränkungen in Bezug auf den Schutz der personenbezogenen Daten haben sich deshalb auf das absolut Notwendige zu beschränken.[235] Ob die betreffenden Informationen über das Privatleben sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben, ist für die Feststellung, ob ein Eingriff in das Recht auf Privatsphäre vorliegt, nicht verlangt.[236]

3.4.3. Datenschutz-Grundverordnung (DSGVO)

Die Datenschutz-Grundverordnung (DSGVO)[237] stellt seit dem 25. Mai 2018 *das zentrale* Regelwerk für den Schutz von personenbezogenen Daten in Europa dar. Sie ersetzt die frühere Datenschutz-Richtlinie 95/46/EG (einschliesslich der sie ergänzenden Richtlinien)[238], ist für die Mitgliedstaaten der EU unmittelbar anwendbar[239] und hat das Ziel, «die Grundrechte und Grundfreiheiten

---

230 Weiterführend, SKMR, Update zu «Das Recht auf Privatsphäre im digitalen Zeitalter».

231 EuGH, C-131/12, Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos, Urteil vom 13.05.2014 (welches ein Recht auf Vergessen statuiert); EuGH, C-507/17, Google LLC, Rechtsnachfolgerin der Google Inc. gegen Commission nationale de l'informatique et des libertés (CNIL), Urteil vom 24.09.2019 (welches sich mit dem territorialen und sachlichen Anwendungsbereich des Rechts auf Vergessen auseinandersetzt). Zudem EuGH, C 136/17, GC, AF, BH, ED gegen Commission nationale de l'informatique et des libertés (CNIL), Urteil vom 24.09.2019 (weiterführend zu den Pflichten von Suchmaschinenbetreibern).

232 EuGH, In den verbundenen Rechtssachen C-203/15 und C-698/15, Tele2 Sverige AB u.a., Urteil vom 21.12.2016; EuGH, In den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland Ltd und Seitlinger u.a., Urteil vom 08.04.2014.

233 EuGH, C-362/14, Schrems gegen Data Protection Commissioner, Urteil vom 06.10.2015 und EuGH, C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems, Urteil vom 16.07.2020.

234 EuGH, C-362/14, Schrems gegen Data Protection Commissioner, Urteil vom 06.10.2015, Ziff. 39 (Hervorhebung hinzugefügt).

235 EuGH, C-473/12, Institut professionnel des agents immobiliers (IPI) gegen Geoffrey Englebert u.a., Urteil vom 07.11.2013, Ziff. 39.

236 EuGH, In den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland Ltd und Seitlinger u.a., Urteil vom 08.04.2014, Ziff. 33.

237 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, ABl L 119 vom 04.05.2016, S. 1-88 (Datenschutz-Grundverordnung; DSGVO).

238 Siehe BERNSDORFF, Art. 8 GRC, N. 32.

239 Art. 288 Abs. 2 AEUV.

natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten» zu gewährleisten.[240]

Durch ihren weitgefassten räumlichen Geltungsbereich ist die DSGVO auch für die Schweiz relevant. Art. 3 (territorialer Anwendungsbereich) legt fest, dass die DSGVO gilt wenn: (1) der Verantwortliche oder Auftragsverarbeiter seine Niederlassung in der EU hat, unabhängig davon, ob die Datenverarbeitung in der Union stattfindet[241]; (2) sich die Niederlassung des Verantwortlichen ausserhalb der EU befindet, die Datenverarbeitung jedoch (a) Waren oder Dienstleistungen betrifft, welche für die EU bestimmt sind oder (b) der Beobachtung des Verhaltens einer betroffenen Person dient, sofern das Verhalten in der EU erfolgt.[242] Für Schweizer Unternehmen, die auch im EU-Ausland tätig sind, ist somit insbesondere Abs. 2 relevant, etwa bei Datenbearbeitungen im Zusammenhang mit Cloud-basierten Softwarelösung, durch externe IT-Dienstleister[243] oder mithilfe welcher Internetaktivitäten von Individuen nachvollzogen werden (z.B. Tracking durch Cookies, Tags).[244]

Ähnlich wie die Datenschutzbestimmungen des Europarates und der OECD muss die Verarbeitung personenbezogener Daten nach Art. 5 DSGVO die folgenden Voraussetzungen erfüllen: Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz (alle lit. a); Zweckbindung (lit. b); Datenminimierung (lit. c); Datenrichtigkeit (lit. d); Speicherbegrenzung (lit. e); Integrität und Vertraulichkeit (lit. f.) sowie Rechenschaftspflicht (Abs. 2). Weiterführende Bestimmungen zur Wahrnehmung der Rechte von betroffenen Personen beziehen sich auf den Grundsatz der Transparenz (Art. 12); das Recht auf Information (Art. 13/14); das Auskunftsrecht (Art. 15); das Recht auf Berichtigung unrichtiger Daten (Art. 16); das Recht auf Löschung (respektive Vergessenwerden – Art. 17); das Recht auf Einschränkung der Verarbeitung (Art. 18); das Recht auf Mitteilung (Art. 19); das Recht auf Datenübertragbarkeit (Art. 20); das Widerspruchsrecht (Art. 21); das Recht auf Verzicht auf eine automatisierte Entscheidung im Einzelfall (Art. 22) und das Recht auf Benachrichtigung über Datenverletzungen (Art. 34).

Relevant ist auch die in Art. 25 DSGVO eingeführte Verpflichtung, datenschutzfreundliche Technologien (*privacy by design*) und Grundeinstellungen (*privacy by default*) zu verwenden. Diese beiden Konzepte sollen dazu beitragen, digitale Technologien bereits vor Anwendung im Einklang mit datenschutzrechtlichen Vorgaben auszugestalten und somit *ex ante* das Risiko von Persönlichkeitsverletzungen zu verringern.[245] Mögliche Anwendungen können eine automatisierte Datenminimierung oder präventive Vorkehrungen zum Schutz von personenbezogenen Daten von Arbeitnehmenden – wie z.B. eine Anonymisierung oder Pseudonymisierung – vorsehen. Diese Vorschrift ist jedoch «nur» eine Verfahrensvorschrift und stellt *keine* Voraussetzung für die Rechtmässigkeit eines Datenverarbeitungsvorganges i.S.v. Art. 6 DSGVO dar.[246]

Art. 88 DSGVO adressiert spezifisch den Beschäftigungskontext. Es handelt sich um eine sog. Öffnungsklausel, welche Mitgliedstaaten erlaubt, «spezifischere Vorschriften zur Gewährleistung

[240] Art. 1 Abs. 2 DSGVO.

[241] Zum Kriterium der Niederlassung, EDÖB, EU-DSGVO, S. 3.

[242] Zum Kriterium des Zielmarktes, EDÖB, EU-DSGVO, S. 3f.

[243] PILTZ, Art. 3 DSGVO, N. 28.

[244] PILTZ, Art. 3 DSGVO, N. 31ff.

[245] U.a. NOLTE UND WERKMEISTER, Art. 25 DSGVO, N. 1f.; EPINEY UND KERN, S. 55f. und EDÖB, Tätigkeitsbericht 2016/7, S. 6.

[246] U.a. NOLTE UND WERKMEISTER, Art. 25 DSGVO, N. 3.

des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung [und] der Erfüllung des Arbeitsvertrags» zu erlassen.[247] Diese Vorschriften können «Massnahmen zur Wahrung […] der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten […] und die Überwachungssysteme am Arbeitsplatz» umfassen.[248] Erwägungsgrund 155 nennt exemplarisch «Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke der Einstellung [und] der Erfüllung des Arbeitsvertrags».[249] Aus der offenen Formulierung und den allgemeinen Verweisen auf die «Erfüllung des Arbeitsvertrages» und den Prozess der «Einstellung» kann geschlossen werden, dass der sachliche Anwendungsbereich von Art. 88 DSGVO breit gesteckt ist und sowohl die Entstehung als auch die Erfüllung des Arbeitsvertrages umfasst. Der persönliche Anwendungsbereich erstreckt sich damit nicht nur auf vertraglich bereits gebundene Arbeitnehmende, sondern auch auf Bewerbende, welche noch in keinem Vertragsverhältnis stehen.[250] Sofern Mitgliedstaaten basierend auf Art. 88 DSGVO sektorenspezifische Vorschriften für den Beschäftigungskontext erstellen, sind diese weitergehenden Regelungen auch für Schweizer Unternehmen mit Aktivitäten in diesen Ländern zu beachten.[251]

Mit Blick auf die Privatsphäre am Arbeitsplatz weiter relevant sind die Bestimmungen im Zusammenhang mit dem sog. Profiling, einer automatisierten Verarbeitung personenbezogener Daten um bestimmte persönliche Aspekte, wie z.B. persönliche Vorlieben, Gesundheit, Interessen, Aufenthaltsort, wirtschaftliche Lage oder Arbeitsleitung, einer Person zu bewerten.[252] In einem Beschäftigungsverhältnis besteht das Risiko, dass personenbezogene Daten, welche *nicht* die Eignung der Arbeitnehmenden für ein Arbeitsverhältnis betreffen oder für die Durchführung des Arbeitsvertrages notwendig sind, im Rahmen einer automatisierten Verarbeitung als Entscheidungsgrundlage zum Nachteil von Arbeitnehmenden herangezogen werden (insbesondere Ziff. III.2 – III.5).[253] Im Zusammenhang mit einem Profiling ist deshalb immer eine Datenschutz-Folgenabschätzung (*data protection impact assessment*/*privacy impact assessment*) erforderlich. Eine solche verpflichtet Arbeitgebende bei Bestehen von hohen Risiken für die Rechte/Freiheiten von Arbeitnehmenden im Vorfeld der Datenverarbeitung eine Abschätzung der datenschutzrechtlichen Folgen vorzunehmen.[254]

Die Artikel-29-Datenschutzgruppe[255], die Vorläuferin des europäischen Datenschutzausschusses[256], hat sich in einem Bericht ebenfalls eingehend mit der Verarbeitung von personenbezogenen

---

[247] Art. 88 Abs. 1 DSGVO; siehe PÖTTERS, N. 2.

[248] Art. 88 Abs. 2 DSGVO.

[249] Weiterführend, EK, Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017, S. 10f. Der Begriff «Vorschriften» umfasst einerseits Regelungen auf Gesetzesstufe, andererseits auch solche, die in Kollektiv- und Betriebsvereinbarungen umgesetzt werden (Ziff. 155 Präambel DSGVO; PÖTTERS, N. 11, 13.)

[250] Zum Ganzen PÖTTERS, N. 12.

[251] Vgl. PÄRLI, DSGVO, Folie 22.

[252] Art. 4 Abs. 4 DSGVO; siehe weiter Art. 13 Abs. 2 lit. f/Art. 22 DSGVO.

[253] Vgl. Art. 328b OR.

[254] Art. 35 DSGVO. Siehe auch EK, Artikel-29-Datenschutzgruppe, Datenschutz-Folgenabschätzung und EPINEY UND KERN, S. 57.

[255] Art. 29 Richtlinie 95/46/EG.

[256] Art. 68ff. DSGVO.

Daten im Arbeitsverhältnis beschäftigt.[257] Unter Einbezug der DSGVO hat sie u.a. die folgenden für die vorliegende Untersuchung relevanten Regeln formuliert:

- «Arbeitgeber sollten sich stets bewusst sein, dass unabhängig von der eingesetzten Technologie elementare Datenschutzgrundsätze einzuhalten sind.
- Für den Inhalt der elektronischen Kommunikation aus Geschäftsräumen gilt derselbe Schutz grundlegender Rechte wie für die analoge Kommunikation.
- Es ist überaus unwahrscheinlich, dass die Einwilligung der Beschäftigten eine Rechtsgrundlage für die Datenverarbeitung am Arbeitsplatz darstellt, es sei denn die Beschäftigten können die Einwilligung ohne nachteilige Folgen verweigern.
- In einigen Fällen können die Erfüllung eines Vertrags und berechtigte Interessen als Rechtsgrundlage herangezogen werden, sofern die Verarbeitung für einen rechtmäßigen Zweck unbedingt erforderlich ist und den Grundsätzen der Verhältnismäßigkeit und der Subsidiarität entspricht.
- Die Beschäftigten sollten wirksam über die zu erfolgende Überwachung informiert werden.»[258]

3.4.4. Art. 31 Charta der Grundrechte (GRC)

Im Zusammenhang mit der Privatsphäre am Arbeitsplatz ist überdies Art. 31 GRC («gerechte und angemessene Arbeitsbedingungen») von Bedeutung. Art. 31 GRC verankert den Persönlichkeitsschutz am Arbeitsplatz im Primärrecht.[259] In dessen «Mittelpunkt steht die physische und psychische Integrität des Arbeitnehmers».[260] Art. 31 GRC bezieht sich vorrangig auf die positiven Verpflichtungen des Staates im Bereich des Arbeitsschutzrechtes, er hat jedoch auch eine abwehrrechtliche Funktion im Kontext von öffentlich-rechtlichen Arbeitsverhältnissen.[261]

Art. 31 Abs. 1 GRC steht in engem Zusammenhang mit der Arbeitsschutz-Rahmenrichtlinie[262], welche analog zu den arbeitsrechtlichen Grundlagen in der Schweiz[263] verlangt, dass Arbeitnehmende bei der Planung und Einführung neuer Technologien angehört und informiert werden und eine Mitwirkungsmöglichkeit haben, wenn es um Massnahmen zur Beseitigung von gesundheitlichen Risiken geht.[264] Abs. 2 orientiert sich an der sog. Arbeitszeitrichtlinie.[265]

---

[257] EK, Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017.

[258] EK, Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017, S. 3.

[259] SCHUBERT, N. 1 (Hervorhebung hinzugefügt); ebenfalls HÜPERS UND REESE.

[260] SCHUBERT, N. 1.

[261] SCHUBERT, N. 3.

[262] Richtlinie des Rates der Europäischen Gemeinschaften vom 12.06.1989 über die Durchführung von Maßnahmen zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Arbeitnehmer bei der Arbeit (89/391/EWG), ABl L 183 vom 29.06.1989, S. 1-8. Art. 31 GRC lehnt sich überdies an Art. 3 der (revidierten) Europäischen Sozialcharta vom 03.05.1996, SEV Nr. 163, sowie Nr. 19 der Gemeinschaftscharta der Sozialen Grundrecht der Arbeitnehmer vom 09.12.1989, Kom (89) 248 endg. (GCh), an (vgl. EU, Erläuterungen zur GRC, Art. 31, S. 26).

[263] Ziff. II.4.3.

[264] Vgl. Art. 6 (3) c) Richtlinie 89/391/EWG.

[265] Richtlinie 93/104/EG des Rates der Europäischen Union vom 23.11.1993 über bestimmte Aspekte der Arbeitszeitgestaltung, ABl L 307 vom 13.12.1993, S. 18-24. In der Zwischenzeit wurde diese Richtlinie durch Richtlinie 2003/88/EG des Europäischen Parlaments und des Rates vom 04.11.2003 über bestimmte Aspekte der Arbeitszeitgestaltung, ABl L 299 vom 18.11.2003, S. 9-18 ersetzt. Art. 31 Abs. 2 lehnt sich überdies an Art. 2 ESC sowie Nr. 8 GCh an (vgl. Erläuterungen zur GRC, Art. 31, S. 26).

Die arbeitsschutzrechtlichen Bestimmungen von Art. 31 GRC können im Beschäftigungskontext für die Ausübung des Rechts auf Privatsphäre relevant sein, wie nachfolgend im Zusammenhang mit den gesundheitlichen Folgen von Überwachungssystemen (Ziff. III.4.4.3) und im Kontext der (zeitlichen) Trennung zwischen Privat- und Berufsleben (Ziff. III.6.4.3) aufgezeigt wird.

3.4.5. Ethik-Leitlinien für eine Vertrauenswürdige KI

Mit Blick auf das Potenzial, die Risiken und die Herausforderungen der Künstlichen Intelligenz (KI, *supra* Ziff. 2.2.5) hat die Europäische Kommission 2018 eine hochrangige Expertengruppe zu KI (AI-HLEG) ins Leben gerufen, welche *Ethik-Leitlinien für eine vertrauenswürdige KI*[266] formuliert hat.[267] Diese adressieren ethische und rechtliche Fragen zu KI und zeigen auf, wie eine vertrauenswürdige und menschenzentrierte KI umgesetzt werden kann.[268] Sie richten sich primär an Entwickler[269] und Betreiber[270] von KI-Systemen. Die Leitlinien sind *nicht* verbindlich und begründen keine neuen rechtlichen Verpflichtungen.[271] Sie entsprechen weitgehend den Empfehlungen der OECD-Expertengruppe zu KI (*supra* Ziff. 3.3.4).

Nach den Leitlinien soll KI grundsätzlich (a) rechtmässig, (b) ethisch und (c) robust sein.[272] Für die vorliegende Untersuchung relevant ist insbesondere das Kriterium der Rechtmässigkeit, welches im Umgang mit KI die Einhaltung der international und in der EU garantierten Grund- und Menschenrechte voraussetzt.[273] Genannt sind u.a. die Achtung der Menschenwürde, die Freiheit des Einzelnen, einschliesslich des Rechts auf Privatsphäre, sowie Gleichheit und Nichtdiskriminierung.[274] Im Rahmen der *Verwirklichung* von KI soll sichergestellt werden, dass die menschliche Autonomie bei KI-Systemen im Zentrum verbleibt, eine grundrechtliche Risiko-Folgenabschätzung erfolgt, der Schutz der Privatsphäre und der Datenschutz in allen Phasen des Lebenszyklus eines KI-Systems gewährleistet ist und die Grundsätze der Transparenz, Fairness und Rechenschaftspflicht geachtet werden.[275]

Die in diesen Leitlinien aufgelisteten (rechtlichen) Kriterien zur Nutzung von KI sind nicht neu, sondern existieren bereits in unterschiedlichen Rechtsgrundlagen auf nationaler, europäischer und internationaler Ebene, u.a. im Bereich der Grund- und Menschenrechte (Recht auf Privatsphäre, Nichtdiskriminierung) sowie in spezialgesetzlichen Erlassen (Datenschutz, Produktehaftpflicht, Verbraucherschutz, Gesundheitsschutz, Arbeitssicherheit usw.). Die Leitlinien sind in ihren grund-

[266] EK, AI-HLEG, Ethik-Leitlinien (zum Verhältnis zwischen Grundrechten und ethischen Grundsätzen siehe ebenda, Rz. 37ff., insb. 40).

[267] Umfassend zur Strategie der EK in diesem Bereich: EK, Weissbuch 2020; EK, KI 2019; EK KI Plan 2018; EK, KI Europa 2018 und EK, Digitaler Binnenmarkt.

[268] EK, KI 2019, S. 3.

[269] Entwickler sind alle Akteure, «die KI-Systeme erforschen, entwerfen und/oder entwickeln» (EK, AI-HLEG, Ethik-Leitlinien, Rz. 56).

[270] Betreiber sind «öffentliche oder private Organisationen und Unternehmen, die KI Systeme als Teil ihrer Geschäftsprozesse oder zum Bereitstellen von Produkten und Dienstleistungen an Dritte verwenden» (EK, AI-HLEG, Ethik-Leitlinien, Rz. 56).

[271] EK, AI-HLEG, Ethik-Leitlinien, Rz. 5, 25.

[272] EK, AI-HLEG, Ethik-Leitlinien, Rz. 1, 15, 22-27.

[273] EK, AI-HLEG, Ethik-Leitlinien, Rz. 40.

[274] EK, AI-HLEG, Ethik-Leitlinien, Rz. 41ff.

[275] EK, AI-HLEG, Ethik-Leitlinien, Rz. 55ff., 71ff.

menschenrechtlichen Bezügen zwar sehr allgemein gehalten könnten jedoch einen ersten sinnvollen «Schritt hin zu einem EU-einheitlichen Konzept «ethisch vertretbarer» KI» darstellen.[276]

Ein weiterer Schritt in diese Richtung erfolgte im April 2021 mit der Verabschiedung eines Verordnungsvorschlags der EU-Kommission zu KI zuhanden des EU-Parlaments.[277] Mit Blick auf die vorliegende Untersuchung ist relevant, dass die Verwendung von KI in Bewerbungsverfahren darin ebenfalls als eine Anwendung mit hohem Risiko für die Grundrechte eingestuft wird, welche erhöhten Anforderungen genügen muss.[278]

3.4.6. Fazit

Das umfassende Datenschutzregelwerk der EU bestätigt, dass das Recht auf Privatsphäre im digitalen Zeitalter vor Verletzungen aufgrund privatwirtschaftlicher Aktivitäten schützen soll. Insbesondere ist es durch die DSGVO gelungen, aktuelle technologische Entwicklungen mit innovativen, von Unternehmen umzusetzenden Ansätzen (*privacy by design, privacy by default*, Datenschutz-Folgenabschätzung, etc.) rechtlich zu erfassen.[279] Aus grundrechtlicher Sicht ist erwähnenswert, dass die DSGVO explizit alle Grundrechte und Grundfreiheiten und nicht nur die Persönlichkeit der betroffenen Personen schützt. Für die vorliegende Untersuchung relevant ist zudem der direkte Einbezug des Beschäftigungskontexts in Art. 88 DSGVO.

Der progressive grundrechtliche Ansatz der EU im Bereich des Datenschutzes wird durch die separate Nennung des «Schutzes von personenbezogenen Daten» in Art. 8 GRC und die Rechtsprechung des EuGHs in diesem Bereich bestätigt. Dieser hat dazu beigetragen, den Schutz einzelner Personen gegenüber grossen privaten Unternehmen (Google, Facebook), welche riesige Mengen an personenbezogenen Daten verarbeiten, zu stärken und einen hohen datenschutzrechtlichen Standard zu etablieren.[280]

Kombiniert mit der arbeitsschutzrechtlichen Bestimmung von Art. 31 GRC und weiteren Initiativen im Bereich der Digitalisierung wie etwa zu KI nimmt die EU weltweit eine führende Rolle ein bei der Setzung eines globalen Standards für einen grund- und menschenrechtsbasierten Ansatz im digitalen Zeitalter, welcher auch auf Beschäftigungsverhältnisse Anwendung findet.

4. Rechtsgrundlagen in der Schweiz

4.1. Bundesverfassung (BV)

Analog zu Art. 8 EMRK (*supra* Ziff. 3.2.2) gibt Art. 13 BV[281] jeder Person einen Anspruch auf «Achtung ihres Privat- und Familienlebens, ihrer Wohnung […] ihres Brief-, Post- und Fernmeldeverkehrs» (Abs. 1) sowie auf «Schutz vor Missbrauch ihrer persönlichen Daten» (Abs. 2). Obwohl die

[276] Zum Ganzen siehe CEP, Ethik-Leitlinien. Kritisch gegenüber dem ethischen Ansatz, METZINGER, welcher als Teil der EU-AI-HLEG die Ethik-Leitlinien zu KI der EU mitentworfen hat.

[277] EK, AI Act.

[278] Ziff. 36 Präambel, EK, AI Act.

[279] Siehe auch EPINEY UND KERN, S. 75.

[280] Vgl. Ziff. II.3.4.2.

[281] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18.04.1999, SR 101 (BV).

Garantie der Privatsphäre erst seit 1999 in der Bundesverfassung enthalten ist, beinhalteten bereits die Bundesverfassungen von 1848 und 1874 einzelne Aspekte eines solchen Rechts.[282] Zudem anerkennt das Bundesgericht seit den 1960-er Jahren einen grundrechtlichen Persönlichkeitsschutz[283], wozu unter dem Einfluss der Rechtsprechung des EGMR auch das Recht auf informationelle Selbstbestimmung zählt.[284]

Der Anspruch auf Schutz der Privatsphäre stellt eine Spezialgarantie zum Recht auf persönliche Freiheit (Art. 10 Abs. 2 BV) dar.[285] Wie bereits dargelegt wurde, kommt grundrechtlichen Garantien nach heutigem Grundrechtsverständnis nicht nur eine Abwehrfunktion zu.[286] Vielmehr besteht auch eine staatliche Schutzpflicht, Individuen vor Verletzungen der Privatsphäre durch Dritte zu bewahren. Der Gesetzgeber hat demnach die Rechtsordnung so auszugestalten, dass «Übergriffe in grundrechtlich geschützte Rechtsgüter» auch im Verhältnis unter Privaten verhindert werden.[287]

Das Bundesgericht umschreibt den Anspruch auf Achtung des Privatlebens nach Art. 13 Abs. 1 BV als das Recht einer Person, ihre Lebensweise wählen, ihre Freizeit organisieren und mit anderen Personen Kontakt haben zu können.[288] Geschützt ist weiterführend das Recht einer Person, ihre eigene Persönlichkeit zu verwirklichen und weiter zu entwickeln.[289] Auch wenn Art. 13 BV keinen direkten Bezug zum Arbeitsplatz enthält, wird gleichwohl analog zu Art. 8 EMRK die Meinung vertreten, dass die Ausübung beruflicher Tätigkeiten unter diese Bestimmung fallen kann und geschäftliche Kontakte und Räumlichkeiten ebenfalls davon erfasst sind.[290] Mit Blick auf den Arbeitsplatz ist zudem das Brief-, Post- und Fernmeldegeheimnis relevant, welches die vertrauliche Kommunikation schützt.[291]

Der in Art. 13 Abs. 2 BV verankerte verfassungsrechtliche Datenschutz ist ebenfalls Teil des Rechts auf Privatsphäre.[292] Davon geschützt sind analog zu den internationalen Bestimmungen Personendaten, die sich auf «bestimmte oder bestimmbare Personen beziehen».[293] Dem Wortlaut nach beschränkt sich der grundrechtliche Anspruch von Art. 13 Abs. 2 BV auf den Schutz *vor Missbrauch* personenbezogener Daten. Bundesgericht und Lehre gehen jedoch davon aus, dass *jede* Datenbearbeitung (Erhebung, Sammlung, Speicherung, Bearbeitung und Weiter- resp. Bekanntgabe) personenbezogener Daten darunter zu subsumieren ist.[294] Der verfassungsrechtliche Datenschutz nach Art. 13 Abs. 2 BV ist Teil des ungeschriebenen Grundrechts auf informationelle

---

[282] Vgl. DIGGELMANN, N. 1ff.

[283] BGE 89 I 92 E. 3., S. 98; spätere Urteile haben dies bestätigt, BGE 97 I 45 E. 3, S. 49;

[284] BGE 113 Ia 257 E. 4c, S. 263f.; weiterführend, BREITENMOSER UND SCHWEIZER, N. 72; DIGGELMANN, N. 5 und WALTER, Rz. 5.

[285] Vgl. DIGGELMANN, N. 10; BIAGGINI, Art. 13 N. 2; im Gegensatz dazu siehe BREITENMOSER UND SCHWEIZER, N. 5, welche Art. 13 BV als subsidiäres Auffangrecht gegenüber Art. 10 Abs. 2 BV qualifizieren.

[286] S*upra* Ziff. II.1.

[287] KIENER/KÄLIN/WYTTENBACH, § 4, Rz. 21 sowie BREITENMOSER UND SCHWEIZER, N. 6.

[288] Frei übersetzt – im Original: «de choisir son mode de vie, d'organiser ses loisirs et d'avoir des contacts avec autrui» (siehe BGE 103 Ia 293 E. 4a, S. 295). Weiterführend, KIENER/KÄLIN/WYTTENBACH, § 14, Rz. 11 sowie BREITENMOSER UND SCHWEIZER, N. 10.

[289] BGE 133 I 58 E. 6.1, S. 66f.

[290] Vgl. KIENER/KÄLIN/WYTTENBACH, § 14, Rz. 41; DIGGELMANN, N. 25; BREITENMOSER UND SCHWEIZER, N. 18 (m.w.H. auf die Rechtsprechung).

[291] DIGGELMANN, N. 29.

[292] Siehe z.B. BGE 128 II 259 E.3.2., S. 268.

[293] BREITENMOSER UND SCHWEIZER, N. 75.

[294] U.a. BGE 122 I 360 E. 5a, S. 362; KIENER/KÄLIN/WYTTENBACH, § 14, Rz. 55ff.; BREITENMOSER UND SCHWEIZER, N. 74; EPINEY/CIVITELLA/ZBINDEN, S. 17. Spezifisch zum Begriff des Missbrauchs siehe MAHON, Rz. 21ff. und WALTER, Rz. 5.

Selbstbestimmung, welches an die Verfügungshoheit des Grundrechtsträgers über alle seine persönlichen Daten anknüpft.[295]

Angesichts des im Kontext der Digitalisierung immer stärker werdenden Einflusses von Privaten auf die Privatsphäre von einzelnen Personen (in *casu* Arbeitgebende und Arbeitnehmende) liegt es in der Pflicht des Staates, diesem wachsenden Einfluss mit einer angemessenen grundrechtlichen Antwort zu begegnen, z.B. durch den Erlass von wirksamen Schutznormen.[296] Diese Auffassung teilt auch der EGMR, der sich im Urteil ***Bărbulescu gegen Rumänien*** (*supra* Ziff. 3.2.2) klar für das Bestehen einer solchen Pflicht ausspricht.[297] Im Bereich des Datenschutzes hat der Gesetzgeber in der Schweiz das Datenschutzgesetz und die Datenschutzverordnung erlassen (*infra* Ziff. 4.2). Im Beschäftigungskontext ist er diesen Pflichten durch den Erlass des Arbeitsgesetzes und dazugehörigen Verordnungen nachgekommen (*infra* Ziff. 4.3).

4.2. Das Datenschutzrecht

4.2.1. Allgemeines

Das Schweizerische Datenschutzrecht besteht aus dem Datenschutzgesetz (DSG)[298], der Datenschutzverordnung (VDSG)[299] sowie vereinzelten Bestimmungen in anderen Bundesgesetzen.[300] Nach diversen Teilrevisionen[301] wurde 2011 eine Totalrevision des DSG begonnen[302], welche im September 2020 abgeschlossen wurde (N-DSG).[303] Mit der Revision hat der Gesetzgeber auch den Entwicklungen im Europarat (*supra* Ziff. 3.2.3) und der EU (DSGVO – *supra* Ziff. 3.4.3) Rechnung getragen. Das neue Gesetz soll voraussichtlich 2022 in Kraft treten.[304]

Im Einklang mit den Vorgaben des Völker- und Europarechts gelten die allgemeinen Grundsätze der Datenbearbeitung und die wesentlichen Schutzinstrumente des Datenschutzrechts in der Schweiz «gleichermassen für Datenbearbeitungen von Privaten wie von Behörden».[305] Art. 1 DSG nennt den «Schutz der Grundrechte» als eines der Ziele des Gesetzes. Der ebenfalls genannte «Schutz der Persönlichkeit» schlägt des Weiteren die Brücke zu Art. 27ff. ZGB.[306] Im N-DSG wurden weitere Grundrechtsbezüge integriert, u.a. im Zusammenhang mit den neu formulierten Pflichten zum «Datenschutz durch Technik und datenschutzfreundlichen Voreinstellungen» (Art. 7 N-DSG) sowie der Datenschutz-Folgenabschätzung (Art. 22 N-DSG). Trotz diesen Bezügen zu den Grundrechten führt das neue DSG keine horizontale Wirkung von Grundrechten unter Privaten

---

[295] WEBER, Grundrechtskonzeption, S. 15f. und BGE 128 II 259 E.3.2., S. 268 und BGE 122 I 153 E. 6b) aa) und bb). Weiterführend zum Recht auf informationelle Selbstbestimmung, BREITENMOSER UND SCHWEIZER, N. 72; EPINEY/CIVITELLA/ZBINDEN, S. 17; FLÜCKIGER und MAHON, Rz. 18ff.

[296] DIGGELMANN, N. 31.

[297] EGMR, Bărbulescu v Romania, 61496/08 (2017), Ziff. 114f. Weiterführend DIGGELMANN, N. 32; BREITENMOSER UND SCHWEIZER, N. 84; WEBER, Grundrechtskonzeption, S. 28f. (m.w.H.).

[298] Bundesgesetz über den Datenschutz vom 19.07.1992, SR 235.1 (DSG).

[299] Verordnung zum Bundesgesetz über den Datenschutz vom 14.06.1993, SR 235.11.

[300] Für eine Übersicht siehe BUNDESRAT, Botschaft N-DSG, S. 7109ff.

[301] Vgl. HUSI-STÄMPFLI, S. N. 10ff.

[302] BUNDESRAT, Evaluation DSG 2011, insb. S. 347ff.

[303] Bundesgesetz über den Datenschutz vom 25.09.2020, BBl 2020, S. 7639ff.

[304] ROSENTHAL, N-DSG, RZ. 4.

[305] BREITENMOSER UND SCHWEIZER, N. 84; Art. 2 Abs. 1 lit. a DSG.

[306] Schweizerisches Zivilgesetzbuch vom 10.12.1907, SR 210 (ZGB).

ein.[307] So wird der Begriff «Grundrechte» im neuen DSG im Zusammenhang mit der Datenbearbeitung durch Bundesorgane verwendet; erfolgt die Datenbearbeitung hingegen durch Private, spricht das Gesetz vom «Schutz der Persönlichkeit».[308]

In der Folge werden die wichtigsten für den Schutz der Privatsphäre am Arbeitsplatz relevanten Grundsätze der schweizerischen Datenschutzgesetzgebung kurz erklärt und mit den für die vorliegende Untersuchung relevanten Neuerungen des N-DSG verglichen.

4.2.2. Datenschutzgesetz (DSG) und revidiertes Datenschutzgesetz (N-DSG)

Der Geltungsbereich des DSG ist in Art. 2 Abs. 1 definiert und umfasst den Schutz der Daten von natürlichen und juristischen Personen (Objekt der Datenbearbeitung) bei der Bearbeitung durch Privatpersonen (lit. a) oder durch Bundesorgane (lit. b) (Subjekt der Datenbearbeitung). Zukünftig *nicht* mehr unter den Schutzbereich des DSG fallen Daten juristischer Personen, diese bleiben jedoch durch Art. 28 ZGB geschützt.[309] Die Datenbearbeitung durch kantonale Behörden wird auf kantonaler Ebene geregelt und fällt ebenfalls nicht in den Anwendungsbereich des DSG.[310]

Art. 3 DSG umschreibt die wichtigsten Begriffe des Gesetzes.[311] Wie im europäischen Datenschutzrecht und analog zu Art. 13 Abs. 2 BV sieht das DSG vor, dass sich Personendaten auf eine bestimmte oder bestimmbare Person beziehen müssen.[312] Die Datenbearbeitung umfasst *jeden* Umgang mit Personendaten, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.[313] Eine wichtige begriffliche Neuerung im N-DSG betrifft das Profiling, die Bewertung bestimmter persönlicher Aspekte einer natürlichen Person auf Grundlage einer *automatisierten* Datenbearbeitung.[314] Es ersetzt den bisherigen Begriff «Persönlichkeitsprofil», welcher auch manuelle Bearbeitungsvorgänge umfasst.[315] Neu ist zudem das *Profiling mit hohem Risiko* für die Persönlichkeit oder die Grundrechte der betroffenen Person (z.B. bei einer Verknüpfung von Daten).[316] Das N-DSG spricht zudem statt vom «Inhaber der Datensammlung» (Person, die über Zweck und Inhalt entscheidet)[317] neu vom «Verantwortlichen», der über Zweck und Mittel der Bearbeitung entscheidet, und vom «Auftragsbearbeiter», der die Bearbeitung vornimmt.[318] Schliesslich wurde die Kategorie der besonders schützenswerten Personendaten (u.a. Gesundheitsdaten, Daten zur Intimsphäre, Rassenzugehörigkeit) im Rahmen der Revision um genetische und biometrische Daten ergänzt.[319]

---

[307] Siehe Botschaft N-DSG, S. 7029; vgl. auch ROSENTHAL, Entwurf N-DSG, Rz. 15.

