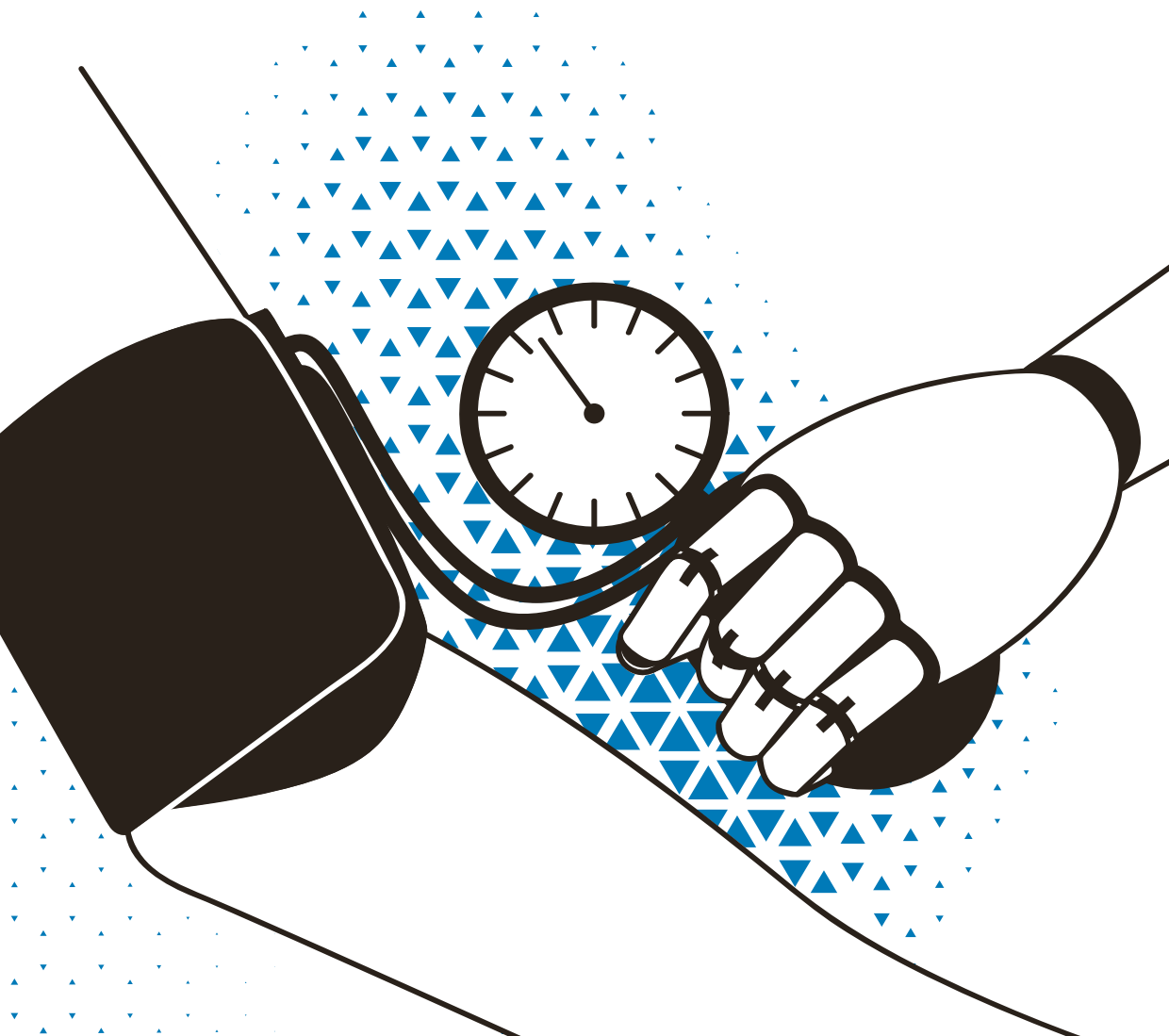
Grund- und Menschenrechte in einer digitalen Welt

Sabrina Ghielmini, Christine Kaufmann, Charlotte Post,
Tina Büchler, Mara Wehrli, Michèle Amacker



Grund- und Menschenrechte in einer digitalen Welt

Sabrina Ghielmini, Christine Kaufmann, Charlotte Post, Tina Büchler, Mara Wehrli und Michèle Amacker

Herausgeber: Schweizerisches Kompetenzzentrum für Menschenrechte (SKMR)
Projektleitung: Sabrina Ghielmini
Lektorat: Antonia Bertschinger
Umschlaggestaltung und Illustrationen: buch & netz, Carolina Flores (buchundnetz.com)
Verlag & Produktion: buch & netz (buchundnetz.com)

ISBN:
978-3-03805-361-3 (Print – Softcover)
978-3-03805-395-8 (PDF)
978-3-03805-396-5 (ePub)
978-3-03805-397-2 (mobi/Kindle)
Version: 1.00-20210414

Dieses Werk ist als buch & netz Online-Buch und als eBook in verschiedenen Formaten sowie als gedrucktes Buch verfügbar. Weitere Informationen finden Sie unter der URL:
https://buchundnetz.com/werke/grund-und-menschenrechte-in-einer-digitalen-welt/.

Die französische Ausgabe des Werks ist verfügbar unter: https://buchundnetz.com/werke/droits-fondamentaux-et-droits-humains-à-l'ère-numérique/.

Dieses Buch ist eine Publikation des Schweizerischen Kompetenzzentrums für Menschenrechte (SKMR).

Die Herausgabe dieses Buches wurde durch einen Beitrag der Hirschmann-Stiftung ermöglicht.
www.hirschmann-stiftung.ch

HIRSCHMANN STIFTUNG

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

Inhalt

Teil II
Fallbeispiele

Dank

Verschiedene Personen haben dieses Buch mit wertvollen fachlichen Anregungen unterstützt. Wir bedanken uns herzlich bei Sophie Achermann (alliance F), Dr. Kathrin Arioli (Staatsschreiberin des Kantons Zürich), Dr. Bruno Baeriswyl (ehem. Datenschutzbeauftragter des Kantons Zürich), Dr. Stefanie Becker (Alzheimer Schweiz), Prof. Dr. Abraham Bernstein (Digital Society Initiative, Universität Zürich), Prof. Dr. Corinna Bath (TU Braunschweig), Prof. Dr. Nadja Braun Binder (Universität Basel), Dr. Markus Christen (Digital Society Initiative, Universität Zürich), Guy Ehrler (Post AG), Dr. Alfred Früh (Universität Basel, ehem. Center for Information Technology, Society and Law, Universität Zürich), Giulia Reimann (Eidgenössische Kommission gegen Rassismus) und Prof. Dr. Marc Thommen (Open Science Delegierter, Universität Zürich). Weiter danken wir Prof. Dr. Rolf H. Weber (Center for Information Technology, Society and Law, Universität Zürich) für die kritische Durchsicht des Manuskripts.

Dr. Res Schuerch (SKMR) und Moritz Senn (Lehrstuhl für Öffentliches Recht, Völker- und Europarecht, Universität Zürich) danken wir für die Unterstützung bei der Recherche und Dr. Antonia Bertschinger (SKMR) für das Lektorat.

Ohne finanziellen Beitrag der Hirschmann-Stiftung wäre die Realisierung dieses Buches nicht möglich gewesen. Für die grosszügige Unterstützung und das Vertrauen in unsere Arbeit möchten wir uns ebenfalls herzlich bedanken.

Für das SKMR

Christine Kaufmann und Michèle Amacker

Vorwort

Neue Technologien sollten dazu dienen, das Leben der Menschen leichter zu machen, zu vereinfachen, und Nutzen stiften. Zumeist schaffen sie viele Chancen, aber sie bergen auch Risiken und Herausforderungen für eine Gesellschaft. Die digitalen Technologien durchdringen jede Facette unseres Lebens, ethische Fragestellungen nehmen zu etwa im Bereich der künstlichen Intelligenz oder beim Einsatz von Robotern. Datenspuren hinterlassen viele Informationen, und wir verlieren schnell die Kontrolle darüber. Auch ist es leichter geworden, via Social Media zu Kundgebungen aufzurufen, aber auch zu manipulieren, falsch zu informieren. Beispiele wie die Sperrung des Twitter-Accounts von Präsident Trump oder die Einschränkung des Internets in China oder Weissrussland zeigen Problematik und Handlungsbedarf in Bezug auf die Meinungsäusserungsfreiheit oder die Versammlungsfreiheit etc. auf.

Ich bin daher sehr froh über dieses Werk. Die digitale Welt ist an sich schon reichlich komplex aufgrund der technischen und rasanten Entwicklung. Sie im Kontext der Grund- und Menschenrechte zu analysieren und zu begleiten, ist umso wichtiger. Die digitalen Technologien können der Menschheit viel Nutzen stiften, aber wie bei jeder Technologie gibt es Schattenseiten, Risiken und Missbrauchsmöglichkeiten. Die Wissenschaft ist gefordert und gibt uns Orientierung, zeigt aber auch auf, wo der Rechtsrahmen ungenügend ist.

Das Buch gibt nicht nur eine gute Übersicht über die einzelnen Grundrechte und deren Problematik im digitalen Raum, sondern auch Hinweise an den Staat, wo Regulierung nötig ist. Regulierung ist nötig, damit Menschen auf Rechtsstaatlichkeit vertrauen können. Nur mit diesem rechtsstaatlichen Schutz und durchsetzbaren Rechten gelingt es, das Vertrauen der Menschen in die neuen Technologien zu stärken. Der Cyberspace ist ein wichtiges neues Rechtsgebiet, mit dem wir uns beschäftigen müssen.

Grundsätzlich gelten die universellen Menschenrechte sowohl im analogen wie im digitalen Raum. Viele Errungenschaften und deren Anwendung und Auslegung müssen daher nicht neu erfunden werden, sondern haben ihre Gültigkeit. Allerdings gibt es viele Auslegungsfragen und neue Anwendungs-

bereiche, und hier braucht es Prinzipien, Werte, die zu beachten sind, an denen sich Regierungen, der Privatsektor und die Zivilgesellschaft orientieren können. Das UN Panel on Digital Cooperation, dessen Mitglied ich bin, identifizierte neun menschliche Werte, die beachtet werden sollten: Inclusiveness, Respect, Human-Centeredness, Human Flourishing, Transparency, Collaboration, Accessibility, Sustainability und Harmony. Eine internationale Anerkennung dieser Prinzipien würde helfen bei der Entwicklung und Anwendung digitaler Technologien. Ein globales Bekenntnis zu digitaler Kooperation unter Anwendung der Werte und Prinzipien würde ein gemeinsames Verständnis fördern. Schliesslich sollte man dazu auch eine neue Gouvernanz, sprich Architektur, erarbeiten, weil eben auch die Zusammenarbeit, wie wir sie bislang kannten, nicht mehr stimmt im digitalen Raum. Solange wir keine klaren Normen und wenig Rechtsprechung haben, wird die Unsicherheit gross bleiben. Die grossen Tech-Unternehmen profitieren davon. Der einzelne Nutzer ist meist nicht in der Lage, Verletzungen seiner Persönlichkeitsrechte einzuklagen.

Das Engagement der Schweiz für die Menschenrechte ist in der Bundesverfassung (Art. 54 Abs. 2) und in ihrer Tradition fest verankert. Zahlreiche Institutionen des Völkerrechts haben ihren Sitz im internationalen Genf. Diese Ausgangslage sollte die Schweiz nutzen und sich aktiv einbringen, Vorbild sein. Die EU hat etwa mit der Datenschutzverordnung bereits einen Standard gesetzt, der internationale Beachtung findet. Die politische wie wissenschaftliche Schweiz tut gut daran, sich einzubringen, mitzugestalten und zu investieren in die offenen Fragestellungen. Das setzt ein stärkeres Bewusstsein für die Bedeutung der Grund- und Menschenrechte in unserem digitalen Alltag voraus. Dazu will dieses Buch beitragen.

Doris Leuthard, alt Bundesrätin

Einleitung

Die fortschreitende digitale Transformation konfrontiert unsere Gesellschaft mit tiefgreifenden Veränderungen. Robotik, künstliche Intelligenz, Big Data und Internet of Things sind nur einige Stichworte, die für den digitalen Wandel stehen.

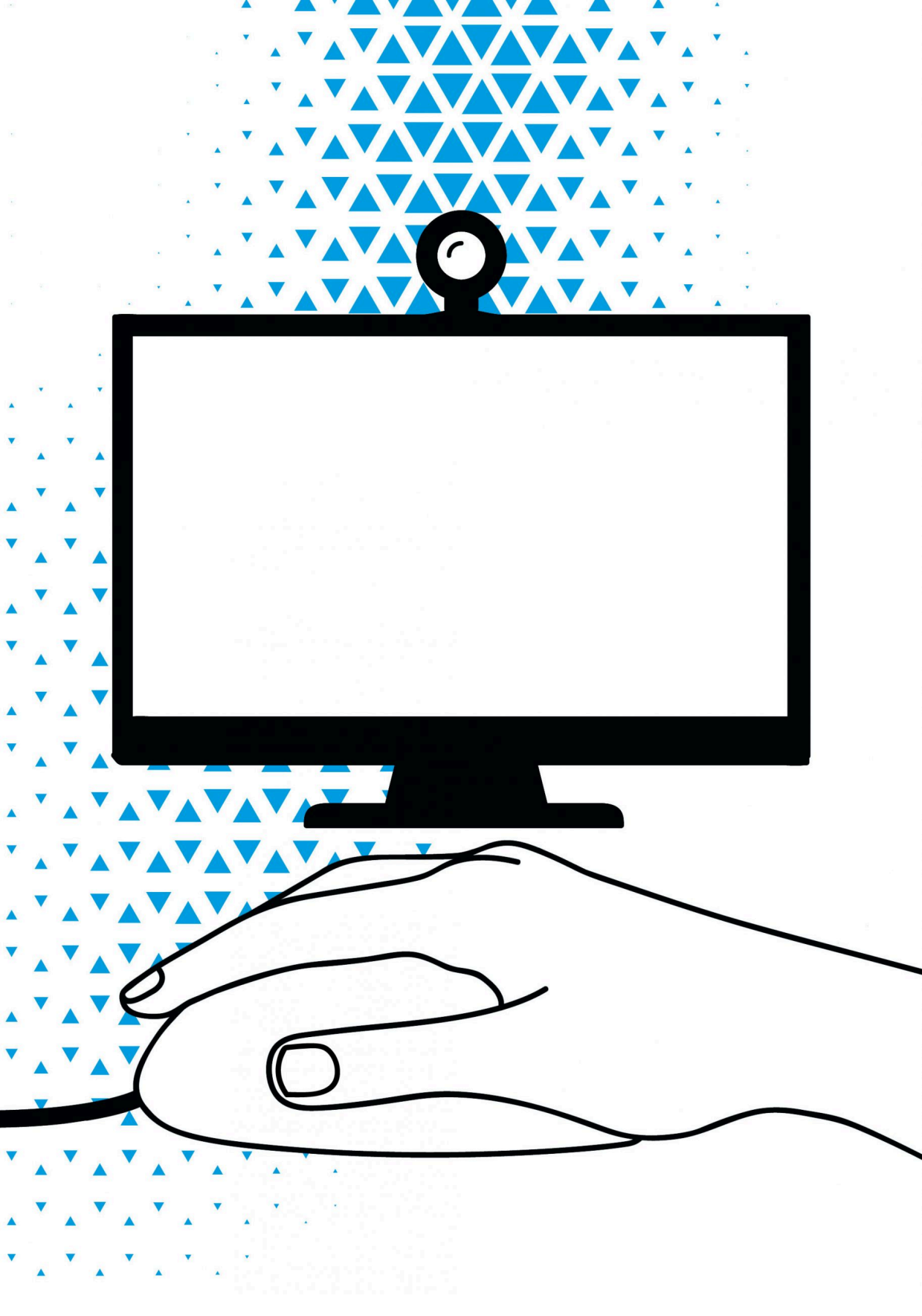
Die Digitalisierung hat ein grosses Potenzial, Grund- und Menschenrechte in ganz unterschiedlichen Lebensbereichen zu stärken. So eröffnet das Internet den Zugang zu einer globalen Informations- und Kommunikationsinfrastruktur, Roboter können in der Pflege eingesetzt werden, und «intelligente» Arbeitsbekleidung vermag Arbeitnehmende zu schützen. Gleichzeitig besteht die Gefahr, dass digitale Technologien zu neuen oder verschärften Formen von Grund- und Menschenrechtsverletzungen führen. Das Sammeln von Daten über einzelne Personen oder die Überwachung mithilfe digitaler Technologien werfen beispielsweise Fragen im Zusammenhang mit dem Recht auf Privatsphäre und mit der Bewegungsfreiheit auf.

Das vorliegende Buch richtet sich an ein breites Publikum ohne technisches oder juristisches Fachwissen. Es gibt einen Überblick, wie sich digitale Technologien im Alltag auf die Grund- und Menschenrechte auswirken. Anhand konkreter Fallbeispiele zeigt es auf, in welchen Lebensbereichen Grund- und Menschenrechte durch digitale Technologien tangiert werden, wie dies aus rechtlicher Sicht zu bewerten ist und welche Handlungsoptionen sich daraus ergeben.

Das Buch besteht aus zwei Teilen. Im ersten Teil werden wichtige Technologien und Anwendungen sowie die relevanten rechtlichen Grundlagen erläutert. Der zweite Teil besteht aus Fallbeispielen aus unterschiedlichen Lebensbereichen. Angesichts der unzähligen Einsatzbereiche von digitalen Technologien wird hier nur eine Auswahl besprochen, welche nicht alle betroffenen Lebensbereiche und juristischen Fragestellungen abbilden kann. Die Fallbeispiele sind im Interesse der Verständlichkeit vereinfacht. Sie eignen sich daher nicht als Rechtsratgeber. Vielmehr sollen sie als Orientierungshilfe für die Frage dienen, welche Grund- und Menschenrechte bei der

Entwicklung und Anwendung von digitalen Technologien betroffen sind, und einen Beitrag zur Diskussion leisten, wie Grund- und Menschenrechte und Digitalisierung miteinander vereinbar sind.

Der Aufbau des vorliegenden Buches folgt in weiten Teilen den Publikationen «Grund- und Menschenrechte in der Sozialhilfe – Ein Leitfaden für die Praxis» und «Grund- und Menschenrechte von Menschen mit Behinderungen – Ein Leitfaden für die Praxis der sozialen Arbeit», welche gemeinsam von der Hochschule Luzern und dem SKMR herausgegeben wurden, sowie der SKMR–Publikation «Grundrechte im Alter – Ein Handbuch». Wir möchten deshalb den Autorinnen dieser drei Publikationen, Gülcan Akkaya, Eva Maria Belser, Andrea Egbuna-Joss, Sandra Egli, Sabrina Ghielmini, Jasmin Jung-Blattmann und Christine Kaufmann, für die dort geleistete konzeptionelle Vorarbeit danken.



Teil I

Grundlagen

1 Digitale Technologien und Anwendungen

Der gesellschaftliche Wandel, den wir seit den 1990er-Jahren erleben, wird oft als «industrielle Revolution 4.0» bezeichnet. Digitale Technologien und digitale Infrastrukturen kennzeichnen diese Revolution 4.0. «Digitalisierung» meint in diesem Zusammenhang den kulturellen, sozialen und politischen Wandel, den der Einsatz neuer digitaler Technologien mit sich bringt. Sie zeichnet sich vor allem durch eine immer weiter fortschreitende Automatisierung verschiedenster Lebensbereiche aus, von der Produktion bis hin zum Umgang mit Informationen, sowie durch die Vernetzung von virtueller und physischer Welt.

Das nachfolgende Kapitel erläutert die digitalen Technologien, die einen besonders relevanten Einfluss auf die Grund- und Menschenrechte haben. Verdeutlicht werden die Technologien anhand verschiedener Anwendungsbeispiele.

1.1 Daten, Metadaten und Big Data

Daten als gespeicherte Informationen gab es schon vor der Digitalisierung. Neu ist, dass sie dank digitaler Technologien auf verschiedenen Medien gespeichert werden können. Unter «Daten» versteht man heute einerseits die auf einem Gerät gespeicherten Informationen, die durch Beobachtungen oder Messungen erfasst wurden und verändert, verarbeitet oder verschlüsselt werden können.[1] Andererseits erfasst der Begriff auch sogenannte Metadaten, das heisst Informationen über die Merkmale anderer Daten wie beispielsweise das Erscheinungsdatum eines Textdokuments oder das Datum der letzten Änderung. Als Randdaten bezeichnet man solche Metadaten, die Auskunft über Kommunikation im Internet geben, beispielsweise wann und an wen eine E-Mail verschickt wurde.[2]

1 Hattenhauer, Computerlexikon, 2019, S. 98 f.; Weber/Laux/Oertly, Datenpolitik, 2016, S. 10 f.

2 EDÖB, Leitfaden Internet- und E-Mailüberwachung am Arbeitsplatz (Privatwirtschaft), 2013, S. 4.

Ein Begriff, der besonders oft im Zusammenhang mit der Digitalisierung genannt wird, ist Big Data. Dabei handelt es sich um riesige, unstrukturierte oder nur beschränkt strukturierte Datenmengen. Dank neuer technologischer Entwicklungen ist es inzwischen möglich, solche Datenmengen wesentlich schneller und effizienter zu analysieren als noch vor einigen Jahren.[3]

Big Data zeichnet sich insbesondere durch vier Merkmale aus: Zunächst handelt es sich um eine grosse Menge an Daten. Diese wird beispielsweise dadurch erreicht, dass Unternehmen ihren Kundinnen und Kunden Apps kostenlos, aber nur im Tausch gegen Zugriffsrechte auf ihre Daten, zur Verfügung stellen. Zweitens handelt es sich bei Big Data um sehr vielfältige Daten, drittens sind diese Daten korrekt, und viertens werden sie mit sehr hoher Geschwindigkeit analysiert. Big Data profitiert vor allem vom Internet of Things (→ **Grundlagen Kapitel 1.5**) als Datenquelle und von Cloud Computing (→ **Grundlagen Kapitel 1.6**) als Werkzeug zur Datenverarbeitung.[4]

Anwendungsbeispiele:

Medizinische Forschung und Diagnostik: Angaben über den Gesundheitszustand von Patientinnen und Patienten werden als Daten in der Medizin verwendet, um eine bestmögliche Versorgung zu gewährleisten. Hierbei spielt vor allem die biomedizinische Informatik eine grosse Rolle: Die zuvor gesammelten Informationen werden mithilfe von Algorithmen (→ **Grundlagen Kapitel 1.2**) ausgewertet, um festzustellen, welche Therapieansätze bei verschiedenen Krankheiten am vielversprechendsten sind oder welche Merkmale im Erbgut ein erhöhtes Risiko für den Ausbruch bestimmter Krankheiten darstellen.[5] Im Bereich der Diagnostik durchsucht Software eine grosse Menge von Daten nach verschiedensten Merkmalen. Treten diese in einer ganz bestimmten Kombination auf, wird die Software gestützt auf die entsprechenden Algorithmen eine passende Diagnose vorschlagen. Als Grundlage dienen beispielsweise Aufzeichnungen von medizinischen Geräten oder Laborbefunde, die einer bestimmten Diagnose (bzw. Krankheit) zugeordnet werden können (→ **Fallbeispiel KI und Big Data in der Diagnostik 2.2**).[6]

3 Weber/Thouvenin, Big Data und Datenschutz, 2014, S. 1.

4 Hattenhauer, Computerlexikon, 2019, S. 101.

5 Jiang/Jiang/Zhi et al., Artificial intelligence in healthcare, 2017, S. 230 f.

6 Jiang/Jiang/Zhi et al., Artificial intelligence in healthcare, 2017, S. 230; weiterführende Hinweise, auch zum Recht auf Datenschutz: Wirth/Johns/Meurers et al., Anonymisierung medizinischer Daten, 2020, S. 74.