[308] ROSENTHAL, N-DSG, Rz. 12.

[309] Art. 2 Abs. 1 N-DSG; ausführlich ROSENTHAL, N-DSG, Rz. 19.

[310] Siehe EPINEY/CIVITELLA/ZBINDEN, S. 18f.

[311] Folgende Begriffe werden im Art. 3 DSG definiert: Personendaten, betroffene Personen, besonders schützenswerte Personendaten, Persönlichkeitsprofil, Bearbeiten, Bekanntgeben, Datensammlung, Bundesorgane, Inhaber der Datensammlung, Gesetz im formellen Sinn.

[312] Art. 3 lit. a DSG/Art. 5 lit. a N-DSG.

[313] Art. 3 lit. e DSG/Art. 5 lit. d N-DSG.

[314] Art. 5 lit. f. N-DSG; zum Profiling in der DSGVO, *supra* Ziff. II.3.4.3. Für ein Beispiel am Arbeitsplatz, Ziff. III.3.4./III.5.4.

[315] Gem. Art. 3 lit. d DSG ist ein Persönlichkeitsprofil «eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt».

[316] Art. 5 lit. g N-DSG; ausführlich zu diesen Begriffen, ROSENTHAL, N-DSG, Rz. 24ff.

[317] Art. 3 lit. i DSG.

[318] Art. 5 lit. j und k N-DSG.

[319] Art. 5 lit. a Ziff.4 N-DSG; weiterführend ROSENTHAL, N-DSG, RZ. 22; vgl. für den Arbeitsplatz Ziff. III.4.4.5.

Die Grundsätze, wie Daten zu bearbeiten sind, finden sich in Art. 4, 5 Abs. 1 und 7 Abs. 1 DSG und in analogen Bestimmungen im N-DSG.[320] Dazu zählen Rechtmässigkeit[321], Treu und Glauben[322], Verhältnismässigkeit[323], Zweckbindung[324], Erkennbarkeit/Transparenz[325], Richtigkeit der Daten[326] sowie Datensicherheit[327]. Werden diese Grundsätze bei einer Datenbearbeitung verletzt, liegt eine Persönlichkeitsverletzung vor.[328] Dies gilt auch für Datenbearbeitungen, welche gegen den *ausdrücklichen* Willen einer betroffenen Person erfolgen[329] sowie die Bekanntgabe von besonders schützenswerten Personendaten an Dritte[330]. Eine Persönlichkeitsverletzung ist widerrechtlich, wenn die betreffende Datenverarbeitung nicht durch Einwilligung der betroffenen Person, ein überwiegendes privates/öffentliches Interesse oder durch Gesetz gerechtfertigt ist.[331] Das Schweizer Datenschutzrecht erlaubt somit grundsätzlich die (einwilligungsfreie) Bearbeitung von personenbezogenen Daten, sofern diese grundsatzkonform erfolgt oder anderweitig gerechtfertigt ist. Dies gilt auch für die Bearbeitung von besonders schützenswerten Personendaten und die Erstellung von Persönlichkeitsprofilen/Profiling.[332]

Mit Blick auf den Rechtfertigungsgrund der Einwilligung (Art. 13 Abs. 1 DSG) verlangt das Grundrecht auf informationelle Selbstbestimmung in jedem Fall, dass eine Einwilligung freiwillig erfolgt, d.h. sie muss ohne nachteilige Folgen verweigert werden können.[333] Deshalb ist die Freiwilligkeit bei Machtasymmetrien/Abhängigkeiten zwischen den Vertragsparteien, wie sie typischerweise z.B. in Arbeits- oder Mietverhältnissen vorliegen, kritisch zu hinterfragen.[334] Im Kontext eines Beschäftigungsverhältnisses gilt zudem Art. 328b OR, wonach jede personenbezogene Datenbearbeitung «die Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich [sein]» muss. Eine Einwilligung von Arbeitnehmenden kann deshalb eine Datenbearbeitung nur rechtfertigen, wenn sie zwar anderen Datenbearbeitungsgrundsätzen zuwiderläuft, aber in Einklang mit Art. 328b OR erfolgt (ausführlich zu Art. 328b OR, *infra* Ziff. 4.3.2). Der Vorrang von Art. 328b OR gilt auch in jenen Fällen, in welchen das DSG ein überwiegendes Interesse der bearbeitenden Person «in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags» annimmt (Art. 13 Abs. 2 lit. a DSG).[335]

Betroffenen Personen stehen verschiedene Instrumente zur Verfügung, um gegen die Bearbeitung ihrer Daten vorzugehen. Dazu gehören das Auskunftsrecht zu den über sie gesammelten Daten[336]

---

320 Ausführlich zu den Grundsätzen, ROSENTHAL, N-DSG, Rz. 33ff.

321 Art. 4 Abs. 1 DSG/Art. 6 Abs. 1 N-DSG.

322 Art. 4 Abs. 2 DSG/Art. 6 Abs. 2 N-DSG.

323 Art. 4 Abs. 2 DSG/Art. 6 Abs. 2 N-DSG.

324 Art. 4 Abs. 3 DSG/Art. 6 Abs. 3 N-DSG.

325 Art. 4 Abs. 4 DSG/Art. 6 Abs. 3 N-DSG.

326 Art. 5 Abs. 1 DSG/Art. 6 Abs. 5 N-DSG.

327 Art. 7 Abs. 1 DSG/Art. 8 N-DSG.

328 Art. 12 Abs. 2 lit. a DSG; siehe auch Art. 30 Abs. 2 lit. a N-DSG. Ausführlich, ROSENTHAL, N-DSG, Rz. 7, 38ff.

329 Art. 12 Abs. 2 lit. b DSG; Art. 30 Abs. 2 lit. b N-DSG.

330 Art. 12 Abs. 2 lit. c DSG; Art. 30 Abs. 2 lit. c N-DSG.

331 Art. 13 Abs. 1 DSG; Art. 31 N-DSG

332 ROSENTHAL, N-DSG, Rz. 7f.

333 BAERISWYL, Art. 4 DSG, N. 73ff.; siehe auch EK, Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017, S. 3 und Ziff. II.3.4.3.

334 Vgl. WERMELINGER, Art. 13 DSG, N. 19.

335 Art. 31 Abs. 2 lit. a N-DSG; weiterführend WERMELINGER, Art. 13 DSG, N. 19.

336 Art. 8 Abs. 1 DSG.

sowie die datenschutzrechtlichen Rechtsansprüche von Art. 15 DSG bei Vorliegen einer widerrechtlichen Persönlichkeitsverletzung.[337] Zudem gibt es gewisse Informationspflichten bei der Beschaffung von Personendaten.[338]

Das N-DSG erweitert das Auskunftsrecht der Betroffenen und enthält neu ein Recht auf Datenherausgabe oder -übertragung.[339] Um die Rechte der betroffenen Personen zu stärken, sieht das N-DSG auch umfassendere Informationspflichten vor, welche nicht nur bei der Beschaffung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen Anwendung findet, sondern bei allen Datenbearbeitungen.[340] Datenverantwortliche (und somit Arbeitgebende) sind unter dem N-DSG zudem verpflichtet, betroffene Personen zu informieren, wenn eine Entscheidung ausschliesslich aufgrund einer automatisierten Bearbeitung (einschliesslich Profiling) beruht und für die «betroffene Person mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt».[341] Automatisierte Einzelentscheidungen sind Entscheide basierend auf maschinellen Bewertungen von Personendaten.[342] Die betroffene Person hat in einer solchen Situation die Möglichkeit, ihren Standpunkt darzulegen und die Entscheidung von einer natürlichen Person überprüfen zu lassen.[343]

Ein Beispiel einer automatisierten Entscheidung im Kontext der Beschäftigung ist die Auswahl eines/einer Bewerbenden alleine aufgrund eines automatisierten Auswahlprozesses (vgl. Ziff. III.3). Nach Art. 21 Abs. 3 lit. a N-DSG bedarf es keiner Information/Anhörung der betroffenen Person, wenn «die automatisierte Einzelentscheidung in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags zwischen dem Verantwortlichen und der betroffenen Person steht und ihrem Begehren stattgegeben wird». Im Beispiel des Bewerbungsprozesses hiesse dies, dass nur abgelehnte Bewerbende ein Recht auf Information und Anhörung haben, nicht jedoch jene Person, welche ausgewählt wurde.[344] Zudem kann eine Anhörung unterbleiben, wenn die betroffene Person ausdrücklich in eine automatisierte Entscheidung eingewilligt hat.[345] Eine allgemeine arbeitsvertragliche Einwilligung genügt jedoch diesen Anforderungen nicht.

Das N-DSG beinhaltet neu auch eine Pflicht zur Vernichtung oder Anonymisierung von Daten, wenn der Zweck der Bearbeitung nicht mehr gegeben ist.[346] Wie in der DSGVO sind Datenverantwortliche und Auftragsbearbeiter zudem verpflichtet, Vorkehrungen zur Verhinderung von Datenschutzverletzungen treffen. Technologien müssen deshalb datenschutzfreundlich konzipiert (*privacy by design*) sein; zudem sind datenschutzfreundliche Voreinstellungen zu verwenden (*privacy by default*).[347] Technische und organisatorische Massnahmen müssen nach Art. 7 Abs. 2 N-DSG «dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie dem Risiko, das die Bearbeitung für die Persönlichkeit oder die Grundrechte der betroffenen

---

337 Art. 25 N-DSG (Auskunftsrecht); Art. 32 N-DSG (Rechtsansprüche).

338 Art. 14, 18, 18a DSG.

339 Art. 25-28 N-DSG; weiterführend, BIERI UND POWELL, Rz. 21ff.

340 Art. 19-21 N-DSG; ausführlich, ROSENTHAL, N-DSG, Rz. 92ff.

341 Art. 21 Abs. 1 N-DSG.

342 ROSENTHAL, N-DSG, Rz. 107. Gemäss dem Bundesrat fallen sog. «Wenn-Dann Entscheidungen» nicht darunter – ein Beispiel hierfür ist die Nichtherausgabe eines Geldbetrages am Bancomat, wenn die Kontodeckung ungenügend ist (Botschaft E-DSG, S. 7057).

343 Art. 21 Abs. 2 N-DSG.

344 ROSENTHAL, N-DSG, Rz. 114.

345 Art. 21 Abs. 3 lit. b N-DSG; ROSENTHAL, N-DSG, Rz. 114.

346 Art. 6 Abs. 4 N-DSG.

347 Art. 7 Abs. 1 und Abs. 3 N-DSG. Ausführlich zu diesen Konzepten, BUNDESRAT, Botschaft N-DSG, S. 7029f. und ROSENTHAL, N-DSG, Rz. 43ff.

Personen mit sich bringt, angemessen sein». Im Gegensatz zur aktuellen Regelung zur Datensicherheit in Art. 7 Abs. 1 DSG gilt Art. 7 N-DSG nicht als Bearbeitungsgrundsatz, d.h. das Fehlen von technischen und organisatorischen Massnahmen stellt nicht mehr automatisch eine Persönlichkeitsverletzung dar – was zu Recht kritisiert wird.[348]

Wenn eine Bearbeitung mit einem hohen Risiko für die Persönlichkeit/Grundrechte der betroffenen Person verbunden ist, muss vorgängig zudem eine Datenschutz-Folgenabschätzung (*privacy impact assessment*) gemacht werden[349], d.h. der Verantwortliche muss eine Prognose erstellen, wie und in welchem Umfang sich eine Bearbeitung auf die Persönlichkeit/Grundrechte einer Person auswirkt.[350]

4.3. Das Arbeitsrecht

4.3.1. Allgemeines

Die arbeitsvertraglichen Bestimmungen des OR, des Arbeitsgesetzes (ArG[351]) sowie der fünf dazugehörige Verordnungen (ArGV) setzen die aus dem Recht auf Privatsphäre fliessenden Schutzpflichten der Schweiz um.

Innerhalb des vertraglichen Abhängigkeitsverhältnisses gelten für Arbeitnehmende nach Art. 321d OR[352] die Anordnungen und Weisungen der Arbeitgebenden sowie die Treuepflicht nach Art. 321a Abs. 1 OR. Umgekehrt haben Arbeitgebende gegenüber ihren Arbeitnehmenden eine Fürsorgepflicht, die u.a. die Wahrung ihrer schutzwürdigen Interessen nach Art. 328 OR und damit auch den Schutz vor ungerechtfertigten Eingriffen in die Persönlichkeit beinhaltet (*infra* Ziff. 4.3.2).[353] Das Weisungs- und Kontrollrecht von Arbeitgebenden findet seine Grenzen somit in den Persönlichkeitsrechten der Arbeitnehmenden.

Nebst Art. 328 OR sind für die vorliegende Untersuchung Art. 328b OR, Art. 6 ArG sowie Art. 26 ArGV3 relevant. Art. 328b OR konkretisiert die Arbeitgeberfürsorgepflicht im Umgang mit Daten von Arbeitnehmenden, Art. 6 ArG befasst sich mit dem Schutz der Gesundheit von Arbeitnehmenden und Art. 26 ArGV3 beinhaltet gesetzliche Schranken mit Blick auf Überwachungs- und Kontrollsysteme am Arbeitsplatz.

4.3.2. Fürsorgepflicht der Arbeitgebenden (Art. 328/328b OR)

Ein spezifischer Anspruch von Arbeitnehmenden auf den Schutz ihrer Privatsphäre gegenüber Arbeitgebenden ergibt sich aus dem in Art. 328 OR enthaltenen arbeitsrechtlichen Persönlichkeitsschutz und der damit verbundenen Fürsorgepflicht.[354] Nach Abs. 1 haben Arbeitgebende die Pflicht, «die Persönlichkeit des Arbeitnehmers zu achten und zu schützen» und Eingriffe in die

---

348 Art. 30 Abs. 2 lit. a N-DSG. Kritisch zur neuen Regelung, ROSENTHAL, N-DSG, Rz. 43.

349 Art. 22 N-DSG; weiterführend hierzu ROSENTHAL, N-DSG, Rz. 148ff.

350 BUNDESRAT, Botschaft N-DSG, S. 7059f.

351 Bundesgesetz über die Arbeit in Industrie, Gewerbe und Handel vom 13.03.1964, SR 822.11 (ArG).

352 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30.03.1911, SR 220 (OR).

353 VISCHER UND MÜLLER, § 16 Rz. 1.

354 BRÜHWILER, OR 328, N. 12.

Persönlichkeit zu unterlassen, die nicht arbeitsvertraglich gerechtfertigt sind.[355] Abs. 2 verpflichtet Arbeitgebende Massnahmen zu treffen, um den «Schutz von Leben, Gesundheit und persönlicher Integrität» von Arbeitnehmenden zu gewährleisten. Eine praktisch identische Bestimmung findet sich in Art. 6 Abs. 1 ArG.

Die Fürsorgepflicht besteht während der Dauer des Arbeitsvertrages, kann aber im Sinne einer Vorwirkung auch bereits in der Bewerbungsphase analoge Anwendung finden.[356] Sie wird durch die datenschutzrechtliche Sonderbestimmung in Art. 328b OR ergänzt: «Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind». Die Bestimmung präzisiert in materieller Hinsicht den «Persönlichkeitsschutz des Arbeitnehmers beim Umgang mit Arbeitnehmerdaten»[357] und konkretisiert als *lex specialis* den in Art. 4 Abs. 2 DSG enthaltenen Verhältnismässigkeitsgrundsatz.[358] Ob Personendaten die Eignung für das Arbeitsverhältnis nach Art. 328b OR betreffen, muss im Einzelfall unter Würdigung aller Umstände abgeklärt werden.[359] Ergänzend zu Art. 328b OR sind die Bestimmungen des DSG anwendbar (*supra* Ziff. 4.2.2).

Im Unterschied zu allgemeinen Datenbearbeitungen (*supra* Ziff. 4.2.2) sind Datenbearbeitungen im Kontext von Beschäftigungsverhältnissen somit grundsätzlich *unzulässig*, ausser sie betreffen die Eignung des Arbeitnehmers oder sind zur Durchführung des Arbeitsvertrages erforderlich. Eine nach Art. 328b OR unrechtmässige Datenbearbeitung kann nach herrschender Lehre *nicht* durch einen Rechtfertigungsgrund nach Art. 13 DSG legitimiert werden.[360] Anderer Meinung sind ROSENTHAL UND JÖHRI, welche Art. 328b OR *nicht* als eine Verbotsnorm qualifizieren und auch bei einer Verletzung dieser Bestimmung eine Rechtfertigungsmöglichkeit nach Art. 13 DSG bejahen.[361]

Allerdings kann eine Einwilligung von Arbeitnehmenden in eine Datenbearbeitung, welche *nicht* deren Eignung oder die Durchführung des Arbeitsvertrags betreffen, ein Indiz dafür sein, dass eine Abrede nach Art. 362 Abs. 1 OR vorliegt. Eine solche Konstellation liegt z.B. vor, wenn Arbeitgebende einer Vermieterin/einem Vermieter eine Lohnreferenz mit Einverständnis des/der Arbeitnehmenden erteilen, welche sich für eine neue Wohnung bewerben.[362]

Im Zusammenhang mit der Fürsorgepflicht ist zusätzlich Art. 26 ArGV3 relevant.[363] Nach dieser Bestimmung sind Systeme zur Überwachung und Kontrolle des Verhaltens am Arbeitsplatz verboten (Abs. 1). Der Gebrauch von Kontroll- und Überwachungssystemen aus anderen Gründen darf weder Gesundheit noch Bewegungsfreiheit der Arbeitnehmenden beeinträchtigen (Abs. 2).

---

355 Zu dieser Bestimmung siehe REHBINDER UND STÖCKLI, OR 328, N. 4.

356 REHBINDER UND STÖCKLI, OR 328, N. 1. Siehe auch BRÜHWILER, OR 328, N 12, bezüglich des Persönlichkeitsschutzes von Bewerbenden. Brühwiler lehnt jedoch die analoge Anwendung der Fürsorgepflicht auf die Phase der Vertragsverhandlung ab, da eine Solche seiner Ansicht nach den Bestand (und somit den vorgängigen Abschluss) eines Arbeitsvertrages voraussetzt (BRÜHWILER, OR 320, N. 8 a).

357 BRÜHWILER, OR 328b, S. 242 (II.).

358 Vgl. BUNDESRAT, Botschaft DSG, S. 488 sowie PAPA UND PIETRUSZAK, Rz. 17.5 und REHBINDER UND STÖCKLI, OR 328b, N 4.

359 BRÜHWILER, OR 328b, N. 1.

360 STREIFF ET AL., OR 328b, N. 3; STAEHELIN, OR 328b, N. 1; PÄRLI, Art. 328b OR, N. 8.

361 ROSENTHAL UND JÖHRI, Art. 328b OR, N. 12; zur Auseinandersetzung siehe auch ALLENSPACH, Rz. 9f.

362 STREIFF ET AL., OR 328b, N. 3.

363 Verordnung 3 zum Arbeitsgesetz (Gesundheitsschutz) vom 18.08.1993, SR 822.113 (ArGV3).

Verletzungen der Fürsorgepflicht gegenüber Arbeitnehmenden stellen Vertragsverletzungen nach Art. 97ff. OR dar.[364] Zudem können sich Arbeitnehmende auf Art. 28a ZGB berufen, und Verletzungen von Schutzpflichten nach Art. 328 OR können zu Sanktionen des öffentlichen Arbeitsschutzrechts nach Art. 51ff. ArG führen.

4.4. Fazit

Analog zur GRC hat die Schweiz auf Verfassungsstufe nicht nur eine Bestimmung zum Recht auf Privatsphäre, sondern explizit auch eine zum Datenschutz verankert. Die Anwendbarkeit des Rechts auf Privatsphäre im beruflichen Kontext ist zwar nicht ausdrücklich festgehalten, ergibt sich aber aus den offenen Formulierungen von Art. 13 Abs. 1 BV (Schutz der Privatsphäre) sowie Art. 10 Abs. 2 BV (Persönliche Freiheit). Art. 13 Abs. 2 BV garantiert zudem das Recht auf informationelle Selbstbestimmung und die Verfügungshoheit einer natürlichen Person über ihre Daten.

Auf Gesetzesstufe setzt der Bund seine Schutzpflichten primär im ArG und dem DSG um. Diese Gesetze gewährleisten den Schutz der Persönlichkeit und der Privatsphäre sowie den Datenschutz von Arbeitnehmenden im Kontext des digitalen Wandels am Arbeitsplatz. Während im Bereich des Arbeitsrechts die Arbeitgeberfürsorgepflicht nach Art. 328/328b OR im Vordergrund steht, sind beim DSG die in Art 4, 5 und 7 DSG enthaltenen datenschutzrechtlichen Grundsätze von Bedeutung um zu prüfen, ob eine Persönlichkeitsverletzung am Arbeitsplatz vorliegt.

Das N-DSG übernimmt diesen Ansatz und stärkt zugleich den Schutz der betroffenen Personen über ihre eigenen Daten. Zudem wird mit der Übernahme der Konzepte «*privacy by design*», «*privacy by default*» oder der Datenschutz-Folgenabschätzung (*privacy impact assessment*) den Entwicklungen im Rahmen der DSGVO Rechnung getragen.

[364] REHBINDER UND STÖCKLI, OR 328, N. 22; BRÜHWILER, OR 328, S. 218 (II.).

III. SZENARIEN – DIGITALISIERUNG UND PRIVATSPHÄRE AM ARBEITSPLATZ

1. Einleitung

Die nachfolgenden Szenarien beschreiben im Zusammenhang mit der Digitalisierung stehende und das Berufsleben betreffende Sachverhalte, in welchen eine Verletzung der Privatsphäre von Arbeitnehmenden durch Arbeitgebende möglich ist. Ziel dieses Abschnitts ist es (1) grundrechtlich relevante Sachverhalte zum Schutz der Privatsphäre von Arbeitnehmenden im Zeitalter der Digitalisierung zu identifizieren und (2) die Anwendbarkeit des bestehenden rechtlichen Rahmens (in der Schweiz) auf diese Sachverhalte zu untersuchen.

Die in den Szenarien geschilderten Sachverhalte wurden vom Projektteam entworfen und in Konsultationen mit wichtigen Akteuren des Arbeitsmarktes – privatrechtliche und öffentlich-rechtliche Arbeitgebende, Arbeitgebendenverbände, Gewerkschaften und Datenschutzbeauftragte – auf ihre Relevanz überprüft. Bei der Auswahl der Technologien hat das Projektteam darauf geachtet, sowohl aktuelle, als auch zukünftig relevante Technologien in den Szenarien einzubeziehen. «Ältere» Technologien wie z.B. die Telefonüberwachung wurden hingegen ausgeklammert.

Die ausgewählten Szenarien beschränken sich auf das Verhältnis zwischen *Arbeitgebenden und Arbeitnehmenden* und befassen sich nicht mit potenziellen Verletzungen der Privatsphäre von Arbeitnehmenden durch Drittparteien (z.B. Bewertung von Lehrpersonen durch Schulkinder, Bewertung von Uber-Fahrdienst durch Kundschaft) und von Drittparteien durch Arbeitgebende (z.B. unbefugte Weitergabe von Kundendaten) aus.

2. Szenario 1: Informationsbeschaffung im Internet/in sozialen Netzwerken während des Bewerbungsverfahrens

2.1. Sachverhalt

Während des Auswahlprozesses für die Besetzung einer vakanten Arbeitsstelle gibt es heute eine Vielzahl von Möglichkeiten für Arbeitgebende, sich zusätzlich zum Gespräch mit Stellenbewerbenden und den von diesen eingereichten Unterlagen über das Internet und digitale soziale Netzwerke[365] weitere Informationen über die Bewerbenden zu verschaffen. Diese digital verfügbaren Informationen werden oft von den bewerbenden Personen selbst oder von Dritten «aufgeschaltet», sind häufig öffentlich zugänglich und bleiben ohne spezielle Vorkehrungen in zeitlicher Hinsicht für andere Internetnutzende praktisch unbeschränkt abrufbar.[366]

Die Informationsbeschaffung über Stellenbewerbende im Internet kann zum einen manuell durch Arbeitgebende selber vorgenommen werden. Zum andern gibt es auch auf Algorithmen basierte Programme, welche das Internet nach diesen Informationen durchsuchen und Bewerbende gestützt auf (programmierte) Kriterien auf deren Eignung für eine ausgeschriebene Stelle bewerten.

---

[365] Zum Begriff siehe WILDHABER UND HÄNSENBERGER, Social Media im Arbeitsverhältnis, S. 529f.

[366] Vgl. WEBER UND HEINRICH. Siehe auch EuGH, C-131/12, Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos, Urteil vom 13.05.2014.

Das vorliegende Szenario befasst sich mit der rechtlichen Beurteilung der manuellen online-Informationsbeschaffung durch Arbeitgebende. Die automatisierte Informationsbeschaffung innerhalb eines Bewerbungsprozesses wird in Szenario 2 (*infra* Ziff. 3) behandelt.

2.2. Relevanz und Problembereiche

Bereits vor mehr als zehn Jahren haben gemäss den Erläuterungen des Eidgenössischen Datenschutzbeauftragten (EDÖB) zu sozialen Netzwerken rund zwei Drittel aller Personalverantwortlichen Internetsuchmaschinen benutzt, um zusätzliche Informationen über bewerbende Personen zu erhalten.[367] Vergleichbare aktuelle Schätzungen liegen für das Durchforsten von beruflichen und sozialen Medien (*social media screening*) von Bewerbenden vor.[368]

Im Rahmen der qualitativen Umfrage bei den relevanten Akteuren wurden als mögliche Mittel der Informationsbeschaffung in einem Bewerbungsprozess insbesondere Suchmaschinen («googeln»), persönliche Webseiten und Blogs sowie soziale Netzwerke mit oder ohne beruflichen Bezug (z.B. LinkedIn, Xing bzw. Facebook, Instagram) genannt. Dabei ergibt sich hinsichtlich der Häufigkeit und Art der verwendeten Methoden kein einheitliches Bild. Vergleichsweise oft wird die Informationsbeschaffung über soziale Netzwerke mit beruflichem Bezug genutzt, gefolgt von der gewöhnlichen Internetrecherche («googeln»). Die meisten Unternehmen geben an, soziale Netzwerke ohne beruflichen Bezug eher selten zu konsultieren. Verschiedene Interviewpartner haben überdies darauf hingewiesen, dass die Unternehmen inzwischen aktiv über berufliche soziale Medien rekrutieren (*active sourcing*).

Bei der Beschaffung von Informationen über Bewerbende aus dem Internet befürchten die konsultierten Akteure, dass aufgrund von frei verfügbaren und einsehbaren persönlichen Daten nicht arbeitsplatzrelevante Informationen bei der Beurteilung einer Bewerbung mitberücksichtigt werden. Zudem wurde der praktische Aspekt der «Verwechslungsgefahr» hervorgehoben. Gerade bei sehr geläufigen Namen bestünde ein Risiko, dass persönliche Informationen einer anderen Person in die Beurteilung der Bewerbung einflössen. Andererseits wird auch die Eigenverantwortung jeder Einzelperson für die Veröffentlichung von persönlichen Informationen auf (teils öffentlich zugänglichen) Plattformen hervorgehoben. Damit verbunden ist die Frage, ob es sich bei öffentlich zugänglichen Informationen wirklich um private oder nicht doch um öffentliche Informationen handelt.

Bei sozialen Netzwerken *ohne* beruflichen Bezug überwog die Ansicht, dass eine Einwilligung der Bewerbenden grundsätzlich notwendig ist, wenn über diese Plattformen Informationen beschafft werden. Hinsichtlich dem Erwerb von Informationen über soziale Medien *mit* beruflichem Bezug wurde diese Ansicht hingegen nur vereinzelt vertreten, da solche Plattformen einem beruflichen Zweck und somit der Eigenvermarktung dienten und deshalb eine stillschweigende Einwilligung bereits vorhanden sei. Jede vermeintlich «freiwillige» Einwilligung im Arbeitsbereich (einschliesslich des Bewerbungsverfahrens) sei jedoch aufgrund des dem Arbeitsverhältnis zugrundeliegenden Subordinationsverhältnisses kritisch zu überprüfen.

---

[367] EDÖB, Erläuterungen Soziale Netzwerke und EGLI, Rz. 63, Fn. 43. Weiterführend, PÄRLI, Evaluieren, kontrollieren, überwachen, S. 38ff.

[368] Siehe z.B. http://press.careerbuilder.com/2018-08-09-More-Than-Half-of-Employers-Have-Found-Content-on-Social-Media-That-Caused-Them-NOT-to-Hire-a-Candidate-According-to-Recent-CareerBuilder-Survey (zuletzt besucht am 20.04.2021); vgl. auch CUSTERS UND URSIC, S. 328 und MÜLLER, Schweizer Konzerne überprüfen Bewerber im Internet.

Andere Untersuchungen zeigen, dass stellensuchende Personen der Praxis des *social media screening* im Rahmen von Bewerbungsprozessen – auch hinsichtlich ihrer öffentlich zugänglichen Daten – sehr skeptisch gegenüberstehen, da es nicht möglich ist, festzustellen, wie diese Daten von Drittpersonen tatsächlich genutzt werden.[369]

Die nachfolgende Analyse beschränkt sich angesichts der grossen Anzahl an unterschiedlichen Online-Plattformen auf drei Methoden/Medien: die gewöhnliche Internetrecherche sowie soziale Netzwerke mit (z.B. LinkedIn) und ohne beruflichen Bezug (z.B. Facebook). Aufgrund der Vielzahl von Konstellationen, wie das Internet und unterschiedliche soziale Medien von einzelnen Personen genutzt werden können, beinhalten die nachfolgenden Aussagen gewisse Verallgemeinerungen.

2.3. Grund- und menschenrechtliche Fragestellungen

Vorab ist zu definieren, welche Daten im Zusammenhang mit Bewerbungsverfahren privat sind und welche Kriterien (z.B. Urheberschaft) für diese Beurteilung gelten. Hinsichtlich der Urheberschaft muss beachtet werden, dass die Privatsphäre betreffende Informationen ohne das Wissen und auch gegen den Willen einer Person im Internet vorhanden sein können.[370] Weiter stellt sich die Frage, ob öffentlich zugängliche Informationen im Internet und auf beruflichen/freizeitlichen sozialen Netzwerken grundsätzlich als öffentlich gelten, da sie oft ohne Zugangsbeschränkung abrufbar sind. Abzuklären ist auch, ob Informationen von beruflichen sozialen Netzwerken (z.B. LinkedIn, Xing) rechtlich anders zu beurteilen sind als Informationen aus freizeitlichen sozialen Medien (z.B. Facebook, Instagram).[371] Schliesslich ist zu prüfen, unter welchen Voraussetzungen private Daten durch potenzielle Arbeitgebende dennoch bearbeitet werden können und welche Grundsätze der Datenbearbeitung für das Bewerbungsverfahren gelten.

2.4. Rechtliche Beurteilung

2.4.1. Rechtliche Grundlagen

Obwohl Art. 328b OR dem Wortlaut nach nur auf das Verhältnis zwischen Arbeitgebenden und Arbeitnehmenden anwendbar ist, erstreckt sich dessen zeitlicher Anwendungsbereich auch auf den Bewerbungsprozess.[372] Bei der Prüfung, ob sich Bewerbende für die in Frage stehende Stelle eignen, ist es grundsätzlich erlaubt, Informationen im Rahmen eines Einstellungsgesprächs oder durch das Einholen von Referenzen, Zeugnissen etc. zu erheben.[373] Dieser Informationsbeschaffung sind aber rechtliche Grenzen gesetzt.

Arbeitgebende dürfen nach Art. 328b OR nur Informationen einholen, welche sich objektiv auf die Eignung der bewerbenden Person für die in Frage stehende Anstellung beziehen.[374] Zusätzlich zu

---

369 Vgl. JACOBSON UND GRUZD.

370 DATENSCHUTZBEAUFTRAGTER KANTON ZÜRICH, Ziff. 3.1.

371 Je nach Land oder Beschäftigungsfeld können auch freizeitliche soziale Netzwerke einen beruflichen Bezug aufweisen und umgekehrt – diese Bewertung hat jeweils einzelfallbezogen zu erfolgen.

372 STREIFF ET. AL., OR 328b, N. 4.

373 REHBINDER UND STÖCKLI, OR 320, N 3f.

374 U.a. REHBINDER UND STÖCKLI, OR 328b, N 25; BRÜHWILER, OR 320, N 8b und OR 328b, N 9a. Siehe auch EDÖB, Leitfaden Bearbeitung Personendaten im Arbeitsbereich, S. 8 und BGE 122 V 267 E. 3b, S. 268f.

Art. 328b OR kommt Art. 4 DSG[375] zur Anwendung, da alle Angaben von Bewerbenden Personendaten im Sinne des DSG darstellen. Art. 4 DSG definiert die Grundsätze, welche im Rahmen von Datenbearbeitungen eingehalten werden müssen, wobei *in casu* v.a. die Verhältnismässigkeit nach Art. 4 Abs. 2 DSG von Bedeutung ist. In einem Bewerbungsprozess notwendig und geeignet sind insbesondere Daten «über die *fachliche und persönliche* Eignung einer Stellenbewerberin oder eines Stellenbewerbers für die Ausübung der ausgeschriebenen Stelle.»[376]

Das Einholen von zusätzlichen Informationen, welche das Privatleben von Bewerbenden betreffen, ist deshalb grundsätzlich *nicht* zulässig. Dabei handelt es sich um alle Informationen, welche die bewerbende Person als Privatsache definiert haben möchte.[377] Bekannte Beispiele für eine unzulässige Datenerhebung im Rahmen von Rekrutierungsprozessen betreffen z.B. eine Schwangerschaft, Lebensgewohnheiten, Kinderwünsche, die sexuelle oder politische Ausrichtung oder den allgemeinen Gesundheitszustand.[378] Das Fragerecht der Arbeitgebenden findet seine Grenzen somit in der Persönlichkeit und der Privatsphäre der Bewerbenden.[379] Informationen über Bewerbende müssen zudem grundsätzlich bei diesen selber eingeholt werden, um die Richtigkeit der Daten nach Art. 5 DSG zu gewährleisten.[380]

2.4.2. Internetrecherche

Vor der Beantwortung der relevanten rechtlichen Fragen im Zusammenhang mit der Internetrecherche von Arbeitgebenden ist die Rolle von Internetsuchmaschinenbetreibern bei der Bereitstellung von personenbezogenen Daten im Internet kurz zu erläutern. Diese Intermediäre stellen personenbezogene Daten nicht von sich auch ins Internet, sondern geben «nur» bereits vorhandene Informationen wieder.[381] Der EuGH hat sich 2014 in *Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos*[382] ausführlich dazu geäussert. Eine natürliche Person hatte vor nationalen Gerichten beantragt, dass ihn betreffende personenbezogene Daten nicht mehr in den Suchergebnissen von Google erscheinen und/oder gelöscht werden sollen. Der Gerichtshof hielt fest, dass Suchmaschinenbetreiber durch das Durchforsten des Internets, die Indexierung von Suchresultaten und die Wiedergabe der Ergebnislisten personenbezogene Daten *verarbeiten* und deshalb als Datenverantwortliche anzusehen sind.[383] Mittels den von den Suchmaschinenbetreibern zur Verfügung gestellten Ergebnislisten könnten Suchende deshalb leichter an Informationen kommen, welche sie ohne die Suchmaschine nicht gefunden hätten. Die Betreiber hätten so einen «massgeblichen Anteil an der weltweiten Verbreitung

---

375 Zum Verhältnis zwischen Art. 328b OR und Art. 4 DSG siehe STREIFF ET AL., OR 328b, N. 3.

376 DATENSCHUTZBEAUFTRAGTER KANTON ZÜRICH, Ziff. 2 (Hervorhebung hinzugefügt).

377 KIENER/KÄLIN/WYTTENBACH, § 14, Rz. 11.

378 Auch bei diesen Beispielen ist es allerdings nicht ausgeschlossen, dass es sich um rechtlich zulässige Fragen handelt, sofern diese Informationen zur Erfüllung der jeweiligen Arbeit notwendig sind (z.B. bei sog. Tendenzbetrieben). Ausführlich, STREIFF ET. AL., OR 328b, N. 10.

379 VISCHER UND MÜLLER, § 9 Rz. 7 und BGE 122 V 267 E. 3b, S. 268f. Allgemein zur Auskunftspflicht von Bewerbenden, VISCHER UND MÜLLER, § 9 Rz. 4ff.; BRÜHWILER, OR 320, N 8b.

380 DSB ZH, Online-Recherche, Ziff. 2.

381 Vgl. EGLI, Rz. 78.

382 EuGH, C-131/12, Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos, Urteil vom 13.05.2014.

383 EuGH, C-131/12, Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos, Urteil vom 13.05.2014, Ziff. 32f.

personenbezogener Daten» sowie deren Sichtbarmachung gegenüber Dritten.[384] Bezüglich der beantragten Löschung der Daten hat der Gerichtshof festgehalten, dass eine Löschung des Links zur fraglichen Information – nicht die Löschung der Information selbst – möglich ist, «wenn die Daten für die Zwecke, für die sie erhoben oder verarbeitet worden sind, [in Anbetracht der verstrichenen Zeit] nicht mehr erforderlich sind.»[385] Mit dieser Argumentation hat der EuGH die datenschutzrechtliche Verantwortung von Suchmaschinenbetreibern und ein Löschungsrecht des Antragstellers bejaht. Dieser etwas unpräzis als «Recht auf Vergessenwerden»[386] bezeichnete Anspruch wurde daraufhin auch in Art. 17 DSGVO verankert.

Ein Recht auf Vergessenwerden ist in der Schweiz nicht explizit normiert. Dies hängt u.a. damit zusammen, dass ein solches Recht in technischer Hinsicht gar nicht umsetzbar ist. Vielmehr geht es darum, dass personenbezogene Informationen von den Suchmaschinenbetreibern nicht mehr indexiert und angezeigt werden dürfen.[387] In der Schweiz schafft Art. 12 Abs. 2 lit. b DSG[388] Abhilfe. So dürfen Daten *gegen den ausdrücklichen Willen* einer Person nur bearbeitet werden, wenn ein Rechtfertigungsgrund vorliegt. Ist dies nicht der Fall, liegt eine widerrechtliche Persönlichkeitsverletzung vor und betroffenen Personen stehen die Rechtsansprüche von Art. 15 DSG offen.

Während die datenschutzrechtliche Verantwortlichkeit von Internetsuchdiensten durch den EuGH bestätigt wurde und auch gemäss DSG gilt, stellt sich die weitergehende Frage, ob Arbeitgebende davon profitieren dürfen, dass diese Betreiber personenbezogene Daten von Bewerbenden mit oder ohne deren Wissen in strukturierter Form wiedergeben. Diese Frage ist unter Einbezug der in Art. 328b OR und Art. 4 DSG genannten Grundsätze zu beantworten. Demnach dürfen Arbeitgebende nur Daten von Bewerbenden aus dem Internet erheben und bearbeiten, welche die Eignung eines Bewerbenden für das Arbeitsverhältnis betreffen. Eine generelle online-Durchleuchtung von Bewerbenden ist unzulässig, da beruflich Relevantes nicht auf Anhieb von anderen Informationen zu unterscheiden ist.[389] Des Weiteren muss bei der Internetrecherche der Grundsatz der Datenrichtigkeit nach Art. 5 DSG beachtet werden. Dieser verlangt, dass sich Datenbearbeitende vergewissern, dass die von ihnen erhobenen und bearbeiteten Daten richtig sind. In einem Bewerbungsverfahren ist dies in der Regel nicht möglich, da Arbeitgebende nur über sehr eingeschränkte Informationen zu den Bewerbenden verfügen (z.B. den Lebenslauf). Aufgrund der Tatsache, dass die Auflistung der Suchergebnisse in Internetsuchmaschinen von den betroffenen Personen nicht oder nur sehr beschränkt beeinflussbar ist, können zudem Daten gegen den Willen von betroffenen Personen im Netz vorhanden und auffindbar sein.[390]

Zusammenfassend lässt sich festhalten, dass die online-Informationsbeschaffung von Arbeitgebenden über Bewerbende weder mit Art. 328b OR noch mit den Grundsätzen im DSG vereinbar ist und eine widerrechtliche Persönlichkeitsverletzung nach Art. 12/13 DSG darstellt.

---

[384] EuGH, C-131/12, Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos, Urteil vom 13.05.2014, Ziff. 36.

[385] EuGH, C-131/12, Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos, Urteil vom 13.05.2014, Ziff. 93.

[386] EuGH, C-131/12, Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos, Urteil vom 13.05.2014, Ziff. 91.

[387] Weiterführend zum Recht auf Vergessen WEBER UND HEINRICH.

[388] Art. 30 Abs. 2 lit. b N-DSG.

[389] STREIFF ET AL., OR 328b, N. 5; BRÜHWILER, OR 320, N 8b; SCHÜRER UND WANNER, S. 56; siehe auch DATENSCHUTZBEAUFTRAGTER KANTON ZÜRICH, Ziff. 3.1 und BGE 122 V 267 E. 3b, S. 268.

[390] Zum Ganzen, EGLI, Rz. 77ff., welcher die Recherche im Internet mit der systematischen Ausleuchtung einer Person durch einen Privatdetektiv vergleicht (Rz. 79).

2.4.3. Soziale Medien

A. Freizeitliche Soziale Medien

Freizeitliche soziale Medien enthalten typischerweise Informationen über das Privatleben der nutzenden Personen, wie z.B. soziale Kontakte, Freizeitaktivitäten oder andere persönliche Informationen. In der Schweiz populär sind u.a. Facebook, Twitter, Instagram, WhatsApp oder Pinterest. Allerdings werden auch diese Medien – je nach Person, beruflichem Kontext oder geographischen Hintergrund – für berufliche Zwecke genutzt. Für die Zwecke der vorliegenden Studie wird der Einfachheit halber davon ausgegangen, dass freizeitliche soziale Medien nur private Informationen enthalten.

Obwohl sich die konsultierten Akteure hinsichtlich der Informationsbeschaffung über freizeitliche soziale Medien eher zurückhaltend geäussert haben (*supra* Ziff. 2.2), gibt es durchaus Hinweise darauf, dass diese Art der Informationsgewinnung von vielen Arbeitgebenden regelmässig genutzt wird.[391] Auf diesen Plattformen werden private Informationen mit einem mehr oder weniger breiten Benutzerkreis (bis hin zu einer breiteren Öffentlichkeit) geteilt. Durch das Einsehen von freizeitlichen sozialen Medien können Arbeitgebende private Informationen über Bewerbende, deren familiäre Situation, sexuelle Orientierung, politische und persönliche Überzeugungen, Freizeitaktivitäten oder über deren Freundeskreis erfahren. Dadurch ist es ihnen möglich, ein Profil der bewerbenden Person zu erstellen, welches mehr private Informationen beinhaltet als die eingereichten Bewerbungsunterlagen offenlegen. Diese Art der Informationsgewinnung – analog zur gewöhnlichen Internetrecherche (*supra* Ziff. 2.4.2) – ist nicht mit Art. 328b OR und somit unzulässig.

Im Zusammenhang mit der Preisgabe von privaten Informationen auf freizeitlichen sozialen Medien bleibt allerdings zu prüfen, ob die betroffene Person auf den sozialen Medien bewusst einen offenen Adressatenkreis gewählt hat und private Informationen deshalb auch für nicht «befreundete» Arbeitgebende *uneingeschränkt* zugänglich sind (Art. 12 Abs. 3 DSG). Diese Rechtfertigungsbestimmung beruht auf der Überlegung, dass von einer Person allgemein zugänglich gemachte Daten die Privatsphäre und Persönlichkeit dieser Person nicht verletzen.[392] Im Kontext des Beschäftigungsverhältnisses ist diese Argumentation jedoch abzulehnen. Wie bereits unter Ziff. II.4.3.2 erläutert, müssen grundsätzlich *alle* Datenbearbeitungen im Bewerbungsprozess oder im Arbeitsverhältnis einen Arbeitsplatzbezug aufweisen – Art. 328b OR kommt hier eine eigenständige Bedeutung und Vorrang gegenüber Art 12 Abs. 3 DSG zu.[393]

Selbst wenn eine Verletzung von Art. 328b OR den Rechtfertigungsmöglichkeiten von Art. 12 Abs. 3 und Art 13 DSG unterliegen würde – so Rosenthal und Jöhri[394] –, ist die Rechtmässigkeit für eine solche «freizeitliche» Recherche abzulehnen. Dies deshalb, da sich der Charakter der Information nicht über den Adressatenkreis, sondern deren Inhalt definiert. Die Tatsache, dass jemand eine private Information zugänglich macht, bedeutet nicht automatisch, dass diese auch für Zwecke verwendet werden darf, an welche der Dateninhaber bei der Veröffentlichung nicht gedacht hatte.[395] Analog zur Internetrecherche stellt sich zudem auch bei Profilen in sozialen Medien das Problem, dass Firmen nicht wissen können, ob eine bewerbende Person ein solches Profil

---

[391] Siehe *supra* Fn. 368.

[392] WERMELINGER, Art. 12 DSG, N. 12.

[393] STREIFF ET AL., OR 328b, N. 3 Siehe auch WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz, S. 326ff.

[394] Vgl. Ziff. II.4.3.2.

[395] EGLI, Rz. 72. Gleicher Meinung SCHÜRER UND WANNER, S. 56; STREIFF ET AL., Art. 328b, N. 9 und 10 (mit den abweichenden Ansichten in N 10 aufgelistet). Siehe auch DATENSCHUTZBEAUFTRAGTER KANTON ZÜRICH, Ziff. 3.2

tatsächlich selber veröffentlicht hat.[396] Wesentlich ist auch, dass eine Veröffentlichung online oftmals einen permanenten Charakter aufweist und eine nachträgliche Löschung der Daten unmöglich oder zumindest schwierig ist.[397] Nur aufgrund von (nicht manuell angepassten) Privatsphäre-Einstellungen sollte ebenfalls nicht pauschal von einer konkludenten Einwilligung ausgegangen werden, da die Betreiber von sozialen Medien standardmässig oft ein eher geringeres Schutzniveau der Privatsphäre der Nutzerinnen und Nutzer gewährleisten und die Anpassung der Einstellungen in technischer Hinsicht nicht immer einfach ist.[398] Obwohl es in der jüngeren Vergangenheit Bestrebungen von Betreibern von sozialen Medien gegeben hat, die Privatsphäre-Einstellungen benutzerfreundlicher auszugestalten, so scheint noch kein grundlegender Paradigmenwechsel diesbezüglich stattgefunden zu haben.[399]

Eine Konsultation von freizeitlichen Profilen von Bewerbenden auf sozialen Medien kann hingegen erlaubt sein, wenn es die Art der Arbeit verlangen würde, über gewisse private Aktivitäten Bescheid zu wissen, z.B. bei sog. Tendenzbetrieben.[400] So können im Rahmen einer beruflichen Tätigkeit für eine religiöse/politische Gemeinschaft die religiöse/politische Ausrichtung einer Person zu den berufsrelevanten Informationen zählen – in diesen Fällen würde eine entsprechende Datenbearbeitung auch dem Grundsatz von Art. 328b OR entsprechen.

Wird wie durch ROSENTHAL UND JÖHRI[401] die Ansicht vertreten, dass es sich bei Art. 328b OR nicht um eine Verbotsnorm handelt und dass eine Bearbeitung privater Daten durch Arbeitgebende durch die in Art. 13 DSG aufgelisteten Gründe gerechtfertigt werden kann, bleibt zudem zu prüfen, ob das Zusammentragen von persönlichen Aspekten von Bewerbenden als «Persönlichkeitsprofil» im Sinne des DSG qualifiziert werden kann.[402] Hierzu müssten die von Arbeitgebenden gewonnenen Informationen geeignet sein, um «wesentliche (Teil-)Aspekte» der Persönlichkeit eines Bewerbenden beurteilen zu können.[403] Ist dies der Fall, liegt ein Persönlichkeitsprofil vor, das nur erhoben werden darf, wenn die betroffene Person *ausdrücklich* in die Datenbearbeitung eingewilligt hat oder ein anderer Rechtfertigungsgrund vorliegt.[404]

Grundsätzlich ist jedoch davon auszugehen, dass nicht jede Zusammenstellung von zusätzlichen Informationen von Bewerbenden ausreicht, um als Persönlichkeitsprofil im Sinne des DSG zu gelten. Vielmehr dürfte es nötig sein, dass diese persönlichen Aspekte mit einer gewissen Systematik zusammengetragen und in Beziehung zueinander gesetzt werden. Diese zurückhaltende Interpretation ist ebenfalls im Einklang mit dem neuen DSG, in welchem der Begriff «Persönlichkeitsprofil» durch «Profiling» ersetzt wird (Ziff. II.4.2.2). Ein solches verlangt analog zur

---

und EU, Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017, S. 12f. Zurückhaltend, WERMELINGER, Art. 12 DSG, N. 9ff.

396 So auch GEISER, zitiert in: MÜLLER, Schweizer Konzerne überprüfen Bewerber im Internet.

397 WERMELINGER, Art. 12 DSG, N. 11.

398 Z.B. CUSTERS UND URSIC, S. 328; EGLI, Rz. 72. Siehe zum Bewusstsein von Personen hinsichtlich der Privatsphäre-Einstellungen auch JACOBSON UND GRUZD, S. 182f.

399 Siehe z.B. https://www.facebook.com/help/203805466323736 (zuletzt besucht am 20.04.2021) – öffentlich zugänglich sind z.B. Informationen zur Altersgruppe, des Geschlechts, der Sprache und des Landes sowie das «öffentliche Profil» (u.a. Name, Geschlecht, Profilbild, Titelbild, Netzwerke).

400 Vgl. z.B. STREIFF ET AL., OR 328b, N. 5.

401 Vgl. Ziff. II.4.3.2

402 Zum Persönlichkeitsprofil, Ziff. II.4.2.2.

403 RUDIN, N. 31.

404 Art. 3 lit. d i.V.m. Art. 4 Abs. 5 DSG.

DSGVO eine *automatisierte* Datenverarbeitung; manuelle Recherchen fallen gar nicht erst nicht darunter.

Analog zur Internetrecherche kann geschlussfolgert werden, dass die manuelle Informationsbeschaffung von Arbeitgebenden über Bewerbende in freizeitlichen sozialen Medien eine widerrechtliche Persönlichkeitsverletzung nach Art. 328b OR i.V.m. Art. 12/13 DSG darstellt, sofern diese Informationen nicht berufsrelevant sind (z.B. bei Tendenzbetrieben).[405] Aufgrund der fehlenden Systematik handelt es sich bei der manuellen Recherche im Normalfall wohl auch nicht um ein Persönlichkeitsprofil (Art. 3 lit. d DSG), welches von Arbeitgebenden erstellt wird.

B. Berufliche Soziale Medien

In beruflichen sozialen Netzwerken (u.a. LinkedIn, Xing) können Nutzerinnen und Nutzer ein Profil erstellen, um ihren beruflichen Werdegang mit anderen Personen zu teilen und ein professionelles Netzwerk zu pflegen. Solche Profile dienen der beruflichen Selbstdarstellung, der Aufrechterhaltung von geschäftlichen Kontakten und sie können die Chancen auf eine neue Anstellung erhöhen. Das Profil kann, je nach Einstellungen, von den verlinkten Kontakten oder einer breiteren Öffentlichkeit eingesehen werden.[406] Wie bereits erwähnt, nutzen Unternehmen diese Plattformen auch zur proaktiven Personalrekrutierung – d.h. Unternehmen recherchieren von sich aus geeignete Kandidatinnen und Kandidaten und stellen den Kontakt zu diesen selber her (*active sourcing*).[407]

Recherchen von Arbeitgebenden auf den beruflichen Profilen von Bewerbenden sind im Unterschied zur Recherche auf freizeitlichen sozialen Netzwerken oder der Internetrecherche zulässig, da sie einen genügenden Beschäftigungsbezug nach Art. 328b OR i.V.m. Art. 4 DSG aufweisen. Folglich lässt sich aus einer Recherche solcher Profile keine Persönlichkeitsverletzung i.S. des DSG ableiten, unabhängig von den Benutzereinstellungen zur «Öffentlichkeit» des Profils.[408]

2.5. Fazit

Arbeitgebende dürfen über Arbeitnehmende nach Art. 328b OR nur Daten bearbeiten «soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind». Mit Blick auf das Internet beschränkt sich die Rechtmässigkeit der Informationsbeschaffung im Rahmen eines Bewerbungsverfahrens deshalb auf die von den Bewerbenden erstellten Profile in den *beruflichen* sozialen Medien, selbst wenn die Bewerbungsunterlagen der Kandidaten *keinen* Verweis auf diese Profile beinhalten. Die Verwendung dieser Informationen ist zulässig, da Bewerbende damit ihre beruflichen Qualifikationen und Erfahrungen einem beruflichen

---

[405] Diese Schlussfolgerung deckt sich mit jener der Artikel-29 Datenschutzgruppe über die Verarbeitungsvorgänge beim Einstellungsprozess (EU, Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017, S. 12f.) und der Empfehlung des Ministerkomitees des Europarates zum Gebrauch von persönlichen Daten in Beschäftigungsverhältnissen: «*[E]mployers should refrain from collecting data relating to job applicants or employees without their knowledge*» (MINISTERKOMITEE, Explanatory Memorandum to «The processing of personal data in the context of employment», Ziff. 45; ähnlich, MINISTERKOMITEE, The processing of personal data in the context of employment, Ziff. 5.3).

[406] Bei LinkedIn sind es gemäss Standardvoreinstellungen alle weiteren Nutzerinnen und Nutzer, welche das Profil einer Person sehen können, siehe https://www.linkedin.com/legal/privacy-policy, Ziff. 3.1 (zuletzt besucht am 20.04.2021). Für eine Statistik, wie Nutzerinnen und Nutzer diese Profile einstellen, JACOBSON UND GRUZD (insb., Table 4, S. 183).

[407] MCDONALD/THOMPSON/O'CONNOR umschreiben *active sourcing* als «the collection of online information, often via social networking sites or generic search engines, for the purpose of evaluating prospective employees and monitoring current employees with regards to their fitness for and in the job.» (MCDONALD/THOMPSON/O'CONNOR, S. 541).

[408] Vgl. STREIFF ET AL., OR 328b, N. 9; DATENSCHUTZBEAUFTRAGTER KANTON ZÜRICH, Ziff. 3.3; EGLI, Rz. 71.

Nutzerkreis zugänglich machen und diese Daten die berufliche Eignung betreffen. Dies ist bei freizeitlichen Informationen im Internet/sozialen Medien – mit wenigen Ausnahmen, z.B. bei sog. Tendenzbetrieben – nicht der Fall. Bei privaten Informationen spielt es auch keine Rolle, ob diese allgemein, oder nur für einen bestimmten Benutzerkreis, zugänglich sind.

Die durchgeführten Konsultationen zeigen, dass sich die befragten Unternehmen dieser Rechtslage grösstenteils bewusst sind. Weitere Quellen weisen hingegen darauf hin, dass es dennoch Unternehmen gibt, welche sich zusätzlich zu den von den Bewerbenden zur Verfügung gestellten Unterlagen private Informationen über die bewerbende Person im Internet einholen und Bewerbende gestützt darauf ablehnen.[409]

Für abgelehnte Bewerbende ist es jedoch kaum möglich nachzuweisen, dass unrechtmässig erlangte und nicht die Eignung für das Arbeitsverhältnis betreffende private Informationen einen negativen Einfluss auf den Einstellungsentscheid gehabt haben. So existiert weder ein Recht auf Einstellung noch ein Anspruch auf eine Begründung bei einer Nichteinstellung. Sollte dieser Nachweis dennoch gelingen, so stünden den in ihren Persönlichkeitsrechten Verletzten gegenüber privatrechtlichen Arbeitgebenden grundsätzlich die Klagen auf (a) Schadenersatz und/oder (b) Genugtuung nach Art. 28a Abs. 3 ZGB offen. Somit müssen abgewiesene Bewerbende (a) einen spezifischen Schaden (z.B. Kosten für die Bewerbung) und/oder (b) eine über den finanziellen Schaden hinausgehende schwere Verletzung der Persönlichkeit nachweisen.[410] Öffentlich-rechtliche Arbeitgebende hingegen sind in jedem Fall an die Grundrechte gebunden; eine Verletzung der Privatsphäre könnte somit vor einem zuständigen Verwaltungsgericht angefochten werden.

Lediglich Art. 8 Abs. 1 GLG[411] sieht bei Verdacht auf eine geschlechterbezogene Diskriminierung die Möglichkeit vor, dass Bewerbende eine Begründung hinsichtlich des negativen Einstellungsentscheides verlangen können. Im Falle einer Nichtanstellung aufgrund einer Diskriminierung kann der betroffenen Person eine Entschädigung zugesprochen werden.[412]

3. Szenario 2: Verwendung von Algorithmen und KI im Bewerbungsverfahren

3.1. Sachverhalt

"*HR Analytics*", «*Hiring by Algorithm*» oder «*E-Recruiting*"[413] – in heutigen Anstellungsverfahren werden zusätzlich zu herkömmlichen Evaluierungsmethoden immer häufiger Algorithmen (Ziff. II.2.2.1) und Systeme der künstlichen Intelligenz (KI – Ziff. II.2.2.5) eingesetzt, um Arbeitgebende im Auswahlprozess zu unterstützen und entlasten.[414] Es gibt Systeme, die automatisiert Bewerbungsunterlagen erfassen und auswerten, nach geeigneten Kandidatinnen und Kandidaten in sozialen Netzwerken suchen und, je nach Grad der Automatisierung, Empfehlungen zu

[409] Siehe *supra* Fn. 368.

[410] Vgl. PÄRLI, Evaluieren, kontrollieren, überwachen, S. 39.

[411] Bundesgesetz über die Gleichstellung von Frau und Mann (GIG) vom 24.03.1995, SR 151.1.

[412] Art. 3 i.V.m Art. 5 Abs. 2 GIG.

[413] Siehe WILDHABER, Répercussions juridiques de la robotique; S. 213f. und WILDHABER, Robotik.

[414] Allgemein zu KI am Arbeitsplatz/im Bewerbungsverfahren, SÖBBING; WILDHABER, Répercussions juridiques de la robotique S. 213ff.; WILDHABER, Robotik; HEILMANN sowie TWOMEY. Für eine Definition von KI, Ziff. II.2.2.5.

geeigneten Bewerbenden abgeben. Andere Anwendungen können automatisiert Bewerbungsinterviews ohne menschliche Einwirkung durchführen, analysieren und auswerten.[415] Bei der Verwendung von Algorithmen und KI in Bewerbungsverfahren scheinen zwei Szenarien mit Blick auf *die Privatsphäre* von Stellenbewerbenden von besonderer Relevanz:

a) auf Algorithmen gestützte Internet-Datenanalysen: Mithilfe von Algorithmen werden im Internet vorhandene Daten von Bewerbenden zusätzlich zu den vorhandenen Bewerbungsunterlagen zum Zweck der Persönlichkeitsbewertung analysiert. Solche Anwendungen können mit Informationen über die Werdegänge sowie mit beruflichen und/oder persönlichen Merkmalen von aktuellen/früheren Mitarbeitenden und Personen in vergleichbaren Positionen gespiesen und für die zu besetzende Stelle programmiert werden. Unternehmen verwenden solche Datenanalysesysteme wie beschrieben auch dazu, proaktiv geeignete Kandidaten zu finden, um diese aktiv anzuwerben (*active sourcing*, *supra* Ziff. 2.4.3.B.).[416]

b) Verwendung von KI-Systemen im Rahmen von Bewerbungsgesprächen: Bei der Verwendung von KI im Rahmen von Bewerbungsgesprächen wird der/die Arbeitgebende durch ein auf KI basiertes System ersetzt, welches das Interview selbständig führen, auf Fragen Folgefragen formulieren und die Antworten von Bewerbenden sowie deren Emotionen und physiologische Reaktionen – wie z.B. den Gesichtsausdruck, die Sprache oder den Herzschlag – analysieren kann.[417]

3.2. Relevanz und Problembereiche

Gemäss den Konsultationen spielt der Einsatz von KI im Rahmen von Bewerbungsprozessen bei den befragten Akteuren bislang keine grosse Rolle. Zwei der Befragten gaben an, dass «nicht intelligente» auf Algorithmen basierte Systeme bei der Analyse von Lebensläufen eingesetzt werden, um eingereichte Bewerbungen anhand von Stichworten auf deren Eignung zu priorisieren und eine Vorselektion vorzunehmen (sog. *applicant tracking systems* (ATS)).[418] Hierbei werde darauf geachtet, dass die Systeme «nur» eine Priorisierung vornähmen und keine Anstellungsentscheidungen träfen. Mit Blick auf die genannten Systeme wurde auf die Problematik hingewiesen, dass Algorithmen, welche auf stereotypen Kriterien basieren, diskriminierende Auswirkungen haben können. Da es in der vorliegenden Untersuchung um die *Privatsphäre* von bewerbenden Personen geht, werden rechtliche Fragen zum diskriminierungsfreien Zugang zum Arbeitsplatz an dieser Stelle jedoch nicht weiter vertieft.[419]

Der Grund, weshalb die im Sachverhalt genannten Methoden bei den konsultierten Unternehmen bislang (noch) nicht verbreitet sind, scheint in einer Skepsis gegenüber dem Reifegrad algorithmischer Systeme zu liegen. Diese äusserte sich in der Befragung etwa in Befürchtungen, dass durch den Einbezug solcher Systeme gute Bewerbungen, welche nicht den programmierten Kriterien entsprechen, gar nicht mehr angeschaut würden oder dass wichtige persönlichkeitsrelevante Eigenschaften von Bewerbenden dadurch unberücksichtigt blieben. Als problematisch erachtet

---

[415] Siehe *infra* Fn. 417.

[416] U.a. DAEDELOW; MCDONALD/THOMPSON/O'CONNOR sowie HEILMANN; bezgl. Profiling, Ziff. II.4.2.2

[417] Z.B. STECK; WILDHABER, Répercussions juridiques de la robotique, S. 213ff.; HUSMANN; DIMOV UND JUZENAITE und HANSEN. Illustrativ ist auch der folgende Videobeitrag von CBS New York, abrufbar unter https://www.youtube.com/watch?v=Y1Rd10E2etA (zuletzt besucht am 20.04.2021).

[418] Gemäss einer Umfrage von Jobscan 2019 nutzen 99% der grössten Unternehmen weltweit ATS (siehe https://www.jobscan.co/blog/99-percent-fortune-500-ats/ (zuletzt besucht am 20.04.2021).

[419] Zu diesen Fragen, DAEDELOW sowie GOODMAN.

wurde auch, dass Entscheidungen von komplexen KI-Systemen von Menschen nicht mehr nachvollzogen werden könnten.[420] Allgemein mit Blick auf die Verwendung solcher Systeme wurde kritisiert, dass Unternehmen zu wenig transparent darlegen würden, wann sie solche Systeme einsetzen und auf welchen Parametern die angewendeten KI-Systeme basieren.

Der EDÖB erhielt im Berichtsjahr 2019/20 vermehrt Anfragen zur Verwendung von KI im Zusammenhang mit der automatisierten Analyse von Online-Bewerbungsgesprächen, was darauf hindeutet, dass auch in der Schweiz zunehmend auf solche Systeme zurückgegriffen wird.[421] Zum Thema Verhaltens- und Stimmanalysen hatte er sich zudem bereits in seinem Tätigkeitsbericht 2018/9 geäussert.[422] Auch andere Quellen deuten darauf hin, dass die Verwendung von Algorithmen/KI innerhalb des Bewerbungsprozesses insbesondere bei grösseren Unternehmen zunehmend relevant wird.[423]

3.3. Grund- und menschenrechtliche Fragestellungen

3.3.1. Algorithmen-gestützte Internet-Datenanalysen

Analog zu Szenario 1 besteht bei auf Algorithmen gestützten Internet-Datenanalysen – je nachdem, welche Handlungsanweisung dem Algorithmus zugrunde liegt – das Risiko, dass nicht nur berufliche, sondern auch nicht-stellenrelevante, freizeitliche Informationen ausgewertet werden und in eine Entscheidung über die Stellenvergabe miteinfliessen. Mit Blick auf die Privatheit/Öffentlichkeit der im Internet zugänglichen Informationen sind bei der Verwendung von Algorithmen dieselben rechtlichen Grundsätze wie bei einer manuellen Recherche anwendbar und es kann an dieser Stelle auf das vorhergehende Szenario verwiesen werden (*supra* Ziff. 2.4).

Allerdings sind algorithmische Systeme zur *automatisierten* Durchforstung des Internets/sozialen Medien verglichen mit einem Menschen sehr viel effizienter. Mithilfe von Big Data Analysen können umfassende Persönlichkeitsprofile von potenziellen Arbeitnehmenden, einschliesslich beruflichen und privaten Informationen, erstellt werden. Da die Privatsphäre von bewerbenden Personen hierbei ungleich stärker betroffen ist als bei der manuellen Recherche, stellt sich die Frage, welchen erhöhten rechtlichen Anforderungen eine *automatisierte* Datenbearbeitung standhalten muss.

3.3.2. KI-Systeme im Rahmen von Anstellungsinterviews

Wie bei «normalen» Bewerbungsinterviews müssen im automatisierten Interviewprozess gestellte Fragen ebenfalls den Anforderungen an rechtlich zulässige Interviewfragen genügen (*supra* Ziff. 2.4.1).[424] Dies gilt hinsichtlich eines möglichen Eingriffs in die Privatsphäre der Stellenbewerbenden auch dann, wenn Bewerbungsgespräche von KI-Systemen «autonom», d.h. ohne menschliche

[420] Dieser Auffassung wird in der Literatur teilweise jedoch auch widersprochen und entgegengehalten, dass «Roboter» im Gegensatz zu Menschen weniger diskriminieren, z.B. HERMANN.

[421] EDÖB, Tätigkeitsbericht 2019/20, S. 46.

[422] Vgl. EDÖB, Tätigkeitsbericht 2018/9, S. 42.

[423] U.a. STECK; HANSEN; HEILMANN oder STEPHAN.

[424] WILDHABER, Répercussions juridiques de la robotique, S. 215f. Zum Fragerecht der Arbeitgebenden, VISCHER UND MÜLLER, § 9 Rz. 4ff sowie BRÜHWILER, OR 320, N 8b.

Einflussnahme, geleitet werden und in deren Verlauf rechtlich geschützte Interessen von Arbeitgebenden (Fragerecht) und Stellenbewerbenden (Recht auf Privatsphäre) gegeneinander abgewogen werden müssen.[425]

Gewisse KI Systeme ermöglichen es überdies, Emotionen und physiologische Reaktionen von Stellenbewerbenden z.B. anhand von Gesichtsausdruck, Sprache oder Puls zu messen,[426] so dass vielfältige persönliche Daten der Stellenbewerbenden in automatisierte Entscheidungsprozesse einfliessen können. Deshalb muss geklärt werden, welche Datenbearbeitungsgrundsätze im Zusammenhang mit sensiblen Daten anwendbar sind.[427]

3.4. Rechtliche Beurteilung

3.4.1. Algorithmengestützte Datenanalysen

Wie unter Ziff. II.4.2.2 ausgeführt, unterscheidet das DSG beim Begriff «Persönlichkeitsprofil» nicht zwischen einer automatisierten oder manuellen «Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt».[428] Sowohl Art. 4 Abs. 4 DSGVO als auch Art. 5 lit. f. N-DSG weichen von dieser Definition ab und verlangen, dass eine Bewertung von persönlichen Aspekten einer natürlichen Person durch eine *automatisierte* Datenbearbeitung erfolgt. Persönliche Aspekte können z.B. die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort, Ortswechsel oder ähnliches sein.[429]

Im Rahmen von auf Algorithmen gestützten Internet-Datenanalysen findet grundsätzlich eine *automatisierte* Durchforstung des Internets nach personenbezogenen Daten von Bewerbenden statt. Ein solcher Vorgang erfüllt sowohl die Kriterien der Erstellung eines Persönlichkeitsprofils nach aktuellem DSG als auch jene des «Profilings» nach N-DSG. Eine Datenbearbeitung im Zusammenhang mit Persönlichkeitsprofilen unterliegt qualifizierten gesetzlichen Anforderungen.

Art. 14 DSG verlangt, dass die betroffene Person über die Erstellung eines Persönlichkeitsprofils und die damit verfolgten Zwecke informiert wird. Das N-DSG sieht überdies vor, dass betroffene Personen immer dann informiert werden, wenn sie einer *automatisierten* Entscheidung unterworfen werden, welche ihre Rechte in erheblicher Weise beeinträchtigt.[430] Diese Informationspflicht wird mit dem Antragsrecht einer betroffenen Person verbunden, dass diese automatisierte Entscheidung von einer natürlichen Person überprüft wird.[431] Die DSGVO geht diesbezüglich noch etwas weiter und verankert für betroffene Personen ein Recht, *nicht* einer automatisierten Entscheidung unterworfen zu werden, wenn diese eine rechtliche Wirkung entfaltet.[432]

Sowohl die DSGVO als auch das N-DSG sehen eine Ausnahme von der Informationspflicht vor, wenn die automatisierte Einzelentscheidung (a) «mit dem Abschluss oder der Abwicklung eines

---

[425] Ausführlich, BRÜHWILER, OR 320, N 8b.

[426] *Supra* note 417.

[427] WILDHABER, Répercussions juridiques de la robotique, S. 216f.

[428] Art. 3 lit. d DSG.

[429] Art. 5 lit. f. N-DSG.

[430] Art. 21 Abs. 1 N-DSG; vgl. auch Art. 14 Abs. 2 lit. g DSGVO.

[431] Art. 21 Abs. 2 N-DSG.

[432] Art. 22 Abs. 1 DSGVO.

Vertrages zwischen dem Verantwortlichen und der betroffenen Person»[433] im Zusammenhang steht oder (b) eine ausdrückliche Einwilligung der betroffenen Person vorliegt.[434] Wie erwähnt enthält auch das DSG in Art. 13 analoge Rechtfertigungsbestimmungen.[435] Aufgrund der dem Arbeitsverhältnis innewohnenden Machtasymmetrie sind diese Rechtfertigungsbestimmungen zur vertraglichen und ausdrücklichen Einwilligung im Kontext des Arbeitsrechts allerdings nur mit Zurückhaltung anzunehmen (vgl. Ziff. II.4.3.2).

Wie bei der manuellen Recherche[436] gelten auch für das automatische Profiling im Bewerbungsverfahren die Grundsätze von Art. 328b OR und Art. 4 DSG. Somit dürfen nur Daten über Bewerbende bearbeitet werden, welche sich objektiv auf die Eignung der bewerbenden Person für die in Frage stehende Anstellung beziehen. Ein automatisiertes Profiling, welches persönliche Aspekte von Bewerbenden umfasst, die nicht für die ausgeschriebene Stelle relevant sind, stellt somit in jedem Fall eine unzulässige Datenbearbeitung nach Art. 328b OR dar. Auch eine vorgängige Information nach Art. 14 DSG oder eine ausdrückliche Einwilligung vermag ein solche Datenbearbeitung nicht zu rechtfertigen, es sei denn sie erfolgt *zugunsten* der Arbeitnehmenden (Art. 362 Abs. 1 OR).