Microtargeting: Diese Methode kommt im Marketing und in politischen Wahl- oder Abstimmungskampagnen zum Einsatz. Die Auswertung grosser Mengen an Daten ermöglicht es, einzelne Zielpersonen gezielt anzusprechen. Zu diesem Zweck werden Zielgruppen definiert und dazugehörige Persönlichkeitsprofile erstellt. So lassen beispielsweise Parteien die über persönliche Kontakte oder Websites gesammelten Daten mit den Daten auf Social-Media-Plattformen vergleichen und ggf. verknüpfen (Social Match). Auf diese Weise können sie politische Botschaften auf bestimmte Zielgruppen zuschneiden und beispielsweise gezielt mit bestimmten Aussagen in den sozialen Medien für politische Vorlagen werben (→ **Fallbeispiel Microtargeting im Abstimmungskampf 3.4**).[7]

1.2 Algorithmen

Algorithmen sind Verfahren zur Lösung eines Problems nach vordefinierten Einzelschritten. Werden gleiche Ausgangsdaten in derselben Reihenfolge eingegeben, führt der Algorithmus immer dieselben vorher definierten Einzelschritte aus, sodass die Ergebnisse immer gleich sind; bei Eingabe unterschiedlicher Ausgangsdaten unterscheiden sich die Ergebnisse.[8] Algorithmen tragen auf diese Weise dazu bei, dass verschiedenste Datensätze nach einem zuvor festgelegten Merkmal durchsucht werden können oder dass bei gleichen Eingaben in eine Suchmaschine dieselben Ergebnisse vorgeschlagen werden.[9]

Anwendungsbeispiele:

Filterblasen: Unter einer Filterblase versteht man das Phänomen, dass Internetnutzenden häufig nur Werbung oder Informationen angezeigt werden, die ihre Interessen und Meinungen unterstützen. So lassen sich beispielsweise Menschen, die konservative politische Ansichten vertreten, eher mit Beiträgen von konservativen Parteien oder Zeitungen konfrontieren. Dies führt dazu, dass sich Menschen im Internet immer weniger mit gegensätzlichen Meinungen auseinandersetzen müssen. Filterblasen entstehen, weil die Betreibenden von Suchmaschinen Algorithmen nutzen, die auch frühere (Such-)Aktivitäten der jeweiligen Nutzenden mitberücksichtigen, weil die Betreibenden davon ausgehen, dass Nutzerinnen und Nutzer Beiträge präferieren, die ihre Ansichten unterstützen.[10]

7 EDÖB/Privatim, Datenschutzrecht Wahlen und Abstimmungen, 2019, S. 6 f.
8 Hattenhauer, Computerlexikon, 2019, S. 17.
9 Bitkom e.V./DKFI, Künstliche Intelligenz, 2017, S. 67 f. und 71 f.
10 Bezemek, Filter Bubble and Human Rights, 2020, S. 34 ff.

Risikoberechnung: Versicherungen und Banken können beim Entscheid über den Abschluss einer Versicherung bzw. die Vergabe eines Kredits auf Algorithmen zurückgreifen. Diese sind darauf trainiert, bestimmte Merkmale der Kundinnen und Kunden bestimmten Konditionen zuzuordnen, nach denen die Versicherung bzw. ein Kredit gewährt werden soll.[11]

Automatische Fahrzeugfahndung: Hierbei handelt es sich um eine Technologie, die in der Schweiz mit dem Programm «Automatische Fahrzeugfahndung und Verkehrsüberwachung» (AFV) eingesetzt wird. Ein mobiles Scan-Gerät erfasst Nummernschilder und gleicht diese mit registrierten Nummernschildern in der Fahndungsdatenbank ab. Gibt es eine Übereinstimmung, kann die Polizei das betroffene Fahrzeug zur Kontrolle anhalten.[12]

1.3 Maschinelles Lernen

Maschinelles Lernen bedeutet, dass ein Algorithmus so programmiert wird, dass er aus Daten gewisse Muster erkennen und entsprechend der ihm vorgegebenen Parameter «reagieren» kann. Zu diesem Zweck wird ein System mit Daten gefüttert, bei denen ein oder mehrere Merkmale übereinstimmen. Bei diesen Daten handelt es sich um einen sogenannten Trainingssatz.[13] Erkennt der Algorithmus das Merkmal bei einer anderen, fremden Datei wieder, ordnet er diese automatisch der Gruppe der vorher ausgewerteten Daten zu.[14] Er kann folglich in neuen Situationen auf Grundlage des Trainingssatzes Vorhersagen treffen.[15]

Zum maschinellen Lernen gehört auch das komplexere «Deep Learning». Hierbei wird mit Hilfe sogenannter neuronaler Netzwerke versucht, die Grundstrukturen des menschlichen Gehirns nachzubilden. Diese künstlichen Neuronen sind selbstständig dazu imstande, sich untereinander zu vernetzen und Informationen zu verarbeiten. Die Folge ist, dass die Arbeitsschritte des Systems für die Entwicklerinnen und Entwickler häufig nicht

11 Sprecher, Datenschutzrecht und Big Data, 2018, S. 519; Raso/Hilligoss/Krishnamurthy et al., Artificial Intelligence & Human Rights, 2018, S. 26 ff.

12 Urteil Bundesgericht 6B_908/2018, 7.10.2019, E. 2.1; SRF, Aargauer und Solothurner Polizei bleiben beim Autonummern-Scanner, 2019.

13 Bitkom e.V./DKFI, Künstliche Intelligenz, 2017, S. 27.

14 Hattenhauer, Computerlexikon, 2019, S. 220 f.

15 SBFI, Künstliche Intelligenz, 2019, S. 20.

mehr nachvollziehbar sind. Sie können also nicht mehr herausfinden, auf welchen Grundlagen der Algorithmus arbeitet. Dieses Phänomen wird auch als das Black-Box-Problem bezeichnet.[16]

Anwendungsbeispiele:

Fitness-Apps: Bei Fitness-Apps werden Informationen, die sich aus dem Verhalten der Nutzenden ableiten lassen, in eine Cloud (→ **Grundlagen Kapitel 1.6**) hochgeladen. Auf ihrer Grundlage (die in diesem Fall den Trainingssatz bildet) erstellt ein Algorithmus neue Vorschläge bezüglich der sportlichen Betätigung der jeweiligen Person.

Autonomes Fahren: Um ein Fahrprogramm auf selbstständiges Fahren im Strassenverkehr zu trainieren, wird ein Fahrzeug einige Zeit von einem Menschen betätigt, damit der Algorithmus dessen Verhaltensweise übernehmen kann.[17]

1.4 Künstliche Intelligenz

Künstliche Intelligenz (KI) liegt dann vor, wenn Systeme dazu fähig sind, ihre Umgebung zu analysieren und mit einem gewissen Grad an Autonomie zu handeln, um bestimmte Ziele zu erreichen. Die Systeme sollen also den menschlichen Geist «nachbilden». Dies ist sowohl bei softwaregestützten Systemen (zum Beispiel Sprachassistenten oder Suchmaschinen) als auch bei Hardware-Systemen (zum Beispiel Roboter oder moderne Autos) möglich.[18] Diese Definition von künstlicher Intelligenz ist jedoch sehr allgemein. Aus diesem Grund ist es hilfreich, sich drei zentrale «Fähigkeiten», die bei der überwiegenden Anzahl heutiger KI-Systeme vorhanden sind, vor Augen zu führen. Künstliche Intelligenz kann

- eine grosse Anzahl komplexer Daten in einer Art und Weise auswerten, die mit anderen Technologien bisher nicht möglich war;
- mithilfe dieser Daten Vorhersagen treffen, die dann als Grundlage für Entscheidungen dienen;
- auf Basis dieser Vorhersagen agieren.

16 Vallone, Wenn sich Algorithmen absprechen, 2018, S. 37 f. und 45.
17 Bitkom e.V./DKFI, Künstliche Intelligenz, 2017, S. 27.
18 Europäische Kommission, Künstliche Intelligenz für Europa, 2018, S. 1.

Im Zentrum steht somit unter anderem die Fähigkeit, Vorgänge zu verstehen und lernfähig zu sein.[19] Eine der wichtigsten Methoden ist hierbei das maschinelle Lernen (→ **Grundlagen Kapitel 1.3**).[20]

Anwendungsbeispiele:

Chatbots/Sprachassistenten: Diese Assistenten können in natürlicher Sprache mit dem Menschen kommunizieren und werden häufig dazu genutzt, auf einfachem Weg Fragen zu beantworten oder gewünschte Informationen zu liefern. Bei ihrer Tätigkeit spielt das maschinelle Lernen eine grosse Rolle: Mithilfe der hierdurch ausgebauten Fähigkeiten können Chatbots die an sie gerichtete Frage analysieren, die Absichten der Nutzenden aus dem Text herausfiltern und schliesslich selbstständig auf digitale Datenbanken zugreifen, um eine zufriedenstellende Antwort zu geben.[21] Manche Chatbots sind auch darauf programmiert, den Sprachgebrauch ihrer Nutzenden zu erlernen. Dies kann dazu führen, dass der Chatbot beginnt, diese zu beleidigen, wenn er zuvor mit Schimpfwörtern «gefüttert» wurde.[22]

Gesichtserkennung mithilfe intelligenter Software: Gesichtserkennung kann auf zwei Arten verwendet werden. Zum einen lässt sich mit ihr überprüfen, ob eine Person zu einer bestimmten Handlung berechtigt ist (zum Beispiel bei der Einreise in ein Land, beim Entsperren eines Smartphones oder beim Betreten eines Gebäudes). Zum andern ermöglicht die Software die Identifikation von vorerst unbekannten Personen. Mit ihrer Hilfe können beispielsweise einer Straftat verdächtigte Personen gefunden werden. Hierfür wird das Bild einer unbekannten Person erfasst und mit einer Datenbank abgeglichen, in der Bilder von Personen und deren Identität abgespeichert sind. Für die Gesichtserkennung braucht es deshalb einerseits eine Software, die Gesichter erfassen und analysieren kann, und andererseits eine Datenbank, mit der die neu erfassten Bilder abgeglichen werden können (→ **Fallbeispiel Staatliche Videoüberwachung mit Gesichtserkennung im öffentlichen Raum 3.5** und → **Fallbeispiel Digitalisierter Laden 6.1**).

19 SBFI, Künstliche Intelligenz, 2019, S. 7 f.

20 Bitkom e.V./DKFI, Künstliche Intelligenz, 2017, S. 32.

21 Bitkom e.V./DKFI, Künstliche Intelligenz, 2017, S. 44 f.

22 Zeit Online, Twitter-Nutzer machen Chatbot zur Rassistin, 2016.

1.5 Internet of Things (Internet der Dinge)

Das Internet of Things (IoT) beschreibt die zunehmende Vernetzung von Gegenständen aller Art über das Internet durch den Einbau von Chips und die Vergabe von digitalen Kennungen. Diese Gegenstände sind beispielsweise Fahrzeuge, Haushaltsgeräte oder Werkzeuge.[23] Durch die Vernetzung ist es möglich, Daten von diesen Objekten zu sammeln und an andere Objekte weiterzugeben.[24] Die Gegenstände können also selbstständig miteinander kommunizieren und verschiedene Aufgaben erledigen, ohne dass die Besitzerin oder der Besitzer irgendeine Handlung vornehmen muss.

Anwendungsbeispiele:

Smart Homes: Als ein Smart Home bezeichnet man Wohnraum, in dem Haustechnik und Haushaltsgeräte miteinander und/oder mit dem Internet vernetzt sind. Dies wird oftmals durch den Einbau von Sensoren oder Motoren erreicht, die mithilfe einer App oder eines Sprachassistenten gesteuert werden können. Auf diesem Weg lassen sich per «Knopfdruck» oder durch eine gesprochene Anweisung zum Beispiel die Beleuchtung, das Alarmsystem oder der Fernseher an- und ausschalten. Zudem können intelligente Kühlschränke registrieren, wann Lebensmittel entnommen werden, und diese selbstständig auf eine Einkaufsliste setzen.[25]

Wearables: Wearables sind Geräte, die während der Nutzung am Körper getragen werden oder in die Kleidung integriert sind. Sie können beispielsweise Informationen zur Häufigkeit und Art der täglichen Bewegung, zur Herzfrequenz oder zum Schlafverhalten erheben und auswerten (→ **Fallbeispiel Überwachung am Arbeitsplatz 1.3** und → **Fallbeispiel Fitnesstracker einer Krankenkasse 2.3**).[26]

1.6 Cloud Computing

Unter dem Begriff Cloud Computing versteht man die Möglichkeit, Daten von einem Computer auf einen weltweit zugänglichen, dezentralen Server

23 Bitkom e.V./DKFI, Künstliche Intelligenz, 2017, S. 28. Die Weiterentwicklung von Internet of Things ist Internet of Everything und Internet of Bodies.

24 OECD, Going Digital, 2019, S. 19.

25 Eggen, Home Smart Home, 2016, S. 1131 f.

26 Eggen/Stengel, Wearables, 2018, Rz. 4 ff.

auszulagern. Dies hat den Vorteil, dass diese Daten überall zur Verfügung stehen, unabhängig davon, wo man sich gerade aufhält.[27] Cloud Computing wird häufig dazu genutzt, verschiedenen Personen einen dezentralen Zugang zu Informations- und Kommunikationstechnologien zu ermöglichen.[28]

Anwendungsbeispiele:

Streamingdienste: Bei Streamingdiensten wie Netflix, Spotify oder Amazon Prime werden zahlreiche Dateien (oftmals Filme oder Songs) dezentral gespeichert und auf Wunsch auf einem Endgerät direkt wiedergegeben.[29]

Cloud-Speicherdienste: Speicherdienste wie Google Drive, Amazon Cloud oder Microsoft One Drive sollen die Projektarbeit in Gruppen vereinfachen. Sie bieten die Möglichkeit, Dateien dezentral auf einem Server (der sogenannten Cloud) abzulegen, sodass sie anderen Mitgliedern der Gruppe über das Internet zugänglich sind.[30] Zugleich besteht bei Cloudspeichern jedoch auch die Gefahr des Kontrollverlustes über die Daten sowie das Risiko der Verletzung von Datenschutz- und Geheimnisschutzregeln (zum Beispiel in besonderen Berufen wie Anwältinnen und Anwälte, im Gesundheitsbereich und in regulierten Sektoren wie den Finanzmärkten). So ist für die Kundinnen und Kunden oftmals nicht ersichtlich, wo genau sich der Server befindet, auf dem die Daten gespeichert werden, oder ob Subunternehmen involviert sind. Zudem werden die Daten vieler Menschen durch dasselbe System gespeichert und verarbeitet. Wird nun ein Nutzer Opfer eines Hackerangriffs, kann dies auch die Daten von Unbeteiligten in Mitleidenschaft ziehen, da das gesamte System betroffen ist.[31]

1.7 Robotik

Unter Robotik versteht man KI-Systeme, die oftmals in Form bewegungsfähiger Maschinen und Apparaturen auftreten. Einerseits übernehmen Roboter Arbeiten, die für Menschen gefährlich, anstrengend oder eintönig sind, und erledigen diese häufig auch präziser. Andererseits erhöht ihr Einsatz das Risiko eines Stellenabbaus in verschiedenen Branchen, da die Mitarbeitenden durch die Roboter ersetzt werden können.

27 Hattenhauer, Computerlexikon, 2019, S. 318.
28 OECD, Going Digital, 2019, S. 19 f.
29 Hattenhauer, Computerlexikon, 2019, S. 360.
30 Hattenhauer, Computerlexikon, 2019, S. 78 f.
31 EDÖB, Erläuterungen zu Cloud-Computing, o.D.

Anwendungsbeispiele:

Roboter am Fliessband: In Produktionsprozessen kommen Roboter besonders bei standardisierbaren Abläufen zum Einsatz. Sie werden so programmiert, dass sie die immer gleichen Arbeitsschritte in immer derselben Reihenfolge abarbeiten.[32]

Pflegeroboter: Es gibt drei Arten von Pflegerobotern: Serviceroboter können für die Pflegebedürftigen kleinere Hol- und Bringdienste erledigen. Assistenzroboter helfen dem Pflegepersonal beim Umlagern oder Aufrichten von Patientinnen und Patienten. Unterhaltungsroboter haben die Aufgabe, Menschen sowohl geistig als auch körperlich zu animieren. Hierfür sind sie mit Sensoren ausgestattet, die Bewegungen und Berührungen wahrnehmen, sodass sie auf das Verhalten der Pflegebedürftigen reagieren können (→ **Fallbeispiel Pflegeroboter 2.1**).[33]

1.8 Blockchain

Eine Blockchain ist eine Kette von Datenblöcken, die zusammen eine dezentral organisierte Datenstruktur bilden. Damit sollen Transaktionen sicher, verifizierbar und unabhängig voneinander durchgeführt werden können. Technisch wird dieses Ziel dadurch erreicht, dass erstens jede Transaktion elektronisch signiert werden muss und zweitens jede neue Transaktion am Ende der Datenkette als neuer Block angehängt wird. Dadurch entsteht eine Art elektronisches Register, in dem jede Transaktion in genauer chronologischer Reihenfolge gespeichert wird. Das Besondere an der Blockchain ist, dass diese Reihenfolge nicht geändert werden kann.[34] Der Vorteil besteht darin, dass sie dezentral verwaltet wird. Das heisst, die Datenbank wird nicht nur auf einem Server gespeichert. Zusätzlich existieren Kopien der jeweiligen Datenbank auf jedem an dem Netzwerk beteiligten Computer. Die Blockchain ist somit fälschungssicher, da für eine Manipulation nicht nur ein, sondern unzählig viele Rechner gehackt werden müssten. Durch eine Zugangssoftware wird einzelnen Personen der Zugriff zum Protokoll ermöglicht.[35] Neue Ereignisse oder Transaktionen werden automatisch gespeichert

32 Hattenhauer, Computerlexikon, 2019, S. 318 f.
33 Kreis, Pflegeroboter, 2018, S. 224 f.
34 Weber, Blockchain, 2017, Rz. 1.
35 Hattenhauer, Computerlexikon, 2019, S. 59 ff.

und können somit von allen Beteiligten nachvollzogen werden. Der Versuch, die Informationen zu ändern, führt zu einem Bruch der gespeicherten Informationen, welcher wiederum auf allen Servern einsehbar ist. Bekannte Anwendungsbeispiele für Blockchain sind virtuelle Währungen (zum Beispiel Bitcoin, Ether, Ripple) und Smart Contracts. Weniger bekannt, aber praktisch sehr wichtig ist der Einsatz von Blockchain, um in Lieferketten die Herkunft von Produkten zu verfolgen.[36]

Anwendungsbeispiel:

Überwachung von Lieferketten: Ein von Anfang bis Ende digitalisierter Lieferprozess kann dazu beitragen, die Informationen über Güter transparenter zu machen und sie besser zu verwalten. Ziel dieser Anwendung ist es, die Einhaltung sozialer und ökologischer Standards zu garantieren. Ein gutes Beispiel hierfür bietet das Markieren des Schwarzen Seehechts durch ein australisches Fischereiunternehmen: Unmittelbar nach dem Fang eines Fisches wird ihm ein Chip implantiert, der bei jeder einzelnen neuen Transaktion Informationen über den Verarbeitungsschritt speichert. Hierzu gehören beispielsweise der Ort des Fangs oder die für das Schiff Verantwortlichen. Die gespeicherten Informationen werden mithilfe der Blockchain-Technologie verschlüsselt und sind somit vor Manipulationen geschützt. Am Ende des Verarbeitungsprozesses werden die Daten in einen QR-Code übertragen. Dieser kann dann von den Konsumierenden, die sich über die Herkunft des Fisches informieren wollen, gescannt werden.[37]

36 OECD, Blockchain in responsible supply chains, 2019.

37 FAZ Online, Blockchain für den Schwarzen Seehecht, 2019.

2 Grund- und Menschenrechte

Grund- und Menschenrechte schützen die zentralen Aspekte des Lebens jeder einzelnen Person und sollen ein menschenwürdiges Dasein garantieren. Mit Grundrechten sind in der Regel die Garantien gemeint, die in der Bundesverfassung oder in den Kantonsverfassungen enthalten sind. Der Begriff Menschenrechte hingegen bezeichnet die Rechte, die auf internationaler Ebene, meist in internationalen Abkommen, geregelt sind.[38] Grund- und Menschenrechte stimmen in der Schweiz inhaltlich grösstenteils überein.

Nachfolgend werden zuerst die Herausforderungen skizziert, welche die Digitalisierung für die Grund- und Menschenrechte mit sich bringt (**Kapitel 2.1**). Anschliessend werden die wichtigsten juristischen Grundlagen erklärt (**Kapitel 2.2**). **Kapitel 2.3** erläutert schliesslich den Inhalt ausgewählter Grund- und Menschenrechte und zeigt deren Zusammenhang mit der Digitalisierung auf.

2.1 Herausforderungen der digitalen Welt für die Grund- und Menschenrechte

Die stetige Weiterentwicklung digitaler Technologien beeinflusst unser Zusammenleben enorm und bringt sowohl kulturelle und soziale als auch politische, wirtschaftliche und ökologische Veränderungen mit sich. Sie ermöglicht zum Beispiel die Nutzung riesiger Datenmengen oder künstlicher Intelligenz und hat somit Auswirkungen auf sämtliche Lebensbereiche.[39]

Die neuen Technologien können den Schutz von Grund- und Menschenrechten stärken. Beispielsweise können soziale Medien die Teilhabe am gesellschaftlichen Leben, den Zugang zu Informationen und die freie Meinungsäusserung fördern. Zudem erleichtern digitale Technologien die Teilhabe an Bildung und kulturellen Angeboten. Allerdings birgt die Digitalisierung auch Risiken für die Grund- und Menschenrechte: Sie ermöglicht Massenüberwachung, Zensur und ein fast unbegrenztes Sammeln von persönlichen Daten. Zudem kann die zunehmende Digitalisierung auch dazu führen, dass Men-

38 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 1 Rz. 26.
39 Deutscher Bundestag, Menschenrechte im digitalen Zeitalter, 2018, S. 5.

schen, die keinen Zugang zu den neuen Technologien haben, von entscheidenden Entwicklungen ausgeschlossen bleiben und die digitale Kluft grösser wird.[40]

Auf diese Risiken müssen insbesondere die Staaten reagieren. Sie sind verpflichtet, Grund- und Menschenrechte zu achten und vor Verletzungen zu schützen. Dies gilt auch im Bereich der Digitalisierung. Gerade deren rasante Entwicklung wirft immer wieder die Frage auf, wie einzelne Personen vor den negativen Auswirkungen neuer Technologien auf ihre Grund- und Menschenrechte geschützt werden können. Gleichzeitig besteht ein gesellschaftliches Interesse an einer möglichst effizienten Nutzung dieser Technologien.[41] Auch der Bundesrat hat erkannt, dass die Digitalisierung unser Zusammenleben nachhaltig verändert, und deshalb 2020 das Strategiepapier «Digitale Schweiz» verabschiedet. Dieses legt als Grundsatz fest, dass bei der digitalen Entwicklung der Mensch im Mittelpunkt stehen soll und der Schutz der Rechte jeder einzelnen Person gewährleistet sein muss.[42]

Grund- und Menschenrechte gelten in der analogen wie auch in der digitalen Welt. Die fortschreitende Digitalisierung bringt aber für deren Schutz besondere Herausforderungen mit sich:

Zum einen stammen die meisten Menschenrechtsverträge und nationalen Grundrechtskataloge aus einer Zeit vor der Digitalisierung. Sie sind daher von ihrem ursprünglichen Konzept her nicht auf menschenrechtliche Fragen im Zusammenhang mit digitalen Vorgängen ausgerichtet. So stellt sich durch die Etablierung sozialer Netzwerke beispielsweise die völlig neue Frage, ob ein Tweet in den Schutzbereich der Meinungsfreiheit fällt. Die grund- und menschenrechtlichen Schutzkonzepte müssen somit an den gesellschaftlichen Wandel angepasst und neu interpretiert werden, damit sie auch grund- und menschenrechtliche Probleme erfassen können, die sich aus der Digitalisierung ergeben.[43]

Eine weitere Schwierigkeit für den Grund- und Menschenrechtsschutz in der digitalen Welt ergibt sich aus den beteiligten Akteurinnen und Akteuren. Digitale Technologien werden überwiegend von Privaten entwickelt. Diese be-

40 UNO-Hochkommissariat für Menschenrechte, Human Rights in a New Era, 2018.
41 Weber, Digitalisierung, 2019, S. 4.
42 Bundesrat, Digitale Schweiz, 2020, S. 4 ff.
43 Weber, Digitalisierung, 2019, S. 5.

stimmen weitgehend darüber, was entwickelt wird und welche Regeln für die Nutzung der Dienstleistungen und Technologien gelten. Staatliche Regulierungen und Vorgaben fehlen oft. Auch haben die betreffenden Unternehmen oftmals grössere Fachkenntnisse als die zuständigen staatlichen Stellen. Der Privatsektor verfügt somit im digitalen Bereich über erheblichen Einfluss und oft einen Wissensvorsprung gegenüber dem Staat.[44]

Das Problem dabei ist, dass Unternehmen nicht direkt an die Grund- und Menschenrechte gebunden sind. Diese gelten vielmehr für den Staat sowie für Private, die staatliche Aufgaben wahrnehmen (Art. 35 Abs. 2 BV). Wenn private Unternehmen die Grund- und Menschenrechte beeinträchtigen, können sich die Betroffenen daher nicht direkt auf diese berufen und sich gegen die Beeinträchtigung zur Wehr setzen. Deshalb wird auf nationaler und internationaler Ebene diskutiert, ob und wie Unternehmen zur Einhaltung der Grund- und Menschenrechte angehalten und/oder verpflichtet werden können.[45]

Staaten haben eine grund- und menschenrechtliche Pflicht, Private vor der Beeinträchtigung ihrer Grund- und Menschenrechte durch andere Private zu schützen (Schutzpflicht → **Grundlagen Kapitel 2.2.5**). Zu diesem Zweck erlassen sie beispielsweise ein Datenschutzgesetz oder ein Gesetz, das vor Persönlichkeitsverletzungen schützt. Im Bereich der Digitalisierung ist dies aber in der Praxis schwierig umzusetzen: Zum einen schreitet die Digitalisierung so schnell voran, dass der Ausbau von Gesetzen nur schwer mithalten kann. Zum anderen finden digitale Vorgänge oftmals grenzüberschreitend statt. So sind beispielsweise über soziale Netzwerke viele Personen aus verschiedensten Nationen miteinander verbunden. Dies erschwert eine Regulierung der Netzwerke auf nationaler Ebene.[46]

44 Jørgensen, Private Actors in the Online Domain, 2018, S. 244 ff.

45 Siehe dazu insbesondere die UNO-Leitprinzipien zu Wirtschaft und Menschenrechten. Für weitere Ausführungen: Kälin/Künzli, Menschenrechtsschutz, 2019, S. 91 ff.