Auch *active sourcing* kann automatisiert erfolgen. Analog zur vorhergehenden Schlussfolgerung sind auch hier grundsätzlich nur jene Datenbearbeitungen rechtmässig, welche die berufliche Qualifikation von recherchierten Personen betreffen (z.B. LinkedIn – *supra* Ziff. 2.4.3.B.).

3.4.2. Verwendung von KI-Systemen im Rahmen von Anstellungsinterviews

Wie bereits unter *supra* Ziff. 2.4.1 ausgeführt, findet im Bewerbungsgespräch das Fragerecht der Arbeitgebenden (und somit die Auskunftspflicht der Bewerbenden) seine Grenzen in der Persönlichkeit und der Privatsphäre der Bewerbenden. Fragen sind nur erlaubt, wenn sie die Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind.[437] Diese Anforderungen gelten auch für den automatisierten Interviewprozess.[438]

Auch die automatisierte Analyse von persönlichen Eigenschaften wie Emotionen oder physiologischen Reaktionen von Stellenbewerbenden tangiert deren Privatsphäre.[439] Die Bearbeitung solcher Daten stellt regelmässig eine Verletzung der Persönlichkeit nach Art. 12 Abs. 1 DSG dar, da kein plausibler Zusammenhang zur Eignung für das Arbeitsverhältnis nach Art. 328b OR i.V.m. Art. 4 Abs. 2 DSG besteht. Eine Einwilligung der Bewerbenden vermag daran wie bereits ausgeführt grundsätzlich nichts zu ändern.[440]

Der EDÖB kam im Zusammenhang mit der Anwendung von Verhaltens- oder Stimmanalysesystemen in Bewerbungsverfahren zum Schluss, dass solche Datenbearbeitungen als Persönlichkeitsprofil i.S.v. Art. 3 lit. d DSG zu qualifizieren sind und deshalb geeignete Massnahmen zur Datensicherheit ergriffen werden müssen.[441] Zudem müssten die Auswertungen

---

[433] Art. 21 Abs. 3 lit. a N-DSG, vgl. auch Art. 22 Abs. 2 lit. a DSGVO.

[434] Art. 21 Abs. 3 lit. b N-DSG, vgl. auch Art. 22 Abs. 2 lit. c DSGVO.

[435] Art. 13 Abs. 1 und Art. 13 Abs. 2 lit. a DSG.

[436] Ziff. III.2.4.

[437] Art. 328b OR.

[438] Z.B. WILDHABER, Répercussions juridiques de la robotique, S. 215f.

[439] Z.B. STECK.

[440] Vgl. Art. 362 Abs. 1 i.V.m. Art. 328b OR sowie Ziff. II.4.3.2.

[441] EDÖB, Tätigkeitsbericht 2018/9, S. 42ff.

verhältnismässig sein und die Bewerbenden vorgängig über Art und Zweck der Verwendung der Ergebnisse, die Dauer der Aufbewahrung sowie ihr Auskunftsrecht informiert werden.[442] Ob solche Datenbearbeitungen mit Art. 328b OR in Einklang sind war nicht Gegenstand der Untersuchung. Offen blieb auch, ob es sich bei den personenbezogenen Daten im Kontext von Analysesoftware um Gesundheitsdaten i.S.v. Art. 3 lit. c Ziff. 2 DSG handeln kann (*infra* Ziff. 5.4).

3.5. Fazit

Während zumindest gewisse internationale Studien darauf hinweisen, dass «*HR Analytics*», «*Hiring by Algorithm*» oder «*E-Recruiting*» von grossen Unternehmen bereits heute systematisch verwendet werden, steht diese Entwicklung in der Schweiz noch am Anfang. Die Anwendung von Systemen zum Profiling von Bewerbenden wurde von den konsultieren Akteuren ebenso verneint, wie das Einsetzen von KI-Systemen zur Durchführung von Bewerbungsgesprächen. Insbesondere wurde darauf hingewiesen, dass solche Systeme in der Praxis noch nicht die verlangte Zuverlässigkeit und Fairness bieten und grosse rechtliche Risiken beinhalten würden.

Mit Blick auf eine mögliche Verletzung der Privatsphäre hat die rechtliche Beurteilung bestätigt, dass die Risiken für die Bewerbenden im Zusammenhang mit algorithmischen Systemen/Systemen der KI grösser sind als bei der manuellen Datenbearbeitung. Ein Grund liegt darin, dass solche Systeme in hoher Geschwindigkeit ein allein mit menschlichen Ressourcen nicht bearbeitbares Volumen an Daten erheben und in Bezug zu anderen Daten(sätzen) setzen können (Big Data Analysen, Ziff. II.2.2.2). «Intelligente» Systeme können überdies anhand von Erfahrungsbeispielen darauf trainiert werden, Daten und somit menschliche Verhaltensweisen zu analysieren, interpretieren und basierend darauf selbständig (Ermessens-)Entscheide zu fällen (vgl. Ziff. II.2.2.5/Ziff. II.4.2.2).

Bei der Verwendung von automatisierten Datenanalysesystemen besteht deshalb eine hohe Wahrscheinlichkeit, dass sowohl private, als auch geschäftlich relevante Informationen bearbeitet und umfassende Persönlichkeitsprofile von Bewerbenden erstellt werden. Sofern private Informationen im Bewerbungsprozess von algorithmischen Systemen bearbeitet werden, handelt es sich um eine unrechtmässige Datenbearbeitung von Seiten der Arbeitgebenden, es sei denn, die erhobenen Daten sind für die Eignung der Arbeitsstelle relevant – z.B. bei sog. Tendenzbetrieben.

4. Szenario 3: Überwachungs- und Kontrollsysteme am Arbeitsplatz

4.1. Sachverhalt

Die vielseitige Verwendung von Algorithmen, Big Data Analysen und dem IoT im Rahmen der digitalen Überwachung ermöglicht Arbeitgebenden eine umfassende und systematische Kontrolle von Angestellten. Als Überwachungs- und Kontrollsysteme gelten «alle technischen Systeme (optisch, akustisch, elektronisch, etc.) […] welche einzelne oder mehrere Tätigkeiten oder Verhaltensweisen von Arbeitnehmerinnen und Arbeitnehmern erfass[en] […] können».[443]

[442] Vgl. Art. 14 DSG.

[443] SECO, Wegleitung, S. 326-2.

Arbeitgebende wenden solche Technologien an, um missbräuchliches Verhalten von Arbeitnehmenden aufzudecken, betriebliche Prozesse zu optimieren oder die Sicherheit von Arbeitgebenden und/oder Arbeitnehmenden zu gewährleisten.

Aufgrund der grossen Vielfalt an digitalen Überwachungsmöglichkeiten am Arbeitsplatz werden in diesem Kapitel exemplarisch einige in den Konsultationen genannte Überwachungs- und Kontrollsysteme beschrieben und deren Implikationen für die Privatsphäre der Mitarbeitenden aufgezeigt.

4.2. Relevanz und Problembereiche

Bereits seit längerer Zeit verfügen Arbeitgebende über die technischen Möglichkeiten, das Internetverhalten von Mitarbeitenden, einschliesslich des (privaten) E-Mail-Verkehrs, zu überwachen.[444] In den Konsultationen aufgeführte betriebliche Interessen umfassen u.a. die Cybersicherheit, mögliche Gesetzesbrüche (z.B. Insiderhandel im Finanzbereich), die Informationssicherheit sowie ethische Anliegen. Eine Mehrheit der konsultierten Akteure hob hervor, personenbezogene Daten bei der Überwachung grundsätzlich nur in *anonymisierter* Form zu bearbeiten. Zudem seien präventive Massnahmen (z.B. Sperrung von privaten E-Mailserviceprovidern)[445] ein effizientes Mittel, um private Tätigkeiten von Mitarbeitenden während der Arbeitszeit zu reduzieren.

Auch die Videoüberwachung wurde als nützliches Überwachungsmittel in einem betrieblichen Kontext genannt. Diese wird überwiegend in sicherheitsrelevanten Bereichen, zum Schutz der Mitarbeitenden und Vermögenswerten sowie in den Zugangsbereichen zu den Unternehmen eingesetzt. Alle Befragten gaben zudem an, in den Büroräumlichkeiten der Mitarbeitenden *keine* Videoüberwachung installiert zu haben.

Vor allem im Logistikbereich werden GPS-gestützte Computersysteme (sog. Geotracking) eingesetzt, um Routenprofile zu erstellen und eine Optimierung von betrieblichen Prozessen zu erreichen. Diese Daten würden zwar personenbezogen erhoben, jedoch nur anonymisiert ausgewertet. Überdies kommen an gewissen Arbeitsplätzen auch betriebliche Apps (z.B. zur Zeiterfassung; Remote-Access Apps) zur Anwendung, welche ebenfalls GPS-basiert funktionieren.[446] In Zusammenhang mit dem Geotracking wurde auf die schwierige Abgrenzung zwischen der Leistungs- und Verhaltenskontrolle hingewiesen.

Insbesondere in sicherheitsrelevanten Bereichen werden biometrische Erkennungsverfahren eingesetzt (z.B. Face ID oder Fingerabdruckverfahren). Die fraglichen Akteure haben in diesem Zusammenhang anerkannt, dass es sich bei biometrischen Informationen um sensible Daten handelt, deren Bearbeitung für Arbeitnehmende einen grossen Eingriff in die Privatsphäre mit sich bringt.

4.3. Grund- und menschenrechtliche Fragestellungen

In den genannten Überwachungs- und Kontrollbeispielen wird eine grosse Fülle an personenbezogenen Daten von Arbeitnehmenden bearbeitet mit dem Risiko, die Privatsphäre von Angestellten dadurch zu verletzen. Dabei ist zu prüfen, zu welchem Zweck die Überwachung erfolgt, insbesondere ob sie der Leistungs- und/oder der Verhaltenskontrolle eines

444 Der EDÖB hat bereits 2001 ein Merkblatt zu diesem Thema publiziert, EDÖB, E-Mail- und Internetüberwachung. Siehe auch EDÖB, Leitfaden Privatwirtschaft und EDÖB, Leitfaden Bundesverwaltung.

445 Vgl. auch WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz, S. 332.

446 EDÖB, Tätigkeitsbericht 2019/20, S. 45.

Arbeitnehmenden dient oder ob weitere betriebliche Interessen eine Überwachung rechtfertigen.[447] Weitergehend stellt sich die Frage, inwieweit Art. 328 Abs. 2 OR Arbeitgebende verpflichtet, Massnahmen zu ergreifen, um im Rahmen der Kontrolle von Mitarbeitenden den Schutz vor Missbrauch von privaten Daten der Arbeitnehmenden zu gewährleisten.

Im Folgenden werden zuerst die allgemein anwendbaren Rechtsgrundlagen zu Überwachungs- und Kontrollsystemen erläutert, bevor im Einzelnen auf die unterschiedlichen Arten der Überwachung und deren rechtliche Implikationen eingegangen wird.

4.4. Rechtliche Beurteilung:

4.4.1. Rechtliche Grundlagen

Wie bereits angesprochen wird die in Art. 328/328b OR und Art. 6 ArG enthaltene Fürsorgepflicht von Arbeitgebenden im Kontext der Überwachung durch Art. 26 ArGV3 ergänzt. Diese Bestimmung sieht vor, dass alle Überwachungs- und Kontrollsysteme, welche darauf ausgerichtet sind, *das Verhalten* von Mitarbeitenden zu überwachen, *nicht* eingesetzt werden *dürfen* (Abs. 1). Eine Überwachung des Verhaltens liegt vor bei «eine[r] ständige[n] (ununterbrochene[n]) oder nicht ständige[n] (kurzzeitig periodische oder stichprobenmässige) Kontrolle bestimmter Aktivitäten der Arbeitnehmenden in detaillierter Form».[448] Sind Überwachungs- oder Kontrollsysteme aus anderen Gründen als zur Verhaltensüberwachung erforderlich, darf weder die Gesundheit noch die Bewegungsfreiheit der Arbeitnehmenden dadurch beeinträchtigt werden (Abs. 2). Mit dieser Formulierung wird anerkannt, dass eine gezielte Überwachung negative Auswirkungen auf das Recht auf (die psychische) Gesundheit sowie die Bewegungsfreiheit haben kann – beides Ausprägungen der persönlichen Freiheit nach Art. 10 Abs. 2 BV. Somit ist Art. 26 ArGV3 auch aus grundrechtlicher Sicht von Bedeutung.[449]

In der Praxis ist die Abgrenzung zwischen einer verbotenen Verhaltensüberwachung und der erlaubten Leistungsüberwachung nach Art. 26 Abs. 1 ArGV3 oftmals schwierig, da Verhalten und Leistung einer Person am Arbeitsplatz in engem Zusammenhang stehen können.[450] Ist diese Abgrenzung nicht eindeutig, ist im Einzelfall abzuwägen, ob das betriebliche Interesse an einem Überwachungs- und Kontrollsystem höher zu bewerten ist als der Gesundheits- und Persönlichkeitsschutz von Arbeitnehmenden.[451] Überwachungs- und Kontrollanlagen sind grundsätzlich *unproblematisch* an Orten, wo es betrieblich notwendig ist und sich keine oder nur selten Mitarbeitende aufhalten, z.B. in einer Tiefgarage oder in Zutrittsbereichen.[452] Sind regelmässig Mitarbeitende anwesend, ist die Interessenabwägung schwieriger.

Art. 328b OR findet auch im Kontext von Überwachungs- und Kontrollsystemen auf alle Datenbearbeitungen Anwendung, d.h. jede Überwachung muss für die Durchführung des Arbeitsvertrages erforderlich sein. Zudem sind die folgenden Grundsätze des DSG zu beachten[453]:

---

[447] Art. 26 ArGV3.

[448] SECO, Wegleitung, S. 326-2.

[449] Siehe auch BGer 6B_536/2009 (Urteil vom 12.11.2009), E. 3.3.3. und 3.4.1.

[450] Siehe SECO, Wegleitung, S. 326-1 sowie FREYTAG.

[451] Vgl. BGer 6B_536/2009 (Urteil vom 12.11.2009), E. 3.6.2.

[452] SECO, Wegleitung zur Verordnung 3 zum Arbeitsgesetz, S. 326-2. Siehe auch FREYTAG.

[453] Vgl. auch SECO, Wegleitung, S. 326-4ff.

- Verhältnismässigkeit (Art. 4 Abs. 2 DSG): Prüfung von Eignung, Erforderlichkeit und Zumutbarkeit der Überwachung.
- Zweckbindung (Art. 4 Abs. 3 DSG): Personendaten dürfen nur zu dem (betrieblichen) Zweck bearbeitet werden, welcher den Arbeitnehmenden bei der Datenbeschaffung angegeben wurde.
- Transparenz (Art. 4 Abs. 4 DSG i.V.m. Art. 48 ArG i.V.m. Art. 5/6 ArGV3): Die Mitarbeitenden müssen vorgängig über die Installation eines Überwachungs- und Kontrollsystems informiert und angehört werden. Während sich die Informationspflicht der Arbeitgebenden im Rahmen des DSG «nur» auf Persönlichkeitsprofile und besonders schützenswerte Personendaten erstreckt (Art. 14 DSG), beinhaltet Art. 5 ArGV3 eine Mitteilungspflicht *über alle gesundheitsrelevanten Gefährdungen* am Arbeitsplatz. Von einer vorgängigen Information kann abgesehen werden, wenn ein Verdacht auf eine arbeitsrechtliche Pflichtverletzung oder die Begehung von Verbrechen oder Offizialdelikten von Seiten von Arbeitnehmenden besteht.[454]

Mit einer unzulässigen Überwachung verletzen Arbeitgebende ihre Fürsorgepflicht. Die betroffenen Arbeitnehmenden können gestützt auf diese Persönlichkeitsverletzung Ansprüche nach Art.15 DSG und Art. 27ff. ZGB geltend machen (Ziff. II.4.3.2). Zudem kann z.B. die Aufnahme fremder Gespräche[455] sowie die Anfertigung von Videoaufnahmen ohne Einwilligung der betroffenen Personen auch strafrechtliche Konsequenzen haben.[456]

4.4.2. Internetverhalten und E-Mailverkehr

2019 benutzte über die Hälfte der Schweizer Bevölkerung Internet am Arbeitsplatz.[457] Oft lässt sich dabei nicht scharf zwischen privater und beruflicher Nutzung unterscheiden, was die Abgrenzung zwischen Privat- und Berufsleben erschwert.[458] Eine geschäftliche Nutzung des Internets liegt vor, wenn Arbeitnehmende beabsichtigen, die von ihnen verlangten Arbeitsleistungen voranzubringen.[459] Durch eine private Nutzung des Internets können Arbeitnehmende ihre arbeitsvertraglichen Pflichten nach Art. 319 Abs. 1 OR (Leistungspflicht) und Art. 321a Abs. 1 OR (Sorgfalts- und Treuepflicht) verletzen.[460] Zur Aufdeckung der privaten Nutzung des Internets können Arbeitgebende deshalb Überwachungsmassnahmen anordnen.

Wer am Arbeitsplatz das Internet benutzt, hinterlässt Spuren. So werden Internetaktivitäten auf gemeinschaftlich genutzten Informatikmitteln (z.B. Servern) in sog. Logdateien protokolliert.[461] Gemäss dem EDÖB handelt es sich bei diesen Spuren typischerweise um personenbezogene Daten und die Auswertung dieser Logdateien stellt eine Datenbearbeitung im Sinne des DSG dar.[462] Eine Überwachung der Internetnutzung ist auch mithilfe von sog. multifunktionalen

---

[454] VISCHER, §16, Rz. 31 und BGer 8C_79/2016 vom 30.06.2017.

[455] Art. 179bis StGB (Schweizerisches Strafgesetzbuch vom 21.12.1937, SR 311).

[456] Art. 179quater StGB. Zum Ganzen, HEIZ UND NÄF.

[457] Vgl. Tabelle «Internetnutzung» für den Zeitraum 1997-2019 des Bundesamt für Statistik (https://www.bfs.admin.ch/asset/de/ind-d-30106 (zuletzt besucht am 20.04.2021)).

[458] Sog. Entgrenzung zwischen Arbeit und Privatleben (siehe auch Szenarien zur Telearbeit, Ziff. III.6 und BYOD, Ziff. III.7).

[459] WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz, S. 309.

[460] Ausführlich, WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz, S. 309ff. ANANDARJAN z.B. spricht sich deshalb für die Nutzung von KI aus, um das Internetverhalten von Mitarbeitenden umfassend zu überwachen.

[461] Detailliert zu diesen Vorgängen, EDÖB, Leitfaden Privatwirtschaft, S. 4.

[462] EDÖB, Leitfaden Privatwirtschaft, S. 4f.

Überwachungsprogrammen möglich, welche die gesamte Nutzung eines Rechners (einschliesslich dem Internet) überwachen und deshalb nur in Ausnahmefällen zulässig sind, wie weiter unten ausgeführt wird.[463] Alle personenbezogenen Kontrollen der Internetnutzung am Arbeitsplatz grundsätzlich die Voraussetzungen von Art. 328b OR, dem DSG sowie Art 26 ArGV3 erfüllen.

Die Aufdeckung einer privaten Nutzung des Internets kann eine Überwachung von Arbeitnehmenden rechtfertigen. Weitere betriebliche Interessen können beispielsweise die Gewährleistung der Daten- und Anwendungssicherheit (Verhindern von Viren, Trojanern, etc.), finanzielle Interessen (Einhaltung der Arbeitszeit, Produktivitätsverringerung etc.), Vermeiden von Reputationsrisiken, Wahrung von Fabrikations- und Geschäftsgeheimnissen, Einhaltung des Datenschutzes sowie das Vermeiden einer Überlastung der Speicherkapazität sein.[464]

Für die Beurteilung, ob eine Persönlichkeitsverletzung im Zusammenhang mit einer Überwachung der Internetnutzung von Mitarbeitenden vorliegt, sind insbesondere die Grundsätze der (1) Verhältnismässigkeit (Art. 4 Abs. 2 DSG), (2) Zweckbindung (Art. 4 Abs. 3 DSG) und (3) Transparenz (Art. 4 Abs. 4 DSG) von Bedeutung.[465]

(1) Der Grundsatz der Verhältnismässigkeit verlangt dass: (a) die Überwachungsmassnahme geeignet ist, um eine missbräuchliche Verwendung des Internets durch Arbeitnehmende aufzudecken; (b) es mit Blick auf den Eingriff in die Gesundheit und die Persönlichkeitsrechte der Arbeitnehmenden keine mildere Massnahme gibt[466] und (c) das private Interesse der Arbeitgebenden den Schutz der Persönlichkeit der Arbeitnehmenden übersteigt.[467] In einem ersten Schritt haben Arbeitgebende die Möglichkeit, rechtlich unproblematische technische und organisatorische Schutzmassnahmen[468] zu ergreifen, um die private Nutzung zu minimieren. Beispiele hierfür umfassen die präventive Sperrung einer Webseite, Downloadfilter, Firewalls oder die Schulung der Mitarbeitenden.[469] Überdies haben Arbeitgebende im Zusammenhang mit der Dauer der Überwachung sowie der Art und Weise der Datenauswertung einen grossen Spielraum, die Persönlichkeitsrechte von Mitarbeitenden in verhältnismässiger Art und Weise zu wahren. So können Unternehmen z.B. eine *anonyme* Auswertung der Internetnutzung *aller* Mitarbeitenden vornehmen.[470] Eine solche lässt allgemeine Rückschlüsse auf das Internetnutzungsverhalten der Mitarbeitenden zu und gibt Aufschlüsse, ob eine einzelfallbezogene Überwachung überhaupt notwendig ist.[471] Weitere Möglichkeiten bieten die pseudonyme Auswertung sowie als *ultima ratio* die namentliche Auswertung.[472] Während die beiden erstgenannten Auswertungsformen grundsätzlich erlaubt sind, bedarf es bei der namentlichen Auswertung eines hinreichenden Missbrauchsverdachts.[473]

---

[463] Zum Ganzen, z.B. WOLFER, Rz. 480; EDÖB, Leitfaden Privatwirtschaft, S. 8. Eine solche Art von Überwachung kann ebenfalls im Kontext der Telearbeit, Ziff. III.6.4.3 und BYOD, Ziff. III.7.4 von Bedeutung sein. Zur Rechtmässigkeit von Spyware, BGE 139 II 7 und WILDHABER UND HÄNSEBERGER, SBB, S. 1255.

[464] Siehe EDÖB, Leitfaden Privatwirtschaft, S. 4.

[465] Vgl. Ziff. III.4.4.1 und EDÖB, Leitfaden Privatwirtschaft, S. 5f.

[466] In BGE 139 II 7 hat das Bundesgericht z.B. entschieden, dass der verdeckte Einsatz eines Überwachungsprogrammes unverhältnismässig war, da es mildere Mittel gegeben hätte, um den Missbrauch aufzuklären.

[467] Z.B. EDÖB, Leitfaden Privatwirtschaft, S. 5 sowie WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz, S. 333.

[468] Vgl. Art. 7 Abs. 1 DSG.

[469] Ausführlich WOLFER, Rz. 489ff.; EDÖB, Leitfaden Privatwirtschaft, S. 7f. und WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz, S. 332.

[470] Vgl. BGer 8C_79/2016 vom 30.06.2017.

[471] Verschiedene Auswertungsformen sind aufgelistet in: EDÖB, Leitfaden Privatwirtschaft, S. 9.

[472] EDÖB, Leitfaden Privatwirtschaft, S. 9.

[473] EDÖB, Leitfaden Privatwirtschaft, S. 9.

(2) Der Zweckbindungsgrundsatz verlangt, dass die Auswertung von Internetnutzungsaktivitäten tatsächlich betrieblich relevant ist und dass damit nur der den Mitarbeitenden im Vorfeld mitgeteilte Zweck verfolgt wird.[474]

(3) Der Grundsatz der Transparenz verpflichtet Arbeitgebende, Mitarbeitende über den Zweck der Überwachung und die hierfür eingesetzten Mittel zu informieren – beides kann z.B. mit einem auf Art. 321 OR (Weisungsrecht) abgestützten Internetnutzungsreglement erfolgen, in welchem die Ausgestaltung der vorgenommenen Überwachungsmassnahmen detailliert darlegt wird.[475] Ein solches dient der Transparenz und Rechtssicherheit im Verhältnis zwischen Arbeitgebenden und Arbeitnehmenden.

Die folgenden zwei Beispiele verdeutlichen, welche Kriterien bei der Überprüfung der Überwachung im Alltag eine Rolle spielen können. Im ersten Fall hatte das Bundesgericht die Frage zu beurteilen, ob die fristlose Entlassung eines SBB-Angestellten rechtmässig war, welcher an 17 Tagen während über 80 Stunden pornographische Internet-Seiten besucht hatte, wobei in zwei Fällen auch strafrechtlich relevantes Material dabei war.[476] Die Arbeitgeberin wurde durch eine periodisch durchgeführte, anonymisierte Auswertung der Internetnutzung aller Arbeitnehmenden auf den möglichen Missbrauch aufmerksam.[477] Erst danach erfolgte die personenbezogene Rückverfolgung. Obwohl der Arbeitnehmer vorgängig nicht über diese personalisierte Rückverfolgung informiert worden war, wurde die Verhältnismässigkeit der Datenbearbeitung aufgrund dieses abgestuften Vorgehens als rechtmässig angesehen.[478]

In *Bărbulescu gegen Rumänien*[479] befasste sich der EGMR mit der Frage, ob die Überwachung der privaten mittels eines Messenger Dienstes geführten Internetkorrespondenz eines Arbeitnehmenden mit dem Grundsatz der Verhältnismässigkeit vereinbar ist.[480] Der Gerichtshof identifizierte in diesem Urteil eine Reihe von Kriterien[481] – vorgängige Information, Vorliegen von legitimen Gründen, Erforderlichkeit, Folgen der Überwachung für die betroffene Person, Treffen von angemessenen Schutzvorkehrungen durch Arbeitgebende – welche in die Abwägung zwischen Arbeitgebenden- und Arbeitnehmendeninteressen miteinbezogen werden müssen. Da die innerstaatlichen Gerichte viele der genannten Kriterien gar nicht berücksichtigt hatten und der Beschwerdeführer vorgängig nicht angemessen über die Art und das Ausmass der Überwachung informiert wurde, kam der EGMR zum Schluss, dass der Schutz der Privatsphäre des Beschwerdeführers bei der Interessenabwägung nicht angemessen einbezogen wurde (im Detail, Ziff. II.3.2.2).[482]

In gewissen Beschäftigungsverhältnissen werden dauerhafte und systematische digitale Überwachungs- und Kontrollsysteme eingesetzt, welche die Überwachung eines gesamten Rechners ermöglichen (siehe auch *infra* Ziff. 7.4). Verbreitet sind diese bei Anstellungsverhältnissen in Berei-

---

474 EDÖB, Leitfaden Privatwirtschaft, S. 6.

475 Z.B. EDÖB, Leitfaden Privatwirtschaft, S. 6 – ein Beispiel für ein solches Reglement findet sich in Anhang B. Weiterführend, WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz, S. 333; allgemein zu Reglementen als Ergänzung des Arbeitsvertrages, SENTI.

476 BGer 8C_79/2016 vom 30.06.2017, E. 7.1.; ausführlich, WILDHABER UND HÄNSEBERGER, SBB.

477 BGer 8C_79/2016 vom 30.06.2017, E. 5.1.

478 Ausführlich, WILDHABER UND HÄNSEBERGER, SBB.

479 EGMR, Bărbulescu v Romania, 61496/08 (2017).

480 EGMR, Bărbulescu v Romania, 61496/08 (2017), Ziff. 121.

481 Vgl. Ziff. II.3.2.2.

482 EGMR, Bărbulescu v Romania, 61496/08 (2017), Ziff. 136ff.

chen, in welchen besondere rechtliche Vorgaben zur Verhinderung von Straftaten eingehalten werden müssen, wie etwa zur Bekämpfung von Insiderhandel im Bankenwesen.[483] Der Einsatz solcher umfassenden Überwachungssysteme ist nur ausnahmsweise und unter strengen Voraussetzungen erlaubt. Zunächst muss die Massnahme für die Durchführung des Arbeitsverhältnisses erforderlich sein (Art. 328b OR). In einem zweiten Schritt ist die Kompatibilität mit dem DSG zu prüfen, wobei eine ständige und systematische Überwachung regelmässig dem Verhältnismässigkeitsgrundsatz nach Art. 4 Abs. 2 DSG zuwiderlaufen und somit die Persönlichkeit von Arbeitnehmenden nach Art. 12 DSG verletzen dürfte. Besteht ein überwiegendes Interesse oder eine gesetzliche Grundlage für die Massnahme, liegt ein Rechtfertigungsgrund nach Art. 13 DSG vor und die Persönlichkeitsverletzung ist nicht widerrechtlich. Ein Beispiel sind gesetzliche Grundlagen zur Kontrolle der Mitarbeitenden im Kontext des Insiderhandels.[484] In solchen Fällen kann eine ständige Überwachung der Internetnutzung von Arbeitgebenden auch vertraglich vereinbart werden.

4.4.3. Videosysteme

Videoüberwachungsanlagen werden heutzutage üblicherweise über Sensoren gesteuert und funktionieren oftmals vollständig automatisiert.[485] Im Rahmen von «smarten» oder «intelligenten», auf die Bedürfnisse der Nutzerinnen und Nutzer abgestimmten Videoüberwachungsanlagen, können überdies die überwachten Vorgänge maschinell analysiert und ausgewertet werden.[486] In diese Kategorie fallen z.B. Videoüberwachungen mit biometrischer Gesichtserkennung (*infra* Ziff. 4.4.5).

Die Konsultationen bestätigen, dass Videoüberwachungsanlagen auch im Kontext des Arbeitsplatzes verbreitet sind, insbesondere in Zugangsbereichen, sicherheitsrelevanten Bereichen oder zum Schutz von Mitarbeitenden. Auch der EDÖB hat sich wiederholt mit dieser Art der Arbeitsplatzüberwachung beschäftigt, etwa im Zusammenhang mit dem Einsatz von Videoüberwachungsanlagen bei Kiosken, im Detailhandelsbereich oder auf Baustellen.[487] Im Gegensatz zur Internetüberwachung dürfte bei der Videoüberwachung oftmals nicht zwingend die (Leistungs-)Kontrolle von Arbeitnehmenden im Vordergrund stehen, sondern Sicherheits-, Vermögens- oder andere betriebliche Interessen (z.B. Sicherung einer fehlerfreien Produktion).[488]

Für die Rechtmässigkeit von Videoüberwachungsanlagen gelten die gleichen unter *supra* Ziff. 4.4.1 erläuterten Anforderungen wie bei anderen Überwachungsmassnahmen.[489] Es gibt technische und organisatorische Schutzmassnahmen, um die Datensicherheit zu gewährleisten, z.B. *Privacy Filter*, keine oder zeitlich beschränkte Aufbewahrung der Aufnahmen oder die Kameraposition, welche einem Eingriff in die Persönlichkeit der betroffenen Personen vorbeugen oder diesen zumindest mildern.[490] In besonders sensiblen Bereichen wie z.B. Umkleidekabinen oder Toiletten

---

[483] Siehe EDÖB, Leitfaden Privatwirtschaft, S. 5; OGer ZH, Urteil vom 27.03.2015, LA150002-O/U.doc, E. 3.1, S. 14.

[484] OGer ZH, Urteil vom 27.03.2015, LA150002-O/U.doc, E. 3.1, S. 14.

[485] Vgl. HELLE, S. 341.

[486] Z.B. https://www.telsec-ess.ch/unternehmen/videoueberwachung/ (zuletzt besucht am 20.04.2021).

[487] Z.B. EDÖB, Erläuterungen zur Videoüberwachung; EDÖB, Tätigkeitsbericht 2014/5, S. 55; EDÖB, Tätigkeitsbericht 2003/4, S. 52 und 88ff. sowie EDÖB, Tätigkeitsbericht 1999/2000, S. 31ff.

[488] Zur sog. Sicherheitsüberwachung und Produktionsüberwachung, WOLFER, Rz. 346ff. und 373ff.

[489] Ebenfalls ausführlich zur Videoüberwachung, WOLFER Rz. 322ff.

[490] Z.B. WOLFER, Rz. 332ff.; EDÖB, Erläuterungen zur Videoüberwachung.

ist die Videoüberwachung am Arbeitsplatz grundsätzlich verboten, da sie nicht nur unverhältnismässig, sondern ausschliesslich auf das Verhalten von Arbeitnehmenden ausgerichtet ist und keinen Arbeitsplatzbezug nach Art. 328b OR aufweist.[491]

Für die vorliegende Studie von besonderem Interesse ist ein Fall, in dem das Bundesgericht sich eingehend mit den gesundheitlichen Risiken einer Videoüberwachung am Arbeitsplatz und der Abgrenzung zwischen einer Verhaltens- und Leistungsüberwachung (Art. 26 ArGV3) befasst hat. Konkret ging es um die Rechtmässigkeit einer Kamerainstallation in einem Nebenraum eines Geschäfts, in welchem sich eine Kasse befand.[492] Dieser Raum war nur für das Personal bestimmt und wurde grundsätzlich nur von diesem benutzt, war aber potenziell auch für die Kundschaft zugänglich. Die beschwerdeführende Angestellte hatte angegeben, sie hätte nichts von der Kamera gewusst. Aufnahmen der Kamera belegten, dass sie während der ordentlichen Geschäftszeit Geld aus einer in diesem Raum befindlichen Kasse entwendet hatte. Die Vorinstanz stellte sich auf den Standpunkt, dass die Angestellte über die Installation der Kamera hätte informiert werden müssen und beurteilte die heimliche Aufnahme deshalb als eine rechtswidrige Verhaltensüberwachung. Das Bundesgericht folgte dieser Einschätzung nicht.[493] In seiner Begründung legte es Art 26 ArGV3 eng aus, indem es festhielt, dass diese Bestimmung

> «[…] in dem Sinne einschränkend auszulegen [sei], dass Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden dürfen, soweit sie geeignet sind, die Gesundheit oder das Wohlbefinden der Arbeitnehmer zu beeinträchtigen.»[494]

Basierend auf der Grundüberlegung, dass nicht die Art der Überwachung, sondern die Systematik und Intensität der Überwachung und die damit verbundenen Folgen für die Gesundheit der Mitarbeitenden im Vordergrund stehen sollten, führte es weiter aus:

> «Ein Überwachungssystem kann daher, auch wenn es (hauptsächlich) der gezielten Überwachung des Verhaltens der Arbeitnehmer am Arbeitsplatz dient, erlaubt sein, wenn die Arbeitnehmer nur sporadisch und kurzzeitig bei bestimmten Gelegenheiten vom Überwachungssystem erfasst werden.»[495]

Das Bundesgericht kam zum Schluss, dass in diesem Fall nicht primär die Überwachung des Verhaltens der Mitarbeiterin im Vordergrund stehe, welche nur sporadisch und jeweils während kurzer Zeit im Kassenraum war, sondern die Kasse. Da die Überwachung keine starke Beeinträchtigung der Gesundheit der Beschwerdeführerin nach sich ziehe, greife das Verbot nach Art 26 ArGV3 nicht. Überdies hätten überwiegende betriebliche Interessen (Verhinderung von Straftaten durch Dritte) vorgelegen und eine Überwachung des Kassenraumes gerechtfertigt (Art. 13 Abs. 1 DSG).[496] Analog zum vorherigen Fall des SBB-Mitarbeiters[497] verneinte das Bundesgericht im Ergebnis somit eine *widerrechtliche* Verletzung der Persönlichkeit der Mitarbeiterin, obwohl diese *nicht* über die Überwachungsmassnahme informiert war und damit der Transparenzgrundsatz nach Art. 4 Abs. 4 DSG verletzt wurde.

---

491 WOLFER, Rz. 337.

492 BGer 6B_536/2009 (Urteil vom 12.11.2009).

493 BGer 6B_536/2009 (Urteil vom 12.11.2009), E. 2.2.1.

494 BGer 6B_536/2009 (Urteil vom 12.11.2009), E. 3.6.1.

495 BGer 6B_536/2009 (Urteil vom 12.11.2009), E. 3.6.2.

496 BGer 6B_536/2009 (Urteil vom 12.11.2009), E. 3.7.

497 Ziff. III.4.4.2 und BGer 8C_79/2016 vom 30.06.2017.

Im gleichen Sinne argumentierte der EGMR im bereits unter Ziff. II.3.2.2 geschilderten Urteil *López Ribalda and Others v. Spain*[498]*.* In diesem Fall wurde im Rahmen einer *heimlichen* Überwachung der Angestellten ein überwiegendes betriebliches Interesse eines Supermarktbetreibers an der Überwachung bejaht.

Diese Fälle zeigen, dass für die Rechtmässigkeitsprüfung einer Überwachungsmassnahme am Arbeitsplatz die verschiedenen Grundsätze und Rechtfertigungsgründe des DSG im Einzelfall zu prüfen und gewichten sind. Somit sind jeweils situationsbezogen das Ausmass der Auswirkungen einer Überwachung auf die Privatsphäre und die Gesundheit der Arbeitnehmenden zu analysieren und gegen die betrieblichen Interessen abzuwägen.

4.4.4. Geolokalisierung

Mit dem globalen Positionsbestimmungssystem (*global positioning system* – GPS) ist es möglich, jederzeit eine Position mithilfe des Satellitensystems zu bestimmen.[499] Insbesondere im Logistik-, Personentransport- und Aussendienstbereich erfreut sich der Einsatz von Navigationsgeräten mit GPS-Funktion grosser Beliebtheit. Diese ermöglichen z.B. die Nachverfolgung der Routen von Arbeitnehmenden in Aussendiensteinsätzen und bei Dienstleistungen wie Uber wird über die GPS-Standortlokalisierung automatisiert eine Verbindung zwischen Fahrerinnen/Fahrern und Kunden hergestellt.[500] Neben Navigationssystemen bieten auch Smartphones und arbeitsplatzspezifische Wearables (*infra* Ziff. 5) die Möglichkeit, mittels GPS den Standort von Arbeitnehmenden jederzeit zu lokalisieren.[501]

Die GPS-Daten eines Dienstfahrzeuges oder eines geschäftlichen Mobiltelefons lassen grundsätzlich eindeutige Rückschlüsse auf deren Nutzerinnen und Nutzer zu, es handelt sich bei den erhobenen Geodaten deshalb um personenbezogene Daten im Sinne des DSG. Dient ein in diesen Geräten installiertes GPS-basiertes Überwachungssystem der Kontrolle während der Arbeitszeit, liegt eine arbeitsbezogene Leistungsüberwachung vor, solange die Geolokalisierung mit der Arbeitserfüllung im Zusammenhang steht.[502] Eine solche Art der Überwachung ist mit Art. 328b OR im Einklang und deshalb grundsätzlich möglich (*supra* Ziff. 4.4.1). Dasselbe gilt auch bei von Arbeitgebenden installierten GPS-Systemen in privaten Fahrzeugen/Mobiltelefonen, welche zur Arbeitserbringung benutzt werden. Allerdings sind hierbei im Vergleich zu geschäftlichen Geräten erhöhte Anforderungen an die betrieblichen Interessen zu stellen (vgl. BYOD, *infra* Ziff. 7).

---

498 EGMR, López Ribalda and Others v. Spain, 1874/13 and 8567/13 (2019).

499 Siehe WOLFER, Rz. 421f.

500 Vgl. HAYES/SNOW/ALTUWAYJIRI.

501 Siehe EDÖB, Tätigkeitsbericht 2019/20, S. 45; WOLFER, Rz. 423ff.

502 EDÖB, Tätigkeitsbericht 2017/8, S. 28.

In Konstellationen ausserhalb einer Anstellung – z.B. bei gewissen Arbeitserfüllungsformen im Kontext der internetbasierten Plattformökonomie[503] – sind Art. 328b OR und die weiteren arbeitsrechtlichen Schutzbestimmungen *nicht* anwendbar.[504] Die Einordnung in selbstständige und unselbstständige Erwerbstätigkeit ist jedoch nicht immer einfach, wie das Beispiel des Personenfahrdienstes Uber zeigt. So werden dessen Fahrerinnen und Fahrer in gewissen Kantonen als unselbständig Erwerbende und in anderen als selbstständig Erwerbende klassifiziert.[505] Unabhängig von der arbeitsrechtlichen Einordnung sind die Grundsätze des DSG auf alle Kategorien von Erwerbstätigen anwendbar und im Rahmen einer Überwachung zu prüfen.

Im Kontext der GPS-Überwachung ist es zentral, dass die Betroffenen vorgängig über dessen Installation informiert werden (Grundsatz der Transparenz).[506] Überdies muss die Überwachung für die Abwicklung des Arbeitsverhältnisses oder den Geschäftszweck tatsächlich relevant sein (Grundsatz der Zweckgebundenheit).[507] Zu den legitimen Zielen zählen etwa arbeitsorganisatorische Interessen (z.B. effiziente Einsatzplanung, Flottenmanagement)[508], das Aufdecken von Missbrauch, die Verminderung eines finanziellen Schadens für das Unternehmen/die Kundschaft (z.B. Einhaltung der Arbeitszeit, Erbringung der Arbeitsleistung) oder Sicherheitsinteressen (z.B. Diebstahlschutz).[509] Überdies darf es keine mildere Massnahme geben, und die Interessen der Arbeitnehmenden an Gesundheit und Persönlichkeitsschutz müssen angemessen berücksichtigt werden (Grundsatz der Verhältnismässigkeit).[510]

Im Entscheid BGE 130 II 425 befasste sich das Bundesgericht mit den Kriterien für die Zulässigkeit der GPS-Überwachung von Aussendienstmitarbeitenden, welche autonom Kundenaufträge an unterschiedlichen Orten in der Schweiz wahrnahmen. Diese Form der Geolokalisierung kann einen gravierenden Eingriff in die Persönlichkeit darstellen, da die Erstellung gesamter Bewegungsprofile einer Person während (und potenziell auch ausserhalb) der Arbeitszeit ermöglicht wird und somit in einer profilbildenden Verhaltensüberwachung resultieren kann.[511] Das Bundesgericht hielt fest, dass eine GPS-Überwachung grundsätzlich nicht geeignet sei, die Qualität der Arbeitserbringung der Mitarbeitenden vor Ort zu überprüfen, da die blosse Erfassung der Geodaten keine entsprechende Rückschlüsse zulässt.[512] Ein milderes Mittel zur Kontrolle der Mitarbeitenden in solchen

---

503 Solche Plattformen «eignen sich zum Anbieten eigener Produkte und Dienstleistungen, zur Suche nach Dienstleistungen und Produkten, zur Zusammenarbeit mit Bezug auf ein gemeinsames Projekt (Crowdworking bzw. Collaborative Economy) oder zur blossen Vermittlung von Dienstleistungen und Produkten (On-Demand-Economy)» (RIEMER-KAFKA, S. 588, mit Verweis auf BUNDESRAT, Auswirkungen der Digitalisierung, S. 39f. Siehe auch PÄRLI, Formen der Arbeitsorganisation; OECD, New Forms of Work und SECO, Atypische Arbeitsverhältnisse, S. 69ff.).

504 Die unselbstständige Erwerbstätigkeit ist typischerweise charakterisiert durch die Eingliederung in eine fremde Arbeitsorganisation, eine wirtschaftliche Abhängigkeit sowie das Fehlen eines Unternehmerrisikos (RIEMER-KAFKA, S. 588).

505 So hat das Kantonsgericht des Kanton Waadt am 23.04.2020 Uber-Fahrerinnen und -Fahrer als Angestellte qualifiziert (Cour d'Appel Civile du Canton de Vaud, Urteil vom 23.04.2020 (veröffentlicht am 11. September 2020), HC/220/535). In den meisten anderen Kantonen werden diese jedoch noch immer als selbstständig Erwerbende angesehen, siehe KELLER.

506 Art. 4 Abs. 4 DSG. Weiterführend, EDÖB, Tätigkeitsbericht 2017/8, S. 28 und BGE 130 II 425 E. 4.2. und 4.4., S. 435ff.

507 Art. 4 Abs. 3 DSG. Weiterführend, EDÖB, Tätigkeitsbericht 2017/8, S. 28.

508 Vgl. Ziff. III.5.4.

509 Siehe WOLFER, Rz. 438ff.; sowie BGE 130 II 425 E. 5.3 und 5.4., S. 438ff.

510 Art. 4 Abs. 2 DSG; BGE 130 II 425 E. 5.2, S: 438f.

511 Vgl. EDÖB, Tätigkeitsbericht 2017/8, S. 28.

512 BGE 130 II 425 E.5.5, S. 442ff. Siehe auch EDÖB, Tätigkeitsbericht 2017/8, S. 27f. und EDÖB, Tätigkeitsbericht 2005/6, S. 68f.

Fällen wäre z.B. die Anforderung, dass ein Arbeitsrapport von der auftragsgebenden Person unterschrieben werden muss.[513] Für die Aufdeckung eines Diebstahls oder die missbräuchliche Verwendung des Dienstfahrzeugs zu privaten Zwecken kann der *punktuelle* Einsatz von GPS-Systemen jedoch zielführend sein.[514] Dies dürfte ebenfalls für den mobilen Zugriff auf Kundendaten – z.B. im Bankenwesen – gelten, welcher aus Sicherheitsgründen nur aus der Schweiz erfolgen darf.[515]

4.4.5. Biometrie am Arbeitsplatz

Biometrische Verfahren werden zunehmend auch in einem beruflichen Kontext angewendet, u.a. bei Zugangssystemen zu sicherheitsrelevanten Bereichen oder im Zusammenhang mit der FaceID/Fingerabdruckverfahren zum Login bei Mobiltelefonen oder Arbeitsplätzen. Der EDÖB hat zudem auf den vermehrten Einsatz von biometrischen Verfahren im Bereich der Gastronomie, z.B. bei biometrischen Zeiterfassungs-, Zutritts-, oder Kassensystemen, hingewiesen.[516]

Biometrische Erkennungsverfahren basieren auf einer «automatisierte[n] Messung von natürlichen, hoch charakteristischen, physiologischen oder verhaltenstypischen Merkmalen von Menschen zum Zweck der Unterscheidung von anderen Personen».[517] Biometrische Merkmale sind somit körpereigene persönliche Kennzeichen, welche theoretisch zumindest nur dieser einen Person zugeordnet werden können.[518] Neben dem Fingerabdruckverfahren gibt es auch biometrische Verfahren zur Erkennung von Gesicht, Stimme, Handgeometrie und Handschrift.[519] Diese Merkmale werden digital erfasst und mit gespeicherten Referenzdaten abgeglichen. Biometrische Verfahren werden somit automatisiert durchgeführt.[520]

Während im aktuellen DSG biometrische Daten nicht als separate Kategorie aufgeführt sind, wurde diese Datenkategorie im N-DSG bei den besonders schützenswerten Personendaten integriert. Demnach sind biometrische Daten Personendaten, «die eine natürliche Person eindeutig identifizieren».[521] Mit Blick auf die Erfassung von biometrischen Daten ist darauf hinzuweisen, dass die erfassten biometrischen *Rohdaten* oftmals mehr Informationen enthalten, als die später für das Erkennungsverfahren verwendeten Muster (*Templates*). So kann beispielsweise ein Bild eines Gesichtes zusätzliche Informationen über das Geschlecht, das Alter, die Religion, die Stimmung oder Krankheiten einer Person enthalten.[522] Bereits heute sind gewisse dieser Daten, welche durch ein biometrisches Erkennungsverfahren als Begleiterscheinung zum Vorschein kommen können, als eigene Kategorie der «besonders schützenswerten Personendaten» im DSG enthalten, wie z.B. Informationen zu religiösen Ansichten (z.B. Tragen eines Kopftuches auf einem Bild), zur Gesund-

513 BGE 130 II 425 E.5.5.3, S. 443.

514 EDÖB, Tätigkeitsbericht 2005/6, S. 69.

515 Z.B. https://news.ti8m.ch/blog/-Das-Gesetz-unterscheidet-nicht-zwischen--in--und-ausl-ndischen-Clouds-.html (zuletzt besucht am 20.04.2021).

516 Z.B. EDÖB, Tätigkeitsbericht 2017/8, S. 28.

517 HORNUNG UND STEIDLE, S. 203 und PRIVATIM. S. 3.

518 PRIVATIM. S. 3.

519 HORNUNG UND STEIDLE, S. 203.

520 HORNUNG UND STEIDLE, S. 203; PRIVATIM. S. 6.

521 Art. 5 lit. c Ziff. 4 N-DSG.

522 PRIVATIM. S. 5.

heit (z.B. Erkennung von Augenkrankheiten bei einem Irisscan) oder der Rassenzugehörigkeit (aufgrund der Hautfarbe).[523] Eine Zusammenstellung von biometrischen Daten ermöglicht somit das Erstellen eines Persönlichkeitsprofil einer Person i.S.v. Art. 3 lit. d DSG.

Biometrische Personendaten werden in der Regel bei der betroffenen Person erhoben, welche nach dem Grundsatz der Transparenz (Art. 4 Abs. 4 DSG i.V.m. Art. 5 Abs. 1 ArGV3) eingehend über die biometrischen Verfahren und die damit verbunden Folgen und Datenbearbeitungsvorgänge aufgeklärt werden müssen.[524] Nach dem Grundsatz der Zweckbindung (Art. 4 Abs. 3 DSG) dürfen biometrische Daten im Bereich von Arbeitsverhältnissen zudem nur erhoben werden, wenn diese nach Art. 328b OR für die Durchführung des Arbeitsvertrages erforderlich sind.[525] Das biometrische Verfahren ist technisch so auszugestalten, dass der Zweck der Datenbearbeitung erreicht wird, eine Änderung des Bearbeitungszwecks aber ausgeschlossen ist.[526] Von grosser Bedeutung im Zusammenhang mit biometrischen Verfahren ist das Prinzip der Verhältnismässigkeit (Art. 4 Abs. 2 DSG). In einem ersten Schritt ist zu prüfen, ob ein milderes Mittel existiert als ein biometrisches Erkennungsverfahren – z.B. durch Verwendung von Pins, Passwörtern, Ausweisen, Badges, Schlüssel etc. Falls nur ein biometrisches Erkennungsverfahren in Frage kommt, sind «[w]ann immer möglich […] biometrische Merkmale zu erfassen, die keine Spuren hinterlassen und deren Erfassung ohne das Wissen der betroffenen Person nicht möglich ist (z.B. Handumriss oder Handvenenmuster)».[527] Zudem sollte durch technische Vorkehrungen sichergestellt werden, dass aus biometrischen Daten keine Rückschlüsse auf weitere besonders schützenswerte Personendaten möglich sind.[528] Um den Zugriff von unberechtigten Dritten auf biometrische Daten zu erschweren, sollten diese nicht zentral, sondern lokal, auf einem Server gespeichert werden.[529]

Wie bei anderen Überwachungs- und Kontrollsystemen muss im Einzelfall abgewogen werden, ob die Massnahmen den genannten arbeits- und datenschutzrechtlichen Grundsätzen standhalten. Da es sich um personenbezogene Daten handelt, welche untrennbar mit einer Person verknüpft sind und oftmals Rückschlüsse auf besonders schützenswerte Personendaten zulassen, sind die Anforderungen an die vorgebrachten Rechtfertigungsgründe nach Art. 13 Abs. 1 DSG streng.

4.4.6. Fazit

Zusammenfassend lässt sich festhalten, dass die Überwachung von Arbeitnehmenden in Art 26 ArGV3 zwar klar geregelt zu sein scheint, die Abgrenzung zwischen der Verhaltens- und Leistungsüberwachung in der Praxis aber schwierig ist.

Unproblematisch sind jene technischen und organisatorischen Massnahmen, welche präventiver Natur sind oder nicht personenbezogen ausgewertet werden können (Positionierung der Kamera, Sperrung einer Webseite, Downloadfilter, anonymisierte Auswertung etc.), sowie Überwachungsanlagen an Orten, wo sich Mitarbeitende nicht oder nur sehr selten aufhalten.

Sofern eine Überwachung im Einklang mit Art. 328b OR ist, bedarf es jeweils einer weiteren Abwägung zwischen den unterschiedlichen involvierten Interessen. Hier stehen die Gesundheits- und

---

523 Art. 3 lit. c DSG; vgl. EDÖB, Datenspeicherung, S. 2.

524 PRIVATIM. S. 13.

525 EDÖB, Leitfaden Biometrie, S. 7.

526 PRIVATIM. S. 11.

527 EDÖB, Arbeitszeiterfassung.

528 PRIVATIM. S. 12.

529 EDÖB, Datenspeicherung; EDÖB, Tätigkeitsbericht 2017/8, S. 28; EDÖB, Arbeitszeiterfassung.

Persönlichkeitsinteressen von Arbeitnehmenden den Sicherheits-, Betriebsoptimierungs-, finanziellen oder gesundheitlichen Interessen der Arbeitgebenden gegenüber. Überdies müssen Arbeitgebende Arbeitnehmende transparent und umfassend über jene Überwachungsmassnahmen informieren, welche die Privatsphäre letzter tangieren. Eine ständige, systematische und personenbezogene Überwachung von Arbeitnehmenden ist grundsätzlich nicht erlaubt, es sei denn, eine solche ist z.B. von Gesetzes wegen vorgesehen oder es liegen überwiegende private/öffentliche Interessen vor (Art. 13 DSG).

Wie bereits weiter oben angedeutet wurde, wird im Beschäftigungskontext oftmals nicht nur ein einzelnes Überwachungs- und Kontrollsystem benutzt, sondern je nach Art der Beschäftigung und den damit verbundenen betrieblichen Interessen mehrere gleichzeitig. Hinzu kommen digitale Arbeitsmittel, die ebenfalls eine Kontrolle und die Lenkung von Mitarbeitenden erlauben wie etwa die nachfolgend behandelten Wearables (*infra* Ziff. 5). Eine Interaktion zwischen diesen unterschiedlichen digitalen Anwendungen, mithilfe welcher laufend personenbezogene Daten aus der physischen Welt in die digitale übertragen und systematisch mithilfe von Big Data Analysen ausgewertet werden können, wird durch das sog. Internet of Things (IoT – Ziff. II.2.2.4) ermöglicht.

Auch wenn solche «intelligenten» Arbeitsumgebungen (*smart workplaces*) in der Schweiz noch nicht sehr verbreitet sind, stellen sie aus Sicht der Privatsphäre von Arbeitnehmenden eine grosse Herausforderung dar, da dadurch die Erstellung umfassender Verhaltens- und Persönlichkeitsprofile möglich ist. Das neue DSG trägt diesen Entwicklungen mit Bestimmungen zum «Profiling mit hohem Risiko»[530] Rechnung. Arbeitgebende werden deshalb zukünftig verpflichtet sein, in solchen Fällen vorgängig eine Datenschutz-Folgenabschätzung zu machen.[531]

5. Szenario 4: Arbeitsplatzspezifische Wearables

5.1. Sachverhalt

> «Frühmorgens am Arbeitsplatz setzt Katja ihre smarten Handschuhe auf. Diese überwachen ihre Bewegungen und geben Anweisungen für den Zusammenbau medizinischer Geräte. Ihre smarten Socken warnen sie vor allfälligen Stürzen. Über Mittag geniesst sie eine Massage, da ihre Stressmessung ihr leichten Stress attestiert. Am Nachmittag liefert sie die fertigen Teile mit dem Transporter aus. Dabei trägt Katja ihre smarte Schirmmütze, welche sie vor einer allfälligen Übermüdung warnen würde. Während der Fahrt wird sie von ihrem Wearable am Rücken daran erinnert, die richtige Haltungsposition einzunehmen. Nach Feierabend bestätigt ein Blick auf den Fitness Tracker am Handgelenk, dass sie noch eine Runde joggen sollte. Ansonsten wird sie beim betrieblichen Fitnesswettbewerb nie zu den Besten gehören.»[532]

Wearables sind «mobile Computersysteme, die während der Anwendung vom Benutzer getragen werden oder an seinem Körper befestigt sind».[533] Sensoren zeichnen unterschiedliche Körperfunk-

[530] Art. 5 lit. g N-DSG.

[531] Art. 22 N-DSG und Ziff. II.4.2.2.

[532] Fiktives Beispiel eines möglichen Einsatzes von Wearables am Arbeitsplatz, zu finden in: ALLENSPACH, Rz. 4.

[533] DZIDA, S. 146. Allgemein zu Wearables am Arbeitsplatz ALLENSPACH; BAUER/WUTZKE/BAUERNHANSL und DR. DATENSCHUTZ. Für Beispiele von Wearables, welche KI-Technologie verwenden, DE JESUS.

tionen, die Umgebung und/oder den Standort einer Person auf. Diese Daten werden «anschliessend direkt vom Wearable verarbeitet oder an ein anderes Gerät übertragen und dort ausgewertet».[534] Die Daten können entweder lokal (auf dem Wearable), extern (z.B. Smartphone/Computer/Cloud), oder an beiden Orten gleichzeitig gespeichert werden.[535]

Wearables können in vielseitiger Weise genutzt werden und je nach Ausprägung der Steuerung und Optimierung von betrieblichen Prozessen dienen und/oder dem Schutz der Gesundheit und Sicherheit der Arbeitnehmenden förderlich sein.[536] Wie das obige fiktive Beispiel zeigt, können z.B. intelligente Handschuhe dazu verwendet werden, manuelle Arbeitsschritte vorzugeben/zu dokumentieren, Socken, um Mitarbeitende vor allfälligen Stürzen zu warnen, Brillen für die Anleitung von Arbeitnehmenden im Rahmen von komplexen Sortierabläufen oder smarte Schirmmützen zur Warnung von Fahrerzeugführenden vor Übermüdung.[537] Der Anwendungsbereich von Wearables am Arbeitsplatz beschränkt sich jedoch nicht auf das Tragen von «Arbeitskleidung», sondern umfasst auch weitere mit dem Körper einer Person verbundene Anwendungen, wie z.B. intelligente Armbänder (*smart watches*), die auch im Privatbereich verbreitet sind. Ein aktueller Trend sind durch «*smarte*» Fitnessarmbänder unterstützte betriebliche Gesundheitsprogramme *(corporate wellness)*, im Rahmen welcher Unternehmen Zugriff auf Gesundheitsdaten der Mitarbeitenden während wie auch ausserhalb der Arbeitszeit, erhalten.[538]

5.2. Relevanz und Problembereiche

Die Konsultationen ergaben, dass Wearables in der Schweiz bisher eher selten am Arbeitsplatz eingesetzt werden. Einzelne Rückmeldungen weisen aber darauf hin, dass diese Art der digitalen Hilfsmittel zunehmend Verbreitung findet und Unternehmen das damit verbundene unternehmerische Potenzial erkannt haben. So verwendet z.B. ein Logistikunternehmen einen digitalen Fahrzeugassistenten für das Management seiner Fahrzeugflotten. Ziel sei die «intelligente Vernetzung» von Autos, fahrenden Personen und Flottenmanagement.[539] Mithilfe des IoT (Ziff. II.2.2.4) werden die am Fahrzeug erhobenen Daten – z.B. zu den gefahrenen Routen, dem Zustand der Autos, dem Treibstoffverbrauch – per Cloud in Echtzeit an die Fahrzeugnutzenden und das Flottenmanagement übermittelt. Als weiterführende Funktion können Informationen über das persönliche Fahrverhalten an die Fahrzeugnutzenden weitergeleitet werden.[540] Ein anderes Unternehmen gab an, dass es im Rahmen eines Innovations- und Pilotprojektes intelligente Datenbrillen (*smart glasses*) zur Optimierung von Sortierprozessen einsetzt. Solche Brillen ermöglich den Angestellten die einfache Identifikation von Gegenständen und geben ihnen eine entsprechende Anweisung, wo diese Gegenstände wieder einsortiert werden müssen.

---

534 ALLENSPACH, Rz. 2

535 ALLENSPACH, Rz. 2

536 ALLENSPACH, Rz. 1.

537 Z.B. DZIDA, S. 146 und ALLENSPACH, Rz. 4ff. Zum Einsatz von Smart Glasses im Bankensektor, MÜHLEMATTER UND DONNO.

538 Z.B. FARR; HANCOCK und ROWLAND. Für den deutschen Rechtsbereich, z.B. KOPP UND SOKOLL, S. 1356ff. In der Schweiz hat der Einsatz von Gesundheits-Apps und Fitnessarmbändern in datenschutzrechtlicher Hinsicht bislang vor allem im Versicherungsbereich für Aufsehen gesorgt (siehe EDÖB, Erläuterungen Fitnesstracker).

539 Siehe https://autosense.ch/en/ (zuletzt besucht am 20.04.2021).

540 Siehe https://autosense.ch/en/products/#how-to (zuletzt besucht am 20.04.2021).

Die bisherige Zurückhaltung wurde von den konsultierten Akteuren u.a. mit dem Risiko von *massiven* Eingriffen in die Persönlichkeit der Arbeitnehmenden bei der Verwendung von Wearables begründet, da damit oftmals nicht nur arbeitsplatzspezifische Daten, sondern auch ganze Verhaltensprofile von Mitarbeitenden aufgezeichnet werden. Somit stehen aus einer datenschutzrechtlichen Perspektive weniger die Steuerungsmöglichkeiten von Arbeitnehmenden im Vordergrund, als die damit verbundenen Möglichkeiten der (Verhaltens-)Überwachung. Das betriebliche Interesse an einer solchen Datenbearbeitung wurde deshalb kritisch hinterfragt.

5.3. Grund- und menschenrechtliche Fragestellungen

Einerseits bringt die Verwendung dieser Technologien es mit sich, dass unablässig Daten über die Tätigkeiten von Arbeitnehmenden gesammelt werden. Dabei dürften solche Geräte regelmässig nicht nur die einzelnen Arbeitsschritte von Arbeitnehmenden erfassen und analysieren, sondern auch das Verhalten zwischen den einzelnen Arbeitsschritten sowie möglicherweise auch physiologische Eigenschaften/Reaktionen der Arbeitnehmenden. Analog zum vorhergehenden «Überwachungs-Szenario» ist deshalb zu prüfen, wo die Grenzen einer damit verbundenen Datenbearbeitung sind und ob diese nur der Leistungsüberwachung dient oder auch einer Verhaltenskontrolle von Arbeitnehmenden. Andererseits werden Datenbearbeitungen im Zusammenhang mit Wearables oftmals nicht nur von Arbeitgebenden vorgenommen, sondern auch von externen IT-Dienstleistern (z.B. App-Herstellern). In diesem Kontext müssen die rechtlichen Anforderungen geprüft werden, welche bei der Datenbearbeitung durch Dritte zu beachten sind.

Neben den datenschutzrechtlichen Fragen bleibt zu untersuchen, ob ein Eingriff in die Privatsphäre von Arbeitnehmenden in jenen Fällen vorliegen könnte, in welchen Wearables die Arbeits- und Ruhezeiten von Arbeitnehmenden digital festlegen.

5.4. Rechtliche Beurteilung

Bei der Erhebung von aktivitätsbezogenen Daten am Arbeitsplatz, die eindeutig einer Person zugeordnet werden können, handelt es sich um personenbezogene Daten im Sinne des DSG.[541] Da durch Wearables erhobene Daten «direkt oder indirekt Rückschlüsse über den physischen oder psychischen Gesundheitszustand einer Person geben», spricht sich GORDON dafür aus, diese Daten als besonders schützenswerte Personendaten nach Art. 3 lit. c Ziff. 2 DSG zu qualifizieren.[542] Diese Ansicht steht allerdings im Widerspruch zur herrschenden Lehre, die unter Verweis auf die Botschaft zum DSG von 1988[543] Gesundheitsdaten nur zu den besonders schützenswerten Daten zählt, wenn diese einen «medizinischen Befund» darstellen.[544] Angesichts der Tatsache, dass Wearables und vergleichbare Technologien heutzutage praktisch *unbegrenzt* Daten erheben und bearbeiten können, sprechen teleologische Argumente – wie von GORDON vertreten – für eine breitere Interpretation des Begriffes «Gesundheitsdaten» im digitalen Zeitalter. Überdies dürfte es sich bei Datensätzen im Zusammenhang mit Wearables regelmässig um eine «Zusammenstellung von

[541] GORDON, S. 72.

[542] GORDON, S. 72.

[543] BUNDESRAT, Botschaft DSG, S. 446.

[544] ROSENTHAL UND JÖHRI, Art. 3 DSG, N. 48 und RUDIN, N. 26.

Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt» und somit ein Persönlichkeitsprofil nach Art. 3 lit. d DSG handeln.[545]

Mit Blick auf die Abgrenzung zwischen den von Wearables erhobenen und bearbeiteten personenbezogenen Leistungs- und Verhaltensdaten und der damit verbundenen Kontrolle von Arbeitnehmenden kann an dieser Stelle auf die anwendbaren rechtlichen Grundsätze des vorherigen Überwachungsszenarios verwiesen werden (*supra* Ziff. 4.4).

Im Zusammenhang mit der Verwendung von Fitnessarmbändern im Rahmen von betrieblichen Gesundheitsprogrammen bleibt anzumerken, dass eine solche Massnahme nicht unter die Fürsorgepflicht von Arbeitgebenden fällt.[546] Zwar beinhaltet diese gemäss dem EDÖB auch Gesundheitsschutz und Gesundheitsprävention, allerdings nur hinsichtlich «arbeitstechnischer Gegebenheiten und Probleme».[547] Nicht der Erfüllung des Arbeitsvertrages dienende gesundheitliche Unterstützungsmassnahmen setzen deshalb zusätzlich eine freiwillige Einwilligung sowohl der Arbeitgebenden als auch der Arbeitnehmenden im Einzelfall voraus.[548] Eine solche beidseitige Einwilligung zur Verwendung von Fitnessarmbändern kann als Abrede i.S.v. Art. 362 Abs. 1 i.V.m. Art 328b OR qualifiziert werden, sofern die im Zusammenhang mit Fitnessarmbändern stehende Datenbearbeitung *zugunsten* der Arbeitnehmenden erfolgt.[549]

Weitergehend stellt sich bei der Nutzung von Wearables die Frage, welche rechtlichen Grundsätze anwendbar sind, wenn eine Datenbearbeitung oder- Auswertung nicht von Arbeitgebenden, sondern von externen IT-Dienstleistern vorgenommen wird.[550] Daten von Arbeitnehmenden sind potenziell auch für diese Unternehmen interessant, sei es zur Weiterentwicklung der Anwendungen oder aus kommerziellen Interessen (z.B. bei Gesundheitsinformationen).[551] Nach Art. 10a DSG ist eine Auslagerung der Datenbearbeitung an Dritte erlaubt, wenn diese (a) die Daten nach *denselben* Grundsätzen bearbeiten, welche auch von den Auftraggebenden, d.h. in unserem Kontext den Arbeitgebenden, einzuhalten sind und es (b) keine entgegenstehenden gesetzlichen oder vertraglichen Geheimhaltungspflichten gibt.[552] Durch diese Bestimmung werden somit zusammen mit den Daten auch die gesetzlichen Anforderungen an eine Datenbearbeitung am Arbeitsplatz nach Art. 328b OR i.V.m. Art. 26 ArGV3 sowie den Grundsätzen des DSG von den Arbeitgebenden auf die Drittparteien übertragen.

Weil nicht nur die Berechtigung der bearbeitenden Person, sondern auch jene der empfangenden Person kritisch zu hinterfragen ist, betrachtet WERMELINGER die Weitergabe (oder Bekanntgabe – vgl. Art. 3 lit. f DSG) von Daten zudem als qualifizierte Form der Datenbearbeitung mit einem erhöhten Risiko für eine Persönlichkeitsverletzung.[553] Daraus leitet er ab, dass eine Rechtfertigung nach Art. 13 DSG in jedem Fall, und damit nicht nur hinsichtlich besonders schützenswerten Daten oder bei Persönlichkeitsprofilen, notwendig ist.[554]

---

545 GORDON, S. 72. Zum Begriff Persönlichkeitsprofil, Ziff. II.4.2.2

546 EDÖB, Tätigkeitsbericht 2009/10, S. 69; zudem Art. 328 OR, Art. 6 ArG sowie ArGV3.

547 EDÖB, Tätigkeitsbericht 2009/10, S. 69.

548 EDÖB, Tätigkeitsbericht 2009/10, S. 69.

549 Siehe auch Ziff. II.4.3.2

550 ALLENSPACH, Rz. 6; GORDON, S. 70f.

551 EDÖB, datum – Folgen der Selbstvermessung, S. 1f.

552 ALLENSPACH, Rz. 6.

553 WERMELINGER, Art. 12 DSG, N. 8

554 Art. 12 Abs. 2 lit. c DSG und die Ausführungen in: WERMELINGER, Art. 12 DSG, N. 8. Anderer Meinung sind ROSENTHAL UND JÖHRI, Art. 12 Abs. 2 lit. c, N. 44.

Für die rechtlichen Fragen, welche sich im Zusammenhang mit der digitalen Steuerung von Arbeits- und Ruhezeiten ergeben, kann auf die nachfolgenden Ausführungen zur Telearbeit und der automatischen Arbeitszeiterfassung verwiesen werden (*infra* Ziff. 6.4).

5.5. Fazit

Wearables am Arbeitsplatz haben ein grosses Potenzial für betriebliche Prozessoptimierungen und Produktionssteigerungen, sie können Mitarbeitende bei komplexen Arbeitsabläufen unterstützen und Arbeitsunfällen vorbeugen. Gleichzeitig stellt diese Technologie durch die systematische und ständige Erhebung von personenbezogenen, besonders schützenswerten Daten sowie Persönlichkeitsprofilen eine grosse Herausforderung für den Schutz der Privatsphäre von Arbeitnehmenden dar. Dem grundrechtlichen Aspekt ist deshalb bei der einzelfallbezogenen Interessenabwägung entsprechend stark Rechnung zu tragen.