46 Jørgensen, Private Actors in the Online Domain, 2018, S. 268.

2.2 Juristische Grundlagen

2.2.1 Welche Grund- und Menschenrechte gibt es, und in welchen Dokumenten sind sie festgelegt?

Die schweizerische Bundesverfassung und die meisten Kantonsverfassungen enthalten ausführliche Grundrechtskataloge. Weiter findet sich in Art. 41 der Bundesverfassung ein Katalog mit sieben Sozialzielen. Zu diesen zählen soziale Sicherheit, Gesundheit, angemessene Arbeit und Wohnung, Bildung, Schutz von Familien sowie die Förderung und Unterstützung von Kindern und Jugendlichen. Diese Ziele lehnen sich inhaltlich zwar an verschiedene Menschenrechte an, im Unterschied zu den Grundrechten sind sie gerichtlich aber nicht durchsetzbar (→ **Grundlagen Kapitel 2.2.4**). Auf internationaler Ebene sind für die Schweiz insbesondere die Europäische Menschenrechtskonvention (EMRK), das Internationale Abkommen über die wirtschaftlichen, sozialen und kulturellen Rechte (UNO-Sozialpakt) und das Internationale Abkommen über die bürgerlichen und politischen Rechte (UNO-Zivilpakt) wichtig.

Inhaltlich stimmen die Grundrechte der Bundesverfassung und die Menschenrechte zu einem grossen Teil überein. Die nachfolgenden Tabellen enthalten eine Übersicht über die Garantien der Bundesverfassung, der EMRK, des UNO-Sozialpakts und des UNO-Zivilpakts:

Grundprinzipien	
Menschenwürde	Art. 7 BV
Rechtsgleichheit	Art. 8 Abs. 1 BV, Art. 26 UNO-Zivilpakt
Diskriminierungsverbot	Art. 8 Abs. 2 BV, Art. 14 EMRK, Art. 2 Abs. 1 und Art. 26 UNO-Zivilpakt, Art. 2 Abs. 2 UNO-Sozialpakt
Gleichstellung von Frau und Mann	Art. 8 Abs. 3 BV, Art. 7 UNO-Sozialpakt
Gleichstellung von Menschen mit Behinderungen	Art. 8 Abs. 4 BV
Schutz der Kinder und Jugendlichen	Art. 11 BV, Art. 24 UNO-Zivilpakt, Art. 10 UNO-Sozialpakt
Schutz von Minderheiten	Art. 27 UNO-Zivilpakt
Recht auf Anerkennung der Rechtsfähigkeit	Art. 16 UNO-Zivilpakt
Verbot von Kriegspropaganda und Aufruf zu Hass	Art. 20 UNO-Zivilpakt

Schutz von Körper, Psyche, Gesundheit und Selbstbestimmung	
Recht auf Leben	Art. 10 Abs. 1 BV, Art. 2 EMRK, Art. 6 UNO-Zivilpakt
Recht auf körperliche und geistige Unversehrtheit	Art. 10 Abs. 2 BV
Verbot der Folter und der grausamen, unmenschlichen oder erniedrigenden Behandlung oder Bestrafung	Art. 10 Abs. 3 BV, Art. 3 EMRK, Art. 7 UNO-Zivilpakt
Recht auf persönliche Freiheit	Art. 10 Abs. 2 BV
Bewegungsfreiheit	Art. 10 Abs. 2 BV, Art. 12 UNO-Zivilpakt
Niederlassungsfreiheit	Art. 24 BV, Art. 12 UNO-Zivilpakt
Recht auf Gesundheit	Art. 12 UNO-Sozialpakt
Schutz vor Ausweisung, Auslieferung und Ausschaffung	Art. 25 BV, Art. 13 UNO-Zivilpakt

Schutz von Gedanken, Ansichten und Kommunikation	
Glaubens- und Gewissensfreiheit	Art. 15 BV, Art. 9 EMRK, Art. 18 UNO-Zivilpakt
Meinungs- und Informationsfreiheit	Art. 16 BV, Art. 10 EMRK, Art. 19 UNO-Zivilpakt
Medienfreiheit	Art. 17 BV, Art. 10 EMRK, Art. 19 UNO-Zivilpakt
Sprachenfreiheit	Art. 18 BV
Kunstfreiheit	Art. 21 BV, Art. 15 UNO-Sozialpakt
Recht auf Teilhabe am kulturellen Leben	Art. 15 Abs. 1 Bst. a UNO-Sozialpakt

Schutz des sozialen und politischen Lebens	
Recht auf Achtung des Privat- und Familienlebens	Art. 13 BV, Art. 8 EMRK, Art. 17 UNO-Zivilpakt
Recht auf Ehe und Familie bzw. Schutz der Familie	Art. 14 BV, Art. 8 und 12 EMRK, Art. 23 UNO-Zivilpakt, Art. 10 UNO-Sozialpakt
Versammlungsfreiheit	Art. 22 BV, Art. 11 EMRK, Art. 21 UNO-Zivilpakt
Vereinigungsfreiheit	Art. 23 BV, Art. 11 EMRK, Art. 22 UNO-Zivilpakt, Art. 8 UNO-Sozialpakt
Petitionsrecht	Art. 33 BV
Politische Rechte	Art. 34 BV, Art. 25 UNO-Zivilpakt

Wirtschaftliche Existenz	
Eigentumsgarantie	Art. 26 BV, Art. 15 Abs. 1 Bst. c UNO-Sozialpakt
Wirtschaftsfreiheit	Art. 27 BV
Koalitionsfreiheit und Streikrecht	Art. 28 BV, Art. 11 EMRK, Art. 22 UNO-Zivilpakt, Art. 8 UNO-Sozialpakt
Verbot der Sklaverei und der Zwangsarbeit	Art. 4 EMRK, Art. 8 UNO-Zivilpakt
Recht auf Arbeit	Art. 6 UNO-Sozialpakt
Recht auf gerechte und günstige Arbeitsbedingungen	Art. 7 UNO-Sozialpakt
Recht auf Hilfe in Notlagen	Art. 12 BV
Recht auf soziale Sicherheit	Art. 9 UNO-Sozialpakt
Recht auf angemessenen Lebensstandard (inkl. Nahrung, Bekleidung und Unterbringung)	Art. 11 UNO-Sozialpakt

Wissen	
Anspruch auf Grundschulunterricht	Art. 19 BV, Art. 13 und 14 UNO-Sozialpakt
Recht auf Bildung	Art. 13 UNO-Sozialpakt
Wissenschaftsfreiheit	Art. 20 BV, Art. 15 UNO-Sozialpakt
Recht auf Teilhabe am wissenschaftlichen Fortschritt	Art. 15 Abs. 1 Bst. b UNO-Sozialpakt
Schutz des geistigen Eigentums	Art. 15 Abs. 1 Bst. c UNO-Sozialpakt

Verfahrensrechte	
Schutz vor Willkür	Art. 9 BV
Wahrung von Treu und Glauben	Art. 9 BV
Recht auf ein faires Verfahren	Art. 29, 29a und 30 BV, Art. 6 EMRK, Art. 14 UNO-Zivilpakt
Verfahrensgarantien im Freiheitsentzug	Art. 31 BV, Art. 5 EMRK, Art. 9, 10 und 11 UNO-Zivilpakt
Garantien im Strafverfahren	Art. 32 BV, Art. 6 und 7 EMRK, Art. 14 und 15 UNO-Zivilpakt

Weiter gibt es verschiedene Abkommen der UNO, die für die Schweiz ebenfalls wichtig sind. Diese umfassen unter anderem die folgenden Themen: Rassendiskriminierung, Frauenrechte, Verbot der Folter, Kinderrechte und Rechte von Menschen mit Behinderungen.

2.2.2 Dürfen Grund- und Menschenrechte eingeschränkt werden?

Staaten dürfen Grund- und Menschenrechte unter gewissen Bedingungen einschränken. Die Voraussetzungen in Bezug auf die Grundrechte sind für die Schweiz in Art. 36 BV aufgeführt und gelten ähnlich auch bei den Menschenrechten.

- Erstens muss die Einschränkung in einem Gesetz oder einer Verordnung vorgesehen sein; bei schweren Einschränkungen ist ein durch das Parlament verabschiedetes Gesetz notwendig.
- Zweitens benötigt die Einschränkung einen guten Grund. Ein solcher liegt vor, wenn die Einschränkung entweder im öffentlichen Interesse liegt (zum Beispiel zum Schutz der öffentlichen Gesundheit, Sicherheit oder der Umwelt) oder zum Schutz der Grundrechte von anderen Personen erfolgt.
- Drittens muss jede Einschränkung verhältnismässig sein. Dafür ist zu prüfen, ob die einschränkende Massnahme geeignet und zugleich das mildeste Mittel ist, das angestrebte Ziel zu erreichen. Zudem muss das ergriffene Mittel in einem angemessenen Verhältnis zum angestrebten Zweck stehen und damit zumutbar sein.
- Viertens hat jedes Grundrecht einen Mindestbereich, den sogenannten Kerngehalt, der unter keinen Umständen eingeschränkt werden darf.

Sind bei einem Eingriff in ein Grundrecht alle vier Voraussetzungen gegeben, handelt es sich um eine rechtmässige Einschränkung. Fehlt es an einer Voraussetzung, ist die Einschränkung unrechtmässig: In diesem Fall liegt eine Verletzung der Grundrechte vor.[47]

47 Für detaillierte Informationen zur Grundrechtseinschränkung: Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 9.

2.2.3 Was kann bei einer Verletzung der Grund- und Menschenrechte unternommen werden?

Grund- und Menschenrechte können durch verschiedene staatliche Massnahmen und in allen Lebensbereichen verletzt werden. Ob und wie sich eine Person gegen die Verletzung ihrer Grund- und Menschenrechte zur Wehr setzen kann, ist für deren Schutz von entscheidender Bedeutung. Verletzt die Verfügung einer Verwaltungsbehörde oder das Urteil eines Gerichts ein Grund- oder Menschenrecht, kann der Entscheid bei der nächsten Rechtsmittelinstanz angefochten werden. Diese muss die angefochtene staatliche Massnahme bzw. das angefochtene Urteil auf seine Vereinbarkeit mit den Grund- und Menschenrechten überprüfen. Wird eine Verletzung festgestellt, ist die Massnahme bzw. der Entscheid aufzuheben. Kann die Grund- oder Menschenrechtsverletzung damit nicht behoben werden, hat die betroffene Person einen Anspruch auf Entschädigung.[48]

2.2.4 Können alle Grund- und Menschenrechte gerichtlich durchgesetzt werden?

Nicht bei allen Grund- und Menschenrechten können Einzelpersonen eine Verletzung in einem Gerichtsverfahren geltend machen. Die nachfolgende Tabelle[49] gibt einen Überblick darüber, bei welchen Rechten dies gemäss der Rechtsprechung des Bundesgerichts möglich ist und bei welchen nicht:

Rechtsquelle	Gerichtliche Durchsetzbarkeit
Ebene Schweiz	
Grundrechte (Art. 7 bis 34 BV)	Gerichtlich durchsetzbar
Sozialziele (Art. 41 BV)	Gerichtlich nicht durchsetzbar
Internationale Ebene	
Garantien der EMRK	Gerichtlich durchsetzbar
Garantien des UNO-Zivilpaktes	Gerichtlich durchsetzbar
Garantien des UNO-Sozialpaktes	Umstritten: die meisten Garantien sind gemäss Bundesgericht nicht gerichtlich durchsetzbar
Garantien in den weiteren UNO-Menschenrechtsabkommen	Bundesgericht entscheidet für jede Garantie einzeln, ob sie gerichtlich durchsetzbar ist

48 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 8 Rz. 1 ff. und 25 ff.

49 Diese Übersicht ist angelehnt an: Egli/Egbuna-Joss/Ghielmini/Belser/Kaufmann, Grundrechte im Alter, 2019, S. 21.

Nicht gerichtlich durchgesetzt werden können insbesondere die Sozialziele der Bundesverfassung und die meisten im UNO-Sozialpakt enthaltenen Menschenrechte (zum Beispiel das Recht auf angemessenen Wohnraum oder das Recht auf angemessenen Lebensstandard). Das Bundesgericht vertritt die Ansicht, dass diese Bestimmungen eher als Auftrag an den Gesetzgeber zur Regelung gesellschaftspolitischer Entwicklungen zu verstehen sind und deshalb keine einklagbaren Rechte enthalten.

2.2.5 Welche Pflichten hat der Staat?

Die Grund- und Menschenrechte verpflichten in erster Linie den Staat. Parlamente, Gerichte, Regierungen und Verwaltungen auf eidgenössischer, kantonaler und kommunaler Ebene müssen sie bei all ihren Tätigkeiten, das heisst in der Gesetzgebung, der Rechtsprechung und der Verwaltungstätigkeit, achten und zu ihrer Verwirklichung beitragen.[50] Dies gilt auch, wenn der Staat Private zur Erfüllung einer staatlichen Aufgabe beizieht (Art. 35 Abs. 2 BV).

So betreibt beispielsweise die Stiftung SWITCH im Auftrag des Bundesamts für Kommunikation das Register für die Domain «.ch» und sogenannte generische Top-Level-Domains (gTLD) wie zum Beispiel «.photo». Da die SWITCH damit im Auftrag des Staats eine öffentliche Aufgabe wahrnimmt, ist sie in diesem Zusammenhang an die Grund- und Menschenrechte gebunden.[51]

Grund- und Menschenrechte verleihen jeder Einzelperson drei Arten von Ansprüchen und auferlegen damit gleichzeitig dem Staat entsprechende Pflichten:[52]

Erstens besteht ein Abwehranspruch. Demnach dürfen die Behörden bei ihren Tätigkeiten die Grund- und Menschenrechte nicht verletzen. Einzelpersonen haben grundsätzlich das Recht, vom Staat «in Ruhe gelassen zu

50 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 4 Rz. 39 ff. und 42 ff.

51 BGE 138 I 289 E. 2.3.

52 Zu den drei Arten von Ansprüchen/Pflichten: Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 4 Rz. 7 ff.

werden».[53] So darf der Staat beispielsweise die Aktivitäten einer Person im Internet nur beim Vorliegen strenger Voraussetzungen, unter anderem zur Aufklärung einer Straftat, überwachen.

Zweitens verpflichten Grund- und Menschenrechte den Staat, in verschiedenen Situationen aktiv bestimmte Leistungen zu erbringen. Ein Beispiel hierfür ist das Recht auf Grundschulunterricht während der Corona-Pandemie. In dieser Zeit wurden die Schülerinnen und Schüler eine gewisse Zeit zu Hause unterrichtet. Setzten die Lehrpersonen hierfür Online-Lehrmittel ein, mussten die Schulen sicherstellen, dass jedes Kind auch über die erforderliche Infrastruktur verfügte, um auf Online-Lehrmittel zugreifen zu können. Nötigenfalls mussten sie den Schülerinnen und Schülern Laptops und Software zur Verfügung stellen und damit aktiv eine staatliche Leistung erbringen (→ **Fallbeispiel Online-Unterricht in der Schule 5.1**).

Drittens beinhalten die Grund- und Menschenrechte auch einen Schutzanspruch bzw. eine Schutzpflicht. Demnach muss der Staat Einzelpersonen vor Grund- und Menschenrechtsbeeinträchtigungen durch andere, zum Beispiel durch Privatpersonen oder Unternehmen, schützen. Im Kontext der Digitalisierung ist die Schutzpflicht besonders relevant, weil die Beeinträchtigungen der Grund- und Menschenrechte häufig von Privaten ausgehen (→ **Grundlagen Kapitel 2.2.7**).

2.2.6 Gelten Grund- und Menschenrechte auf für Private?

Beschäftigt man sich näher mit dem Einfluss der Digitalisierung auf die Grund- und Menschenrechte, so fällt auf, dass es oft nicht der Staat ist, der Grund- und Menschenrechte verletzt; Beeinträchtigungen gehen vielmehr häufig von Privatpersonen oder Unternehmen aus. So kann beispielsweise das Recht auf Privatsphäre beeinträchtigt sein, wenn über eine App eine Dienstleistung kostenlos angeboten wird, die Anbieterin dafür aber Daten der Benutzerinnen und Benutzer sammelt, um diesen hernach personalisierte Werbung zukommen zu lassen. Ein weiteres Beispiel ist die Überwachung der privaten Kommunikation von Arbeitnehmenden über deren Computer am Arbeitsplatz.

53 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 4 Rz. 10.

Grundsätzlich sind Private (wie die Anbieterin der App oder die Arbeitgebenden in diesen beiden Beispielen), wenn sie keine staatlichen Aufgaben wahrnehmen, nicht direkt an die Grund- und Menschenrechte gebunden.[54] Zwar hält die Bundesverfassung in Art. 35 Abs. 3 fest, dass Grundrechte, «so weit sie sich dafür eignen», auch für Private gelten, bislang wird diese Bestimmung aber nicht angewandt.[55] Es stellt sich somit die Frage, wie Einzelpersonen trotzdem wirksam vor Beeinträchtigungen ihrer Grund- und Menschenrechte durch andere Private geschützt werden können.

Da Private nicht direkt an die Grund- und Menschenrechte gebunden sind, kann eine Einzelperson bei einem Rechtsstreit mit einer anderen privaten Person oder einem Unternehmen, beispielsweise bei einem Konflikt einer Arbeitnehmerin mit ihrer Arbeitgeberin, nicht wegen Verletzung eines Grund- oder Menschenrechts klagen. Trotzdem haben Grund- und Menschenrechte einen Einfluss auf Verhältnisse zwischen Privaten, und zwar durch die Schutzpflicht des Staats.

Der Staat muss dafür sorgen, dass Private die Grund- und Menschenrechte anderer Privater nicht beeinträchtigen.[56] Dies tut er, indem er beispielsweise Gesetze und Verordnungen erlässt, die das Verhältnis zwischen Privaten regeln. Ein Beispiel dafür sind verschiedene Vorschriften im Obligationenrecht zum Schutz der Arbeitnehmenden, die unter anderem festlegen, dass Arbeitgebende die Privatsphäre ihrer Arbeitnehmenden achten und schützen müssen. Bei einem Rechtsstreit unter Privaten können sich diese somit nicht direkt auf die Grund- und Menschenrechte berufen; sie können sich jedoch auf Gesetze stützen, die diese Garantien indirekt auch im Verhältnis zwischen Privaten schützen.

2.2.7 Welche Gesetze schützen die Grund- und Menschenrechte im Bereich Digitalisierung?

Im Bereich der Digitalisierung schützen verschiedene Gesetze Privatpersonen vor Grund- und Menschenrechtsbeeinträchtigungen durch andere Pri-

54 Dies mit wenigen Ausnahmen wie zum Beispiel dem Recht auf gleichen Lohn für gleichwertige Arbeit für Frau und Mann (Art. 8 Abs. 3 BV).

55 Müller, Verwirklichung der Grundrechte, 2018, S. 58 ff.

56 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 4 Rz. 90.

vate. Sie sind damit gute Beispiele dafür, wie der Staat seine Schutzpflicht wahrnimmt. Besonders wichtig für die Digitalisierung sind in der Schweiz die folgenden Gesetzesbestimmungen:

- *Schutz der Persönlichkeit nach Art. 28 ff. ZGB:* Art. 28 ZGB soll widerrechtliche Verletzungen der Persönlichkeit von Privatpersonen durch Dritte unterbinden. Eine Persönlichkeitsverletzung ist dann widerrechtlich, wenn es dafür keinen Rechtfertigungsgrund (zum Beispiel Einwilligung, öffentliches Interesse) gibt. Dazu zählen beispielsweise Verunglimpfungen oder Veröffentlichungen von privaten Informationen/Fotos. Solche Verletzungen erfolgen in der digitalen Welt oft schneller und sind einem grösseren Kreis von Adressatinnen und Adressaten zugänglich (zum Beispiel über soziale Netzwerke) als in der analogen Welt. Die betroffene Person kann gerichtlich ein Verbot oder eine Beseitigung der Verletzung erwirken und je nach Situation Schadenersatz und/oder Genugtuung sowie eine Gegendarstellung verlangen.[57]
- *Datenschutzrecht:* Die Datenschutzgesetze des Bundes und der Kantone schützen unter anderem das Recht auf Privatsphäre von Privatpersonen bei der Bearbeitung ihrer Daten durch Behörden oder Unternehmen. Das Datenschutzgesetz des Bundes wurde jüngst überarbeitet. Die Gesetzesrevision wird voraussichtlich 2022 in Kraft treten.[58] Die Bearbeitung von Daten ist grundsätzlich gestattet, dabei müssen aber verschiedene Vorgaben beachtet werden: So dürfen Personendaten beispielsweise nur zum jeweils angegebenen und erkennbaren Zweck bearbeitet werden. Die bearbeiteten Personendaten müssen richtig sein und vor unbefugten Zugriffen geschützt werden (Art. 4, 5 und 7 DSG; Art. 6 und 8 Rev-DSG). Die Persönlichkeit der Betroffenen darf bei der Datenbearbeitung durch private Personen nicht widerrechtlich verletzt werden. Sie ist nicht widerrechtlich, wenn eine rechtsgültige Einwilligung oder ein überwiegendes privates oder öffentliches Interesse vorliegt (Art. 12 und 13 DSG; Art. 30 und 31 Rev-DSG). Schliesslich kann gemäss Art. 15 DSG (Art. 32 Rev-DSG) eine betroffene Person das Sperren einer Datenbearbeitung oder die Berichtigung oder Vernichtung von Daten verlangen.

57 Büchler, Kommentar zu Art. 28 ff. ZGB, 2016.

58 Es werden die noch geltenden Bestimmungen des DSG genannt und die jeweils entsprechende Bestimmung des revidierten DSG (Rev-DSG) erwähnt.

- *Arbeitsrecht:* Das Arbeitsrecht enthält viele Vorschriften, die unter anderem die Privatsphäre der Arbeitnehmenden schützen sollen. So dürfen gemäss Art. 328b OR Arbeitgebende nur solche Informationen über ihre Mitarbeitenden sammeln und auswerten, die in einem engen Zusammenhang mit dem Arbeitsverhältnis stehen. Dies betrifft zum Beispiel die geleisteten Arbeitsstunden oder die Qualität der Arbeitsleistung. Art. 26 der Verordnung 3 zum Arbeitsgesetz sieht ausserdem vor, dass keine Überwachungs- und Kontrollsysteme eingesetzt werden dürfen, wenn deren einziger Zweck darin besteht, das Verhalten der Arbeitnehmenden am Arbeitsplatz zu überwachen. Aus anderen Gründen (zum Beispiel Sicherheit des Personals, Kontrolle der geleisteten Arbeit) dürfen solche Systeme nur so eingesetzt werden, dass sie die Gesundheit und Bewegungsfreiheit der Arbeitnehmenden nicht beeinträchtigen.
- *Strafrecht:* Es gibt Straftatbestände, die nur im Zusammenhang mit digitalen Technologien Anwendung finden. Hierzu zählen beispielsweise das unbefugte Eindringen in ein Datenverarbeitungssystem (Art. 143bis StGB) oder der betrügerische Missbrauch einer Datenverarbeitungsanlage (Art. 147 StGB). Weiter gibt es auch Straftatbestände, welche nicht zwingend einen digitalen Kontext voraussetzen, aber auch mit digitalen «Hilfsmitteln» begangen werden können. Hierunter fallen beispielsweise die Drohung (Art. 180 StGB), die Nötigung (Art. 181 StGB), die sexuelle Nötigung (Art. 189 StGB) oder die Erpressung (Art. 156 StGB) in sozialen Netzwerken oder per E-Mail.[59]
- *Lauterkeitsrecht:* Das Bundesgesetz gegen den unlauteren Wettbewerb (UWG) soll einen lauteren und unverfälschten Wettbewerb gewährleisten. Verschiedene unlautere Handlungen (Art. 3 UWG), können dank der Digitalisierung einfacher ausgeführt werden und sind einem breiteren Kreis von Adressatinnen und Adressaten zugänglich. Hierzu gehören beispielsweise unrichtige Äusserungen über andere Unternehmen oder fremde Waren (Art. 3 Abs. 1 Bst. a UWG) und das breit angelegte Zusenden von Werbung an verschiedene Menschen mithilfe von Fernmeldetechniken (Art. 3 Abs. 1 Bst. o UWG). So ist es beispielsweise untersagt, auf der unternehmenseigenen Website das Einreichen einer Strafanzeige gegen ein anderes Unternehmen zu veröffentlichen,

59 Gyarmati, Cybercrime, 2019, S. 87.

wenn sich die Staatsanwaltschaft der Vorwürfe (noch) nicht angenommen hat. Begründet wird dies damit, dass die Mitteilung über eine eingereichte Strafanzeige bei der durchschnittlichen Kundschaft Zweifel an der Seriosität des betroffenen Unternehmens wecken könnte.[60]

– *Urheberrecht:* Das Urheberrechtsgesetz (URG) will das geistige Eigentum von Urheberinnen und Urhebern gegen widerrechtliche Vervielfältigungen oder Veröffentlichungen schützen. Es wurde in den vergangenen Jahren an die Entwicklungen der Digitalisierung und insbesondere an das Phänomen der Piraterieplattformen angepasst. So haben unter anderem Hosting Provider, deren Geschäftsmodelle einen Anreiz für die Verletzung des geistigen Eigentums setzen, neu eine besondere Überwachungspflicht. Sie müssen dafür sorgen, dass ein illegal hochgeladenes Werk nach seiner Entfernung nicht erneut hochgeladen werden kann (Art. 39d URG). Personen, die im Internet hochgeladene Werke zum Eigengebrauch konsumieren, dürfen dies aber auch weiterhin tun (Art. 19 URG), solange sie dabei selbst keine Werke hochladen.

2.3 Einfluss der Digitalisierung auf einzelne Grund- und Menschenrechte

Digitale Technologien können die Grund- und Menschenrechte stärken, sie können aber auch zu deren Verletzung oder Beeinträchtigung beitragen. Die nachfolgenden Kapitel gehen auf ausgewählte Grund- und Menschenrechte ein, auf die sich die Digitalisierung besonders deutlich auswirkt, und erläutern deren Auswirkungen. Bei den einzelnen Garantien wird jeweils die Bestimmung der Bundesverfassung genannt und zudem auf die inhaltlich weitgehend übereinstimmenden Bestimmungen in den internationalen Menschenrechtsabkommen verwiesen. Die einzelnen Garantien sind thematisch wie folgt gruppiert: 1. Grundprinzipien, 2. Sammeln von Daten und Überwachung, 3. Schutz von Körper, Psyche und Gesundheit, 4. Gedanken, Ansichten und Kommunikation, 5. Soziales und politisches Leben, 6. Arbeitsleben und Wirtschaft, 7. Wissen, 8. Kontakt mit Behörden und Gerichten.

60 Urteil Obergericht Kanton Zug, GVP 2013/1.2.5.1, 17.4.2013, E. 4.2 f.

2.3.1 Grundprinzipien

A Menschenwürde[61]

Art. 7 BV

Die Würde des Menschen ist zu achten und zu schützen.

Der Schutz der Menschenwürde ist die erste Garantie im Grundrechtskatalog der Bundesverfassung und gleichzeitig ein Grundsatz, den die Behörden in jeder Situation beachten müssen. Was die Bestimmung im Detail beinhaltet, hat das Bundesgericht bislang nicht abschliessend geklärt. Im Grunde geht es darum, dass jeder Mensch als einzigartiges oder auch andersartiges Individuum anerkannt und als wertvolles Wesen behandelt werden muss.

Die Menschenwürde ist verletzt, wenn eine Einzelperson als Objekt behandelt wird. Dies ist beispielsweise beim Einsatz von Assistenzrobotern in der Pflege denkbar (→ **Grundlagen Kapitel 1.7** und → **Fallbeispiel Pflegeroboter 2.1**). Einer Ansicht nach wird dadurch die Pflege in eine reine «Wartungsarbeit» umgewandelt, die pflegebedürftige Person zum Objekt degradiert und somit ihre Menschenwürde verletzt.[62]

B Schutz von Kindern und Jugendlichen[63]

Art. 11 BV

Kinder und Jugendliche haben Anspruch auf besonderen Schutz ihrer Unversehrtheit und auf Förderung ihrer Entwicklung.

Art. 41 Abs. 1 Bst. g BV (Sozialziel), Art. 24 UNO-Zivilpakt

Aufgrund der Verletzlichkeit von Kindern und Jugendlichen soll deren geistige und körperliche Unversehrtheit in besonderem Masse geschützt werden. In diesem Zusammenhang ist auch die UNO-Kinderrechtskonvention von grosser Bedeutung.

61 BGE 127 I 6 E. 5b.

62 Kreis, Pflegeroboter, 2018, S. 224 f.

63 Biaggini, Kommentar zu Art. 11 BV, 2017, N. 1 ff.

Die Verpflichtung zum besonderen Schutz von Kindern und Jugendlichen bedeutet nicht, dass Minderjährige gerichtlich einen bestimmten Anspruch einklagen können. Sie hat aber zur Folge, dass bei der Anwendung anderer Grundrechte oder Gesetze immer auch das Kindeswohl mitberücksichtigt werden muss. Sie verpflichtet den Staat zudem, zum Schutz von Kindern und Jugendlichen Gesetze zu erlassen und Massnahmen zu ergreifen.

Im Bereich der digitalen Technologien kann die geistige und körperliche Unversehrtheit von Kindern und Jugendlichen beispielsweise durch Mobbing in sozialen Medien oder durch eine Internetsucht beeinträchtigt sein. Ist eine Jugendliche von Cybermobbing betroffen, ist zu ihrem Schutz die Anwendung verschiedener Bestimmungen des Strafgesetzbuchs und des Persönlichkeitsrechts denkbar (→ **Fallbeispiel Cybermobbing 4.2**).

C Diskriminierungsverbot[64]

Art. 8 Abs. 2 BV

Niemand darf diskriminiert werden, namentlich nicht wegen der Herkunft, der Rasse, des Geschlechts, des Alters, der Sprache, der sozialen Stellung, der Lebensform, der religiösen, weltanschaulichen oder politischen Überzeugung oder wegen einer körperlichen, geistigen oder psychischen Behinderung.

Art. 8 Abs. 3 und 4 BV, Art. 14 EMRK, Art. 2 Abs. 2 UNO-Sozialpakt, Art. 2 Abs. 1 UNO-Zivilpakt

Verboten ist sowohl die direkte als auch die indirekte Diskriminierung. Eine direkte Diskriminierung liegt vor, wenn jemand aufgrund eines der aufgelisteten Merkmale wie Alter, Geschlecht oder Herkunft durch eine staatliche Massnahme anders als andere behandelt und in der Folge benachteiligt wird und es für diese Ungleichbehandlung keinen besonderen Rechtfertigungsgrund gibt. Eine direkte Diskriminierung läge beispielsweise vor, wenn eine Software zur Berechnung der Rückfallgefahr von verurteilten Personen bei einer bestimmten Herkunft diese generell höher einschätzen würde.[65]

Bei einer indirekten Diskriminierung unterscheidet die staatliche Massnahme zwar vordergründig nicht nach einem diskriminierenden, sondern nach

64 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 36.

65 Zur Software COMPAS, die in den USA eingesetzt wurde: Zuiderveen Borgesius, Discrimination, 2018, S. 14 f.

einem «neutralen» Merkmal. Im Ergebnis wird aber dennoch eine Gruppe von Menschen benachteiligt, die eines der geschützten Merkmale aufweist. Kann beispielsweise ein Gesuch um die Verbilligung von Krankenkassenprämien nur noch auf elektronischem Weg eingereicht werden, knüpft dies auf den ersten Blick an keines der verbotenen Merkmale an. In der Realität würden aber aufgrund fehlender Kenntnisse weit mehr ältere als junge Menschen daran gehindert, Prämienverbilligungen zu beantragen. Die älteren Menschen wären damit benachteiligt.

Das Diskriminierungsverbot der Bundesverfassung betrifft grundsätzlich nur staatliche Handlungen; ein allgemeines Diskriminierungsverbot für Private fehlt in der Schweiz. In einzelnen Bereichen gibt es aber einen punktuellen Schutz vor Diskriminierungen durch Private, zum Beispiel im Arbeits-, Miet- und Versicherungsrecht.[66]

Weiter befasst sich das Diskriminierungsverbot in Art. 8 Abs. 3 und 4 BV mit zwei spezifischen Gruppen und verlangt Massnahmen zur Beseitigung ihrer Benachteiligung. Zum einen sieht Art. 8 Abs. 3 BV die Gleichstellung von Frauen und Männern in allen Lebenssituationen vor und verlangt Gesetze, die für die rechtliche und tatsächliche Gleichstellung in Familie, Ausbildung und Arbeit sorgen. Zum anderen verlangt Art. 8 Abs. 4 BV, dass die Benachteiligung von Menschen mit Behinderungen mit geeigneten Gesetzen bekämpft wird.

Digitale Technologien können einen Beitrag zur Gleichstellung von Mann und Frau leisten und auch gewisse Benachteiligungen von Menschen mit Behinderungen beseitigen. Software für das dezentrale und gemeinsame Bearbeiten von Dokumenten und Videotelefonie ermöglichen ein zeitlich und örtlich flexibleres Arbeiten in verschiedenen Berufen und können so zu einer besseren Vereinbarkeit von Familie und Beruf beitragen. Die Erfahrungen während des Corona-Lockdowns im Frühling 2020 zeigen aber auch, dass ein erleichtertes Homeoffice traditionelle Geschlechterrollen verfestigen kann.[67]

Digitale Technologien wie beispielsweise Spracherkennungssoftware oder Assistenzroboter vermögen Menschen mit Behinderungen bei ihrer Arbeits-

66 Art. 271 OR, Art. 336 Abs. 1 Bst. a OR und Art. 117 Abs. 2 AVO.

67 Möhring/Naumann/Reifenscheid et al., Mannheimer Corona-Studie, 2020, S. 12 ff.

tätigkeit oder ihrer Inklusion in das alltägliche Leben zu unterstützen. Die rasche technologische Entwicklung und das Ersetzen von menschlicher Arbeit durch Roboter birgt aber auch die Gefahr, dass Menschen mit Behinderungen im Arbeitsmarkt zusätzlich benachteiligt und aus diesem verdrängt werden.[68]

2.3.2 Sammeln von Daten und Überwachung

A Recht auf Privatsphäre[69]

Art. 13 Abs. 1 BV

Jede Person hat Anspruch auf Achtung ihres Privatlebens (...), ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.

Art. 8 EMRK, Art. 17 UNO-Zivilpakt

Der Begriff der Privatsphäre beschreibt ein Mindestmass an Privatheit, das jeder Person zusteht und das jeder Person ermöglichen soll, ihr Leben ohne staatlichen Einfluss nach dem eigenen Willen zu gestalten und persönliche Beziehungen zu pflegen. Niemand muss private Informationen den Behörden oder der Öffentlichkeit bekannt geben. Das Recht auf Privatsphäre kann beispielsweise dann verletzt sein, wenn private Gespräche ohne Wissen der Beteiligten aufgezeichnet werden. Dies gilt unabhängig davon, ob diese im öffentlichen oder privaten Raum stattfinden. Auch das Ausspionieren eines Grundstücks oder die Überwachung des öffentlichen Raums mittels einer Drohne tangiert die Privatsphäre.[70]

Der Staat muss die Privatsphäre jeder einzelnen Person achten. Darunter fällt auch die Wohnung sowie der Brief-, Post- und Fernmeldeverkehr (inkl. elektronisch übermittelte Nachrichten wie E-Mails oder Online-Telefonie). Das Recht auf Privatsphäre kann beispielsweise bei polizeilichen Ermittlungen eingeschränkt werden. Die Überwachung der (elektronischen) Kommunikation oder die Durchsuchung einer Wohnung sind aber nur unter strengen gesetzlichen Voraussetzungen zulässig.

68 Ständerat, Postulat 16.4169, Inklusives Arbeitsumfeld, 2016.

69 Diggelmann, Kommentar zu Art. 13 BV, 2015; Breitenmoser/Schweizer, Kommentar zu Art. 13 BV, 2014.

70 Urteil Bundesverwaltungsgericht A-2482/2007, 26.6.2007.

Zudem muss der Staat Einzelpersonen auch vor einer Verletzung ihrer Privatsphäre durch andere Personen schützen, beispielsweise mit Vorschriften im Datenschutz- oder Arbeitsrecht. Gerade im Internet können persönliche Informationen sehr einfach und ohne Zustimmung der betroffenen Person verbreitet werden und lassen sich oftmals nur schwer wieder entfernen.

B Recht auf Datenschutz[71]

Art. 13 Abs. 2 BV

Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Art. 8 EMRK, Art. 17 UNO-Zivilpakt

Die Bundesverfassung beinhaltet ein Recht auf Datenschutz und damit das Recht, über die persönlichen Daten selbst zu bestimmen. Anders als es der Wortlaut der Bestimmung vermuten liesse, geht es dabei nicht nur um den Schutz vor einer missbräuchlichen Datenbearbeitung. Vielmehr hat jede Person das Recht, selber zu entscheiden, ob und welche ihrer persönlichen Informationen gesammelt, bearbeitet, gespeichert oder weitergegeben werden (Recht auf informationelle Selbstbestimmung). Von diesem Recht erfasst werden sogenannte Personendaten. Dies sind alle Informationen, die sich auf eine bestimmte oder bestimmbare Person beziehen, wie beispielsweise die Krankheitsgeschichte oder Informationen zum Aussehen, zur wirtschaftlichen Situation, zu sozialen Kontakten oder zur politischen Einstellung.

Auch über das Internet und über Smartphone-Apps werden grosse Mengen an Daten gesammelt und ausgewertet. So erfassen beispielsweise Betreibende von Websites mit sogenannten Cookies die Besucherbewegungen auf ihren Websites, was Rückschlüsse auf Interessen, Gewohnheiten und Persönlichkeitsmerkmale der Nutzerinnen und Nutzer zulässt.[72] Apps, die gratis benutzt werden können (zum Beispiel Übersetzungsdienste, Spiele, Planungstools), sammeln in der Regel ebenfalls Daten, was den Nutzerinnen und Nutzern oftmals nicht bewusst ist.

71 Diggelmann, Kommentar zu Art. 13 BV, 2015, N. 32 ff.; Breitenmoser/Schweizer, Kommentar zu Art. 13 BV, 2014, N. 70 ff.

72 EDÖB, Erläuterungen zu Webtracking, 2014.

Das Recht auf Datenschutz bezieht sich sowohl auf die Datenbearbeitung durch staatliche Behörden als auch durch Privatpersonen und Unternehmen. Das Datenschutzgesetz des Bundes und die kantonalen Datenschutzgesetze legen hierfür bestimmte Richtlinien zum Schutz der persönlichen Daten fest: So hat jede Person das Recht, sowohl von den Behörden als auch von Privaten Auskunft zu erhalten, welche Daten über sie vorhanden sind. Ausserdem kann sie die Löschung oder Berichtigung dieser persönlichen Daten verlangen, nötigenfalls auch mittels gerichtlicher Klage. Gelöscht werden müssen die Daten, wenn es dafür eine gesetzliche Pflicht gibt oder wenn der Löschung keine überwiegenden privaten oder öffentlichen Interessen entgegenstehen. Dies gilt auch in Bezug auf persönliche Daten und Bilder, die im Internet veröffentlicht wurden (das sogenannte Recht auf Vergessenwerden bzw. das Recht auf Löschung im Internet). Die Löschung gestaltet sich jedoch in der Praxis äusserst schwierig.[73]

C Bewegungsfreiheit[74]

Art. 10 Abs. 2 BV

Jeder Mensch hat das Recht (...) auf Bewegungsfreiheit.

Art. 12 Abs. 1 UNO-Zivilpakt

Bewegungsfreiheit bedeutet, sich frei und ohne staatliche Einschränkung bewegen zu dürfen. Jede einzelne Person soll grundsätzlich selbst darüber entscheiden, wo sie verweilen, wo sie sich hinbewegen oder an welchem Ort sie sich nicht aufhalten möchte.

Die Bewegungsfreiheit kann in unterschiedlichen Situationen eingeschränkt werden. Typische Beispiele sind die Haft, Rayonverbote, das Absperren von öffentlichen Räumen (zum Beispiel eines Parks) oder die Anhaltung einer Person bei einer Polizeikontrolle. Auch digitale Technologien können dabei eine Rolle spielen: Elektronische Mittel zur Überwachung von Personen im Strafvollzug (Electronic Monitoring) oder in der Pflege (zum Beispiel Lichtmelder, Matratzensensor)[75] tangieren ebenfalls die Bewegungsfreiheit.

73 Wermelinger, Kommentar zu Art. 15 DSG, 2015, N. 9 f.

74 Schweizer, Kommentar zu Art. 10 BV, 2014, N. 33 ff.

75 Egli/Egbuna-Joss/Ghielmini/Belser/Kaufmann, Grundrechte im Alter, 2019, S. 47.

Die Videoüberwachung von öffentlichen Strassen und Plätzen, allenfalls kombiniert mit Gesichtserkennungssoftware, schränkt die Bewegungsfreiheit nicht direkt ein, da die Orte grundsätzlich frei zugänglich bleiben. Jedoch kann sie die Bewegungsfreiheit indirekt tangieren, wenn Personen, die nicht gefilmt oder registriert werden wollen, die entsprechenden öffentlichen Räume meiden müssen (→ **Fallbeispiel Staatliche Videoüberwachung mit Gesichtserkennung im öffentlichen Raum 3.5**).[76]

Der Staat ist über sein eigenes Handeln hinaus zudem verpflichtet, Einzelpersonen vor einer Verletzung ihrer Bewegungsfreiheit durch Dritte zu schützen. Das gilt auch in Bezug auf den Einsatz von digitalen Technologien durch Private. So sieht beispielsweise das Arbeitsrecht in Art. 26 ArGV 3 vor, dass Technologien wie GPS oder Überwachungssoftware nur eingesetzt werden dürfen, wenn sie die Bewegungsfreiheit der Arbeitnehmenden nicht einschränken (→ **Fallbeispiel Überwachung am Arbeitsplatz 1.3**).[77]

2.3.3 Schutz von Körper, Psyche und Gesundheit

A Recht auf Leben[78]

Art. 10 Abs. 1 BV
Jeder Mensch hat das Recht auf Leben.
Art. 2 EMRK, Art. 6 UNO-Zivilpakt

Das Recht auf Leben schützt Einzelpersonen davor, durch staatliche Behörden gezielt getötet zu werden. Es verpflichtet den Staat zudem, gefährdete Personen vor einer Tötung durch eine andere Person zu schützen. Entsprechende Fälle müssen untersucht und Täterinnen und Täter bestraft werden. Das Recht auf Leben kann unter besonderen Umständen, beispielsweise bei einem zwingend notwendigen und nicht anders durchführbaren Polizeieinsatz, eingeschränkt werden («gezielter Todesschuss»).[79]

76 Schweizer, Kommentar zu Art. 10 BV, 2014, N. 35.
77 SECO, Wegleitung zur ArGV 3 und 4, 2020, Rz. 326.1.
78 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 11.
79 Urteil Kantonsgericht Graubünden, SF 01 30, 28.2.2002, PKG 2002, S. 82 ff.

Der Bezug des Rechts auf Leben zu digitalen Technologien findet sich insbesondere bei der Frage, ob die gezielte Tötung von Personen durch Drohnen im Rahmen der Terrorismusbekämpfung rechtmässig ist.[80]

B Recht auf körperliche und geistige Unversehrtheit[81]

> Art. 10 Abs. 2 BV
>
> Jeder Mensch hat das Recht (...) auf körperliche und geistige Unversehrtheit (...).

Das Recht auf körperliche Unversehrtheit schützt vor jeder Art von staatlichen Eingriffen in den eigenen Körper, unabhängig davon, ob diese schmerzhaft sind oder nicht. Zum Schutzbereich gehört auch das Recht, eigenständig über den eigenen Körper entscheiden zu können. Dies umfasst insbesondere auch Entscheide über allfällige medizinische Eingriffe. Das Recht auf geistige Unversehrtheit schützt die psychische Gesundheit und beinhaltet das Recht, unbeeinflusst Dinge wahrzunehmen, Entscheidungen zu treffen und gemäss eigenen Einschätzungen zu handeln.

Verschiedene Szenarien sind möglich, in denen digitale Technologien die körperliche oder geistige Unversehrtheit tangieren. Zu denken ist beispielsweise an einen Pflegeroboter in einem Altersheim, der aufgrund einer Fehlprogrammierung eine Patientin verletzt (→ **Fallbeispiel Pflegeroboter 2.1**). Die geistige Unversehrtheit kann bei Cybermobbing (→ **Fallbeispiel Cybermobbing 4.2**) oder aber aufgrund der ständigen Kontrolle beim Einsatz von Überwachungstechnologien am Arbeitsplatz oder im öffentlichen Raum tangiert sein (→ **Fallbeispiel Überwachung am Arbeitsplatz 1.3**).

80 UNO-Sonderberichterstatter zu Menschenrechten und Terrorismusbekämpfung, Report, 2017, Rz. 25 ff.

81 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 12 Rz. 18 ff. und 25 ff.

C Verbot der Folter und der unmenschlichen oder erniedrigenden Behandlung oder Bestrafung[82]

Art. 10 Abs. 3 BV

Folter und jede andere Art grausamer, unmenschlicher oder erniedrigender Behandlung oder Bestrafung sind verboten.