Analog zur vorherigen Schlussfolgerung hinsichtlich intelligenter Arbeitsumgebungen dürfte auch die Datenbearbeitung im Rahmen der Nutzung von Wearables am Arbeitsplatz unter dem revidierten Datenschutzgesetz unter den Begriff des «Profiling mit hohem Risiko fallen» und somit zukünftig Arbeitgebende dazu verpflichten, vor der Verwendung eine Datenschutz-Folgenabschätzung vorzunehmen.[555]

6. Szenario 5: Die Telearbeit – Emanzipation der Arbeit von Arbeitszeit und Arbeitsort

6.1. Sachverhalt

In der jüngeren Vergangenheit wurden neue Formen der Arbeitserfüllung, wie Home-Office, die mobile Arbeit von unterwegs, auf Reisen oder in sog. Co-Working Spaces immer populärer. Diese Arbeitsformen werden unter den Begriff der «Telearbeit» subsumiert, welche die Erbringung einer Arbeitsleistung ausserhalb der Betriebsstätte an einem dezentralen Arbeitsplatz beschreibt.[556] Da das Home-Office die bekannteste Form der Telearbeit ist, werden diese beiden Begriffe im weiteren Verlauf des Szenarios als Synonyme verwendet. Telearbeit ist typischerweise möglich in Bereichen, in welchen die Arbeit über einen Computer/Laptop/ein Smartphone oder ähnliches erbracht werden kann und eine telekommunikationsgestützte Verbindung zum betrieblichen Arbeitsplatz vorhanden ist.[557]

Der Trend zur Telearbeit wurde durch die während der COVID-19 Pandemie ergriffenen Massnahmen nochmals verstärkt.[558] Zum einen wurden Arbeitgebende während der Dauer der Massnahmen von den Bundesbehörden angewiesen, gesundheitlich besonders gefährdeten Arbeitnehmenden die Möglichkeit zu bieten, von zu Hause zu arbeiten.[559] Zum anderen sollten Arbeitgebende dafür sorgen, dass auch alle anderen Arbeitnehmenden ihre Arbeitsverpflichtungen

---

[555] Art. 22 N-DSG und Ziff. II.4.2.2.

[556] Zur Abgrenzung zur Heimarbeit, BUNDESRAT, Rechtliche Folgen der Telearbeit, S. 8f.

[557] U.a. BUNDESRAT, Rechtliche Folgen der Telearbeit, S. 7; BUNDESRAT, Auswirkungen der Digitalisierung, S. 38ff. und DÄUBLER, Entgrenzung, S. 59.

[558] Exemplarisch DETTLING UND DETTLING sowie STÄUBLE UND ALICH.

[559] Art. 27a Verordnung 3 über Massnahmen zur Bekämpfung des Coronavirus (Covid-19) vom 19. Juni 2020 (Stand 15.04.2021), SR 818.101.24 (COVID-19-Verordnung 3).

von zu Hause erfüllen, sofern dies mit einem verhältnimässigen Aufwand umsetzbar war.[560] Die zweitgenannte Massnahme war jedoch nur vorübergehender Natur; die restliche Zeit gab es «lediglich» eine allgemeine Empfehlung an die Arbeitgebenden, den Mitarbeitenden das Home-Office *zu ermöglichen*.[561] Das Ziel dieser Anweisungen bestand im Gesundheitsschutz der Mitarbeitenden und bezweckte, alle nicht notwendigen physischen zwischenmenschlichen Kontakte in der Öffentlichkeit zu vermeiden. Erste Schätzungen gehen davon aus, dass sich die Anzahl der Personen, welche während der Corona-Pandemie von zu Hause arbeiteten, verdoppelt hat und dass die gemachten Erfahrungen langfristig zu einem Anstieg des Home-Office führen werden.[562]

6.2. Relevanz und Problembereiche

Die Konsultationen, welche zeitlich vor dem Ausbruch von COVID-19 durchgeführt wurden, haben durchwegs ergeben, dass sowohl das Home-Office, als auch das mobile Büro eine grosse Rolle in der Schweiz spielen und Arbeitnehmenden oftmals die Möglichkeit geboten wird, (zumindest teilweise) von diesen Möglichkeiten Gebrauch zu machen.

Um diese Art der Arbeitserfüllung zu fördern, sei jedoch der Schutz der Datensicherheit von grosser Bedeutung und eine Trennung zwischen geschäftlich und privat genutzter IT-Infrastruktur empfehlenswert. Überdies wurde angemerkt, dass Unternehmen aufgrund eines erhöhten Kontrollbedürfnisses im Kontext des Home-Office oftmals mehr private Daten erheben würden, als dies am betrieblichen Arbeitsplatz der Fall wäre, z.B. wenn es um die Kontrolle des Internetverhalten von Mitarbeitenden geht.[563]

Der mit dem Home-Office verbundenen Individualisierung und Flexibilisierung der Arbeitserfüllungsgestaltung stünden allerdings gesetzliche Grenzen, wie z.B. das Verbot an Sonntagen zu arbeiten[564], entgegen. Dies sei insbesondere in jenen Geschäftsbereichen relevant, in welchen eine zeitversetzte Kommunikation mit dem Ausland für das Tagesgeschäft notwendig ist. Im Zusammenhang mit der auch für das Home-Office verlangten Arbeitszeitkontrolle wurde darauf hingewiesen, dass es sowohl manuelle als auch automatisierte Modelle der Arbeitszeiterfassung gibt.

Praktisch alle interviewten Akteure sprachen sich für die Einführung einer separaten gesetzlichen Regulierung des Home-Office aus. Arbeitgebende, um eine grössere arbeitszeitliche Flexibilisierung zu ermöglichen[565], die Interessenvertretungen der Arbeitnehmenden, um den Gesundheits-, Daten- und Privatsphärenschutz zu stärken.[566]

---

[560] Art. 10 Abs. 3 Verordnung über Massnahmen in der besonderen Lage zur Bekämpfung der Covid-19-Epidemie vom 19. Juni 2020 (Stand 19.04.2021), SR 818.101.26 (Covid-19-Verordnung besondere Lage).

[561] BUNDESRAT, Massnahmen gegen das Coronavirus.

[562] Vgl. DELOITTE; STÄUBLE UND ALICH.

[563] Dies hat auch der Personalchef von Novartis in einem Zeitungsinterview bestätigt, STÄUBLE UND ALICH.

[564] Art. 18 ArG.

[565] Siehe hierzu auch Parlamentarische Initiative BURKART, Mehr Gestaltungsfreiheit bei Arbeit im Homeoffice, Parlamentarische Initiative 16.484 (NR) vom 1.12.2016, abrufbar unter: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20160484 (zuletzt besucht am 20.04.2021).

[566] Ähnlich hat sich auch der schweizerische Gewerkschaftsbund geäussert, CIRIGLIANO, Arbeitnehmende.

6.3. Grund- und menschenrechtliche Fragestellungen

Während Telearbeit einen organisatorischen Autonomiegewinn und somit mehr Gestaltungsfreiheit für das Privatleben der Arbeitnehmenden mit sich bringen kann, kann sie ebenso dazu führen, dass Arbeit ausserhalb der gesetzlichen Arbeitszeit geleistet wird, Arbeitnehmende auch ausserhalb der Arbeitszeit erreichbar sind und gesetzliche Pausen und Ruhezeiten nicht eingehalten werden.[567] Das vorliegende Szenario beschäftigt sich somit unmittelbar mit dem Problem, welches in *Niemietz gegen Deutschland*[568] angesprochen wird, nämlich dass sich die Tätigkeiten von Individuen nicht immer klar dem Privat- oder Berufsleben zuordnen lassen (*infra* Ziff. 6.4.2).

Bei der Erfassung der Arbeitszeit von Arbeitnehmenden ausserhalb der Büroräumlichkeiten stellt sich die Frage, ob eine automatische Arbeitszeiterfassung einen Eingriff in die Privatsphäre der Arbeitnehmenden darstellen könnte, da eine solche je nach technischer Ausprägung Rückschlüsse auf das (freizeitliche) Verhalten von Arbeitnehmenden zulässt (*infra* Ziff. 6.4.3.)

Die rechtlichen Fragen zur Benutzung privater Geräte für die Arbeitserfüllung im Rahmen der Telearbeit werden im nachfolgenden Szenario «BYOD» behandelt (*infra* Ziff. 7).

6.4. Rechtliche Beurteilung

6.4.1. Rechtliche Grundlagen des Home-Office

Für Personen in einem vertraglichen Arbeitsverhältnis gelten während des Home-Office dieselben arbeitsrechtlichen Bestimmungen des OR und des ArG (einschliesslich der ArGV) wie am betrieblichen Arbeitsplatz. Weder kennt das Arbeitsrecht spezifische Bestimmungen zur Telearbeit, noch gibt es eine spezialgesetzliche Grundlage für das Home-Office – auch die Bestimmungen des Heimarbeitsgesetzes (HArG) sind grundsätzlich nicht auf die Telearbeit anwendbar, da dieses die «gewerbliche und industrielle Hand- und Maschinenarbeit» regelt.[569]

Damit ist die Fürsorgepflicht der Arbeitgebenden nach Art. 328/328b OR anwendbar, sowohl was persönlichkeitsschutz- als auch datenschutzrechtliche Fragen betrifft. Zu dieser Fürsorgepflicht gehört im weiteren Sinn auch die Kontrolle der Arbeits- und Ruhezeit der Arbeitnehmenden.[570] Beim Home-Office wird es Arbeitnehmenden grundsätzlich ermöglicht, die Anzahl der zu leistenden Stunden selber einzuteilen. Folgende Bestimmungen des Arbeitsgesetzes sind mit Blick auf die Achtung der Privatsphäre relevant:

- die bewilligungsfreie Tages- und Abendarbeit muss zwischen 6:00-23:00 liegen[571] und darf einschliesslich Pausen 14 Stunden nicht übersteigen[572];

---

567 Zum Ganzen ILO UND EUROFUND, S. 57ff.

568 EGMR, Niemietz v. Germany, 13710/88 (1992), Rz. 29. Weiterführend, Ziff. II.3.2.2.

569 Vgl. Art. 1 Abs. 4 Heimarbeitsgesetz (Bundesgesetz über die Heimarbeit vom 20.03.1981, SR. 822.31). Allerdings gibt es Stimmen, welche eine Anpassung des HArG auf das moderne Home-Office fordern, um die bestehenden rechtlichen Lücken zu schliessen (vgl. CIRIGLIANO, Gesundheitsschutz).

570 Art. 46 ArG i.V.m. Art. 73 Abs. 1 lit. c ArGV1 (Verordnung 1 zum Arbeitsgesetz vom 10.05.2000, SR 822.111).

571 Art. 10 Abs. 1 ArG.

572 Art. 10 Abs. 3 ArG.

- die tägliche Ruhezeit muss mindestens elf aufeinanderfolgende Stunden betragen[573] und die Sonntags- sowie Nachtarbeit sind grundsätzlich verboten.[574]

6.4.2. Entgrenzung zwischen Beruflichem und Privatem

Die bestehenden gesetzlichen Regelungen werden durch das Konzept der Telearbeit und das Prinzip, dass Arbeit *jederzeit* auch ausserhalb der betrieblichen Räumlichkeiten geleistet werden kann, auf die Probe gestellt. So bestimmt jede/jeder Arbeitnehmende selber, ab welchem Zeitpunkt er/sie die Arbeit beginnt, wie lange am Stück gearbeitet wird, wann Pausen gemacht werden, bis wann abends gearbeitet wird und ob nach der gesetzlich erlaubten Abendarbeitszeit oder sonntags noch geschäftliche Mails beantwortet werden. Arbeitnehmende können ihre Arbeitszeiten somit flexibler gestalten, arbeiten dafür möglicherweise aber über eine längere Zeit und mit vermehrten Unterbrechungen der Ruhezeiten. Das Home-Office hat somit grundsätzlich das Potenzial, die Autonomie und Selbstständigkeit der Arbeitnehmenden im Hinblick auf die Arbeitserfüllung zu fördern – dieser Aspekt ist aus grundrechtlicher Sicht dem Recht auf persönliche Freiheit zuzuordnen (Art. 10 Abs. 2 BV).

Während eine solch flexible Arbeitsgestaltung grundsätzlich von vielen Mitarbeitenden als Privileg aufgefasst wird und die Identifikation mit der Arbeit häufig zunimmt, besteht gleichzeitig das Risiko, dass die Arbeit das Privatleben im Rahmen des Home-Office beeinträchtigt, da sich Arbeit und Privates nicht mehr klar trennen lassen.[575] Die genauen Auswirkungen auf das Recht der Privatsphäre einzelner Personen hängen allerdings von einzelfallbedingten Faktoren ab, wie z.B. dem Betätigungsfeld, der Position eines/einer Angestellten innerhalb eines Betriebs, dem Betriebsklima und persönlichen Vorlieben. Auf eine allgemeingültige Schlussfolgerung, ob das Home-Office einen rechtswidrigen Eingriff in die Privatsphäre mit sich bringt, wird an dieser Stelle deshalb verzichtet.

6.4.3. Arbeitszeiterfassung

Im Bereich der Telearbeit haben Arbeitgebende grundsätzlich keine physische Kontrolle darüber, ob die Arbeitsschutzvorschriften und somit auch die Privatsphäre von den einzelnen Mitarbeitenden genügend eingehalten werden, obwohl sie von Gesetzes wegen zu einer solchen Kontrolle verpflichtet sind.[576] Ebenso sind die Möglichkeiten von Arbeitgebenden zur Leistungskontrolle der Arbeitnehmenden eingeschränkt, da die unmittelbare physische Überwachungsmöglichkeit in den Betriebsräumlichkeiten wegfällt.[577] Eine Möglichkeit, ein gewisses Mass an Kontrolle über die Mitarbeitenden zu behalten, liegt in der elektronischen Überwachung der Tätigkeiten der Mitarbeitenden, einschliesslich der Zeiterfassung. Hierbei gibt es unterschiedlich intrusive Systeme, welche eine Gefahr für die Privatsphäre der Mitarbeitenden darstellen können.[578]

---

[573] Art. 15a Abs. 1 ArG.

[574] Zur Sonntagsarbeit, Art. 18f. ArG; zur Nachtarbeit, Art. 16 ArG.

[575] Siehe DÄUBLER, S. 60f.

[576] Art. 6 Abs. 1 ArG; vgl. auch DOMENIG, Rz. 963ff.

[577] DOMENIG, Rz. 982.

[578] Detailliert, WOLFER Rz. 383ff. und DOMENIG, Rz. 993ff.

Zum einen gibt es Programme, welche vergleichbar mit sog. Badges oder Zutrittssystemen am Arbeitsplatz ausschliesslich erfassen, wann Mitarbeitende die Arbeit am Computer beginnen, unterbrechen oder beenden (z.B. durch Einloggen/Ausloggen mithilfe von individualisierten Kennzeichen, Magnet- oder Chipkarten oder biometrischer Erkennung).[579] Diese Art der Kontrolle dient der Erfüllung des Arbeitsverhältnisses und ist grundsätzlich zweckgebunden und verhältnismässig. Es liegt somit keine widerrechtliche Persönlichkeitsverletzung vor.

Andere Systeme wie elektronische Arbeitstagebücher[580] und *workplace-analytics* Systeme[581] erfassen nicht nur die Arbeitszeit der Mitarbeitenden, sondern ebenfalls weitere Informationen, welche Rückschlüsse darauf zulassen, welche elektronischen Tätigkeiten eine Person im Home-Office vornimmt. Es ist deshalb relevant, ob diese Art der Kontrolle lediglich der Leistungskontrolle dient, oder ob damit eine gesundheits- und persönlichkeitsverletzende Verhaltenskontrolle verbunden ist. Für die Abgrenzung zwischen der zulässigen Leistungsüberwachung und der unzulässigen Verhaltensüberwachung sei deshalb auf *supra* Ziff. 4.4.2 verwiesen. Weitere Ausführungen zur Rechtmässigkeit von digitalen Kontrollsystemen, welche einen Zugriff auf private Daten von Mitarbeitenden ermöglichen, sind zudem in *infra* Ziff. 7.4 enthalten.

Es bleibt darauf hinzuweisen, dass Arbeitgebenden im Rahmen ihrer Fürsorgepflicht bei der (manuellen und automatischen) Arbeitszeiterfassung die Pflicht zukommt, Mitarbeitende auf eine allfällige Nichteinhaltung oder Überschreitung der gesetzlichen Arbeitszeiten hinzuweisen. Dadurch können sie sowohl im Rahmen der physischen Präsenz von Mitarbeitenden im Betrieb als auch im Kontext des Home-Office aktiv dazu beitragen, dass Mitarbeitende ihrem Privatleben genügend Raum geben. Dies bedingt, dass Arbeitgebende resp. Vorgesetzte aller Stufen von Arbeitnehmenden ausserhalb der Arbeitszeit nicht die Erfüllung von Arbeitsleistungen verlangen.

6.5. Fazit

Das Home-Office tangiert die Privatsphäre von Mitarbeitenden in unterschiedlicher Hinsicht. Deshalb sind Arbeitgebende im Rahmen ihrer Fürsorgepflicht verantwortlich, organisatorische oder technische Vorkehrungen zu treffen, um negative Auswirkungen auf die Privatsphäre oder die Gesundheit von Mitarbeitenden zu verhindern oder zumindest zu mildern. Unternehmen haben beispielsweise die Möglichkeit, Regelungen über das Home-Office in einem betriebsinternen Reglement oder gesamtarbeitsvertraglich zu regeln sowie mit Mitarbeitenden aktiv das Gespräch zu suchen, wie möglichen Problemen im Rahmen des Home-Office begegnet werden kann.[582] Technische Massnahmen können zudem elektronische Warnsysteme bei der Arbeitszeiterfassung einschliessen, wobei Systeme verboten sind, welche Rückschlüsse auf die privaten Tätigkeiten der Mitarbeitenden ausserhalb der Arbeitserfüllung ermöglichen.

Die aktuellen Entwicklungen rund um die COVID-19 Pandemie bestätigen zudem die im Rahmen der Konsultationen vorgebrachte Notwendigkeit, zusätzlich zu den bereits anwendbaren Regelungen im OR, ArG sowie im DSG, gewisse Grundsätze für das Home-Office rechtlich zu verankern, um die Rechtssicherheit für Arbeitgebende wie auch Arbeitnehmende zukünftig zu stärken.

---

[579] WOLFER Rz. 384f.

[580] Vgl. DOMENIG, Rz. 995ff.

[581] Z.B. STÄUBLE UND ALICH (Interview mit dem Personalchef von Novartis zum «überwachten» Home-Office).

[582] Für ein Beispiel eines solchen Reglements, DOMENIG, Anhang § 3.

7. Szenario 6: Bring Your Own Device (BYOD)

7.1. Sachverhalt

Da heute viele Arbeitnehmende privat über einen Computer/Laptop/ein Smartphone verfügen, werden bei der Telearbeit oftmals auch diese Geräte verwendet.[583] Das vorliegende Szenario beschäftigt sich deshalb mit der Nutzung privater Geräte zur Erbringung einer Arbeitsleistung – auch bekannt als «*bring your own device*» (BYOD) – und dem damit verbundenen Einfluss auf die Privatsphäre der Nutzerinnen und Nutzer.[584] Die Verwendung privater Arbeitsgeräte ist sowohl in den privaten Räumlichkeiten der Arbeitnehmenden als auch in betrieblichen Räumlichkeiten möglich.

Vorteile von BYOD sind aus betrieblicher Sicht z.B. die vereinfachte Erreichbarkeit von Arbeitnehmenden ausserhalb der Arbeitszeit, Kostenüberlegungen sowie die besseren Gerätekenntnisse der Nutzerinnen und Nutzer.[585] Nebst positiven Effekten kann die Nutzung privater Geräte für die Arbeitserbringung auch Probleme mit sich bringen. So fördert BYOD am Arbeitsplatz die Vermischung zwischen Berufs- und Privatsphäre, und der Schutz eines privaten Gerätes ist oftmals nicht gleich gut, wie bei betriebsinternen IT-Infrastrukturen.

7.2. Relevanz und Problembereiche

Bezüglich der Nutzung von privaten Geräten am Arbeitsplatz ergaben die Konsultationen ein gemischtes Bild. Die befragten staatlichen Arbeitgebenden erlauben eine solche Nutzung nur, wenn die Geräte vorgängig von der betriebsinternen IT-Abteilung konfiguriert wurden und einen externen Zugriff auf das Gerät ermöglichen, z.B. durch die Installation von Synchronisations- und Zugriffs-Apps. Bei privatwirtschaftlichen Akteuren scheint die Verwendung von privaten Geräten zur Arbeitserfüllung verbreitet(er) zu sein, wobei auch dort oft spezielle Konfigurationen und Voreinstellungen verlangt werden.

Die rechtliche Problematik in der Zulassung von BYOD liegt aus Sicht der Mehrheit der konsultierten Akteure in der Trennung zwischen privater und geschäftlicher Nutzung des Arbeitsgerätes. Überdies wurde das Problem der Datensicherheit hervorgehoben und die damit verbundene Gefahr eines Missbrauchs geschäftlicher Daten für private Zwecke. Auch auf die Bedeutung eines Zugangs zu einer betrieblichen IT-Infrastruktur für den Datenaustausch wurde hingewiesen – z.B. über verschlüsselte Verbindungen (Virtual Private Network – VPN), Clouds (Ziff. II.2.2.3) oder mithilfe einer Infrastruktur virtueller Desktops (VDI).[586]

Überdies wurden klare betriebliche Regeln für die Nutzung von BYOD befürwortet sowie die Zustimmung sowohl der Arbeitgebenden, als auch der Arbeitnehmenden, als notwendig erachtet.

---

583 BUNDESRAT, Rechtliche Folgen der Telearbeit, S. 47.

584 BUNDESRAT, Rechtliche Folgen der Telearbeit, S. 47, 56f.

585 EDÖB, BYOD.

586 Desktop-Umgebungen werden auf einem zentralen Server «gehostet». Siehe z.B. https://www.citrix.com/de-de/glossary/vdi.html#:~:text=Unter%20einer%20Infrastruktur%20virtueller%20Desktops,Umgebungen%20auf%20einem%20zentralen%20Server (zuletzt besucht am 20.04.2021).

7.3. Grund- und menschenrechtliche Fragestellungen

Bei der Nutzung privater Geräte für die Arbeitserbringung ist eine klare Trennung zwischen Privat- und Berufssphäre typischerweise nicht möglich, da auf demselben Gerät persönliche wie auch berufliche Daten bearbeitet werden.[587] BYOD kann somit persönlichkeits- und datenschutzrechtliche Fragen aufwerfen, z.B. bei der Installation von Sicherheits- oder Datenverwaltungsprogrammen.[588] Überdies können sich rechtliche Fragen im Zusammenhang mit der Löschung von Daten bei Beendigung eines Arbeitsverhältnisses sowie bei Verlust/Diebstahl des privaten Gerätes ergeben.[589]

7.4. Rechtliche Beurteilung

Da Arbeitsgeräte zur Erbringung der Arbeitsleistung nach Art. 327 Abs. 1 OR von Arbeitgebenden grundsätzlich zur Verfügung zu stellen sind, können Arbeitnehmende nicht verpflichtet werden, auf privaten Geräten zu arbeiten. Allerdings besteht aufgrund des Weisungsrechts der Arbeitgebenden auch kein Anspruch von Arbeitnehmenden, private Geräte für die Arbeitserfüllung einsetzen zu können (Art. 321d OR).[590]

Aus datensicherheitstechnischen Überlegungen ist BYOD vor allem mit Risiken verbunden, da Arbeitgebende die Kontrolle über ihre geschäftlichen Daten abgeben. Dieser Verlust der Datenhoheit kann bei Verlust/Diebstahl eines privaten Gerätes sowie im Missbrauchsfall durch Arbeitnehmende relevant sein[591] und deshalb einen externen Zugriff auf BYOD-Geräten rechtfertigen.[592] Allerdings müssen hierbei die rechtlichen Grundsätze der Überwachung beachtet werden (*supra* Ziff. 4.4.1). Daten dürfen deshalb nur im Einklang mit Art. 328b OR i.V.m. Art. 26 ArGV3 bearbeitet werden, d.h. die Datenbearbeitung muss für die Durchführung des Arbeitsvertrages erforderlich sein und darf die (psychische) Gesundheit der Arbeitnehmenden nicht negativ beeinträchtigen. Zudem muss jede Datenbearbeitung mit den Grundsätzen des DSG im Einklang stehen, d.h. transparent sowie zweckgebunden erfolgen und verhältnismässig sein.[593]

Insbesondere besteht die Gefahr, dass Arbeitgebende zu technischen Überwachungsmassnahmen greifen, mit denen nicht nur (a) geschäftliche, sondern auch (b) private personenbezogene Daten bearbeitet werden.

(a) Eine allgemeine Information/Einwilligung von Arbeitnehmenden für die Bearbeitung von *geschäftlichen* Personendaten, beispielsweise im Rahmen einer BYOD-Nutzungsvereinbarung, ist grundsätzlich ausreichend. Eine konkludente Einwilligung wird zudem bei jenen Daten angenom-

---

[587] EDÖB, BYOD.

[588] BUNDESRAT, Rechtliche Folgen der Telearbeit, S. 56.

[589] BUNDESRAT, Rechtliche Folgen der Telearbeit, S. 57.

[590] Allgemein, WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz, S. 328ff.

[591] WILDHABER UND HÄNSEBERGER, BYOD, S. 153; WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz, S. 330. Siehe auch PORTMANN, S: 43, welcher darauf hinweist, dass insbesondere Smartphones besonders sicherheitsanfällig sind.

[592] BIRKHÄUSER UND HADORN, S. 203ff.; WILDHABER UND HÄNSEBERGER, BYOD, S. 159.

[593] Siehe Ziff. III.4.4.2 zur Internet- und E-Mail-Überwachung.

men, welche Arbeitnehmende mit anderen Personen über einen Cloud-Service oder ähnliches teilen.[594] Falls keine Einwilligung vorliegt, kann eine Bearbeitung von geschäftlichen personenbezogenen Daten durch die weiteren in Art. 13 DSG aufgeführten Rechtfertigungsgründe (überwiegendes privates/öffentliches Interesse oder gesetzliche Grundlage) legitimiert sein.[595]

(b) Bei der Bearbeitung von privaten personenbezogenen Daten steht Art. 328b OR im Vordergrund. Wie bereits unter Ziff. II.4.3.2 dargelegt, kann diese Bestimmung nicht *zuungunsten* der Arbeitnehmenden abgeändert werden. Alle Massnahmen zur Überwachung von privaten Geräten müssen deshalb so ausgestaltet sein, dass eine Bearbeitung von personenbezogenen Daten, welche nicht in Bezug zum Arbeitsverhältnis stehen, *nicht* möglich ist.[596] In diesem Zusammenhang reicht auch eine generelle Einwilligung der betroffenen Person, z.B. durch die Unterzeichnung eines Nutzungsreglements, *nicht* aus, da sich eine darauf basierende Überwachung regelmässig zuungunsten der Arbeitnehmenden auswirken dürfte.[597] Eine einzelfallbezogene Einwilligung in die Durchsuchung eines privaten Gerätes *zugunsten* von Arbeitnehmenden wäre jedoch z.B. dann rechtmässig, wenn diese in einer gegen sie gerichteten strafrechtlichen Untersuchung ihre Unschuld beweisen könnten.[598]

Aufgrund der teils komplexen rechtlichen Problemstellungen, welche sich bei der Abgrenzung zwischen geschäftlichen und privaten personenbezogenen Daten bei der Nutzung von privaten Geräten am Arbeitsplatz ergeben, ist es sinnvoll, BYOD detailliert in einen Reglement, welchem die Arbeitnehmenden zuzustimmen haben, zu regeln.[599] Ein solches kann Empfehlungen beinhalten, wie die Nutzerinnen und Nutzer von privaten Geräten einen adäquaten Selbstschutz ihrer Geräte erreichen können (präventive Massnahmen). Zudem können Arbeitgebende darin die für den Zugriff notwendigen technischen Massnahmen erläutern und den Zweck und die Konsequenzen solcher Massnahmen offenlegen.[600]

Mit Blick auf den Schutz der Privatsphäre von Arbeitnehmenden im Rahmen von BYOD ist ebenfalls relevant, dass diese (insbesondere bei Mobiltelefonen) vereinfacht auch ausserhalb der Arbeitszeit erreichbar sind. Dazu kann auf die vorherigen Ausführungen zur «Entgrenzung zwischen Beruflichem und Privaten» unter *supra* Ziff. 6.4.2 verwiesen werden.

Ein weiteres Thema, das insbesondere durch die verordnete Pflicht zum Home-Office während der COVID-19 Pandemie an Bedeutung gewonnen hat, betrifft die Frage der Entschädigung von Arbeitnehmenden für die weisungsbedingte Bereitstellung der privaten Infrastruktur (Räume, Internet, Geräte, Strom etc.). Grundsätzlich sieht das Gesetz vor, dass sowohl für die Nutzung privater Geräte (Art. 327 Abs. 2 OR), als auch für andere im Zusammenhang mit der Arbeitserfüllung entstandene Auslagen (Art. 327a OR) von Arbeitgebenden eine Entschädigung zu leisten ist. Dies gilt insbesondere in jenen Fällen, in welchen Arbeitgebende diese Geräte/Infrastruktur nicht von sich aus zur Verfügung stellen.[601] Im Rahmen der Home-Office Pflicht aufgrund von COVID-19 schulden

---

[594] BIRKHÄUSER UND HADORN, S. 203f.; WILDHABER UND HÄNSEBERGER, BYOD, S. 159.

[595] BIRKHÄUSER UND HADORN, S. 204f.

[596] Vgl. u.a. BIRKHÄUSER UND HADORN, S. 203f. und BUNDESRAT, Rechtliche Folgen der Telearbeit, S. 57.

[597] Vgl. u.a. BIRKHÄUSER UND HADORN, S. 203f. und BUNDESRAT, Rechtliche Folgen der Telearbeit, S. 57.

[598] BIRKHÄUSER UND HADORN, S. 204f.

[599] WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz, S. 328.

[600] Für eine Aufzählung, was in einem solchen Reglement enthalten sein könnte, PORTMANN, S: 43; BIRKHÄUSER UND HADORN, S. 205f.

[601] Ein Entschädigungsanspruch für einen Teil der Mietkosten eines Arbeitnehmers wurde vom BGer in einem Fall bejaht, in welchem die Arbeitgeberin diesem keinen dauernden und geeigneten Arbeitsplatz angeboten hatte

Arbeitgebende Arbeitnehmenden hingegen keine Auslagenentschädigung nach Art 327a OR[602] für die Bereitstellung der privaten Infrastruktur (Strom- und Mietkosten).[603] Von der Pflicht, Arbeitnehmenden die zur Arbeitserfüllung notwendigen Arbeitsmittel (Laptop, Papier etc.) zur Verfügung zu stellen (Art. 327 Abs. 1 OR), sind Arbeitgebende jedoch nicht entbunden.[604]

7.5. Fazit

BYOD schafft die Voraussetzung für mehr Autonomie und Mobilität in der zeitlichen und örtlichen Arbeitsgestaltung von Mitarbeitenden und vereinfacht insbesondere die Telearbeit (*supra* Ziff. 6). Genau dieser vereinfachte Zugang zur Arbeit kann aber auch einen vereinfachten Zugang von Arbeitgebenden auf das Gerät und die (privaten) Daten von Arbeitnehmenden nach sich ziehen und stellt damit eine Gefahr für deren Privatsphäre dar. Von den in den Konsultationen genannten Beispielen illustrieren insbesondere die Synchronisations- und Zugriffs-Apps, welches Risiko für die Privatsphäre mit der Nutzung privater Geräte zur Arbeitserfüllung einhergehen kann. Nebst einer sorgfältigen Prüfung der arbeits- und datenschutzrechtlichen Auswirkungen solcher Anwendungen ist es deshalb zentral, dass klare Regeln und Grenzen für BYOD für den gesamten Betrieb definiert werden.

und dieser deshalb von zuhause arbeiten musste (BGer 4A-533/2018 vom 23.04.2019). Bezüglich weiterer Kostenkategorien, PÄRLI UND EGGMANN, Rechtsfragen des Homeoffice, Rz. 46ff.

602 So vorgesehen in Art. 10 Abs. 3 Verordnung über Massnahmen in der besonderen Lage zur Bekämpfung der Covid-19-Epidemie vom 19. Juni 2020 (Stand 19.04.2021), SR 818.101.26 (Covid-19-Verordnung besondere Lage) und Art. 27a Abs. 1 Verordnung 3 über Massnahmen zur Bekämpfung des Coronavirus (COVID-19) vom 19.06.2020 (Stand 18.01.2021), SR 818.101.24 (COVID-19-Verordnung 3).

603 Ausführlich hierzu, PÄRLI UND EGGMANN, Rechtsfragen des Homeoffice, RZ. 42-56. Zum Verhältnis zwischen der COVID-19-Verordnung 3 zum Arbeitsrecht, PÄRLI UND EGGMANN, Würdigung der aktuellen Rechtslage, RZ. 26-28.

604 PÄRLI UND EGGMANN, Rechtsfragen des Homeoffice, Rz. 46ff.

IV. SCHLUSSBEMERKUNGEN

Ziel der vorliegenden Untersuchung war es, den aktuellen Digitalisierungsdiskurs im Beschäftigungskontext mit Blick auf die Privatsphäre von Arbeitnehmenden zu vertiefen. Hierfür wurden beispielhaft ausgewählte Szenarien zur Verwendung von digitalen Technologien in Beschäftigungsverhältnissen einer (menschen-)rechtlichen Beurteilung unterzogen. Im Fokus standen aktuelle und zukünftig relevante Technologien, einschliesslich Internet, Videosysteme, GPS, auf Biometrie basierte Systemen sowie Wearables und weitere «intelligente» algorithmische Anwendungen, welche das Potenzial haben, den Arbeitsplatz in eine intelligente Umgebung, einen sog. *smart workplace,* zu transformieren.

Die Untersuchung zeigt, dass diese Technologien am Arbeitsplatz unterschiedliche Risiken für die Privatsphäre der Arbeitnehmenden mit sich bringen. Im Vordergrund steht einerseits das damit verbundene Potenzial, praktisch unbegrenzt Daten zu erheben, zu verarbeiten, diese zueinander in Beziehung zu setzen und auszuwerten. Im Rahmen von digitalisierten Datenverarbeitungsvorgängen ist es zudem von Bedeutung, dass Technologien nicht, oder nur begrenzt, zwischen privaten und geschäftlichen Daten unterscheiden (können). Von dieser «technologischen Indifferenz» profitieren jene Arbeitgebenden, welche mehr Informationen über ihre Arbeitnehmenden erhalten wollen, als dies für die Erfüllung eines Arbeitsverhältnisses notwendig wäre.

Andererseits fördert die Digitalisierung am Arbeitsplatz in indirekter Weise auch die Entgrenzung von Arbeit und Freizeit im Kontext von flexiblen Arbeitserfüllungsformen – z.B. beim Home-Office oder im Zusammenhang mit BYOD.

Nicht zuletzt aufgrund der aktuellen Erfahrungen im Rahmen der COVID-19 Massnahmen zeigt sich, dass jene Technologien, welche die Persönlichkeit und die Privatsphäre Einzelner tangieren können, digitale Arbeitsplätze und flexible Arbeitserfüllungsformen überhaupt erst möglich machen. Aus einer menschenrechtlichen Perspektive stellt sich deshalb die grundsätzliche Frage, wie die Vorteile digitaler Technologien bestmöglich genutzt werden können, ohne die Grund- und Menschenrechte Einzelner zu beeinträchtigen.

Unterschiedliche regulatorische Ansätze sollen zukünftig dazu beitragen, dass dieses Gleichgewicht erreicht wird. So haben z.B. die in der DSGVO und im neuen Datenschutzgesetz verankerten Instrumente des Datenschutzes durch Technikgestaltung («*privacy by design*») und der datenschutzfreundlichen Voreinstellungen («*privacy by default*») das Potenzial, den Schutz der Privatsphäre bereits vor der eigentlichen Datenbearbeitung stärken. Im Kern geht es bei diesen Konzepten darum, einen effektiven Datenschutz nicht nur durch eine reaktive *ex post* Betrachtung von Datenverarbeitungsvorgängen zu realisieren, sondern technische Prozesse bereits *ex ante* in Einklang mit den datenschutzrechtlichen Vorgaben zu bringen.[605]

In jenen Fällen, in welchen ein besonders hohes Risiko für die Grund- und Menschenrechte der betroffenen Personen besteht, wird dieser proaktive Ansatz durch die Pflicht ergänzt, eine Datenschutz-Folgenabschätzung – oder *privacy impact assessment* –, vorzunehmen. Hierbei handelt es sich um das datenschutzrechtliche Äquivalent zum *human rights impact assessment*.