Art. 3 EMRK, Art. 7 UNO-Zivilpakt

Das Folterverbot ist ein fundamentales Prinzip des Rechtsstaats und darf unter keinen Umständen eingeschränkt werden. Zusätzlich zu den oben erwähnten Rechtsquellen ist es unter anderem auch in der UNO-Antifolterkonvention[83] enthalten.

Folterhandlungen sind in jedem Fall verboten. Dies betrifft beispielsweise die Arbeit der Polizei, aber auch Institutionen wie Gefängnisse, Pflegeheime, psychiatrische Einrichtungen oder Flüchtlingsunterkünfte. Zusätzlich muss der Staat alle Personen vor Folterhandlungen durch Private schützen. Allfällige Anschuldigungen müssen untersucht und Täterinnen und Täter bestraft werden. Dies erfolgt insbesondere über das Strafrecht. Schliesslich darf eine ausländische Person auch nicht in ein anderes Land ausgeschafft werden, wenn ihr dort Folter droht (Refoulementverbot gemäss Art. 25 BV).

Digitale Technologien können zur Verletzung des Folterverbots beitragen. Beispielsweise können Staaten regimekritische Personen mittels digitaler Technologien gezielt überwachen und später verhaften und foltern.[84] Weil solche Technologien oft von Privaten entwickelt und an die Staaten verkauft werden, ist das Folterverbot für Technologiefirmen relevant. Auch Schweizer Unternehmen könnten betroffen sein: Ihnen kann beispielsweise gestützt auf die Güterkontrollgesetzgebung der Export von Überwachungstechnologien verweigert werden, wenn davon auszugehen ist, dass sie im Ausland zur

82 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 13.

83 Übereinkommen gegen Folter und andere grausame, unmenschliche oder erniedrigende Behandlung oder Strafe.

84 UNO-Sonderberichterstatter über die Förderung der Meinungsfreiheit und das Recht auf freie Meinungsäusserung, Surveillance and human rights, 2019, Rz. 1; Britischer Nationaler Kontaktpunkt für die OECD-Leitsätze für multinationale Unternehmen, Privacy International & Gamma International UK LTD, Final Statement, 2014.

Repression eingesetzt werden.[85] Im Gegensatz dazu gibt es auch Software, die Menschenrechtsorganisationen beim Sammeln und Auswerten von Berichten über Folter unterstützen und damit die Aufklärung solcher Fälle erleichtern können.[86]

D Recht auf Gesundheit[87]

Art. 41 Abs. 1 Bst. b BV (Sozialziel)

Bund und Kantone setzen sich (...) dafür ein, dass jede Person die für ihre Gesundheit notwendige Pflege erhält.

Art. 12 UNO-Sozialpakt

Das Recht auf Gesundheit ist im UNO-Sozialpakt enthalten und als Sozialziel in der Bundesverfassung aufgeführt. Es kann gerichtlich nicht eingeklagt werden, verpflichtet aber Bund und Kantone, Massnahmen für seine Verwirklichung zu ergreifen. Der Staat muss insbesondere für ein funktionierendes und für alle gleichermassen zugängliches Gesundheitssystem sorgen.

Die Digitalisierung vermag das Recht auf Gesundheit zu stärken. So ermöglichen digitale Kommunikationsmittel einen zusätzlichen Zugang zu ärztlicher Beratung. Künstliche Intelligenz und Big Data erleichtern die Entwicklung von neuen Medikamenten oder die Erstellung eines individuellen Behandlungsplans. In vielen Ländern, auch in der Schweiz, wurden während der Corona-Pandemie Apps entwickelt, die die Rückverfolgung von Infektionsketten unterstützen sollten.

Jedoch birgt das Sammeln und Bearbeiten von Gesundheitsdaten das Risiko, dass diese missbräuchlich verwendet oder veröffentlicht werden. So ist beispielsweise denkbar, dass aufgrund solcher Daten einer Person der Abschluss einer Zusatzversicherung verweigert werden könnte.[88]

85 Verordnung über die Ausfuhr und Vermittlung von Gütern zur Internet- und Mobilfunküberwachung.

86 UNO-Hochkommissariat für Menschenrechte, Human Rights in a New Era, 2018.

87 Biaggini, Kommentar zu Art. 41 BV, 2017.

88 UNO-Hochkommissariat für Menschenrechte, Economic, social and cultural rights and new technologies, 2020, Rz. 19 ff.

E Recht auf persönliche Freiheit[89]

> Art. 10 Abs. 2 BV
>
> Jeder Mensch hat das Recht auf persönliche Freiheit (…).

Das Recht auf persönliche Freiheit garantiert jeder einzelnen Person, ohne Einmischung des Staats frei über ihr Leben und ihre Persönlichkeit entscheiden zu können. Die von der persönlichen Freiheit garantierte Entscheidungsfreiheit umfasst kein absolutes Recht auf ein Tun und Lassen in jeder Lebenslage, sondern betrifft die wichtigsten Aspekte des Lebens wie beispielsweise die sexuelle Entfaltung, Kinderwunsch, medizinische Behandlungen und den Entscheid über das Ende des eigenen Lebens.

Auch der Zugang zur Reproduktionsmedizin wird grundsätzlich von der persönlichen Freiheit erfasst,[90] wobei in der Schweiz verschiedene Handlungen grundsätzlich verboten (zum Beispiel Eizellenspende, Leihmutterschaft) oder bislang homosexuellen Paaren verwehrt sind. Dank der Digitalisierung nimmt die Reproduktionsmobilität zu. Personen, die in der Schweiz verbotene Methoden in Anspruch nehmen möchten, können über Plattformen im Internet einfacher entsprechende Angebote im Ausland finden, sich in sozialen Medien austauschen und sich beispielsweise über Videotelefonie beraten lassen, was ihr Recht auf persönliche Freiheit stärkt.

89 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 12.

90 BGE 119 Ia 460.

2.3.4 Gedanken, Ansichten und Kommunikation

A Glaubens- und Gewissensfreiheit[91]

Art. 15 BV
Die Glaubens- und Gewissensfreiheit ist gewährleistet.
Art. 9 EMRK, Art. 18 UNO-Zivilpakt

Die Glaubens- und Gewissensfreiheit beinhaltet das Recht, jede Religion oder Weltanschauung frei zu wählen, auszuüben, einer entsprechenden Gemeinschaft beizutreten oder fernzubleiben. Der Staat muss vor einer Verletzung der Religionsfreiheit durch Private schützen.

In digitalen Medien, insbesondere bei Kommentarfunktionen im Internet, kommt es oft zu verspottenden, beleidigenden oder diskriminierenden Äusserungen gegenüber Angehörigen einer bestimmten Religion. In diesem Zusammenhang sind je nach Situation die Bestimmungen im Strafgesetzbuch zum Verbot der Störung der Glaubens- und Kultusfreiheit (Art. 261 StGB) und zur Rassendiskriminierung (Art. 261bis StGB) relevant (→ **Fallbeispiel Hasskommentare im Internet 4.1**).

Die Digitalisierung kann die Ausübung von Religionen aber auch unterstützen. So kann beispielsweise eine Videokonferenz Zugang zu einer geistlichen Person oder zu Gottesdiensten geben, der sonst nicht möglich wäre. Mitglieder einer Glaubensgemeinschaft können mit digitalen Hilfsmitteln einfacher Informationen und Hilfe finden, wenn sie aus einer Gemeinschaft austreten wollen. Die Bedeutung digitaler Beteiligungsformen kam während des Corona-Lockdowns besonders zum Ausdruck (digitale Gottesdienste und Betreuungsangebote der Landeskirchen).

91 Biaggini, Kommentar zu Art. 15 BV, 2017; Cavelti/Kley, Kommentar zu Art. 15 BV, 2014.

B Meinungs- und Informationsfreiheit[92]

Art. 16 BV

Die Meinungs- und Informationsfreiheit ist gewährleistet.

Art. 10 EMRK, Art. 19 UNO-Zivilpakt

Die Meinungsfreiheit beinhaltet das Recht, die eigene Meinung frei zu bilden, ungehindert zu äussern und zu verbreiten. Als Meinung gilt jede Art von Stellungnahme, Wertung, Anschauung, Ausdruck von Gefühlen und die Wiedergabe von objektiven Informationen und Nachrichten. Meinungen können auch kritisch oder provozierend sein.

Der Staat darf weder Einzelpersonen eine bestimmte Meinung aufdrängen noch die Meinungsäusserung vorab zensieren. Die Meinungsfreiheit kann aber zum Schutz anderer eingeschränkt werden. Beschimpft beispielsweise jemand eine andere Person in den sozialen Medien, kann die betroffene Person über die Bestimmungen des Persönlichkeitsschutzes im Zivilgesetzbuch die Beseitigung der verletzenden Äusserung verlangen (Art. 28 ZGB) und allenfalls auch Strafanzeige wegen Beschimpfung einreichen (Art. 177 StGB) (→ **Fallbeispiel Cybermobbing 4.2** und → **Fallbeispiel Hasskommentare im Internet 4.1**).

Die Informationsfreiheit schützt das Beschaffen, Empfangen und Weitergeben von Informationen aus allgemein zugänglichen Quellen und ermöglicht damit überhaupt erst eine freie Meinungsbildung. Wenn Behörden wichtige Informationen auf ihren Websites zur Verfügung stellen, trägt dies zur Stärkung der Informationsfreiheit bei (→ **Fallbeispiel Barrierefreie Websites von Behörden 3.1**).

92 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 19 und 20.

C Medienfreiheit[93]

Art. 17 BV

Die Freiheit von Presse, Radio und Fernsehen sowie anderer Formen der öffentlichen fernmeldetechnischen Verbreitung von Darbietungen und Informationen ist gewährleistet.

Art. 10 EMRK, Art. 19 UNO-Zivilpakt

Die Medienfreiheit ist eng verbunden mit der Meinungs- und Informationsfreiheit. Sie erfasst sämtliche Aspekte der journalistischen Tätigkeit wie beispielsweise Recherche, Themenwahl und Verbreitung von journalistischen Arbeiten. Als Medienkommunikation, und damit von der Medienfreiheit geschützt, gelten Informationen, die von einer medienschaffenden Person an die Allgemeinheit übermittelt werden. Welches Mittel hierfür verwendet wird, spielt keine Rolle. Neben Presse, Radio und Fernsehen werden somit auch sämtliche digitalen Medien wie Online-Magazine von der Medienfreiheit erfasst.

Die Medienfreiheit schützt die ungestörte journalistische Tätigkeit, verbietet die Zensur und gewährleistet den Quellenschutz. Wie die Meinungsfreiheit kann auch die Medienfreiheit beispielsweise zum Schutz der Persönlichkeitsrechte von Drittpersonen eingeschränkt werden.

D Sprachenfreiheit[94]

Art. 18 BV

Die Sprachenfreiheit ist gewährleistet.

Jede Person hat das Recht, in einer frei gewählten Sprache zu kommunizieren. Dieses Recht umfasst alle Sprachen, Dialekte und auch die Gebärdensprache. Im privaten Bereich gilt die Sprachenfreiheit uneingeschränkt. Eingeschränkt ist sie im Kontakt mit Behörden: Hier müssen die jeweiligen Amtssprachen verwendet werden.

93 Zeller/Kiener, Kommentar zu Art. 17 BV, 2015.

94 Biaggini, Kommentar zu Art. 18 BV, 2017.

Übersetzungssoftware kann zur Stärkung der Sprachenfreiheit beitragen, sie allerdings auch einschränken. Dies ist zum Beispiel der Fall, wenn das Übersetzungsprogramm oder ein Spracherkennungsdienst bestimmte Dialekte oder Akzente nicht korrekt zu erkennen vermag.

E Kunstfreiheit[95]

Art. 21 BV
Die Freiheit der Kunst ist gewährleistet.
Art. 15 UNO-Sozialpakt

Die Kunstfreiheit schützt das Erschaffen und Präsentieren von Kunst in jeder denkbaren Form. Kunstschaffende haben grundsätzlich das Recht, unbeeinträchtigt von staatlichen Eingriffen tätig zu sein. Allerdings kann diese Freiheit zum Schutz der Persönlichkeit anderer Personen eingeschränkt werden. Die Kunstfreiheit vermittelt keinen Anspruch auf Förderung bestimmter Kunstprojekte, jedoch hat der Staat die Pflicht, für Rahmenbedingungen zu sorgen, die förderlich für die Kunstwelt sind.

Die Kunstfreiheit erfasst auch Kunstwerke, die mithilfe von digitalen Technologien erschaffen wurden. Diese Technologien können einerseits bei der Verbreitung, Archivierung oder wissenschaftlichen Analyse, andererseits zur Erschaffung von Kunstwerken eingesetzt werden. Immer häufiger dienen sie den Kunstschaffenden nicht mehr nur als Werkzeug oder Hilfsmittel, sondern kreieren teilweise «selbstständig» Kunst. So gibt es beispielsweise Bilder und Musikstücke, die durch künstliche Intelligenz gemalt bzw. komponiert wurden.[96] Dies wirft neue rechtliche Fragen im Zusammenhang mit der Urheberschaft der Werke auf.

Art. 15 Abs. 1 Bst. a UNO-Sozialpakt beinhaltet weiter das Recht jeder einzelnen Person auf Teilhabe am kulturellen Leben. Die digitale Archivierung und das Zugänglichmachen von Kunst über das Internet tragen erheblich zur Verwirklichung dieses Rechts bei.

95 Biaggini, Kommentar zu Art. 21 BV, 2017.
96 SBFI, Künstliche Intelligenz, 2019, S. 27.

2.3.5 Soziales und politisches Leben

A Recht auf Achtung des Familienlebens[97]

Art. 13 Abs. 1 BV
Jede Person hat Anspruch auf Achtung ihres (...) Familienlebens (...).
Art. 41 Abs. 1 Bst. c BV (Sozialziel), Art. 8 EMRK, Art. 17 UNO-Zivilpakt

Das Recht auf Achtung des Familienlebens schützt das familiäre Zusammenleben und die Kontakte zwischen den Familienmitgliedern. Als Familie gelten Ehepaare, gleichgeschlechtliche Paare, Konkubinatspaare oder Einzelpersonen mit ihren Kindern. Je nach Situation und Enge der Beziehung gehören auch weitere Verwandte wie Grosseltern dazu.

Digitale Kommunikationsmittel können im Zusammenhang mit der Einschränkung des Rechts auf Achtung des Familienlebens im Ausländerrecht eine Rolle spielen. Dies betrifft insbesondere Situationen, in welchen ein Familienmitglied aufgrund einer strafrechtlichen Verurteilung aus der Schweiz weggewiesen wird. In diesen Fällen geht das Bundesgericht davon aus, dass die Beziehung zu den minderjährigen, in der Schweiz lebenden Kindern grundsätzlich auch vom Ausland aus über Kurzbesuche und über moderne Kommunikationsmittel wie Videotelefonie gepflegt werden kann und daher das Recht auf Achtung des Familienlebens nicht verletzt sei.[98]

B Versammlungsfreiheit[99]

Art. 22 BV
Die Versammlungsfreiheit ist gewährleistet.
Art. 11 EMRK, Art. 21 UNO-Zivilpakt

Die Versammlungsfreiheit beinhaltet das Recht, ohne staatliche Beschränkung Versammlungen zu organisieren, an ihnen teilzunehmen oder ihnen fernzubleiben. Digitale Kommunikationsmittel können dabei zur Organisa-

97 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 13 Rz. 22 ff.
98 BGE 144 I 91 E. 5.1.
99 Biaggini, Kommentar zu Art. 22 BV, 2017.

tion herangezogen werden und haben das Potenzial, grosse Menschenmassen rasch zu mobilisieren. Eine grundrechtlich geschützte Versammlung liegt vor, wenn mehrere Personen sich in einem zeitlich begrenzten Rahmen treffen, um sich auszutauschen oder ihre Meinung zu äussern, etwa an Demonstrationen. Nicht von der Versammlungsfreiheit erfasst sind virtuelle Treffen (zum Beispiel Videokonferenzen, Chatrooms).[100] Diese werden aber unter anderem von der Meinungsfreiheit geschützt. Eingeschränkt werden kann die Versammlungsfreiheit im Rahmen von Art. 36 BV beispielsweise aus Sicherheitsgründen oder – wie während der Corona-Pandemie – zum Schutz der öffentlichen Gesundheit.

C Petitionsrecht[101]

Art. 33 BV

Jede Person hat das Recht, Petitionen an Behörden zu richten; es dürfen ihr daraus keine Nachteile erwachsen.

Gemäss dem Petitionsrecht darf sich jede Person in der Schweiz mit ihren Anliegen an die Behörden wenden. Das Recht umfasst unter anderem Bitten, Kritik und Vorschläge zu allen möglichen Themen. Petitionen können von einer einzelnen Person oder auch einer Gruppe eingereicht werden. Es ist möglich, die Unterschriften auch über Online-Portale zu sammeln.[102] Auf der einen Seite vereinfacht dies den Prozess und trägt zur Stärkung des Petitionsrechts bei. Auf der anderen Seite verzichten einzelne Personen allenfalls darauf, eine Online-Petition zu unterstützen, weil sie nicht möchten, dass ihr Name in diesem Zusammenhang über das Internet erfasst wird.

100 Errass, Kommentar zu Art. 22 BV, 2014, N. 16.

101 Tschannen, Kommentar zu Art. 33 BV, 2015.

102 Bundesrat, Bericht CiviTec, 2020, S. 23 ff.

D Politische Rechte[103]

Art. 34 BV

Die politischen Rechte sind gewährleistet.

Die Garantie der politischen Rechte schützt die freie Willensbildung und die unverfälschte Stimmabgabe.

Die politischen Rechte schützen das aktive und passive Wahlrecht bei Volkswahlen und die Teilnahme an Abstimmungen. Auch das Recht, gegen ein vom Parlament erlassenes Gesetz das Referendum zu ergreifen oder eine Volksinitiative einzureichen, gehört dazu. Zudem schützen die politischen Rechte die freie Willensbildung und die unverfälschte Stimmabgabe. Die Stimmbürgerinnen und Stimmbürger sollen ihren Entscheid frei treffen können. Der Staat hat von einer Beeinflussung im Vorfeld von Wahlen und Abstimmungen abzusehen.

Der Staat muss die freie Willensbildung der Stimmberechtigten auch vor einer übermässigen Beeinflussung durch Private schützen. Diese haben grundsätzlich das Recht, sich im Rahmen ihrer Meinungsäusserungsfreiheit zu anstehenden Wahlen und Abstimmungen zu äussern. Das Internet als Informationsquelle und Austauschforum vermag die Willensbildung somit grundsätzlich zu stärken, birgt aber auch Risiken: Unternehmen, Plattformen oder Parteien können mit ihren Algorithmen weitgehend bestimmen, welche Information eine einzelne Person erhält («Blasenbildung» → **Grundlagen Kapitel 1.2**), oder mithilfe von Microtargeting bestimmte Bevölkerungsgruppen gezielt ansprechen, um ihre Meinung zu beeinflussen (→ **Fallbeispiel Microtargeting im Abstimmungskampf 3.4**).[104] Wenn Abstimmende zu Vorlagen in schwerwiegender Weise getäuscht werden, müssen die zuständigen eidgenössischen, kantonalen oder kommunalen Behörden einschreiten und wenn möglich darauf hinweisen, dass die von privater Seite veröffentlichten Informationen falsch sind. In Ausnahmefällen muss die Abstimmung für ungültig erklärt werden.[105]

In den vergangenen Jahren wurde in der Schweiz mehrfach die Stimmabgabe über das Internet (E-Voting) getestet. Dabei stellt sich die Frage, wie

103 Biaggini, Kommentar zu Art. 34 BV, 2017.

104 EDÖB/Privatim, Datenschutzrecht Wahlen und Abstimmungen, 2019, S. 7.

105 BGE 135 I 292.

beim Übermitteln und Aufbewahren der Stimmdaten das Stimmgeheimnis gewahrt und die Manipulation der Abstimmungs- und Wahlergebnisse, beispielsweise durch Hacking, verhindert werden können.[106] Zudem wird aktuell das Sammeln von elektronischen Unterschriften, beispielsweise für eine Volksinitiative, diskutiert (E-Collecting).[107]

2.3.6 Arbeitsleben und Wirtschaft

A Eigentumsgarantie[108]

Art. 26 BV
Das Eigentum ist gewährleistet.
Art. 15 Abs. 1 Bst. c UNO-Sozialpakt

Die Eigentumsgarantie schützt neben dem Eigentum und den Nutzungsrechten an Grundstücken und beweglichen Sachen unter anderem auch sogenannte Immaterialgüterrechte wie zum Beispiel Patente und Urheberrechte. Der Schutz des geistigen Eigentums ist auf internationaler Ebene in Art. 15 Abs. 1 Bst. c UNO-Sozialpakt enthalten. Nicht von der Eigentumsgarantie erfasst werden persönliche Daten.[109] Die Eigentumsgarantie beinhaltet in erster Linie ein Abwehrrecht gegen staatliche Eingriffe. Wird Eigentum durch den Staat entzogen, muss die betroffene Person entschädigt werden. Darüber hinaus muss der Staat Private vor Verletzungen des Eigentums durch andere Private schützen.

Digitale Technologien betreffen das Recht auf Eigentum insbesondere im Bereich des Urheberrechts. Digitale Technologien ermöglichen eine fast unbegrenzte Vervielfältigung und Verbreitung von künstlerischen Werken wie Büchern, Fotografien, Filmen und Musik (unter anderem durch Online-Streaming) ohne die Zustimmung und finanzielle Entschädigung der jeweiligen Urheberinnen und Urheber. In der Schweiz enthält das am 1. April 2020 in

106 Markić, Elektronische Stimmabgabe, 2019, S. 133 f.
107 Bundesrat, Bericht CiviTec, 2020, S. 22 f.
108 Biaggini, Kommentar zu Art. 26 BV, 2017.
109 Weber/Thouvenin, Dateneigentum, 2018.

Kraft getretene revidierte Urheberrechtsgesetz als Reaktion auf die technologische Entwicklung neu zum Beispiel Bestimmungen gegen Pirateriepattformen (→ **Grundlagen Kapitel 2.2.7**).

B Wirtschaftsfreiheit[110]

> Art. 27 BV
>
> Die Wirtschaftsfreiheit ist gewährleistet.

Die Wirtschaftsfreiheit schützt jede selbstständige und unselbstständige Tätigkeit, mit der ein Gewinn oder Erwerb erzielt werden soll. Sie gewährleistet die freie Berufswahl, den freien Zugang zu einer Erwerbstätigkeit und deren freie Ausübung. Sie beinhaltet insbesondere das Recht, ohne staatliche Einmischung über die wichtigen Aspekte einer Geschäftstätigkeit wie die Organisation und Rechtsform und/oder die Auswahl der Mitarbeitenden und Vertragsparteien zu entscheiden. Zudem dürfen staatliche Massnahmen den Wettbewerb zwischen privaten Konkurrenten nicht verzerren, und Private werden untereinander mit der Kartellgesetzgebung vor wettbewerbsbeschränkenden Handlungen geschützt.

Die Wirtschaftsfreiheit erfasst somit grundsätzlich auch internetbasierte, dezentral organisierte Geschäftsmodelle (Plattformökonomie, DLT-/Blockchain-Ökonomie). Aktuell wird jedoch diskutiert, ob leistungsvermittelnde Plattformen (zum Beispiel Fahrdienste) zum Schutz der Leistungserbringenden stärker gesetzlich reguliert und die Dienstleistungserbringenden als Arbeitnehmende qualifiziert und geschützt werden müssten.[111] Dies würde die Wirtschaftsfreiheit zum Schutz der Arbeitnehmenden einschränken (→ **Fallbeispiel Internetbasierte Geschäftsmodelle 6.2**).

110 Biaggini, Kommentar zu Art. 27 BV, 2017.

111 Abegg/Bernauer, Airbnb, Uber & Co., 2018, S. 84.

C Koalitionsfreiheit[112]

Art. 28 BV

Die Arbeitnehmerinnen und Arbeitnehmer, die Arbeitgeberinnen und Arbeitgeber sowie ihre Organisationen haben das Recht, sich zum Schutz ihrer Interessen zusammenzuschliessen, Vereinigungen zu bilden und solchen beizutreten oder fernzubleiben.