Während es im Bereich der Digitalisierung unterschiedliche Bestrebungen gibt, die sich durch digitale Technologien stellenden menschenrechtlichen Herausforderungen in normativer Hinsicht zu

---

[605] NOLTE UND WERKMEISTER, Art. 25 DSGVO, Rz. 2.

bewältigen – neben der DSGVO und dem N-DSG gibt es aktuell auch zahlreiche (nicht-verbindliche) Initiativen zu algorithmischen Systemen/KI – so gilt dies nicht im selben Mass für das Arbeitsrecht. Weder auf internationaler, regionaler noch nationaler Ebene gibt es zurzeit konkrete Initiativen, rechtliche Problemfelder im Schnittbereich der Digitalisierung/Privatsphäre aus einer arbeitsrechtlichen Perspektive verbindlich zu regeln. Einzig im Kontext des Home-Office laufen in der Schweiz erste Bemühungen, die Regelungen zur Arbeitszeit anzupassen, um eine zeitlich flexiblere Arbeitserfüllung zu ermöglichen. Diese Flexibilisierung kann sich allerdings je nach Kontext sowohl positiv als auch negativ auf die individuelle Privatsphäre auswirken.

Aus grundrechtlicher Perspektive ist es deshalb notwendig, nicht nur einen datenschutzrechtlichen Ansatz zu verfolgen, sondern auch die arbeitsrechtlichen Instrumente, welche weitergehende Schutzmassnahmen ermöglichen, einzubeziehen. Bei der Weiterentwicklung des rechtlichen Schutzes ist zu beachten, dass auch die (selbstständigen) Arbeitstätigkeiten erfasst werden, welche aktuell (noch) nicht in den Geltungsbereich des Arbeitsrechtes fallen. Ein Beispiel hierfür ist der Personentransportdienst Uber, dessen Fahrerinnen und Fahrer je nach Kanton als (un-)selbstständige Arbeitnehmende qualifiziert werden und welche somit von unterschiedlichen Arbeitsschutzmassnahmen profitieren.

Abschliessend sei darauf hingewiesen, dass mit den vielseitigen grund- und menschenrechtlichen Herausforderungen im Zusammenhang mit der Verwendung von neuen Technologien im Beschäftigungskontext auch die Verantwortung von Arbeitgebenden wächst, diesen Rechten effektiv Geltung zu verleihen.

LITERATURVERZEICHNIS

Literatur

ALLENSPACH BRIGIT, Wearables am Arbeitsplatz, in: Jusletter 26.11.2018.

ANANDARAJAN MURUGAN, Profiling Web Usage in the Workplace: A Behavior-Based Artificial Intelligence Approach, Journal of Management Information Systems, Vol. 19 (1) 2002, S. 243-266.

BAERISWYL BRUNO,

- Entwicklungen im Datenschutzrecht, in: SJZ 114/2018, S. 450-452, zit: BAERISWYL, Entwicklungen im Datenschutzrecht 2018.
- Vorbemerkungen zu Art. 1-3, in: Baeriswyl Bruno und Pärli Kurt (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz (DSG), Bern 2015, S. 6-7, zit.: BAERISWYL, Vorbemerkungen.
- Art. 4, in: Baeriswyl Bruno und Pärli Kurt (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz (DSG), Bern 2015, S. 50-65, zit.: BAERISWYL, Art. 4 DSG.

BAUER DENNIS/WUTZKE ROLF/BAUERNHANSL THOMAS, Wear@Work – A new approach for data acquisition using wearables, Procedia CIPR 50, 2016, S. 529-534.

BERNSDORFF NORBERT,

- Art. 7 GRC – Achtung des Privat- und Familienlebens, in: Meyer Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden 2019, S. 256-265, zit: BERNSDORFF, Art. 7 GRC.
- Art. 8 GRC – Schutz personenbezogener Daten, in: Meyer Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden 2019, S. 265-283, zit: BERNSDORFF, Art. 8 GRC.

BIAGGINI GIOVANNI, BV Kommentar – Bundesverfassung der Schweizerischen Eidgenossenschaft, OFK, 2. Aufl., Zürich 2017.

BIRKHÄUSER NICOLAS UND HADORN MARCEL, BYOD – Bring Your Own Device, in: SJZ 109/2013, S. 201-207.

BITKOM/DFKI, Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, 2017, abrufbar unter: https://www.dfki.de/fileadmin/user_upload/import/9744_171012-KI-Gipfelpapier-online.pdf (zuletzt besucht am 20.04.2021).

BOEHM FRANZISKA, Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Heidelberg 2012.

BOYD DANAH UND CRAWFORD KATE, Critical Questions for Big Data – Provocations for a cultural, technological, and scholarly phenomenon, Information, Communication & Society, 15:5 (2012), S. 662-679.

BREGIANNIS FOTIS, López Ribalda and Others v. Spain – covert surveillance in the workplace: attenuating the protection of privacy for employees, 2019, abrufbar unter: https://strasbourgobservers.com/2019/12/06/lopez-ribalda-and-others-v-spain-covert-surveillance-in-the-workplace-attenuating-the-protection-of-privacy-for-employees/ (zuletzt besucht am 20.04.2021).

BREITENMOSER STEPHAN UND SCHWEIZER RAINER J., Art. 13, in: Ehrenzeller Bernhard et al., Die Schweizerische Bundesverfassung – St. Galler Kommentar, Zürich 2014.

BRÜHWILER JÜRG, Einzelarbeitsvertrag – Kommentar zu den Art. 319-343 OR, 3. Aufl. Basel 2014, zit.: BRÜHWILER, OR [x].

BIERI ADRIAN UND POWELL JULIAN, Die Totalrevision des Bundesgesetzes über den Datenschutz, in: Jusletter 16.11.2020.

CATE FRED H./CULLEN PETER/MAYER-SCHÖNBERGER VIKTOR, Data Protection Principles for the 21st Century – Revising the 1980 OECD Guidelines, 03/2014, abrufbar unter: https://www.oii.ox.ac.uk/archive/downloads/publications/Data_Protection_Principles_for_the_21st_Century.pdf (zuletzt besucht am 20.04.2021).

CENTRUM FÜR EUROPÄISCHE POLITIK (CEP), Ethik-Leitlinien für KI, 16/2019, abrufbar unter: https://www.cep.eu/fileadmin/user_upload/cep.eu/Analysen/COM_2019_168_Ethik_in_KI/cepAnalyse_COM_2018_168__Ethische_Leitlinien_fuer_Kuenstliche_Intelligenz.pdf (zuletzt besucht am 20.04.2021), zit.: CEP, Ethik-Leitlinien.

CIRIGLIANO LUCA,

- Auch Arbeitnehmende im Home-Office haben Rechte!, 2018, abrufbar unter: https://www.sgb.ch/themen/arbeit/detail/auch-arbeitnehmende-im-home-office-haben-rechte (zuletzt besucht am 20.04.2021), zit. CIRIGLIANO, Arbeitnehmende.
- Home-Office: Bundesrat will nicht handeln – Gesundheitsschutz und Auslagen sind verbindlich zu regeln, 2016, abrufbar unter: https://www.sgb.ch/themen/arbeit/detail/home-office-bundesrat-will-nicht-handeln (zuletzt besucht am 20.04.2021), zit.: CIRIGLIANO, Gesundheitsschutz.

CLAXTON GARY ET. AL. (KAISER FAMILY FOUNDATION), Employer Health Benefits – 2019 Annual Survey, 2019, abrufbar unter: https://www.kff.org/report-section/ehbs-2019-section-1-cost-of-health-insurance/ (zuletzt besucht am 20.04.2021).

CRAVEN MATTHEW C.R., The International Covenant on Economic, Social and Cultural Rights: A Perspective on its Development, Oxford 1995.

CUSTERS BART UND URSIC HELENA, Worker Privacy in a Digitalized World under European Law, 39 Comp. La. L. & Pol'y J., 2018, S. 323-344.

DAEDELOW ROMY, Wenn Algorithmen (unfair) über Menschen entscheiden...: Welchen Schutz bietet die Datenschutz-Grundverordnung?, in: Jusletter 26.11.2018.

DÄUBLER, WOLFGANG, Entgrenzung der Arbeit – ein Problem des Arbeitsrechts?, Soziales Recht, Vol. 4 No. 2 (2014), S. 45-65.

DE JESUS AYN, Using Wearable Data for Artificial Intelligence Applications – Current Use Cases, Emerj Artificial Intelligence Research, 02.10.2018, abrufbar unter: https://www.techemergence.com/using-wearable-data-for-artificial-intelligence-applications-current-use-cases/ (zuletzt besucht am: 20.04.2021).

DELOITTE, How Covid-19 contributes to a long-term boost in remote working, 2020, abrufbar unter: https://www2.deloitte.com/ch/en/pages/human-capital/articles/how-covid-19-contributes-to-a-long-term-boost-in-remote-working.html (zuletzt besucht am 20.04.2021).

DETTLING THOMAS J UND DETTLING DANIEL, Corona wird unsere Arbeitswelt revolutionieren – im Hinblick auf mehr Führungsintelligenz, mehr Empathie und mehr Selbstbestimmung, NZZ vom 15.05.2020, abrufbar unter: https://www.nzz.ch/meinung/digital-im-schwarm-corona-revolutioniert-unsere-arbeitswelt-ld.1556125 (zuletzt besucht am 20.04.2021).

DIGGELMANN OLIVER, Art. 13 BV (Schutz der Privatsphäre), in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Bundesverfassung – Basler Kommentar, Basel 2015, S. 283ff.

DIGGELMANN OLIVER UND CLEIS MARIA NICOLE, How the Right to Privacy Became a Human Right, in: Human Rights Law Review 3/2014, S. 441ff.

DIMOV DANIEL UND JUZENAITE RASA, Privacy Concerns about Emotional Chatbots, Infosec Resources, 16.02.2018, abrufbar unter: https://resources.infosecinstitute.com/privacy-concerns-emotional-chatbots/#gref (zuletzt besucht am: 20.04.2021).

DOMENIG PASCAL, Homeoffice-Arbeit als besondere Erscheinungsform im Einzelarbeitsverhältnis, Bern 2016.

DR. DATENSCHUTZ, Wearables im Beschäftigungsverhältnis – Was ist erlaubt?, 07.06.2017, abrufbar unter: https://www.datenschutzbeauftragter-info.de/wearables-im-beschaeftigungsverhaeltnis-was-ist-erlaubt/ (zuletzt besucht am 20.04.2021).

DUNAND JEAN-PHILIPPE/MAHON PASCAL/WITZIG AURÉLIEN (Hrsg.), La révolution 4.0 au travail – Une approche multidisciplinaire, Genf/Zürich/Basel 2019.

DZIDA BORIS, Wearables am Arbeitsplatz – Wie tragbare Computersysteme Einzug in die Betriebe halten, Serie Arbeitsrechte 4.0., ArbRB 5/2016, S. 146-149.

EGLI URS, Soziale Netzwerke und Arbeitsverhältnis: Über die Auswirkungen von Facebook, Xing & Co auf den betrieblichen Alltag, in: Jusletter 17.01.2011.

EPINEY ASTRID, Big Data und Datenschutzrecht Gibt es einen gesetzgeberischen Handlungsbedarf?, in: Jusletter 27.04.2020.

EPINEY ASTRID UND 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 und Nüesch Daniela, Die Revision des Datenschutzes in Europa und der Schweiz, Zürich et. al. 2016, S. 39-76.

EPINEY ASTRID/CIVITELLA TAMARA/ZBINDEN PATRIZIA, Datenschutzrecht in der Schweiz; Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, in: Freiburger Schriften zum Europarecht Nr. 10, Freiburg 2009, abrufbar unter: https://www3.unifr.ch/ius/euroinstitut/fr/assets/public/files/publications/cahiers%20fribourgeois/Cahier_10.pdf (zuletzt besucht am 20.04.2021).

FARR CHRISTINA, How Fitbit Became The Next Big Thing In Corporate Wellness, Fast Company, 18.04.2016, abrufbar unter: https://www.fastcompany.com/3058462/how-fitbit-became-the-next-big-thing-in-corporate-wellness (zuletzt besucht am 20.04.2021).

FLÜCKIGER ALEXANDRE, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, in: AJP 6/2013, S. 837-864.

FORD MICHAEL, Two Conceptions of Worker Privacy, Industrial Law Journal, Vol. 31 No. 2 (2002), S. 135- 155.

FRENZ WALTER, Handbuch Europarecht, Band 4 Europäische Grundrechte, Berlin und Heidelberg 2009.

FREYTAG URS, Mitarbeiterüberwachung: Was geht, was geht nicht?, in: inside 3/2016, abrufbar unter: https://www.inside-swisst.net/recht-3-2016.html (zuletzt besucht am 20.04.2021).

GOODMAN RACHEL, Why Amazon's Automated Hiring Tool Discriminated against Women, ACLU, 12.10.2018, abrufbar unter: https://www.aclu.org/blog/womens-rights/womens-rights-workplace/why-amazons-automated-hiring-tool-discriminated-against (zuletzt besucht am 20.04.2021).

GORDON CLARA-ANN, Daten aus Selbstvermessung, in: digma 2/2016, S. 70-75.

GREENLEAF GRAHAM/CLARKE ROGER/WATERS NIGEL, International Data Privacy Standards: A Global Approach (Australian Privacy Foundation Policy Statement), 09/2013, abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327325 (zuletzt besucht am 20.04.2021).

HABERMAS JÜRGEN, Strukturwandel der Öffentlichkeit – Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft, 16. Aufl., Darmstadt und Neuwied 1986.

HANCOCK JAY, Workplace wellness programs put employee privacy at risk, CNN, 02.10.2015, abrufbar unter: https://edition.cnn.com/2015/09/28/health/workplace-wellness-privacy-risk-exclusive/ (zuletzt besucht am 20.04.2021).

HANSEN MAJA, Recruiting der Zukunft: Wie künstliche Intelligenz Bewerbungsverfahren beeinflussen wird, OnlineMarketing.de, 03.08.2018, abrufbar unter: https://onlinemarketing.de/jobs/artikel/recruiting-kuenstliche-intelligenz-bewerbungsverfahren (zuletzt besucht am: 20.04.2021).

HAYES DARREN/SNOW CHRISTOPHER/ALTUWAYJIRI SALEH, Geolocation Tracking and Privacy Issues Associated with the Uber Mobile Application, 2017, abrufbar unter: https://www.researchgate.net/profile/Darren_Hayes2/publication/320839993_Geolocation_Tracking_and_Privacy_Issues_Associated_with_the_Uber_Mobile_Application/links/59fcd68da6fdcca1f296ba7b/Geolocation-Tracking-and-Privacy-Issues-Associated-with-the-Uber-Mobile-Application.pdf (zuletzt besucht am 20.04.2021).

HEILMANN CARA, Artificial Intelligence and Recruiting: A Candidate's Perspective, Forbes, 22.06.2018, abrufbar unter: https://www.forbes.com/sites/forbescoachescouncil/2018/06/22/artificial-intelligence-and-recruiting-a-candidates-perspective/# (zuletzt besucht am: 20.04.2021).

HELLE JÜRGEN, Die heimliche Videoüberwachung – zivilrechtlich betrachtet, in: JuristenZeitung 7/2004.

HENDRICKX FRANK UND VAN BEVER ALINE, Article 8 ECHR: Judicial Patterns of Employment Privacy Protection, in: Drossemont Filip et al. (Hrsg.), The European Convention on Human Rights and the Employment Relation, Oxford 2013, S. 183-208.

HERMANN RUDOLF, Der Roboter führt die Vorstellungsgespräche, in: NZZ vom 19.12.2019, abrufbar unter: https://www.nzz.ch/wirtschaft/tengai-der-roboter-der-vorurteilsfreie-vorstellungsgespraeche-fuehrt-ld.1521953 (zuletzt besucht am 20.04.2021).

HEIZ ROMAN UND NÄF PATRICK, Überwachung am Arbeitsplatz, 2019, abrufbar unter: https://www.wengervieli.ch/getattachment/a3b23fc2-0462-46a3-bc52-34b8fe922ae5/1900748_ueberwachung-am-arbeitsplatz_web.pdf.aspx (zuletzt besucht am 20.04.2021).

HÖFER SEBASTIAN, Algorithmen, maschinelles Lernen und die Grenzen der KI, in: Jusletter 26.11.2018.

HORNUNG GERRIT UND STEIDLE ROLAND, Biometrie am Arbeitsplatz – sichere Kontrollverfahren versus ausuferndes Kontrollpotential, Arbeit und Recht, Vol. 53 No. 6 (2005), S. 201-207.

HÜPERS BERND UND REESE BIRGIT, Art. 31 GRC Gerechte und angemessene Arbeitsbedingungen, in: Meyer Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden 2019, S. 508-539.

HUSI-STÄMPFLI SANDRA, Entstehungsgeschichte, in: Baeriswyl Bruno und Pärli Kurt (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz (DSG), Bern 2015, S. 1-5.

HUSMANN NELE, Wenn künstliche Intelligenz über die Bewerbung richtet, Handelszeitung vom 25.10.2017, abrufbar unter: https://www.handelszeitung.ch/management/wenn-kuenstliche-intelligenz-ueber-die-bewerbung-richtet-1510111 (zuletzt besucht am: 20.04.2021).

JACOBSON JENNA UND GRUZD ANATOLIY, Cybervetting job applicants on social media: the new normal?, Ethics and Information Technology 22 (2020), S. 175-195.

JOYCE DANIEL, Privacy in the Digital Era: Human Rights Online?, in: Melbourne Journal of International Law 1/2015, S. 270ff.

KAGERMANN HENNING/LUKAS WOLF-DIETER/WAHLSTER WOLFGANG, Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. Industriellen Revolution, in: VDI Nachrichten, 01.04.2011, abrufbar unter: http://www.wolfgang-wahlster.de/wordpress/wp-content/uploads/Industrie_4_0_Mit_dem_Internet_der_Dinge_auf_dem_Weg_zur_vierten_industriellen_Revolution_2.pdf (zuletzt besucht am 20.04.2021).

KÄLIN WALTER UND KÜNZLI JÜRG, Universeller Menschenrechtsschutz, 4. Aufl., Basel 2019.

KELLER SENTA, Sind Uber-Fahrer selbstständig erwerbend, oder nicht?, 29.11.2019, abrufbar unter: https://www.srf.ch/news/schweiz/der-streit-geht-weiter-sind-uber-fahrer-selbststaendig-erwerbend-oder-nicht (zuletzt besucht am 20.04.2021).

KIENER REGINA/KÄLIN WALTER/WYTTENBACH JUDITH, Grundrechte, 3. Aufl., Bern 2018.

KOPP REINHOLD UND SOKOLL KAREN, Wearables am Arbeitsplatz – Einfallstore für Alltagsüberwachung?, NZA 2015, S. 1352ff.

KÜHLING JÜRGEN UND SACKMANN FLORIAN, Datenschutzordnung 2018 – nach der Reform ist vor der Reform?!, in: NVwZ 2018, S. 681-686.

MAHON PASCAL, Le droit à l'intégrité numérique: réelle innovation ou simple évolution du droit? Le point de vue du droit constitutionnel, in: Guillaume Florence/Mahon Pascal (eds.), Basel 2021, S. 43-63.

MARSCH NIKOLAUS, Das Europäische Datenschutzgrundrecht, Jus Publicum 270, Tübingen 2018.

MCCARTHY J. ET. AL., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955, abrufbar unter: http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf (zuletzt besucht am 20.04.2021).

MCDONALD PAULA/THOMPSON PAUL/O'CONNOR PETER, Profiling employees online: shifting public–private boundaries in organisational life, Human Resource Management Journal, Vol. 26, no. 4 (2016), S. 541-556.

MÉTILLE SYLVAIN UND GUYOT NICOLAS, Le moment est venu de reconnaître un statut juridique aux robots, in: plaidoyer 3/2015, S. 26-29.

METZINGER THOMAS, Nehmt der Industrie die Ethik weg!, in: Tagesspiegel vom 08.04.2019, abrufbar unter: https://www.tagesspiegel.de/politik/eu-ethikrichtlinien-fuer-kuenstliche-intelligenz-nehmt-der-industrie-die-ethik-weg/24195388.html (zuletzt besuch 20.04.2021).

MÜHLEMATTER THOMAS UND DONNO FLAVIA, Why smart bakers wear glasses: Performance and User Acceptance of Smartglasses by Bank Employees, 2016, abrufbar unter: https://dl.acm.org/citation.cfm?id=2967179 (zuletzt besucht am 20.04.2021).

MÜLLER JÖRG PAUL, Verwirklichung der Grundrechte nach Art. 35 BV, Bern 2018, zit.: MÜLLER, Art. 35 BV.

MÜLLER THOMAS, Schweizer Konzerne überprüfen Bewerber im Internet, 2011, abrufbar unter: https://www.tagesanzeiger.ch/leben/gesellschaft/schweizer-konzerne-ueberpruefen-bewerber-im-internet/story/17153295 (zuletzt besucht am 20.04.2021), zit.: MÜLLER, Schweizer Konzerne überprüfen Bewerber im Internet.

NOLTE NORBERT UND WERKMEISTER CHRISTOPH,

- Art. 25 DSGVO, in: Gola Peter (Hrsg), Datenschutz-Grundverordnung: VO (EU) 2016/679 Kommentar, 2. Aufl., München 2018, S. 549-558, zit.: Art. 25 DSGVO.
- Art. 35 DSGVO, Gola Peter (Hrsg), Datenschutz-Grundverordnung: VO (EU) 2016/679 Kommentar, 2. Aufl., München 2018, S. 633-652, zit: NOLTE NORBERT UND WERKMEISTER CHRISTOPH, Art. 35 DSGVO.

PAPA ROBERTA UND PIETRUSZAK THOMAS, Datenschutzrecht im Personalwesen, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht, Handbücher für die Anwaltspraxis, Basel 2015, § 17, S. 577-611.

PÄRLI KURT,

- Die Datenschutz-Grundverordnung und ihre Bedeutung aus Schweizer Optik für das Arbeitsrecht (Präsentation am Datenschutzforum), 2017, abrufbar unter: https://www.datenschutz-forum.ch/files/1485364609.pdf (zuletzt besucht am 20.04.2021), zit: PÄRLI, DSGVO.
- Neue Formen der Arbeitsorganisation: Internet-Plattformen als Arbeitgeber, in ARV 2016, S. 243-254, zit.: PÄRLI, Formen der Arbeitsorganisation.

- Gutachten zur Bedeutung der EMRK und der Beschwerde an den EGMR für das schweizerische Arbeitsrecht (im Auftrag des Schweizerischen Gewerkschaftsbund SGB), 2015, abrufbar unter: https://www.humanrights.ch/cms/upload/pdf/160902_Gutachten_Bedeutung_EMRK_SGB.pdf (zuletzt besucht am 20.04.2021), zit.: PÄRLI, Gutachten EMRK.
- Art. 328b OR, in: Baeriswyl Bruno und Pärli Kurt (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz (DSG), 2015, S. 409-423, zit.: PÄRLI, Art. 328b OR.
- Schutz der Privatsphäre am Arbeitsplatz in digitalen Zeiten – eine menschenrechtliche Herausforderung, EuZA, 2015, S. 48-64, zit.: PÄRLI, Schutz der Privatsphäre.
- Evaluieren, kontrollieren, überwachen: Datenschutz in Arbeitsverhältnissen, in: Kieser Ueli und Pärli Kurt, Datenschutz im Arbeits-, Versicherungs- und Sozialbereich: aktuelle Herausforderungen, Schriftenreihe des Instituts für Rechtswissenschaft und Rechtspraxis, Band 80, St. Gallen 2012, zit.: PÄRLI, Evaluieren, kontrollieren, überwachen.

PÄRLI KURZ UND EGGMANN JONAS,

- Ausgewählte Rechtsfragen des Homeoffice – Im Zusammenhang mit der Corona-Pandemie und darüber hinaus, in: Jusletter 22.02.2021, zit.: PÄRLI UND EGGMANN, Rechtsfragen des Homeoffice.
- Corona und die Arbeitswelt – Bestandsaufnahme und Würdigung der aktuellen Rechtslage, in: Jusletter 8.02.2021, zit.: PÄRLI UND EGGMANN, Würdigung der aktuellen Rechtslage.

PÄTZOLD JULIANE, Art. 8 EMRK, in: Karpenstein Ulrich und Mayer Franz C. (Hrsg.), Konvention zum Schutz der Menschenrechte und Grundfreiheiten, Kommentar, 2. Aufl., München 2015, S. 252-284.

PILTZ CARLO

- Art. 3 DSGVO, in: Gola Peter (Hrsg), Datenschutz-Grundverordnung: VO (EU) 2016/679 Kommentar (ed.), 2. Aufl., München 2018, S. 165-177, zit.: PILTZ, Art. 3 DSGVO.
- Art. 95 DSGVO, in: Gola Peter (Hrsg), Datenschutz-Grundverordnung: VO (EU) 2016/679 Kommentar (ed.), 2. Aufl., München 2018, S. 1022-1027, zit.: PILTZ, Art. 95 DSGVO.

PORTMANN ROLAND, Private Smartphones im Geschäftsumfeld, in: digma 2012/1, S: 42-43.

PÖTTERS STEPHAN, Art. 88 DSVGO, in: Gola Peter (Hrsg), Datenschutz-Grundverordnung: VO (EU) 2016/679 Kommentar (ed.), 2. Aufl., München 2018, S. 957-990.

REHBINDER MANFRED UND STÖCKLI JEAN-FRITZ, Einleitung und Kommentar zu den Art. 319–330b OR, in: Hausherr Heinz und Walter Hans Peter, Berner Kommentar, Band/Nr.VI/2/2/1, 2010, zit.: REHBINDER UND STÖCKLI, OR [Artikel].

RIEMER-KAFKA GABRIELA, Plattformarbeit oder andere Formen der Zusammenarbeit: Sind die Abgrenzungskriterien für selbständige oder für unselbständige Erwerbstätigkeit noch tauglich?, in: Schweizerische Zeitschrift für Sozialversicherung und berufliche Vorsorge, 2019, S. 581-602.

ROSENTHAL DAVID,

- Das neue Datenschutzgesetz, in: Jusletter 16.11.2020, zit.: ROSENTHAL, N-DSG.

- Der Entwurf für ein neues Datenschutzgesetz, in: Jusletter 27.11.2017, zit: ROSENTHAL, Entwurf N-DSG.

ROSENTHAL DAVID UND JÖHRI YVONNE (Hrsg.), Handkommentar zum Datenschutzgesetz, 2008, zit.: ROSENTHAL UND JÖHRI, Art.[x].

ROWLAND CHRISTOPHER, With fitness trackers in the workplace, bosses can monitor your every step – and possibly more, Washington Post vom 17.02.2019, abrufbar unter: https://www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace-bosses-can-monitor-your-every-step--and-possibly-more/2019/02/15/75ee0848-2a45-11e9-b011-d8500644dc98_story.html (zuletzt besucht am 20.04.2021).

RUDIN BEAT, Art. 3, in: Baeriswyl Bruno und Pärli Kurt (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz (DSG), 2015, S. 29-49.

SCHABAS WILLIAM A.,

- The European Convention on Human Rights: A Commentary, Oxford, 2017, zit.: SCHABAS, ECHR Commentary.
- U.N. Covenant on Civil and Political Rights, Nowak's CCPR Commentary, 3. ed., Kehl 2005, zit.: SCHABAS, Nowak's CCPR Commentary.

SCHIEDERMAIR STEPHANIE, Der Schutz des Privaten als Internationales Grundrecht, Jus Publicum 216, Tübingen 2012.

SCHUBERT CLAUDIA, Art. 31 GRC, in: Franzen Martin, Gallner Inken, Oetker Hartmut, Kommentar zum europäischen Arbeitsrecht, 3. Auflage, [München] 2020 beck-online, abrufbar unter: https://beck-online.beck.de/?vpath=bibdata%2Fkomm%2FFraGalOetKOEuArbR_3%2Fcont%2FFraGalOetKOEuArbR%2Ehtm (zuletzt besucht am 20.04.2021).

SCHÜRER HANS UELI UND WANNER MARIANNE, Arbeit und Recht, 13. Aufl., Zürich 2016.

SCHWAB KLAUS, The Fourth Industrial Revolution – What It Means and How to Respond, Foreign Affairs vom 12.12.2015, abrufbar unter: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution (zuletzt besucht am 20.04.2021).

SCHWEIZER RAINER J., Art. 35, in: Ehrenzeller Bernhard et al., Die Schweizerische Bundesverfassung – St. Galler Kommentar, Zürich 2014.

SCHWEIZER RAINER J. UND RECHSTEINER DAVID, Grund- und menschenrechtlicher Datenschutz, in: Passadelis Nicolas/Rosenthal David/Thür Hanspeter (Hrsg.), Datenschutzrecht, Handbücher für die Anwaltspraxis, Basel 2015, § 2, S. 41-71.

SCHWEIZERISCHES KOMPETENZZENTRUM FÜR MENSCHENRECHTE (SKMR),

- Das Recht auf Privatsphäre im digitalen Zeitalter – Staatliche Schutzpflichten bei Aktivitäten von Unternehmen: Update zur SKMR-Studie vom 22.09.2016, verfasst von Soltani Patricia und Ghielmini Sabrina, 2020, zit. SKMR, Update zu «Das Recht auf Privatsphäre im digitalen Zeitalter»
- Das Recht auf Privatsphäre im digitalen Zeitalter – Staatliche Schutzpflichten bei Aktivitäten von Unternehmen, verfasst von Kaufmann Christine et. al, Bern 2016, zit: SKMR, Das Recht auf Privatsphäre im digitalen Zeitalter

- Extraterritorialität im Bereich Wirtschaft und Menschenrechte, Extraterritoriale Rechtsanwendung und Gerichtsbarkeit in der Schweiz bei Menschenrechtsverletzungen durch transnationale Unternehmen, verfasse von Kaufmann Christine et. al., Bern 2016 (nicht veröffentlicht), zit.: SKMR, Extraterritorialität im Bereich Wirtschaft und Menschenrechte.
- Umsetzung der Menschenrechte in der Schweiz – Eine Bestandesaufnahme im Bereich Menschenrechte und Wirtschaft, verfasst von Kaufmann Christine et. al., Bern 2013, zit.: SKMR, Grundlagenstudie.

SEIFERT ACHIM, Die horizontale Wirkung von Grundrechten: Europarechtliche und rechtsvergleichende Überlegungen, in: EuZW 2011, S. 696-702.

SENTI CHRISTOPH, Reglemente als Ergänzung zum Arbeitsvertrag, in: AJP 2004, S. 1083-1092.

SIMITIS SPIROS, Einleitung: Geschichte – Ziele – Prinzipien, in: Simitis Spiros (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 8. Aufl., Baden-Baden 2014, S. 81-196.

SÖBBING THOMAS, Künstliche Intelligenz im HR-Recruiting-Prozess: Rechtliche Rahmenbedingungen und Möglichkeiten, InTeR, 2018, S. 64-67.

STAEHELIN ADRIAN, Der Arbeitsvertrag, Art. 319-330a OR, Zürcher Kommentar, 4. Aufl., Zürich 2006, zit.: STAEHLIN, OR [x].

STÄUBLE MARIO UND ALICH HOLGER, «Wir messen, ob Mitarbeiter telefonieren oder Mails schreiben» (Interview mit Steven Baert, Personalchef Novartis), Tagesanzeiger vom 13.09.2020, abrufbar unter: https://www.tagesanzeiger.ch/wir-messen-ob-die-mitarbeiter-telefonieren-oder-mails-schreiben-731773168277 (zuletzt besucht am 20.04.2021).

STECK ALBERT, Der Roboter ist der neue Personalchef, in: NZZ vom 07.04.2018, abrufbar unter: https://nzzas.nzz.ch/wirtschaft/der-roboter-ist-der-neue-personalchef-ld.1375242 (zuletzt besucht am 20.04.2021).

STEPHAN MICHAEL, Talent acquisition: Enter the cognitive recruiter, Deloitte, 2017, abrufbar unter: https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2017/predictive-hiring-talent-acquisition.html (zuletzt besucht am 20.04.2021).

STREIFF ULLIN/VON KAENEL ADRIAN/RUDOLPH ROGER, Arbeitsvertrag Praxiskommentar zu Art. 319-362 OR, 7. Aufl., Zürich 2012, zit.: STREIFF ET AL., OR [x].

TWOMEY PAUL, Building on the Hamburg Statement and the G20 Roadmap for Digitalization – Toward a G20 framework for artificial intelligence in the workplace, Economics Discussion Papers, Kiel Institute for the World Economy, No. 2018-63.

VISCHER FRANK UND MÜLLER ROLAND M., Der Arbeitsvertrag (vierter Teilband), in: Wiegand Wolfgang, Schweizerisches Privatrecht VII/4, 4. Aufl., Basel 2014.

WACKS RAYMOND, Privacy: A Very Short Introduction, 2nd edn., Oxford 2015.

WALTER JEAN-PHILIPPE, L'intégrité numérique: une nécessité du point de vue du droit à la protection des données, in: Guillaume Florence/Mahon Pascal (eds.), Basel 2021, S. 95-101.

WARREN SAMUEL UND BRANDEIS LOUIS D., The Right to Privacy, Harvard Law Review, Vol. 4 No. 5 (1890), S. 193-220.

WEBER ROLF H.:

- Internet of Things: Privacy Issues Revisited, Computer Law & Security Review 31 (2015), S. 618-627, zit.: WEBER, Internet of Things (2015).
- Can Data Protection be improved through Privacy Impact Assessments?, in: Jusletter IT, 12.09.2012, zit.: WEBER, Privacy Impact Assessments.
- Neue Grundrechtskonzeptionen zum Schutz der Privatheit, in: Weber Rolf H. und Thouvenin Florent (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht, Zürich 2012, S. 7-29, zit.: WEBER, Grundrechtskonzeption.
- Internet of things – Need for a new legal environment?, Computer Law & Security 25 (2009), S. 522-527, zit.: WEBER, Internet of Things (2009).

WEBER ROLF H. UND HEINRICH ULRIKE I., Braucht die Schweiz ein Recht auf Vergessen im Internet?, 2014, abrufbar unter: https://doi.org/10.5167/uzh-108647 (zuletzt besucht am 20.04.2021).

WERMELINGER AMÉDÉO:

- Art. 12, in: Baeriswyl Bruno und Pärli Kurt (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz (DSG), Bern 2015, S. 164-171, zit.: WERMELINGER, Art. 12 DSG.
- Art. 13, in: Baeriswyl Bruno und Pärli Kurt (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz (DSG), Bern 2015, S. 172-186; zit.: WERMELINGER, Art. 13 DSG.

WILDHABER ISABELLE:

- Répercussions juridiques de la robotique et de l'intelligence artificielle sur le lieu de travail, in : Dunand Jean-Philippe/Mahon Pascal/Witzig Aurélien (Hrsg), La révolution 4.0 au travail – Une approche multidisciplinaire, Genf und Zürich, 2019, S. 201-241, zit.: WILDHABER, Répercussions juridiques de la robotique.
- Robotik am Arbeitsplatz: Robo-Kollegen und Robo-Bosse, in: AJP 2/2017, S. 213- 224, zit.: WILDHABER, Robotik.