Art. 11 EMRK, Art. 8 UNO-Sozialpakt, Art. 22 UNO-Zivilpakt

Die Koalitionsfreiheit beinhaltet das Recht aller Arbeitnehmenden, Arbeitgebenden und ihrer Organisationen (Gewerkschaften und Arbeitgeberverbände), sich ohne staatliche Einmischung zum Schutz ihrer Interessen zusammenzuschliessen und sich zu engagieren. Nebst dem Streikrecht beinhaltet das Koalitionsrecht unter anderem das Recht, sich an Kollektivverhandlungen zu beteiligen und mit Gesamtarbeitsverträgen Arbeitsbedingungen zu regeln.

Für Personen, deren Arbeit über internetbasierte Plattformen organisiert ist oder weitgehend im Homeoffice stattfindet, ist ein Austausch untereinander und mit Arbeitnehmendenverbänden schwieriger, was die Koalitionsfreiheit einschränken kann.[113]

D Arbeit zu angemessenen Bedingungen[114]

Art. 41 Abs. 1 Bst. d BV (Sozialziel)

Bund und Kantone setzen sich (...) dafür ein, dass Erwerbsfähige ihren Lebensunterhalt durch Arbeit zu angemessenen Bedingungen bestreiten können.

Art. 6 und 7 UNO-Sozialpakt

Der UNO-Sozialpakt beinhaltet ein Recht auf Arbeit (Art. 6) und ein Recht auf gerechte und günstige Arbeitsbedingungen (Art. 7). Inhaltlich in dieselbe Richtung zielt das Sozialziel der Bundesverfassung, wonach alle Erwerbsfähigen die Möglichkeit haben sollen, sich ihren Lebensunterhalt zu angemes-

112 Biaggini, Kommentar zu Art. 28 BV, 2017.

113 Bundesrat, Digitalisierung und Arbeitsbedingungen, 2017, S. 78 f.; SGB, Dossier Nr. 125 Digitalisierung, 2017, S. 24 f.

114 Biaggini, Kommentar zu Art. 41 BV, 2017.

senen Bedingungen erarbeiten zu können. Diese Bestimmungen vermitteln einzelnen Personen in der Schweiz kein gerichtlich einklagbares Recht auf eine Arbeitsstelle oder bestimmte Arbeitsbedingungen. Sie verpflichten aber die kantonalen und eidgenössischen Behörden, darauf hinzuarbeiten, dass möglichst alle Erwerbstätigen eine Arbeitsstelle finden (zum Beispiel mittels arbeitsmarktlicher Massnahmen für Stellensuchende) und auf dem Arbeitsmarkt faire Bedingungen herrschen (zum Beispiel durch Vorschriften im Arbeitsgesetz oder durch Allgemeinverbindlicherklärung von Arbeitsverträgen).

Die rasche technologische Entwicklung hat verschiedene Einflüsse auf die Arbeitnehmenden, ihre Rechte und ihren Schutz. So ist beispielsweise zu beobachten, dass älteren Arbeitnehmenden häufiger die für den Arbeitsmarkt notwendigen Informatikkenntnisse fehlen. Spezielle Ausbildungskurse in diesem Bereich sind deshalb besonders wichtige arbeitsmarktliche Massnahmen.[115]

Technologien wie GPS, Kameras oder Software können zur Überwachung der Arbeitnehmenden eingesetzt werden. Andere Technologien ersetzen teilweise die Arbeitsleistung von Menschen. So gab es beispielsweise erste Versuche, die Post per Roboter zuzustellen.[116] Durch die Digitalisierung werden oftmals auch das Arbeitstempo und die Kontrolle der Arbeitsschritte einzelner Arbeitnehmenden erhöht, was bei diesen zu erhöhtem Stress und damit zu gesundheitlichen Problemen führen kann. Die Digitalisierung hat aber auch zur Folge, dass verschiedene Tätigkeiten, die traditionellerweise von Angestellten ausgeführt wurden, neu organisiert werden. So werden beispielsweise Personen, die ihre Leistungen über Plattformen anbieten, in der Regel nicht als Arbeitnehmende, sondern als selbstständig Erwerbende behandelt. Dies hat zur Folge, dass sie nicht von den üblichen arbeitsrechtlichen Schutzbestimmungen (zum Beispiel Kündigungsfristen, Bezahlung bei Krankheit, maximale Arbeitsstunden) erfasst werden (→ **Fallbeispiel Internetbasierte Geschäftsmodelle 6.2**). Andere Tätigkeiten werden in Form des Crowdsourcing komplett ausgelagert. Oft erfolgen solche Tätigkeiten freiwillig (zum Beispiel vonseiten der Autorinnen und Autoren von Wikipedia).

115 Egger/Dreher & Partner, Arbeitsmarktliche Massnahmen, 2019, S. 11 und 66.

116 Tagesanzeiger, Lieferroboter, 2019.

Digitale Technologien können aber auch zur Sicherstellung von gewissen arbeitsrechtlichen Mindeststandards eingesetzt werden. So soll gemäss dem Bundesrat untersucht werden, wie der Einsatz von Blockchain (→ **Grundlagen Kapitel 1.8**) die Rückverfolgbarkeit im Goldhandel erleichtern und diese wiederum zur Einhaltung von Arbeitsstandards im Bergbau beitragen könnte.[117]

E Recht auf soziale Sicherheit[118]

Art. 41 Abs. 1 Bst. a BV (Sozialziel)

Bund und Kantone setzen sich (...) dafür ein, dass jede Person an der sozialen Sicherheit teilhat.

Art. 9 UNO-Sozialpakt

Das Recht auf soziale Sicherheit ist im UNO-Sozialpakt enthalten und als Sozialziel in der Bundesverfassung verankert. Es kann in der Schweiz gerichtlich nicht eingeklagt werden, verpflichtet aber den Bund und die Kantone, sich dafür einzusetzen, dass jede Person an der sozialen Sicherheit teilhaben kann. In der Schweiz wird diese insbesondere durch die verschiedenen Sozialversicherungen gewährleistet: Die Alters-, Hinterlassenen- und Invalidenvorsorge der ersten, zweiten und dritten Säule, die Arbeitslosen-, die Mutterschafts- sowie die Kranken- und Unfallversicherung und auf kantonaler Ebene die Sozialhilfe und die Familienzulagen.

In diesem Bereich kann Software zur Prüfung des Anspruchs, zur Berechnung der konkreten Leistung einer Sozialversicherung oder aber zum Aufspüren allfälliger missbräuchlicher Gesuche eingesetzt werden.[119] Dabei stellt sich die Frage, wie die verwendeten Algorithmen (→ **Grundlagen Kapitel 1.2**) ausgestaltet sein müssen, damit die entsprechenden Entscheide das Rechtsgleichheitsgebot, das Diskriminierungsverbot und das Recht auf soziale Sicherheit nicht verletzen.

117 Bundesrat, Goldhandel und Verletzung der Menschenrechte, 2018, S. 12.

118 Biaggini, Kommentar zu Art. 41 BV, 2017.

119 UNO-Sonderberichterstatter für Menschenrechte und extreme Armut, Digital Welfare State, 2019.

2.3.7 Wissen

A Anspruch auf Grundschulunterricht[120]

Art. 19 BV

Der Anspruch auf ausreichenden und unentgeltlichen Grundschulunterricht ist gewährleistet.

Art. 13 und 14 UNO-Sozialpakt

Jedes Kind in der Schweiz hat einen gerichtlich einklagbaren Anspruch auf ausreichenden und unentgeltlichen Grundschulunterricht und damit auf eine konkrete Leistung des Staats. Ausreichend ist der Grundschulunterricht dann, wenn er das Kind auf ein eigenständiges Leben in der heutigen Gesellschaft vorbereitet.

Das Recht auf Grundschulunterricht kann beispielsweise bei einem vorübergehenden disziplinarischen Schulausschluss oder bei vorübergehendem Fernunterricht wie im Fall der Schulschliessung während der Corona-Pandemie eingeschränkt werden. In diesen Situationen besteht für die Schulen die Möglichkeit, den Unterricht soweit als möglich auch über Online-Schulmaterialien oder per Videotelefonie weiterzuführen. Verletzt ist das Recht auf Grundschulunterricht dann, wenn der Unterricht derart eingeschränkt wird, dass die Chancengleichheit zwischen den Kindern nicht mehr gewährleistet ist, oder wenn aus gesellschaftlicher Sicht zentrale Inhalte nicht mehr vermittelt werden können (→ **Fallbeispiel Online-Unterricht in der Schule 5.1**).

120 Biaggini, Kommentar zu Art. 19 BV, 2017.

B Recht auf Bildung[121]

Art. 41 Abs. 1 Bst. f BV (Sozialziel)

Bund und Kantone setzen sich (...) dafür ein, dass Kinder und Jugendliche sowie Personen im erwerbsfähigen Alter sich nach ihren Fähigkeiten bilden, aus- und weiterbilden können.

Art. 13 UNO-Sozialpakt

Art. 13 UNO-Sozialpakt enthält das Recht auf Bildung. Dieses bezieht sich nicht nur auf Kinder, sondern auch auf Erwachsene. Inhaltlich zielt es in die gleiche Richtung wie das Sozialziel in Art. 41 Abs. 1 Bst. f BV, wonach Bund und Kantone sich dafür einsetzen, dass sich Kinder und Jugendliche sowie Personen im erwerbsfähigen Alter nach ihren Fähigkeiten aus- und weiterbilden können.

Im Unterschied zum Recht auf Grundschulunterricht kann das Recht auf Bildung in der Schweiz gerichtlich nicht eingeklagt werden, da es aus Sicht des Bundesgerichts zu allgemein gefasst ist, um daraus konkrete Ansprüche abzuleiten.[122] Der Staat hat aber die Pflicht, Gesetze zu erlassen und sonstige Massnahmen zu ergreifen, damit alle Kinder, Jugendlichen und Erwachsenen sich ausreichend (weiter-)bilden können.

Digitale Technologien beinhalten ein grosses Potenzial, das Recht auf Bildung zu fördern. So ermöglichen sie Lernenden und Lehrenden einen fast unbeschränkten Zugang zu Lehrmitteln wie digitalisierten Büchern, Videos und interaktiven Online-Programmen. MOOCS[123] schaffen zudem ein ortsunabhängiges und oft kostenloses Bildungsangebot. Die Digitalisierung kann aber auch die Chancengleichheit gefährden. Von digitalen Lerninhalten kann nur profitieren, wer Zugang zu Internet, entsprechenden Geräten, Software und Vorwissen hat. Personen, denen dieser Zugang aus finanziellen

121 Kägi-Diener, Kommentar zu Art. 19 BV, 2014, N. 4.

122 BGE 126 I 240 E. 2 f.

123 MOOCS (Massive Open Online Courses) sind Onlinekurse, die ohne Zugangsbeschränkungen von allen interessierten Personen absolviert werden können.

oder anderen Gründen verwehrt ist, können deshalb benachteiligt sein (sogenannter Digital Divide) (→ **Fallbeispiel Online-Unterricht in der Schule 5.1**).[124]

C Wissenschaftsfreiheit[125]

Art. 20 BV

Die Freiheit der wissenschaftlichen Lehre und Forschung ist gewährleistet.

Art. 15 Abs. 1 Bst. b UNO-Sozialpakt

Die Wissenschaftsfreiheit schützt die Forschung, die wissenschaftliche Lehre und die öffentliche Verbreitung von Forschungsergebnissen. Darunter fällt auch jede Forschung zu digitalen Technologien. Die Bestimmung beinhaltet das Recht, ohne staatliche Eingriffe wissenschaftlich tätig zu sein und von den Forschungsergebnissen anderer Kenntnis zu nehmen. Verboten ist die systematische inhaltliche Zensur von wissenschaftlichen Beiträgen. Die Wissenschaftsfreiheit vermittelt einzelnen Forschenden keinen direkt einklagbaren Anspruch auf bestimmte Förderbeiträge. Sie verpflichtet den Staat aber, die Wissenschaft durch Bereitstellung der notwendigen Infrastruktur zu fördern. Einschränkungen der Wissenschaftsfreiheit können sich beispielsweise durch die vorhandenen Fördermittel oder deren inhaltliche Fokussierung ergeben.

Art. 15 Abs. 1 Bst. b UNO-Sozialpakt enthält zudem das Recht jeder einzelnen Person, an den Errungenschaften des wissenschaftlichen Fortschritts teilzuhaben. Dieser Aspekt kann nicht gerichtlich eingeklagt werden. Dennoch ist der Staat verpflichtet, dafür zu sorgen, dass Forschungsergebnisse aufbewahrt und weiterverbreitet werden. Zudem sollen alle Menschen gleichberechtigt davon profitieren können. Ein Schritt in diese Richtung ist beispielsweise die staatliche Förderung von Open-Access-Publikationen (→ **Fallbeispiel Veröffentlichung einer wissenschaftlichen Studie 5.2**).[126]

---

124 UNO-Sonderberichterstatter zum Recht auf Bildung, Right to education in the digital age, 2016, Rz. 26 ff. und 31 ff.

125 Kiener/Kälin/Wyttenbach, Grundrechte, 2018, § 24.

126 UNO-Ausschuss für wirtschaftliche, soziale und kulturelle Rechte, General Comment Nr. 25, 2020, Rz. 4 ff. und 45 ff.

2.3.8 Kontakt mit Behörden und Gerichten

A Wahrung von Treu und Glauben[127]

Art. 9 BV

Jede Person hat Anspruch darauf, von staatlichen Organen (...) nach Treu und Glauben behandelt zu werden.

Der Anspruch auf Behandlung nach Treu und Glauben bedeutet, dass sich Einzelpersonen auf behördliche Informationen verlassen und ihr Handeln danach ausrichten dürfen. Hat eine Person im Vertrauen auf eine behördliche Auskunft eine Handlung vorgenommen und erweist sich die Auskunft später als falsch, darf sich dies für sie (finanziell) nicht nachteilig auswirken (Vertrauensschutz). Im Zusammenhang mit der Digitalisierung stellt sich beispielsweise die Frage, ob Tweets von Behördenmitgliedern verbindliche Aussagen sind, auf die sich einzelne Personen verlassen dürfen.[128]

B Recht auf ein faires Verfahren[129]

Art. 29, 29a, 30 und 32 BV

Jede Person hat das Recht auf ein faires Verfahren.

Art. 6 und 7 EMRK, Art. 14 und 15 UNO-Zivilpakt

Das Recht auf ein faires Verfahren umfasst zahlreiche Aspekte, die in verschiedenen Bestimmungen der Bundesverfassung geregelt sind. Jede Person, die an einem Gerichts- oder Verwaltungsverfahren beteiligt ist, hat einen Anspruch auf gleiche, gerechte und zügige Beurteilung ihres Anliegens. Sie hat zudem das Recht, sich im Verfahren zu äussern (rechtliches Gehör), sowie das Recht auf die Übernahme der Verfahrenskosten durch den Staat und auf einen unentgeltlichen Rechtsbeistand bei fehlenden Mitteln (Art. 29 BV). Weiter besteht ein Anspruch darauf, dass ein Rechtsstreit nicht nur durch eine Verwaltungsbehörde, sondern mindestens durch ein Gericht beurteilt wird (Art. 29a BV), das unabhängig und unparteiisch ist (Art. 30 BV).

127 Biaggini, Kommentar zu Art. 9 BV, 2017, N. 13 ff.

128 Langer, Staatliche Nutzung von Social Media-Plattformen, S. 954 ff.

129 Biaggini, Kommentar zu Art. 29, 29a, 30 und 32 BV, 2017.

Für Strafverfahren sieht die Bundesverfassung in Art. 32 zusätzliche Garantien vor: So gilt eine Person bis zu einem Schuldspruch als unschuldig. Ausserdem muss jede angeklagte Person unverzüglich über die erhobenen Vorwürfe informiert werden und die Möglichkeit haben, sich zu verteidigen.

Verschiedene Arten von Software werden in Strafverfahren eingesetzt. So existieren in der Schweiz Programme, die mithilfe von künstlicher Intelligenz das Vorkommen von Delikten räumlich voraussagen, sodass die Polizeipräsenz entsprechend geplant werden kann (Predictive Policing).[130] Weiter gibt es auch Software für die konkrete Bestimmung der Strafhöhe, die aber in der Schweiz nicht eingesetzt wird.[131] Im Zusammenhang mit solchen Programmen können sich Fragen bezüglich des Rechts auf ein faires Verfahren stellen: Wie wird beispielsweise das rechtliche Gehör gewahrt, wenn zentrale Aspekte für einen Entscheid über die Strafhöhe oder über eine bedingte Entlassung von einem Computerprogramm berechnet werden, dessen Algorithmus für die betroffene Person nicht nachvollziehbar ist? Wie wird überprüft, dass die Software unparteiisch und unvoreingenommen programmiert ist (→ **Fallbeispiel Automatisierter Behördenentscheid 3.2** und → **Fallbeispiel Automatisierte Risikoeinschätzung 3.3**)?

C Verfahrensgarantien bei Freiheitsentzug[132]

Art. 31 BV

Die Freiheit darf einer Person nur in den vom Gesetz selbst vorgeschriebenen Fällen und nur auf die im Gesetz vorgeschriebene Weise entzogen werden.

Art. 5 EMRK, Art. 9, 10 und 11 UNO-Zivilpakt

Die Bundesverfassung sieht in Bezug auf den Freiheitsentzug verschiedene Garantien vor. So darf dieser nur in klar vom Gesetz definierten Situationen erfolgen. Die betroffene Person hat das Recht, unverzüglich und in einer für sie verständlichen Sprache über die Gründe des Freiheitsentzugs und über

130 Simmler/Brunner/Schedler, Smart Criminal Justice, 2020, S. 14 ff.

131 Simmler/Brunner/Schedler, Smart Criminal Justice, 2020, S. 7 und 16.

132 Biaggini, Kommentar zu Art. 31 BV, 2017.

ihre Rechte informiert zu werden, und sie darf ihre nächsten Angehörigen informieren lassen. Zudem muss ein Gericht den Freiheitsentzug regelmässig überprüfen.

Von einem Freiheitsentzug spricht man, wenn eine Person über eine längere Zeit gegen oder ohne ihren Willen an einem Ort festgehalten wird. Dies trifft nicht nur auf Gefängnisstrafen, Haft oder die fürsorgerische Unterbringung in einer Klinik zu. Mit der Digitalisierung haben sich neue Formen des Freiheitsentzugs ergeben wie beispielsweise der Hausarrest, dessen Einhaltung mittels einer elektronischen Fussfessel überwacht wird (Electronic Monitoring).[133]

133 Wohlers, Kommentar zu Art. 79b StGB, 2020, N. 1 ff.

Teil II

Fallbeispiele

Dieser Teil zeigt anhand konkreter Beispiele, wie Grund- und Menschenrechte durch digitale Technologien gestärkt oder eingeschränkt werden. Anhand eines fiktiven Beispiels wird jeweils eine durch die Digitalisierung (mit)verursachte Problemlage dargestellt. Weiter werden die betroffenen Grund- und Menschenrechte erklärt, die für das Fallbeispiel relevanten juristischen Fragen erläutert und in einer kurzen Schlussfolgerung mögliche Handlungsoptionen aufgezeigt. Weiterführende Informationen und Hinweise auf die Praxis ergänzen die Fallbeispiele.[134]

Die Fallbeispiele sollen möglichst vielfältige Situationen des Alltags abbilden: Arbeit, Gesundheit, Kontakt mit Verwaltung, Justiz und Politik, Internetnutzung, Bildung und Forschung sowie Wirtschaft. Diskutiert werden sowohl staatliche Handlungen als auch Handlungen von Privatpersonen oder Unternehmen und ihr jeweiliger Einfluss auf die Grund- und Menschenrechte. Sämtliche Sachverhalte sind fiktiv. Sie wurden jedoch auf der Grundlage von Interviews mit Fachpersonen erarbeitet und lehnen sich teilweise an schweizerische Bundesgerichtsentscheide oder an Beispiele aus dem Ausland an.

Die Fallbeispiele konzentrieren sich auf die im jeweiligen Kontext zentralen Aspekte; sie beinhalten keine umfassende Analyse der Voraussetzungen für die Einschränkung der jeweiligen Grund- und Menschenrechte. Sie sind zudem zur besseren Verständlichkeit teilweise vereinfacht und können daher nicht als Rechtsratgeber dienen.

134 Der Aufbau der Fallbeispiele lehnt sich an folgende Publikationen an: Akkaya, Grund- und Menschenrechte in der Sozialhilfe, 2015; Akkaya/Belser/Egbuna-Joss/Jung-Blattmann, Grund- und Menschenrechte von Menschen mit Behinderungen, 2016; Egli/Egbuna-Joss/Ghielmini/Belser/Kaufmann, Grundrechte im Alter, 2019.

1 Arbeit

1.1 Algorithmus entscheidet über Bewerbungen

Frau A. bewirbt sich auf eine Stelle, wird jedoch nicht zum Vorstellungsgespräch eingeladen und erhält später eine Absage. Im Nachhinein erfährt sie, dass im Rahmen des Bewerbungsprozesses eine Software eingesetzt wurde, die von rund einhundert Bewerbungen nur zehn für ein Vorstellungsgespräch auswählte. Da die Software von einer externen Firma entwickelt wurde, kann in der Personalabteilung niemand Frau A. Auskunft darüber geben, weshalb sie nicht zu einem Vorstellungsgespräch eingeladen wurde.

Betroffene Grund- und Menschenrechte

– Diskriminierungsverbot

Rechtliche Fragestellung

Kann der Einsatz von Software zur Vorauswahl von Bewerbungen das Diskriminierungsverbot verletzen?

Rechtliche Beurteilung

Die eingesetzte Software basiert auf einem Algorithmus, der Datensätze nach bestimmten Merkmalen durchsucht und beurteilt. Konkret dienen die Merkmale von erfolgreichen Bewerbungsprofilen der letzten Jahre als Grundlage für die Beurteilungen der neu eingegangenen Dossiers. Diese Merkmale hat der Algorithmus selbstständig, das heisst ohne menschliches Zutun, aus einem Trainingsdatensatz aus früheren Bewerbungsdossiers abgeleitet (→ **Grundlagen Kapitel 1.3**).

Zur Beurteilung der Frage, ob das Diskriminierungsverbot verletzt wird, kommt es darauf an, ob sich Frau A. bei einem privaten Unternehmen oder bei einer staatlichen Institution bewirbt. Der Staat ist als Arbeitgeber an die Bundesverfassung und damit an das dort enthaltene Diskriminierungsver-

bot gebunden. Anders sieht es bei privaten Arbeitgebenden aus. Diese werden nicht direkt durch das Diskriminierungsverbot der Bundesverfassung verpflichtet. Für sie gelten aber die Bestimmungen des Arbeits- und des Obligationenrechts (→ **Grundlagen Kapitel 2.2.7**). Mit Art. 328 OR werden Arbeitgebende verpflichtet, die Persönlichkeit der Arbeitnehmenden zu achten und Massnahmen zu ihrem Schutz zu ergreifen. Das bedeutet unter anderem auch, dass Arbeitgebende Arbeitnehmende nicht diskriminieren dürfen. Sowohl bei staatlichen als auch bei privaten Arbeitgebenden gilt das Diskriminierungsverbot nicht nur in einem bestehenden Arbeitsverhältnis, sondern auch bereits im Bewerbungsverfahren.[135]

Der Einsatz eines Algorithmus zur Auswahl von geeigneten Bewerbungen könnte gegen das Diskriminierungsverbot verstossen, und zwar dann, wenn er sich dabei auf unzulässige Merkmale wie das Alter, das Geschlecht oder die Herkunft der sich bewerbenden Personen stützt. Ebenfalls möglich ist es, dass sich der Algorithmus zwar auf ein sachlich zulässiges Unterscheidungsmerkmal stützt, in der Praxis aber dennoch zu einer Benachteiligung von Personen aufgrund ihres Alters, Geschlechts etc. führt. Wenn also der Algorithmus beispielsweise wie im vorliegenden Fall nach Kriterien ähnlicher Profile wie die erfolgreichen Bewerbungen der letzten paar Jahre filtert und in den vergangenen Jahren mehrheitlich Männer eingestellt wurden, benachteiligt der Algorithmus Bewerberinnen.[136]

Damit eine Verletzung des Diskriminierungsverbots vorliegt, wäre zudem erforderlich, dass es für den Ausschluss oder die Auswahl bestimmter Personen keine besondere Rechtfertigung gibt. Zulässig wäre beispielsweise, bestimmte Bewerbende aufgrund eines Merkmals auszuschliessen, das für die Arbeitsstelle zwingend notwendig ist. So können Kirchen beispielsweise verlangen, dass ihre Arbeitnehmenden einer bestimmten Religion angehören.

Schlussfolgerungen und Empfehlungen

Sollte die Bewerbung von Frau A. aufgrund ihres Geschlechts aussortiert worden sein, hat sie zwar keinen Anspruch auf Einstellung, jedoch auf eine

135 Pellascio, Kommentar zu Art. 328 OR, 2016, N. 9 und 16.

136 Wildhaber, Robotik am Arbeitsplatz, 2017, S. 215.

Entschädigung (Art. 5 Abs. 2 Gleichstellungsgesetz). Gegen einen staatlichen Arbeitgeber könnte sie diese in einem Verwaltungsverfahren, gegen eine private Arbeitgeberin in einem zivilrechtlichen Verfahren einklagen.

Dieser Anspruch wäre aber in der Praxis nur schwer durchsetzbar. Für alle Beteiligten ist aus einer einzelnen Stellenabsage kaum zu erkennen, ob der eingesetzte Algorithmus ein diskriminierendes Element enthält. Im vorliegenden Fall konnten nicht einmal die Mitarbeitenden der Personalabteilung nachvollziehen, nach welchen Kriterien der Algorithmus die Bewerbungen beurteilt hatte. Im Endeffekt lässt sich damit nicht feststellen, aufgrund welcher Merkmale entschieden wurde und ob es für die allenfalls erfolgte Benachteiligung einen Rechtfertigungsgrund gab.

Ob eine Diskriminierung vorliegt oder nicht, hängt, wie bereits ausgeführt, davon ab, welche Merkmale einer sich bewerbenden Person für eine Software einstellungsrelevant sind. Entscheidend ist somit, welche Merkmale überhaupt im Laufe des Auswahlprozesses herangezogen werden dürfen. Um eine direkte oder indirekte Diskriminierung zu vermeiden, ist es daher wichtig, dass das Programm vor dem Einsatz auf verschiedene Diskriminierungskriterien wie beispielsweise das Geschlecht überprüft und getestet wird. Der Datensatz, mit dem ein solcher Algorithmus trainiert wird, muss eine möglichst grosse Vielfalt erfolgreicher Bewerbenden abdecken. Der Algorithmus darf zudem Bewerbungen nicht aufgrund von Merkmalen aussortieren, die keinen Zusammenhang mit der beruflichen Eignung aufweisen. Auch muss transparent sein, nach welchen Merkmalen der Algorithmus programmiert wurde.[137] Zudem sollte das vom Algorithmus produzierte Ergebnis von einem Menschen plausibilisiert und auf seine Grund- und Menschenrechtskonformität hin überprüft werden.

Weiterführende Hinweise

In der Schweiz setzen Personalabteilungen Software zur Beurteilung von Bewerbungen ein.[138] Das vorliegende Fallbeispiel ist jedoch einem ausländischen Fall nachgebildet, in dem Amazon eine Software für Bewerbungsverfahren testete und schliesslich wieder einstellte. Der Algorithmus wurde auf Grundlage der Bewerbungsdaten von bereits eingestellten Mitarbeitenden

137 Söbbing, Künstliche Intelligenz im HR-Recruiting-Prozess, 2018, S. 65.

138 Glatthaar, Robot Recruiting, 2020, S. 43 ff.; Schafheitle/Weibel, HR Tech Survey, 2020.

mittels maschinellen Lernens entwickelt. Da in der Vergangenheit hauptsächlich Männer angestellt worden waren, nahm der Algorithmus an, Männer seien die bevorzugte Zielgruppe für die Stellenbesetzung. Das Ergebnis war, dass der Algorithmus das männliche Geschlecht als ein massgebendes Einstellungskriterium identifizierte und deshalb Bewerbungen von Männern gegenüber denen von Frauen bevorzugte.[139]

139 Dastin, AI recruiting tool, 2018.

1.2 Bewerbungen und soziale Medien

Herr B. bewirbt sich bei einem Unternehmen, erhält aber eine Absage. Eine Mitarbeiterin der Personalabteilung hat ihn im Verlauf des Bewerbungsverfahrens aus Neugier auf einigen Social-Media-Plattformen gesucht. Dabei sind unter anderem Bilder aus dem letzten Urlaub aufgetaucht, die Herrn B. beim enthemmten Feiern auf einer Party zeigen.

Betroffene Grund- und Menschenrechte

- Recht auf Datenschutz
- Recht auf Privatsphäre

Rechtliche Fragestellung

Dürfen im Rahmen eines Bewerbungsverfahrens soziale Medien nach den Bewerbenden durchsucht werden? Dürfen die daraus gewonnenen Informationen in den Entscheidungsprozess der Arbeitgebenden einfliessen?

Rechtliche Beurteilung

Ein problematischer Aspekt des Internets ist, dass einmal veröffentlichte Informationen grundsätzlich allen anderen Nutzenden zugänglich sind und nur schwer wieder gelöscht werden können. So ist die Gefahr gross, dass die Informationen auch an Personen gelangen, für die sie überhaupt nicht gedacht waren, wie zum Beispiel potenzielle Arbeitgebende. Soziale Netzwerke kennen zwar die Möglichkeit, gewisse Informationen und Bilder nur für ausgewählte Personengruppen zugänglich zu machen. Diese Option wird aber von vielen Nutzenden nicht genutzt.

Jede Person hat grundsätzlich das Recht, selber darüber zu bestimmen, wie Informationen über sie verwendet werden. Sie kann entscheiden, Informationen über ihr Privatleben für sich zu behalten und diese nicht mit dem Staat und anderen Personen zu teilen. Sucht eine Mitarbeitende der Personalabteilung auf sozialen Medien nach privaten Fotos von und Informationen über Herrn B., könnte dies deshalb gegen dessen Recht auf Datenschutz und das Recht auf Privatsphäre verstossen.

Zwar ist die potenzielle Arbeitgeberin als privates Unternehmen im Unterschied zum Staat nicht direkt an die Grund- und Menschenrechte gebunden. Der Schutz der Privatsphäre von Arbeitnehmenden wird aber durch Bestimmungen im Arbeitsgesetz und im Obligationenrecht garantiert (→ **Grundlagen Kapitel 2.2.7**) und zwar nach herrschender Meinung bereits im Bewerbungsverfahren.[140] Arbeitgebende dürfen demnach Informationen nur suchen, einsehen und berücksichtigen, wenn diese die Eignung der Arbeitnehmenden für das Arbeitsverhältnis betreffen.

Dieser Grundsatz lässt sich auch auf die Recherche des Unternehmens in sozialen Medien übertragen. Rein private Postings lassen keinen Rückschluss auf die berufliche Eignung zu. Vielmehr geht es dabei um Informationen, die für die Verbreitung im Privatumfeld gedacht sind. Dieses Verwertungsverbot für den Bewerbungsprozess gilt auch bezüglich Informationen, die mit einer allgemeinen Google-Suche aufzufinden sind.[141]

Anders zu beurteilen sind Daten, die von Arbeitsuchenden auf Business-Netzwerken wie zum Beispiel LinkedIn veröffentlicht wurden. Hier dient die Publikation dem beruflichen Fortkommen. Deshalb dürfen potenzielle Arbeitgebende diese Informationen in ihre Beurteilung einbeziehen und aufgrund des geschäftlichen Kontextes Rückschlüsse auf die Eignung der Bewerbenden ziehen.[142]

Schlussfolgerungen und Empfehlungen

Wurde ein Foto auf einem privat genutzten Account veröffentlicht, darf die Personalabteilung des Unternehmens das Foto während des Bewerbungsverfahrens nicht berücksichtigen. Etwas anderes gilt im Falle einer Veröffentlichung auf einem Business-Netzwerk.

Möchte Herr B. verhindern, dass fremde Personen oder potenzielle Arbeitgebende seine Accounts auf den sozialen Medien betrachten, muss er in den Einstellungen anpassen, was öffentlich sichtbar ist und was nicht. Zudem ist es ihm auch möglich, Fotos, die er selber hochgeladen hat, wieder zu lö-

140 Pellascio, Kommentar zu Art. 328b, 2016, N. 4.

141 Egli, Soziale Netzwerke und Arbeitsverhältnis, 2011, Rz. 79.

142 Egli, Soziale Netzwerke und Arbeitsverhältnisse, 2011, Rz. 71 f.; Streiff/von Kaenel/Rudolph, Arbeitsvertrag, 2012, Art. 328b N. 9.

schen. Bei Fotos, die von einer anderen Person hochgeladen wurden, kann er in einem ersten Schritt diese Person um Löschung des Fotos bitten. Ist dies nicht erfolgreich, kommt eine Konsultierung der Plattformbetreiberin in Betracht. Führt auch dies nicht zum gewünschten Ziel, kann nötigenfalls beim Zivilgericht auf Löschung der Fotos geklagt werden.

Weiterführende Hinweise

Das revidierte DSG beinhaltet neu ausdrücklich das Recht auf Löschung von Daten, auch bekannt als «Recht auf Vergessenwerden» (Art. 32 Abs. 2 RevDSG). Es bedeutet, dass Informationen über Personen nicht für immer im Internet verfügbar resp. auffindbar sein sollen. Die betroffene Person soll die Möglichkeit haben, deren Löschung verlangen zu können, wenn dem keine überwiegenden Interessen entgegenstehen.[143]

Das BAKOM hat einen Leitfaden veröffentlicht zur Frage, wie einzelne Personen die Löschung von Kommentaren und Fotos auf sozialen Medien verlangen können.[144]

143 Bundesrat, Botschaft Totalrevision DSG, 2017, S. 7077.

144 BAKOM, Social Media Plattformen, 2013.

1.3 Überwachung am Arbeitsplatz

Frau C. ist Liftmonteurin. Für ihre Tätigkeit im Aussendienst benutzt sie ein Firmenfahrzeug, welches vor einiger Zeit mit einem GPS ausgestattet wurde. Ihr Ehemann, Herr C., ist Betriebswirtschafter und arbeitet teilweise im Büro, teilweise im Homeoffice. Für seine Arbeit von zu Hause aus wird ihm von der Arbeitgeberin ein Laptop zur Verfügung gestellt.

Aufgrund der mit dem GPS möglichen Überwachung ihrer Fahrzeiten und -wege fühlt sich Frau C. inzwischen unwohl und möchte dieses aus ihrem Dienstfahrzeug entfernt haben. Herr C. wiederum fragt sich, ob es problematisch ist, dass er während der Arbeitszeit teilweise private E-Mails von seinem Büro-Laptop verschickt.

Betroffene Grund- und Menschenrechte

- Recht auf Privatsphäre
- Bewegungsfreiheit
- Recht auf Gesundheit

Rechtliche Fragestellung

Unter welchen Voraussetzungen ist der Einsatz von Überwachungs- und Kontrolltechnologien am Arbeitsplatz zulässig? Können sich Arbeitnehmende gegen die Überwachung zur Wehr setzen?

Rechtliche Beurteilung

Es existieren zahlreiche Technologien, die zur Überwachung oder Kontrolle von Vorgängen am Arbeitsplatz einsetzbar sind: u.a. Videoüberwachung, Ortungssysteme wie das GPS bei Frau C. oder Wearables (zum Beispiel Smartwatch). Auch können mit entsprechender Software die Internetaktivitäten, wie jene von Herrn C., überwacht werden. Der Einsatz solcher Technologien kann der Sicherheit der Arbeitnehmenden oder von Drittpersonen, dem Gesundheitsschutz oder der Sicherung von wichtigen betrieblichen Gütern (zum Beispiel in einem Schmuckladen) dienen. Möglich ist aber auch eine Kontrolle der Arbeitnehmenden und ihres Verhaltens, beispielsweise zur Optimierung der Arbeitsleistung und betrieblichen Abläufe.

Überwachen oder kontrollieren Arbeitgebende ihre Angestellten mittels Technologien, werden damit Daten über diese und deren Verhalten am Arbeitsplatz erhoben, gesammelt und allenfalls ausgewertet.[145] Dies ist ein Eingriff in das Recht auf Privatsphäre. Weiter ist denkbar, dass Arbeitnehmende, weil sie um die Überwachung wissen, sich während ihrer Arbeitszeit nicht mehr frei bewegen und damit in ihrer Bewegungsfreiheit eingeschränkt sind. Eine ständige Überwachung kann zudem zu gesundheitlichen Problemen führen und damit das Recht auf Gesundheit beeinträchtigen.[146]

Anders als staatliche Behörden sind private Arbeitgebende nicht direkt an die Grund- und Menschenrechte gebunden. Jedoch schützen Bestimmungen des Datenschutzgesetzes, des Arbeitsgesetzes und des Obligationenrechts vor Grund- und Menschenrechtsbeeinträchtigungen durch Überwachung im privatrechtlichen Arbeitsverhältnis (→ **Grundlagen Kapitel 2.2.7**). Diese Bestimmungen legen fest, unter welchen Voraussetzungen Überwachungstechnologien eingesetzt und die damit erhobenen Daten verwendet werden dürfen.

Wie bereits im Fallbeispiel zu Bewerbungen und sozialen Medien spielt die arbeitsrechtliche Schutzbestimmung von Art. 328b OR eine wichtige Rolle: Demnach dürfen Arbeitgebende nur solche Informationen über ihre Mitarbeitenden sammeln und auswerten, die in einem engen Zusammenhang mit dem Arbeitsverhältnis stehen. Zu denken ist beispielsweise an Daten zu den geleisteten Arbeitsstunden und zur Qualität der Arbeitsleistung.[147] Weiter sind die Grundsätze des Datenschutzgesetzes zu beachten. Demnach ist eine unrechtmässige Erhebung von Daten verboten, und deren Löschung muss geregelt sein.[148] Zudem ist der Einsatz von Überwachungs- und Kontrollsystemen unzulässig, wenn deren einziger Zweck ist, das Verhalten der Arbeitnehmenden am Arbeitsplatz zu überwachen (Art. 26 Verordnung 3 zum Arbeitsgesetz). Aus anderen Gründen (zum Beispiel Sicherheit des Personals, Kontrolle der geleisteten Arbeit) dürfen sie nur so eingesetzt werden, dass sie die Gesundheit und Bewegungsfreiheit der Arbeitnehmenden nicht beeinträchtigen.

145 Pärli, Kommentar DSG, 2015, Art. 328b OR N. 11.
146 SECO, Wegleitung zur ArGV 3 und 4, 2020, S. 326–1.
147 Streiff/von Kaenel/Rudolph, Arbeitsvertrag, 2012, Art. 328b OR N. 6.
148 Pärli, Kommentar DSG, 2015, Art. 328b OR N. 15 f.

Die Überwachung mittels Technologien ist gemäss aktueller Praxis dann zulässig, wenn ein klar überwiegendes Interesse der Arbeitgeberin (zum Beispiel Aufdeckung von Missbräuchen) vorliegt und das Überwachungssystem verhältnismässig eingesetzt wird. So soll die Überwachung zeitlich und räumlich so weit als möglich begrenzt werden. Zudem müssen Arbeitnehmende über den Einsatz der Technologie vorab informiert und bei deren Planung und Umsetzung mit einbezogen werden.[149]

Das GPS im Dienstfahrzeug von Frau C. dokumentiert die Fahrzeugbewegungen und gibt somit Auskunft über Fahrzeiten und Routen. Diese Daten lassen wiederum gewisse Rückschlüsse auf die Dauer ihrer Arbeitseinsätze und allfällige Pausen zu. Aus Sicht der Arbeitgebenden können mit diesen Informationen unter anderem die Arbeitseinsätze besser geplant, die Arbeitszeiten der Mitarbeitenden kontrolliert und damit auch Missbräuche verhindert werden. Nach Auffassung des Bundesgerichts sind dies legitime Gründe für den Einsatz eines GPS in einem Dienstfahrzeug. Die Überwachung darf aber nicht in Echtzeit und nur bei solchen Fahrzeugen erfolgen, die von den Mitarbeitenden nicht auch für private Fahrten benutzt werden. Sind diese Voraussetzungen erfüllt, ist der Einsatz des GPS grundsätzlich zulässig. Zusätzlich ist erforderlich, dass Frau C. vorab über den Einsatz informiert wurde, sie ihre Zustimmung gegeben hat und sie nach Möglichkeit bei der Planung mit einbezogen wurde.[150]

Bezüglich des Anliegens von Herrn C. lässt sich rechtlich Folgendes festhalten: Arbeitgebende legen – oft in einem Nutzungsreglement – fest, ob und in welchem Umfang die Mitarbeitenden während der Arbeitszeit private Nachrichten von einem Bürocomputer verschicken oder zu privaten Zwecken das Internet benutzen dürfen. Randdaten (→ **Grundlagen Kapitel 1.1**) von während der Arbeitszeit verschickten E-Mails dürfen nur anonym ausgewertet werden. Besteht aber ein begründeter Verdacht, dass Herr C. gegen das Nutzungsreglement verstösst, darf seine Arbeitgeberin gezielt verdächtige E-Mails auswerten.[151]

149 Meier-Gubser, Mitarbeiterüberwachung, 2020, S. 286 f.

150 Zu den Voraussetzungen für den Einsatz eines GPS in einem Dienstfahrzeug: BGE 130 II 425.

151 Hafner, Auswertung E-Mails, 2018, S. 1331 ff.

Schlussfolgerungen und Empfehlungen

Die Überwachung der Fahrten von Frau C. tangiert zwar verschiedene Grund- und Menschenrechte, dürfte aber im Licht der aktuellen Praxis grundsätzlich zulässig sein. Jedoch ist durch die vorgesetzte Person darauf zu achten, dass das Unwohlsein, das Frau C. aufgrund der Überwachung empfindet, ihre psychische Gesundheit nicht belastet. In Fällen, in denen die Voraussetzungen für die rechtmässige Überwachung nicht gegeben sind, kann das kantonale Arbeitsinspektorat konsultiert werden. Dieses ist für die Kontrolle der Vorschriften des Arbeitsgesetzes zuständig.

Ob und in welchem Umfang Herr C. von seinem Bürocomputer private E-Mails verschicken darf, hängt davon ab, was seine Arbeitgeberin im Nutzungsreglement festgelegt hat.

Weiterführende Hinweise

Das Fallbeispiel zu Frau C. ist dem Bundesgerichtsentscheid BGE 130 II 425 nachgebildet. Die Voraussetzungen für den Einsatz von Überwachungs- und Kontrolltechnologien am Arbeitsplatz sind in der Wegleitung zu den Verordnungen 3 und 4 zum Arbeitsgesetz des SECO erklärt.[152] Erläuterungen zur Überwachung von E-Mails am Arbeitsplatz finden sich im Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz für die Privatwirtschaft des EDÖB.[153]

152 SECO, Wegleitung zur ArGV 3 und 4, 2020.

153 EDÖB, Leitfaden Internet- und E-Mailüberwachung am Arbeitsplatz (Privatwirtschaft), 2013.

2 Gesundheit

2.1 Pflegeroboter

Herr D. leidet an fortgeschrittener Demenz und lebt in einem von seiner Wohngemeinde betriebenen Pflegeheim. Seine Tochter sorgt sich um sein Wohlergehen, da bei der Betreuung und Pflege verschiedene Roboter eingesetzt werden. Besorgniserregend findet sie insbesondere, dass ihr Vater teilweise mit der Roboter-Robbe Rosa unterhalten wird. Dabei handelt es sich um ein mit Sensoren ausgestattetes Kuscheltier, das Herrn D. soziale Interaktion vorspielt.

Betroffene Grund- und Menschenrechte

- Menschenwürde
- Verbot der unmenschlichen oder erniedrigenden Behandlung
- Recht auf Arbeit zu angemessenen Bedingungen

Rechtliche Fragestellung

Pflegeroboter können zur Unterstützung der Pflegebedürftigen (zum Beispiel Bringen und Holen von Gegenständen), zur Unterstützung des Pflegepersonals (zum Beispiel Umlagern) und wie im Fall der Roboter-Robbe Rosa zur Unterhaltung der Pflegebedürftigen eingesetzt werden (→ **Grundlagen Kapitel 1.7**). Verletzt die Pflege bzw. Unterhaltung von Herrn D. mittels Pflegeroboter die Menschenwürde oder das Verbot der unmenschlichen oder erniedrigenden Behandlung? Was könnten Herr D. bzw. seine Tochter unternehmen, wenn sie Bedenken bezüglich des Einsatzes von Pflegerobotern haben? Welchen Einfluss haben die Pflegeroboter auf das Recht auf Arbeit zu angemessenen Bedingungen des Pflegepersonals?

Rechtliche Beurteilung

Gemäss dem Grundsatz der Menschenwürde muss jeder Mensch jederzeit als wertvolles Individuum und mit Würde behandelt werden. Gerade bei einer Person mit Demenz ist nicht immer klar, ob sie erkennt, dass es sich

bei der Roboter-Robbe Rosa um eine Maschine und nicht um ein echtes Tier handelt. Der dementen Person wird somit die Interaktion mit einem Lebewesen vorgetäuscht, was unter dem Gesichtspunkt der Menschenwürde problematisch scheint.

Ob beim Einsatz von Service- oder Assistenzrobotern eine Verletzung der Menschenwürde vorliegt, kann mithilfe der sogenannten Objektformel beurteilt werden: Demnach ist die Menschenwürde verletzt, wenn Menschen zu Objekten herabgewürdigt werden. Gerade Handlungen wie das Tragen, Waschen oder Umlagern gehen für gewöhnlich mit physischem und emotionalem Kontakt zwischen dem Pflegepersonal und den pflegebedürftigen Personen einher. Durch den Einsatz von Pflegerobotern entfällt dieser Kontakt teilweise, sodass die Pflege zunehmend nur noch einen «Wartungsvorgang» darstellt, ähnlich wie bei Gegenständen. Das Grundbedürfnis des menschlichen Wesens nach authentischen Emotionen, sozialen Kontakten und menschlicher Berührung würde durch den Einsatz der Pflegeroboter nicht mehr erfüllt. Auch dies könnte eine Verletzung der Menschenwürde darstellen.[154]

Ob der Einsatz von Pflegerobotern das Verbot der unmenschlichen oder erniedrigenden Behandlung verletzt, hängt in erster Linie davon ab, ob einer Person während einer gewissen Dauer körperliches oder psychisches Leid von gewisser Intensität zugefügt wird. Bei regelkonformer Anwendung von Assistenz- und Servicerobotern ist davon auszugehen, dass dies nicht der Fall ist. Verschiedene Studien zum Einsatz der Kuschelrobbe haben zudem ergeben, dass diese von den Pflegebedürftigen nur selten abgelehnt wurde und diese Ablehnung auch nicht mit psychischem Leiden einherging.[155]

In Bezug auf das Pflegepersonal könnten die Pflegeroboter unterstützend eingesetzt werden, sodass mehr Zeit für die Pflege und die persönlichen Kontakte mit den Bewohnenden bliebe. Die Pflege würde somit einen qualitativen Mehrwert erfahren, und die Lebensqualität der Bewohnenden würde steigen. Auch ist es möglich, dass der Einsatz von Assistenzrobotern das Pflegepersonal von schwerer körperlicher Arbeit entlastet. Bei diesen Über-

154 Kreis, Pflegeroboter, 2018, S. 222 ff.

155 Baisch/Kolling/Rühl et al., Emotionale Roboter, 2018.

legungen darf man allerdings nicht vergessen, dass sich viele Pflegende bei dem Gedanken unwohl fühlen, ihre Arbeit in Zukunft von Robotern ausführen zu lassen.