WILDHABER ISABELLE UND HÄNSENBERGER SILVIO:

- Bundesgericht, I. sozialrechtliche Abteilung, Urteil 8C_79/2016 vom 30.06.2017, A. gegen Ferrovie Federali Svizzere FFS, öffentliches Dienstrecht (fristlose Entlassung eines SBB-Mitarbeiters wegen Pornokonsums während der Arbeitszeit), in: AJP 10/2017, S. 1252-1257, zit.: WILDHABER UND HÄNSEBERGER, SBB.
- Social Media-Kontakte im Arbeitsverhältnis: Wem „gehören" Accounts, Kontakte und Zugangsdaten?, in: Müller Roland/Pärli Kurt/Wildhaber Isabelle (Hrsg.), Arbeit und Arbeitsrecht – Festschrift für Thomas Geiser zum 65. Geburtstag, Zürich und St. Gallen 2017, S. 529-48, zit.: WILDHABER UND HÄNSEBERGER, Social Media im Arbeitsverhältnis.
- Bring Your Own Device (BYOD), in: ARV 3/2016, S. 151-165, zit: WILDHABER UND HÄNSEBERGER, BYOD.
- Internet am Arbeitsplatz – Ausgewählte arbeitsrechtliche Fragestellungen, in: ZBJV 152/2016, S. 307-341, zit.: WILDHABER UND HÄNSEBERGER, Internet am Arbeitsplatz.

WOLFER SIMON, Die elektronische Überwachung des Arbeitnehmers im privatrechtlichen Arbeitsverhältnis, Zürich/Basel/Genf 2008.

Amtliche Publikationen

AUSTRALIAN NATIONAL CONTACT POINT, Final Statement – This Specific Instance was submitted by Australian Women Without Borders against Mercer PR for its conduct in relation to activity in Nauru, 09.07.2019, abrufbar unter: https://ausncp.gov.au/sites/default/files/inline-files/16_AusNCP_Final_Statement_Online.pdf (zuletzt besucht am 20.04.2021), zit.: AU NCP.

BUNDESAMT FÜR KOMMUNIKATION (BAKOM), Strategie «Digitale Schweiz», 2020, abrufbar unter: https://www.bakom.admin.ch/dam/bakom/de/dokumente/informationsgesellschaft/strategie/strategie_digitale_schweiz.pdf.download.pdf/Strategie-DS-2020-De.pdf (zuletzt besucht am 20.04.2021), zit. BAKOM, Strategie digitale Schweiz.

BUNDESRAT,

- Bundesrat verschärft Massnahmen gegen das Coronavirus zum Schutz der Gesundheit und unterstützt betroffene Branchen, Medienmitteilung vom 13.03.2020, abrufbar unter: https://www.bag.admin.ch/bag/de/home/das-bag/aktuell/medienmitteilungen.msg-id-78437.html (zuletzt besucht am 20.04.2021), zit. BUNDESRAT, Massnahmen gegen das Coronavirus.
- Kompetenznetzwerk Künstliche Intelligenz wird geprüft, Medienmitteilung vom 04.12.2020, abrufbar unter: https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-81459.html (zuletzt besucht am 20.04.2021), zit.: BUNDESRAT, Medienmitteilung KI.
- Leitlinien «Künstliche Intelligenz» für den Bund – Orientierungsrahmen für den Umgang mit künstlicher Intelligenz in der Bundesverwaltung, 25.11.2020, abrufbar unter: https://www.sbfi.admin.ch/dam/sbfi/de/dokumente/2020/11/leitlinie_ki.pdf.download.pdf/Leitlinien%20K%C3%BCnstliche%20Intelligenz%20-%20DE.pdf (zuletzt besucht am 20.04.2021), zit.: BUNDESRAT, Leitlinien KI.
- Zwölfter Bericht über die Schweiz und die Konventionen des Europarates vom 11.09.2020, BBl 2020 8091, zit.: BUNDESRAT, Konventionen Europarat.
- Botschaft zur Genehmigung des Protokolls vom 10.10.2018 zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 06.12.2019, BBl 2020 566, zit.: BUNDESRAT, Botschaft Änderungsprotokoll.
- Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15.09.2017, BBl 2017 6941, zit.: BUNDESRAT, Botschaft E-DSG.
- Auswirkungen der Digitalisierung auf Beschäftigung und Arbeitsbedingungen – Chancen und Risiken: Bericht des Bundesrates in Erfüllung der Postulate 15.3854 Reynard vom 16.09.2015 und 17.3222 Derder vom 17.03.2017, 2017, zit.: BUNDESRAT, Auswirkungen der Digitalisierung
- Rechtliche Folgen der Telearbeit: Bericht des Bundesrates zum Postulat 12.3166 Meier-Schatz, 2016, zit. BUNDESRAT, Rechtliche Folgen der Telearbeit.

- Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz, 2011, zit.: BUNDESRAT, Evaluation DSG 2011.
- Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23.03.1988, BBl 1988 II 413, zit. BUNDESRAT, Botschaft DSG.

BURKART THIERRY, Mehr Gestaltungsfreiheit bei Arbeit im Homeoffice, Parlamentarische Initiative 16.484 (NR) vom 01.12.2016, abrufbar unter: https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20160484 (zuletzt besucht am 20.04.2021)

DATENSCHUTZBEAUFTRAGTER KANTON ZÜRICH, Merkblatt Online-Recherche über Stellenbewerbende, 2017, abrufbar unter: https://www.zh.ch/content/dam/zhweb/bilder-dokumente/themen/politik-staat/datenschutz/publikationen/formulare-merkblaetter/merkblatt_online_recherchen_ueber_stellenbewerber.pdf (zuletzt besucht am 20.04.2021).

EIDGENÖSSISCHER DATENSCHUTZ- UND ÖFFENTLICHKEITSBEAUFTRAGTER (EDÖB),

- 27. Tätigkeitsbericht 2019/2020, 2020, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/27--taetigkeitsbericht-2019-2020.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Tätigkeitsbericht 2019/20.
- 26. Tätigkeitsbericht 2018/2019, 2019, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/26--taetigkeitsbericht-2018-20190.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Tätigkeitsbericht 2018/9.
- Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz, 2018, abrufbar unter: https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/Die_EU_DSGVO_und_ihre_Auswirkungen_auf_die_Schweiz_DE_Nov18.pdf.download.pdf/Die_EU_DSGVO_und_ihre_Auswirkungen_auf_die_Schweiz_DE_Nov18.pdf (zuletzt besucht am 20.04.2021), zit: EDÖB, EU-DSGVO.
- 25. Tätigkeitsbericht 2017/2018, 2018, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/25--taetigkeitsbericht-2017-2018.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Tätigkeitsbericht 2017/8.
- Erläuterungen zum Einsatz von Fitnesstrackern im Versicherungsbereich, 2017, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/gesundheit/kranken--und-unfallversicherungen/erlaeuterungen-zum-einsatz-von-fitnesstrackern-im-versicherungsb.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Erläuterungen Fitnesstracker.
- 24. Tätigkeitsbericht 2016/2017, 2017, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/24--taetigkeitsbericht-2016-2017.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Tätigkeitsbericht 2016/7.
- Erläuterungen zur Videoüberwachung am Arbeitsplatz, 2016, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/ueberwachung-am-arbeitsplatz/erlaeuterungen-zur-videoueberwachung-am-arbeitsplatz.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Erläuterungen zur Videoüberwachung.
- 22. Tätigkeitsbericht 2014/2015, 2015, abrufbar unter: https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2015/06/22_taetigkeitsbericht20142015.pdf.download.pdf/22_taetigkeitsbericht20142015.pdf (zuletzt besucht am 20.04.2021), zit.: EDÖB, Tätigkeitsbericht 2014/5.

- datum, Newsletter des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten, Dezember 2014, zit.: EDÖB, datum – Folgen der Selbstvermessung.
- Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich – Bearbeitung durch private Personen, 2014, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/bearbeitung-von-personendaten-im-arbeitsbereich.html (zuletzt besucht am 20.04.2021), zit: EDÖB, Leitfaden Bearbeitung Personendaten im Arbeitsbereich.
- Datenspeicherung bei Verifizierungssystemen, 2013, abrufbar unter: https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2013/07/ergaenzung_zu_punkt323ueberdiedatenspeicherungbeibiometrischenve.pdf.download.pdf/ergaenzung_zu_punkt323ueberdiedatenspeicherungbeibiometrischenve.pdf (zuletzt besucht am 20.04.2021), zit.: EDÖB, Datenspeicherung.
- Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz für die Privatwirtschaft, 2013, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/ueberwachung-am-arbeitsplatz/internet--und-e-mail-ueberwachung.html (zuletzt besucht am 20.04.2021), zit: EDÖB, Leitfaden Privatwirtschaft.
- Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz für die Bundesverwaltung, 2013, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/ueberwachung-am-arbeitsplatz/internet--und-e-mail-ueberwachung.html (zuletzt besucht am 20.04.2021), zit: EDÖB, Leitfaden Bundesverwaltung.
- 17. Tätigkeitsbericht 2009/2010, 2010, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/17--taetigkeitsbericht-2009-2010.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Tätigkeitsbericht 2009/10.
- Leitfaden zu biometrischen Erkennungssystemen, 2009, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/dokumentation/leitfaeden/leitfaden-zu-biometrischen-erkennungssystemen.html (zuletzt besucht am 20.04.2021), zit: EDÖB, Leitfaden Biometrie.
- Erläuterungen zu sozialen Netzwerken, in: EDÖB, 16. Tätigkeitsbericht 2008/2009, Anhang 4.1.1., S.113-119, abrufbar unter https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2009/06/16_taetigkeitsbericht20082009.pdf.download.pdf/16_taetigkeitsbericht20082009.pdf (zuletzt besucht am 20.04.2021), zit.: EDÖB, Erläuterungen Soziale Netzwerke.
- 13. Tätigkeitsbericht 2005/2006, 2006, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/13--taetigkeitsbericht-2005-2006.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Tätigkeitsbericht 2005/6.
- 11. Tätigkeitsbericht 2003/2004, 2004, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/11--taetigkeitsbericht-2003-2004.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Tätigkeitsbericht 2003/4.
- Die E-Mail- und Internetüberwachung am Arbeitsplatz, 2001, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/8--taetigkeitsbericht-2000-2001/die-e-mail--und-internetueberwachung-am-arbeitsplatz.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, E-Mail- und Internetüberwachung.

- 7. Tätigkeitsbericht 1999/2000, 2000, abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/7--taetigkeitsbericht-1999-2000.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Tätigkeitsbericht 1999/2000.
- Bring Your Own Device (BYOD), abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/bring-your-own-device--byod-.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, BYOD.
- Sind Arbeitszeiterfassung und Zutrittskontrollen mit biometrischen Daten erlaubt? abrufbar unter: https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/privatsphaere-des-mitarbeiters/sind-arbeitszeiterfassung-und-zutrittskontrollen-mit-biometrisch.html (zuletzt besucht am 20.04.2021), zit.: EDÖB, Arbeitszeiterfassung.

EUROPÄISCHE KOMMISSION,

- Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending certain Union Legislative Acts, COM(2021) 206 final, 21.04.2021, zit. EK, AI Act.
- Weissbuch: Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, COM(2020) 65 final, 19.02.2020, zit. EK, Weissbuch 2020.
- Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rate, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz, COM(2019) 168 final, 08.04.2019, zit.: EK, KI 2019.
- Unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz (eingesetzt von der Europäischen Kommission im Juni 2018), Ethik-Leitlinien für eine Vertrauenswürdige KI, 2019, abrufbar unter: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60425 (zuletzt besucht am 20.04.2021), zit. EK, AI-HLEG, Ethik-Leitlinien.
- Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rate, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Koordinierter Plan für künstliche Intelligenz, COM(2018) 795 final, 07.12.2018, zit.: EK KI Plan 2018.
- Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rate, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, Künstliche Intelligenz für Europa, COM(2018) 237 final, 25.04.2018, zit: EK, KI Europa 2018.
- Artikel-29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, 17/DE WP 248 Rev. 01, 2017, zit: EK, Artikel-29-Datenschutzgruppe, Datenschutz-Folgenabschätzung.
- Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017 zur Datenverarbeitung am Arbeitsplatz, 17/DE WP 249, 2017, zit.: EK, Artikel-29-Datenschutzgruppe, Stellungnahme 2/2017.
- Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rate, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regio-

nen, über die Halbzeitüberprüfung der Strategie für einen digitalen Binnenmarkt: Ein vernetzter digitaler Binnenmarkt für alle, COM(2017) 228 final, 10.05.2017, zit.: EK, Digitaler Binnenmarkt.

- Advancing the Internet of Things in Europe, SWD(2016) 110 final, 19.04.2016, zit.: EK, IoT.

G20, Ministerial Statement on Trade and Digital Economy, 08./09.06.2019, abrufbar unter: http://trade.ec.europa.eu/doclib/docs/2019/june/tradoc_157920.pdf (zuletzt besucht am 20.04.2021).

MINSTERKOMITEE DES EUROPARATES,

- Ad Hoc Committee on Artificial Intelligence (CAHAI) – Feasibility Study, CAHAI(2020)23, 17.12.2020, zit.:, MINISTERKOMITTEE, CAHAI Feasibility Study.
- 1361st (Budget) meeting 19-21.11.2019, CM(2019)131-addfinal, 13.12.2019, zit.: MINISTERKOMITEE, CAHAI.
- The human rights impacts of algorithmic systems, Recommendation CM/Rec(2020)1, 08.04.2020, zit. Ministerkomitee, The Human Rights Impacts of Algorithmic Systems.
- The manipulative capabilities of algorithmic processes, Decl(13/02/2019)1, 13.02.2019, zit.: Ministerkomitee, The manipulative capabilities of algorithmic processes.
- The processing of personal data in the context of employment, Recommendation CM/Rec(2015)5, 01.04.2015, zit.: Ministerkomitee, The processing of personal data in the context of employment.
- Explanatory Memorandum to Recommendation CM/Rec(2015)5, CM(2015)32 addfinal, 01.04.2015, zit.: Ministerkomitee, Explanatory Memorandum to «The processing of personal data in the context of employment».
- The protection of personal data used for employment purposes, Recommendation R (89) 2, 18.01.1989, zit.: Ministerkomitee, The protection of personal data used for employment purposes.

INTERNATIONALE ARBEITSORGANISATION (ILO),

- Centenary Declaration for the Future of Work, adopted by the conference at its 108th session, Genf 2019, zit.: ILO, Centenary Declaration.
- Erklärung der IAO über grundlegende Prinzipien und Rechte bei der Arbeit und ihre Folgemaßnahmen vom 18.06.1998, abrufbar unter: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-berlin/documents/normativeinstrument/wcms_193727.pdf (zuletzt besucht am 20.04.2021), zit.: ILO, Erklärung 1998.

INTERNATIONALE ARBEITSORGANISATION (ILO) UND EUROFUND, Working anytime, anywhere: The effects on the world of Work, Luxemburg, 2017.

INTERNATIONALE FERNMELDEUNION (ITU), The Internet of Things, ITU Internet Reports 2005- Executive Summary, 2005, abrufbar unter: https://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf (zuletzt besucht am 20.04.2021), zit. ITU, Internet of Things.

ORGANISATION FÜR WIRTSCHAFTLICHE ZUSAMMENARBEIT UND ENTWICKLUNG (OECD),

- Digitalisation and Responsible Business Conduct – Stocktaking of policies and initiatives, 2020, abrufbar unter: https://mneguidelines.oecd.org/Digitalisation-and-responsible-business-conduct.pdf (zuletzt besucht am 20.04.2021), zit.: OECD, Digitalisation and RBC.
- Artificial Intelligence in Society, 2019, abrufbar unter: https://doi.org/10.1787/eedfee77-en (zuletzt besucht am 20.04.2021), zit. OECD, AI in society.
- Artificial Intelligence & Responsible Business Conduct, 2019, abrufbar unter: https://mneguidelines.oecd.org/RBC-and-artificial-intelligence.pdf (zuletzt besucht am 20.04.2021), zit.: OECD, AI & RBC.
- Going Digital: Shaping Policies, Improving Lives, 2019, abrufbar unter: https://doi.org/10.1787/9789264312012-en (zuletzt besucht am 20.04.2021), zit. OECD, Going Digital.
- Recommendation of the Council on Artificial Intelligence, 2019, OECD/LEGAL/0449, zit: OECD, Recommendation AI.
- Algorithms and Collusion – Competition Policy in the Digital Age, 2017, abrufbar unter: http://www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm (zuletzt besucht am 20.04.2021), zit.: OECD, Algorithms and Collusion.
- New Forms of Work in the Digital Economy, 2016, abrufbar unter: https://www.oecd-ilibrary.org/docserver/5jlwnklt820x-en.pdf?expires=1601039266&id=id&accname=guest&checksum=12467D30E559DB8E24FEDFC092CBD35E (zuletzt besucht am 20.04.2021), zit.: OECD, New Forms of Work.
- Summary of the CDEP Technology Foresight Forum Economic and Social Implications of Artificial Intelligence, DSTI/CDEP(2016)17, 2017, abrufbar unter https://www.oecd.org/sti/ieconomy/DSTI-CDEP(2016)17-ENG.pdf (zuletzt besucht am 20.04.2021), zit.: OECD, Economic and Social Implications of AI.
- Working Party on Security and Privacy in the Digital Economy, OECD Workshop «Improving the Measurement of Digital Security Incidents and Risk Management» (Draft Summary of the Main Points), 2017, DSTI/CDEP/SPDE(2017)19, abrufbar unter: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CDEP/SPDE(2017)19&docLanguage=En (zuletzt besucht am 20.04.2021), zit: OECD, Digital Security and Risk Management.
- Working Party on Security and Privacy in the Digital Economy, Managing Digital Security and Privacy in the Digital Economy: Background report for Ministerial Panel 3.2., DSTI/ICCP/REG(2016)1/FINAL, 2016, abrufbar unter: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(2016)1/FINAL&docLanguage=En (zuletzt besucht am 20.04.2021), zit: OECD, Managing Digital Security and Privacy.
- Working Party on Security and Privacy in the Digital Economy, Summary of the OECD Privacy Expert Roundtable, Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking, DSTI/ICCP/REG(2014)3, 2014, abrufbar unter: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282014%293&doclanguage=en (zuletzt besucht am 20.04.2021), zit.: OECD, Protecting Privacy.

- Cloud Computing: The Concept, Impacts and the Role of Government Policy, OECD Digital Economy Papers, No. 240, 2014, abrufbar unter: http://dx.doi.org/10.1787/5jxzf4lcc7f5-en (zuletzt besucht am 20.04.2021), zit., OECD, Cloud-Computing.
- Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines, 2013, OECD Digital Economy Papers, N. 229, abrufbar unter: http://www.oecd-ilibrary.org/science-and-technology/privacy-expert-group-report-on-the-review-of-the-1980-oecd-privacy-guidelines_5k3xz5zmj2mx-en (zuletzt besucht am 20.04.2021), zit.: OECD, Privacy Expert Group Report 2013.
- The OECD Privacy Framework, 2013, abrufbar unter: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (besucht am 20.04.2021), zit.: OECD, Privacy Framework 2013.
- Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188, 2013, abrufbar unter: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (zuletzt besucht am 20.04.2021), zit.: OECD, Privacy-Guidelines 2013.
- Leitsätze für Multinationale Unternehmen, 2011, abrufbar unter: http://www.oecd.org/daf/internationalinvestment/guidelinesformultinationalenterprises/48808708.pdf (zuletzt besucht am 20.04.2021), zit.: OECD, Leitsätze 2011.
- Neufassung der Entscheidung des Rats in Bezug auf die OECD-Leitsätze für multinationale Unternehmen, in: Leitsätze für Multinationale Unternehmen, 2011, S. 77f., abrufbar unter: http://www.oecd.org/daf/internationalinvestment/guidelinesformultinationalenterprises/48808708.pdf (zuletzt besucht am 20.04.2021), zit.: OECD, Ratsbeschluss 2011.
- Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188, 1980, abrufbar unter: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (besucht am 20.04.2021), zit.: OECD, Privacy-Guidelines 1980.
- Leitsätze für Multinationale Unternehmen, 1976, abrufbar unter: http://www.oecd.org/daf/inv/mne/50024800.pdf (zuletzt besucht am 20.04.2021), zit.: OECD, Leitsätze 1976.

PRIVATIM (KONFERENZ DER SCHWEIZERISCHEN DATENSCHUTZBEAUFTRAGTEN), Leitfaden zur datenschutzrechtlichen Beurteilung von biometrischen Verfahren, 2006, abrufbar unter: https://www.privatim.ch/wp-content/uploads/2017/06/privatim_Leitfaden_Biometrie_2006_d-1.pdf (zuletzt besucht am 20.04.2021).

STAATSSEKRETARIAT FÜR BILDUNG, FORSCHUNG UND INNOVATION (SBFI), Herausforderungen der künstlichen Intelligenz – Bericht der interdepartementalen Arbeitsgruppe «Künstliche Intelligenz», 13.12.2019, abrufbar unter: https://www.sbfi.admin.ch/dam/sbfi/de/dokumente/2019/12/bericht_idag_ki.pdf.download.pdf/bericht_idag_ki_d.pdf (zuletzt besucht am 20.04.2021), zit. SBFI, Herausforderungen der künstlichen Intelligenz.

STAATSSEKRETARIAT FÜR WIRTSCHAFT (SECO),

- Wegleitung zu den Verordnungen 3 und 4 zum Arbeitsgesetz (Gesundheitsschutz/Plangenehmigung), 2020, abrufbar unter: https://www.seco.admin.ch/seco/de/home/Publikatio-

nen_Dienstleistungen/Publikationen_und_Formulare/Arbeit/Arbeitsbedingungen/Wegleitungen_zum_Arbeitsgesetz/wegleitung-zu-den-verordnungen-3-und-4-zum-arbeitsgesetz.html (zuletzt besucht am 20.04.2021), zit. SECO, Wegleitung.

- , Die Entwicklung atypisch-prekärer Arbeitsverhältnisse in der Schweiz – Nachfolgestudie zu den Studien von 2003 und 2010, unter Berücksichtigung neuer Arbeitsformen, verfasst von Ecoplan (Mattmann Michael et al.), SECO Publikation Arbeitsmarktpolitik No 48 (11.2017), zit.: SECO, Atypische Arbeitsverhältnisse.

UNITED KINGDOM NATIONAL CONTACT POINT, Initial Assessment: Complaint from an NGO against 6 UK based Telecommunication companies, 11.07.2014, abrufbar unter: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/849290/bis-14-1156-uk-ncp-initial-assessment-complaint-from-an-ngo-against-6-uk-based-telecommunication-companies.pdf (zuletzt besucht am 20.04.2021), zit.: UK NCP.

VEREINTE NATIONEN (UNITED NATIONS, UN),

- Final Act of the International Conference on Human Rights, A/CONF.32/41, 22.04.1968 – 13.05.1968, Teheran, zit: UN, Final Act of the International Conference on Human Rights.

Generalversammlung (General Assembly, UNGA),

- The right to privacy in the digital age, Resolution adopted by the General Assembly on 18 December 2013, A/RES/68/167, 21.01.2014, zit.: UNGA, Right to privacy in the digital age 2014.
- Human rights and scientific and technological developments, A/RES/36/56, 25.11.1981, zit.: UNGA, Human Rights and Scientific and Technological Developments 1981.
- Human rights and scientific and technological developments, A/RES/2450(XXIII), 19.12.1968, zit.: UNGA, Human Rights and Scientific and Technological Developments 1968.
- Guidelines for the Regulation of Computerized Personal Data Files, adopted by the UNGA resolution 44/95 (14 December 1990), UN Doc E/CN.4/1990/72, zit.: UNGA, Guidelines for the Regulation of Computerized Personal Data Files 1990.

Menschenrechtsausschuss (Human Rights Committee, MRA),

- General Comment No. 31, The nature of the general legal obligation imposed on States Parties to the Covenant, 26 May 2004, CCPR/C/21/Rev.1/Add.13, zit.: MRA, General Comment No. 31.
- General Comment No. 16, Article 17 (Right to privacy), 28.09.1988, zit.: MRA, General Comment No. 16.

Menschenrechtsrat (Human Rights Council, HRC)

- Report of the Special Rapporteur on the right to privacy (advance unedited version), Joseph A. Cannataci, A/HRC/43/52, 12.02.2020, zit.: HRC, Special Rapporteur Right to Privacy 2020.
- Report of the Special Rapporteur on the right to privacy (advance unedited version), Joseph A. Cannataci, A/HRC/40/63, 27.02.2019, zit.: HRC, Special Rapporteur Right to Privacy 2019.

- Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/HRC/37/62, 25.10.2018, zit.: HRC, Special Rapporteur Right to Privacy 2018.
- Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/HRC/34/60, 06.09.2017, zit.: HRC, Special Rapporteur Right to Privacy 2017.
- -Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, A/HRC/31/64, 24.11.2016, zit.: HRC, Special Rapporteur Right to Privacy 2016.
- Resolution 28/16 adopted by the Human Rights Council, The Right to Privacy in the digital age, A/HRC/RES/28/16, 24.03.2015, zit.: HRC, Right to privacy in the digital age 2015.
- The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, 30.06.2014, zit.: HRC, Right to privacy in the digital age 2014.
- Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework, Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, A/HRC/17/31, 21.03.2011, zit.: HRC, UN-Leitprinzipien zu Wirtschaft und Menschenrechten.

Wirtschafts- und Sozialrat (ECONOMIC AND SOCIAL COUNCIL, ECOSOC),

- General Comment No. 24 on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, 10.08.2017, E/C.12/GC/24, zit.: ECOSOC, General Comment No. 24.
- General Comment No. 23, The right to just and favourable conditions of work (article 7 ICESCR), 07.04.2016, E/C.12/GC/23, zit.: ECOSOC, General Comment No. 23.
- Note by the Secretary-General on Human Rights and Scientific and Technological developments, E/CN.4/1233, 16.12.1976, zit.: ECOSOC, Human Rights and Scientific and Technological Developments 1976.
- Report of the Secretary-General on Human Rights and Scientific and Technological Developments, E/CN.4/1208, 26.02.1970, zit.: ECOSOC, Human Rights and Scientific and Technological Developments 1970.

Entscheidverzeichnis

ARBEITSGERICHT ZÜRICH

Urteil vom 10.12.2003, wiedergegeben in: JAR 2004, S. 606.

CHAMBRE D'APPEL DES PRUD'HOMMES DU CANTON DE GENÈVE

Urteil vom 08.06.1993, wiedergegeben in: JAR 1994, S. 158.

COUR D'APPEL CIVILE DU CANTON DE VAUD

Urteil vom 23.04.2020 (veröffentlicht am 11.09.2020), HC/220/535

COURT OF APPEAL OF ENGLAND AND WALES

Balfour v. Balfour [1919] 2KB 571.

EUROPÄISCHER GERICHTSHOF FÜR MENSCHENRECHTE (EGMR)

López Ribalda and Others v. Spain, 1874/13 and 8567/13 (2019)

Bărbulescu v. Romania, 61496/08 (2017)

Fernández Martínez v. Spain, 56030/07 (2014)

Uzun v. Germany, 35623/05 (2010)

Taliadorou and Stylianou v. Cyprus, 39627/05 and 39631/05 (2008)

Copland v. The United Kingdom, 62617/00 (2007)

Sidabras and Džiautas v. Lithuania, 55480/00 and 59330/00 (2004)

Rotaru v. Romania, 28341/95 (2000)

Amman v. Switzerland, 27798/95 (2000)

Halford v. The United Kingdom, 20605/92 (1997)

Niemietz v. Germany, 13710/88 (1992)

GERICHTSHOF DER EUROPÄISCHEN UNION (EUGH)

C-311/18, Data Protection Commissioner gegen Facebook Ireland Ltd und Maximillian Schrems, Urteil vom 16.07.2020.

C-507/17, Google LLC, Rechtsnachfolgerin der Google Inc. Gegen Commission nationale de l'informatique et des libertés (CNIL), Urteil vom 24.09.2019.

C-136/17, GC, AF, BH, ED gegen Commission nationale de l'informatique et des libertés (CNIL), Urteil vom 24.09.2019.

In den verbundenen Rechtssachen C-203/15 und C-698/15, Tele2 Sverige AB u.a., Urteil vom 21.12.2016.

C-362/14, Schrems gegen Data Protection Commissioner, Urteil vom 06.10.2015.

C-131/12, Google Spain SL, Google Inc. gegen Agencia Española de Protección de Datos, Urteil vom 13.05.2014.

In den verbundenen Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland Ltd und Seitlinger u.a., Urteil vom 08.04.2014.

C-473/12, Institut professionnel des agents immobiliers (IPI) gegen Geoffrey Englebert et. al., Urteil vom 07.11.2013.

In den verbundenen Rechtssachen C-92/09 und C-93/09, Volker und Markus Schecke und Hartmut Eifert gegen Land Hessen, Urteil vom 09.11.2010.

C-450/06, Varec SA gegen Belgischer Staat, Urteil vom 14.02.2008.

In den verbundenen Rechtssachen C-465/00, C-138/01 und C/139/01, Rechnungshof und Christa Neukomm und Joseph Lauermann gegen Österreichischer Rundfunk u.a., Urteil vom 20.05.2003.

OBERGERICHT ZÜRICH

Urteil vom 27.03.2015, LA150002-O/U.doc

SCHWEIZERISCHES BUNDESGERICHT

BGer 4A-533/2018 vom 23.04.2019

BGer 8C_79/2016 vom 30.06.2017

BGE 139 II 7

BGer 6B_536/2009 vom 12.11.2009.

BGE 133 I 58

BGE 130 II 425

BGE 128 II 259

BGE 122 V 267

BGE 122 I 360

BGE 122 I 153

BGE 118 Ia 64

BGE 113 Ia 257

BGE 103 Ia 293

BGE 97 I 45

BGE 89 I 92

Normtexte

EUROPARAT

- Protokoll zur Änderung des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 10.10.2018, SEV Nr. 223 (noch nicht in Kraft getreten – Änderungsprotokoll).
- Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 08.11.2001, SR 0.235.11 (Zusatzprotokoll).
- Verordnung zum Bundesgesetz über den Datenschutz vom 14.06.1993, SR 235.11 (VDSG)
- Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.01.1981, SR 0.235.1 (Datenschutzkonvention)

- (revidierte) Europäische Sozialcharta vom 03.05.1996, SEV Nr. 163 (ESC).
- Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 04.11.1950, SR 0.101.

EUROPÄISCHE UNION

- 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), ABl L 119 vom 04.05.2016, S. 1-88 (EU-Datenschutz-Grundverordnung – DSGVO).
- Vertrag über die Arbeitsweise der Europäischen Union (Konsolidierte Fassung), ABl C 326 vom 26.10.2012, S. 47-388 (AEUV).
- Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25.11.2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl L 337 vom 18.12.2009, S. 11-36.
- Erläuterungen zur Charta der Grundrechte, ABl. C 303 vom 14.12.2007, S. 17-35 (Erläuterungen zur GRC)
- Richtlinie 2003/88/EG des Europäischen Parlaments und des Rates vom 04.11.2003 über bestimmte Aspekte der Arbeitszeitgestaltung, ABl L 299 vom 18.11.2003, S. 9-18.
- 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), ABl L 201 vom 31.07.2002, S. 37-47.
- Charta der Grundrechte der Europäischen Union, 2000/C 364/01, ABl C 364 vom 18.12.2000, S. 1-22 (GRC).
- 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, ABl L 281 vom 23.11.1995, S. 31-50.
- Richtlinie 93/104/EG des Rates der Europäischen Union vom 23.11.1993 über bestimmte Aspekte der Arbeitszeitgestaltung, ABl L 307 vom 13.12.1993, S. 18-24 (Arbeitszeitrichtlinie).
- Gemeinschaftscharta der Sozialen Grundrechte der Arbeitnehmer vom 09.12.1989, Kom (89) 248 endg. (GCh).
- Richtlinie 89/391/EWG des Rates der Europäischen Gemeinschaften vom 12.06.1989 über die Durchführung von Maßnahmen zur Verbesserung der Sicherheit und des Gesundheitsschutzes der Arbeitnehmer bei der Arbeit, ABl L 183 vom 29.06.1989, S. 1-8 (Arbeitsschutz-Rahmenrichtlinie).

INTERNATIONALE ARBEITSORGANISATION (ILO)

- Übereinkommen Nr. 182 über das Verbot und unverzügliche Massnahmen zur Beseitigung der schlimmsten Formen der Kinderarbeit vom 17.06.1999, SR 0.822.728.2
- Übereinkommen Nr. 138 über das Mindestalter für die Zulassung zur Beschäftigung vom 26.06.1973, SR 0.822.723.8.
- Übereinkommen Nr. 111 über die Diskriminierung in Beschäftigung und Beruf vom 25.06.1958, SR 0.822.721.1.
- Übereinkommen Nr. 105 über die Abschaffung der Zwangsarbeit vom 25.06.1957, SR 0.822.720.5.
- Übereinkommen Nr. 100 über die Gleichheit des Entgelts männlicher und weiblicher Arbeitskräfte für gleichwertige Arbeit vom am 29.06.1951, SR 0.822.720.0.
- Übereinkommen Nr. 98 über die Anwendung der Grundsätze des Vereinigungsrechtes und des Rechtes zu Kollektivverhandlungen vom 01.07.1949, SR 0.822.719.9.
- Übereinkommen Nr. 87 über die Vereinigungsfreiheit und den Schutz des Vereinigungsrechtes vom 09.07.1948, SR 0.822.719.7.
- Übereinkommen Nr. 29 über Zwangs- oder Pflichtarbeit vom 28.06.1930, SR 0.822.713.9.

OECD, Übereinkommen über die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung vom 14.12.1960, SR 0.970.4 (OECD-Konvention)

SCHWEIZ

- Bundesgesetz über den Datenschutz vom 25.09.2020, BBl 2020, S. 7639ff
- Verordnung über Massnahmen in der besonderen Lage zur Bekämpfung der Covid-19-Epidemie vom 19. Juni 2020 (Stand 19.04.2021), SR 818.101.26 (Covid-19-Verordnung besondere Lage)
- Verordnung 3 über Massnahmen zur Bekämpfung des Coronavirus (COVID-19) vom 19.06.2020 (Stand 15.04.2021), SR 818.101.24 (COVID-19-Verordnung 3)
- Verordnung 1 zum Arbeitsgesetz vom 10. Mai 2000, SR 822.111 (ArGV1)
- Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18.04.1999, SR 101 (BV)
- Bundesgesetz über die Gleichstellung von Frau und Mann vom 24.03.1995, SR 151.1 (GlG)
- Verordnung 3 zum Arbeitsgesetz (Gesundheitsschutz) vom 18.08.1993, SR 822.113 (ArGV3)
- Verordnung zum Bundesgesetz über den Datenschutz vom 14.06.1993, SR 235.11 (VDSG)
- Bundesgesetz über den Datenschutz vom 19.07.1992, SR 235.1 (DSG)
- Bundesgesetz über die Heimarbeit vom 20.03.1981, SR. 822.31 (HArG)
- Bundesgesetz über die Arbeit in Industrie, Gewerbe und Handel vom 13.03.1964, SR 822.11 (ArG)
- Schweizerisches Strafgesetzbuch vom 21.12.1937, SR 311 (StGB)

- Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30.03.1911, SR 220 (OR)
- Schweizerisches Zivilgesetzbuch vom 10.12.1907, SR 210 (ZGB)

VEREINTE NATIONEN

- Übereinkommen über die Rechte von Menschen mit Behinderungen vom 13.12.2006, SR 0.109 (BRK)
- Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte vom 16.12.1966, SR 0.103.1 (UNO-Pakt I)
- Internationaler Pakt über bürgerliche und politische Rechte vom 16.12.1966, SR 0.103.2 (UNO-Pakt II)
- Allgemeine Erklärung der Menschenrechte vom 10.12.1948 (AEMR)