Schlussfolgerungen und Empfehlungen

Pflegeroboter verletzen die Menschenwürde dann, wenn ihr Einsatz darauf abzielt, menschliche Pflegeleistungen mehrheitlich zu ersetzen, sodass die sozialen Kontakte zu einer pflegenden Person praktisch entfallen. Dies wäre beispielsweise dann der Fall, wenn Unterhaltungsroboter anstelle von menschlicher Zuwendung eingesetzt würden. Soziale Kontakte und das damit verbundene Recht, authentische menschliche Gefühle und Kontakte zu erfahren, gehören zum Menschsein. Die verschiedenen Roboter können hingegen unterstützend eingesetzt werden und unter Aufsicht einer Pflegeperson, die den erforderlichen sozialen oder physischen Kontakt gewährleistet. So dürfte die Roboter-Robbe beispielsweise einer zu pflegenden Person nicht einfach überlassen werden. Vielmehr müsste Herr D. während der Nutzung des Unterhaltungsroboters begleitet und unterstützt werden. Auch dürfte ihm nicht vorgetäuscht werden, es handle sich um ein echtes Tier.

Wenn sich die Tochter von Herrn D. Sorgen über das Wohlergehen ihres Vaters macht, kann sie ihre Bedenken bezüglich des Einsatzes von Pflegerobotern in einem ersten Schritt mit dem Personal und der Institutionsleitung besprechen. In verschiedenen Kantonen existieren zudem Ombudsstellen für Konflikte im Heimkontext.

Weiterführende Hinweise

Das vorliegende Beispiel ist angelehnt an den in Japan entwickelten Unterhaltungsroboter «Paro», der in der Betreuung von Menschen mit Demenz eingesetzt wird.[156] Auch in der Schweiz wird der Einsatz von solchen Pflegerobotern getestet.[157]

156 Ammann, Robotergestützte Pflege, 2019.

157 SRF, Soziale Roboter in Altersheimen, 2020.

2.2 Künstliche Intelligenz und Big Data in der Diagnostik

Frau E. hat schon seit längerer Zeit eine auffällige Hautverfärbung am Oberarm. Sie konsultiert das Universitätsspital, das von der betroffenen Stelle Aufnahmen macht. Diese werden von einer Software analysiert, welche ermitteln soll, ob es sich bei der Verfärbung um Hautkrebs handelt. Der Befund ist negativ. Die Software ist auf dem neuesten Stand der Forschung, das ganze Vorgehen ist in medizinischen Fachkreisen allgemein anerkannt. Einige Wochen später wird bei Frau E. jedoch durch eine andere Dermatologin Hautkrebs diagnostiziert. Die Fehldiagnose der Software hing damit zusammen, dass deren Trainingssatz allein aus Bildern von Hautkrebs bei Personen mit helleren Hauttönen bestand, während die Haut von Frau E. einen dunkleren Ton aufweist. Deshalb konnte die Software den Hautkrebs nicht erkennen.

Betroffene Grund- und Menschenrechte

- Recht auf Gesundheit
- Diskriminierungsverbot

Rechtliche Fragestellung

Wie ist der Einsatz von Big Data und künstlicher Intelligenz in der Diagnostik aus grund- und menschenrechtlicher Sicht zu beurteilen?

Rechtliche Beurteilung

Das Recht auf Gesundheit verpflichtet den Staat dazu, eine bestmögliche medizinische Versorgung zu gewährleisten. Es wird unter anderem dadurch verwirklicht, dass Behandlungen immer nach dem neuesten anerkannten Stand der Forschung und Technik erfolgen müssen.[158] Dies gilt auch für den Einsatz von Software zur Diagnose einer Krankheit. Diese kann Ärztinnen und Ärzte in ihrer täglichen Diagnosearbeit unterstützen. Die Software kann eine grosse Menge an Daten aus den unterschiedlichsten Quellen auswerten und benötigt hierfür nur den Bruchteil der Zeit, die das medizinische Perso-

158 Widmer Lüchinger, Digitale Innovation und ärztliche Sorgfalt, 2019, S. 78 f.

nal bräuchte, um die Daten von Hand bzw. Auge zu analysieren. Zudem arbeiten Algorithmen häufig genauer als Menschen.[159] Das Recht auf Gesundheit wird durch den Einsatz der Software somit grundsätzlich gestärkt.

Der Einsatz von KI kann jedoch auch das Diskriminierungsverbot verletzen. Die Gefahr der Diskriminierung besteht, wenn beim Entwickeln und Trainieren eines Algorithmus Datensätze verwendet werden, in denen gewisse Personengruppen nicht ausreichend vertreten sind. Dies kann dazu führen, dass die Software Krankheiten bei Individuen der betroffenen Personengruppen systematisch nicht erkennt bzw. die Symptome oder Ausprägungen nicht der richtigen Krankheit zuordnet. Dieses Problem ergibt sich auch im vorliegenden Fallbeispiel: Weil die hier eingesetzte Software mit einem Datensatz trainiert wurde, in dem weisse Menschen dominieren, ist sie nicht imstande, Hautkrebs bei Personen mit dunklerer Hautfarbe zu erkennen.

Schlussfolgerungen und Empfehlungen

Es könnte ein Verstoss gegen das Diskriminierungsverbot vorliegen. Damit die Software die Diagnose unabhängig von der Hautfarbe vorschlagen kann, müssen im Trainingsdatensatz die verschiedenen Hautfarben in gleicher Zahl vertreten und die Hautkrebsbilder gleichmässig auf die verschiedenen Hauttypen verteilt sein.[160]

Weiterführende Hinweise

Auch in der Schweiz wird in der Praxis in zahlreichen Bereichen künstliche Intelligenz zur Diagnostik eingesetzt, so beispielsweise zur Diagnose von Brust- und Lungenkrebs.[161]

159 Jannes/Friele/Jannes et al., Digitale Gesundheitsversorgung, 2018, S. 62.

160 Adamson/Smith, Machine Learning, 2018; Zur Ausgestaltung von Algorithmen unter dem Gesichtspunkt des Diskriminierungsverbotes siehe auch: → **Fallbeispiel Algorithmus entscheidet über Bewerbungen 1.1**.

161 NZZ, Diagnose vom Computer, 2019.

2.3 Fitnesstracker einer Krankenkasse

Herr F. beteiligt sich an einem neuen Bonusprogramm zur Förderung der Bewegung im Alltag, das seine Krankenkasse lanciert hat: Er trägt einen Schrittzähler, der seine täglichen Aktivitäten registriert. Diese werden über eine App an die Versicherung weitergeleitet. Pro Tag, an dem er mindestens 10'000 Schritte absolviert, erhält er eine Gutschrift und damit faktisch einen Rabatt auf seine Prämie.

Betroffene Grund- und Menschenrechte

- Recht auf Gesundheit
- Diskriminierungsverbot
- Recht auf Privatsphäre
- Recht auf Datenschutz

Rechtliche Fragestellung

Ist der Rabatt auf Prämien der Grund- und Zusatzversicherung aufgrund der Teilnahme an einem Fitnesstracking-Programm zulässig?

Rechtliche Beurteilung

Prämienrabatte im Rahmen eines Fitnesstracker-Programms werfen Fragen im Zusammenhang mit dem Recht auf Gesundheit und dem Diskriminierungsverbot auf. Das Erheben von Daten zum Bewegungsverhalten von Herrn F. tangiert zudem das Recht auf Privatsphäre und das Recht auf Datenschutz.

Das Recht auf Gesundheit ist in der Bundesverfassung nicht als einklagbares Grundrecht, sondern als Sozialziel enthalten. Demnach müssen sich Bund und Kantone dafür einsetzen, dass jede Person die für ihre Gesundheit notwendige Pflege erhält (Art. 41 Abs. 1 Bst. b BV). Ein zentrales Element hierfür ist die obligatorische Grundversicherung. In diesem Bereich sind die Krankenkassen an die Grundrechte[162] und an verschiedene Prinzipien des Krankenversicherungsgesetzes gebunden. So darf eine Grundversicherung

162 Rütsche, Was sind öffentliche Aufgaben?, 2013, S. 153.

im Unterschied zur Zusatzversicherung niemanden ablehnen (Aufnahmepflicht). Zudem müssen die Prämien der Grundversicherung unabhängig vom jeweiligen Gesundheitszustand oder anderer Merkmale der versicherten Person, wie beispielsweise deren Alter, berechnet sein (Solidaritätsprinzip). Deshalb zahlen mit wenigen Ausnahmen alle Versicherten einer Krankenkasse innerhalb einer Prämienregion den gleichen monatlichen Beitrag.

Bietet eine Grundversicherung ein Bonusprogramm wie im oben beschriebenen Beispiel an, kann dies das Solidaritätsprinzip in Frage stellen und das Diskriminierungsverbot verletzen. Junge und gesunde Versicherte könnten mittels körperlicher Bewegung eine Gutschrift und damit im Ergebnis einen Prämienrabatt erzielen. Damit bestünde die Gefahr, dass beispielsweise ältere oder körperlich beeinträchtigte Versicherte in der Grundversicherung benachteiligt würden. Grundversicherungen dürfen somit keine gesetzlich nicht vorgesehenen Rabatte oder Gutschriften zulasten von anderen Versicherten gewähren. Eine Ausnahme besteht dann, wenn das Bonusprogramm und die daraus folgende Gutschrift nicht von der Grundversicherung selbst angeboten und bezahlt werden, sondern zum Beispiel durch eine Zusatzversicherungsgesellschaft desselben Versicherungsunternehmens.[163]

Zusatzversicherungen sind weder direkt an die Grundrechte noch an das Solidaritätsprinzip des Krankenversicherungsgesetzes gebunden (→ **Grundlagen Kapitel 2.2.6**). Doch auch sie dürfen nicht uneingeschränkt Rabatte im Rahmen von Fitnesstracker-Programmen anbieten. Rabatte sind verboten, wenn sie einzelne Versicherte ungleich behandeln und benachteiligen und dies weder rechtlich noch versicherungstechnisch begründbar ist (Art. 117 Abs. 2 AVO).

Schlussfolgerungen und Empfehlungen

Die Gutschrift an Herrn F. aufgrund dessen Beteiligung am Bonusprogramm ist gesetzlich nur zulässig, wenn das Programm von einer Zusatzversicherungsgesellschaft angeboten und bezahlt wird. Auch darf die Rabattgewährung keine unzulässige Benachteiligung anderer Versicherter zur Folge haben. Nicht zulässig wäre ein entsprechendes Programm, wenn die Gutschrift aus den Prämienzahlungen an die Grundversicherung finanziert würde.

163 Nationalrat, Interpellation 18.3282, Entsolidarisierung in der Grundversicherung verhindern, Stellungnahme des Bundesrates vom 1.6.2018.

Weiterführende Hinweise

Das Fallbeispiel ist inspiriert durch das Urteil 2C_717/2017 des Bundesgerichts vom 25. November 2019 und durch das Urteil A-3548/2018 des Bundesverwaltungsgerichts vom 19. März 2019.

3 Kontakt zu Verwaltung, Justiz und Politik

3.1 Barrierefreie Websites von Behörden

Eine Schweizer Gemeinde betreibt eine Website mit Informationen zu ihrer Arbeit und zu Angeboten für Bürgerinnen und Bürger. Auch Dokumente wie beispielsweise Bewilligungsformulare werden dort bereitgestellt. In letzter Zeit erreichten mehrere Beschwerden die Behörde: Menschen mit einer Sehbehinderung haben Schwierigkeiten, sich auf der Website zurechtzufinden und die veröffentlichten Informationen zu lesen. Zudem meldet sich ein Verband, der die Interessen von Menschen mit geistigen Beeinträchtigungen vertritt. Er bemängelt, dass alle Inhalte in Standardsprache geschrieben sind, und verlangt, dass zumindest die wichtigsten Informationen und Formulare in sogenannter Leichter Sprache verfügbar sein sollen.

Betroffene Grund- und Menschenrechte

- Informationsfreiheit
- Diskriminierungsverbot

Rechtliche Fragestellung

Verletzen unübersichtliche und unzugängliche Websites von Behörden die Informationsfreiheit und das Diskriminierungsverbot? Gibt es einen Anspruch auf barrierefreie Websites?

Rechtliche Beurteilung

Die Informationsfreiheit beinhaltet das Recht, sich Informationen aus allgemein zugänglichen Quellen zu beschaffen. Dazu zählen unter anderem auch Informationen von Behörden. Zwar müssen Verwaltungsbehörden gestützt auf die Informationsfreiheit nicht zwingend von sich aus über ihre Arbeit informieren. Wenn sie dies aber tun, haben sie dabei das Diskriminierungsverbot zu beachten. Darüber hinaus legen die Kantone für die kantonalen

Behörden eine Informationspflicht fest. Das bedeutet, dass kantonale Behörden von sich aus über die Tätigkeiten von allgemeinem Interesse informieren[164] und dabei auch das Diskriminierungsverbot beachten müssen.

Websites von Behörden müssen somit so ausgestaltet sein, dass sie allen Interessierten offenstehen.[165] In Bezug auf Menschen mit Behinderungen[166] verlangt zudem Art. 9 der UNO-Behindertenrechtskonvention, dass Staaten Massnahmen ergreifen, um diesen einen gleichberechtigten Zugang zu Informationen und zu staatlichen Dienstleistungen zu gewährleisten. Sie sollen selbstständig und ohne zusätzliche Kosten die notwendigen Informationen von Behörden erhalten können.

Diese Vorgaben müssen von allen Behörden auf Ebene Bund, Kantone und Gemeinden beachtet werden. So schreibt beispielsweise das Behindertengleichstellungsgesetz für die Bundesbehörden vor, dass diese besondere Rücksicht auf die Anliegen von Sprach-, Hör- und Sehbehinderten nehmen müssen (Art. 14 BehiG) und dass sämtliche Dienstleistungen, die der Bund im Internet anbietet, auch für Menschen mit Behinderungen zugänglich sein müssen (Art. 10 BehiV). Auf kantonaler und kommunaler Ebene haben beispielsweise der Kanton Zürich und die Stadt Bern ihre Webauftritte nach den Grundsätzen der Barrierefreiheit überarbeitet.[167]

Behörden auf Ebene Bund, Kantone und Gemeinde sind deshalb grundsätzlich verpflichtet, ihre Websites barrierefrei zu gestalten. Trotz dieser Vorgaben hat eine Studie von 2016 ergeben, dass die Websites von vielen Kantonen und Städten für Menschen mit Behinderungen noch zu wenig zugänglich gestaltet sind.[168] Auch im obigen Beispiel erfüllt die Website der

164 Zum Beispiel § 14 des Gesetzes über die Information und den Datenschutz des Kantons Zürich (LS 170.4).

165 Langer, Staatliche Nutzung von Social Media-Plattformen, 2014, S. 952.

166 Gemäss der UNO-Behindertenrechtskonvention sind Menschen mit Behinderungen «Menschen, die langfristige, körperliche, seelische, geistige oder Sinnesbeeinträchtigungen haben, welche sie in Wechselwirkung mit verschiedenen Barrieren an der vollen, wirksamen und gleichberechtigten Teilhabe an der Gesellschaft hindern können.» Allerdings stimmen nicht alle Betroffenen dieser Definition zu.

167 Regierungsrat Kanton Zürich, Digitale Verwaltung, 2020, S. 9; Gemeinderat Stadt Bern, Barrierefreiheit, 2018.

168 Schweizerische Stiftung zur behindertengerechten Technologienutzung, Schweizer Accessibility-Studie, 2016.

Gemeinde die Anforderungen an die Barrierefreiheit nicht. Menschen mit einer Sehbehinderung oder einer geistigen Beeinträchtigung können die veröffentlichten Informationen oder Dokumente nicht abrufen oder verstehen.

Schlussfolgerungen und Empfehlungen

Wenn wichtige Informationen auf Websites von Behörden aufgrund fehlender Barrierefreiheit für Menschen mit Behinderungen nicht zugänglich sind, kann dies je nach Umständen des Einzelfalls eine Verletzung des Diskriminierungsverbots und der Informationsfreiheit darstellen. Zwar können Menschen mit Behinderungen nicht generell die Einrichtung barrierefreier Websites auf dem Gerichtsweg einfordern. Wenn aber eine betroffene Person aufgrund der fehlenden Barrierefreiheit eine im Internet angebotene staatliche Dienstleistung nicht in Anspruch nehmen kann, könnte sie dies unter Umständen vor Gericht beanstanden.[169]

Weiterführende Hinweise

Es gibt zahlreiche Möglichkeiten, Websites so zu gestalten, dass auch Menschen mit Behinderungen Zugriff auf die dort veröffentlichten Informationen haben bzw. diese verstehen können. Im Bereich der Sehbehinderung kommen beispielsweise Audio-Systeme zum Einsatz, die Texte «vorlesen». Videobotschaften sind mit Untertiteln auch für gehörlose Menschen zugänglich. Für Menschen mit geistigen oder kognitiven Beeinträchtigungen können die veröffentlichten Informationen in Leichte Sprache übersetzt werden. Dabei wird ein Text in Standardsprache in kurze Hauptsätze mit einfacher Begrifflichkeit umformuliert, so dass er wesentlich besser verständlich ist.[170]

169 Rechtsberatung bietet beispielsweise der Dachverband der Behindertenorganisationen der Schweiz (Inclusion Handicap) an.

170 EBGB, Barrierefreie digitale Kommunikation, 2018, S. 1 f.; EBGB, Faktenblatt Leichte Sprache, 2019.

3.2 Automatisierter Behördenentscheid

G. ist eine Bierbrauerei in der Schweiz und untersteht der Biersteuer. Einmal pro Quartal reicht sie die Biersteueranmeldung ein. Diese wird bei der für die Biersteuer zuständigen Bundesbehörde nicht durch Mitarbeitende, sondern von einer eigens dafür entwickelten Software geprüft. Die Verfügung sowie die dazugehörige Rechnung werden ebenfalls automatisch erstellt.

Betroffene Grund- und Menschenrechte

– Recht auf ein faires Verfahren (rechtliches Gehör)

Rechtliche Fragestellung

Von vollautomatisierten Behördenentscheiden spricht man dann, wenn eine Verfügung oder ein Entscheid einer Behörde vollständig durch eine Software erarbeitet und ohne Mitarbeit eines Menschen erlassen wird.[171] Wie sind solche Entscheide aus Sicht des rechtlichen Gehörs zu beurteilen?

Rechtliche Beurteilung

Der Anspruch auf rechtliches Gehör bedeutet, dass der oder die Betroffene in einem Verfahren die Gelegenheit haben muss, die eigenen Argumente vorzubringen, Akten einzusehen und dazu Stellung zu nehmen. Die Argumente der betroffenen Person müssen wiederum für den erlassenen Entscheid (mit-)berücksichtigt werden. Auch müssen Entscheide und Urteile ausreichend begründet werden. Diese Ansprüche können bei einem automatisierten Entscheid erschwert oder ausgeschlossen sein, da dieser ohne direkten Kontakt zu den Behörden erlassen wird. Zudem besteht die Gefahr, dass sich ein durch eine Software gefällter Entscheid zu wenig am konkreten Einzelfall orientiert.[172]

Der Gesetzgeber hat die Problematik der automatisierten Behördenentscheide erkannt und in der Revision des DSG eine spezifische Bestimmung

171 Braun Binder, Anordnungen der Maschinen, 2020, S. 256.

172 Weber, Automatisierte Entscheidungen, 2020, S. 24; Rechsteiner, Der Algorithmus verfügt, 2018, Rz. 19 ff.

dazu aufgenommen (Art. 21 Rev-DSG). Die Norm gilt nur für Entscheidungen, die ausschliesslich auf einer automatisierten Einzelfallentscheidung beruhen, ohne dass eine natürliche Person am Entscheidungsprozess beteiligt ist.[173] Dies wäre auch im oben beschriebenen automatisierten Steuerverfahren der Fall.

Die betroffene Person muss darüber informiert werden, wenn ein Entscheid automatisiert gefällt wurde (Art. 21 Abs. 1 Rev-DSG). Damit ihr rechtliches Gehör gewahrt wird, muss sie die Möglichkeit haben, ihren Standpunkt darzulegen. Sie kann zudem verlangen, dass der automatisierte Einzelentscheid von einer Mitarbeitenden der zuständigen Behörde überprüft wird (Art. 21 Abs. 2 Rev-DSG).[174]

Schlussfolgerungen und Empfehlungen

Bei der Einführung von automatisierten Entscheiden im Bereich der Biersteuer und anderen Bundessteuern müssten die neuen Vorgaben des DSG berücksichtigt werden. So müsste D. insbesondere darüber informiert werden, dass der Steuerentscheid automatisiert gefällt wurde. Zudem müsste sichergestellt werden, dass D. die Möglichkeit hat, im Verfahren Stellung zu nehmen und den automatisierten Entscheid von einer realen Person überprüfen zu lassen.

Weiterführende Hinweise

Das vorliegende Beispiel ist fiktiv. Mit der Revision des DSG wurde aber in verschiedenen Bundessteuergesetzen die Rechtsgrundlage für zukünftige automatisierte Einzelentscheide geschaffen, etwa für die Zoll- und Schwerverkehrsabgabe sowie die Tabak-, Bier- und Mineralölsteuer. Weiter wurde auch für die Unfall- und Militärversicherung eine gesetzliche Grundlage für allfällige zukünftige Entwicklungen geschaffen.

173 Bundesrat, Botschaft Totalrevision DSG, 2017, S. 7056 f.

174 Braun Binder, Automatisierte Entscheidungen, 2020, S. 31.

3.3 Automatisierte Risikoeinschätzung

Herr H. stellt seit längerer Zeit seiner Exfrau nach und bedroht sie. Nachdem sie sich deswegen bei der Polizei gemeldet hat, führt eine vom Kanton beauftragte und für solche Gespräche geschulte Person ein Gespräch mit ihm. Seine Antworten werden daraufhin an die Polizei weitergeleitet und in ein System eingegeben, das mithilfe eines Algorithmus die Wahrscheinlichkeit errechnet, dass Herr H. gegen seine Exfrau gewalttätig wird. Die Software schätzt das Gefährdungsrisiko mit vier von fünf möglichen Punkten ein.

Betroffene Grund- und Menschenrechte

- Recht auf ein faires Verfahren (rechtliches Gehör und Unschuldsvermutung)
- Diskriminierungsverbot
- Recht auf Freiheit und Sicherheit

Rechtliche Fragestellung

Aus Sicht von Herrn H. stellt sich die Frage, wie die automatisierte Risikoeinschätzung unter dem Gesichtspunkt des Diskriminierungsverbots, der Unschuldsvermutung und des Rechts auf Freiheit und Sicherheit zu beurteilen ist.

Rechtliche Beurteilung

Das im Fallbeispiel eingesetzte Programm ist Teil des sogenannten Predictive Policing. Es handelt sich dabei um einen Vorgang, bei dem ein Behördenentscheid teilweise automatisiert vorbereitet, letztlich aber von Mitarbeitenden der zuständigen Behörde gefällt wird.

Zusätzlich zu dem bereits besprochenen Anspruch auf rechtliches Gehör (→ **Fallbeispiel Automatisierter Behördenentscheid 3.2**) könnte der Einsatz des Algorithmus das Diskriminierungsverbot verletzen. Eine behördliche Entscheidung, die sich auf einen Algorithmus stützt, kann zunächst objektiver wirken als eine Beurteilung durch Mitarbeitende einer Behörde, denn deren Entscheidungen werden von Erfahrungen, Werten und sub-

jektiven Eindrücken beeinflusst. Demgegenüber scheint ein Algorithmus allein datenbasiert und faktenorientiert vorzugehen. Bei dieser Argumentation wird jedoch übersehen, dass auch der Algorithmus von Menschen geschaffen ist und deren Meinungen, Vorurteile und Erfahrungen in die Entwicklung der Software einfliessen. Zudem bilden frühere Fälle die Grundlage für die Entscheidung des Algorithmus. Diese wiederum wurden ebenfalls von Menschen bearbeitet. Deren Wertungen beeinflussen damit auch die Datengrundlage.[175] In der Folge kann eine möglicherweise bereits bestehende Diskriminierung durch den Einsatz des Programms weitergetragen und nach dem Prinzip der Selffulfilling Prophecy sogar verstärkt werden. Anschaulich wird dieser Mechanismus am Beispiel des Programms COMPAS, welches in den USA Afroamerikanern und Afroamerikanerinnen fast doppelt so häufig eine hohe Rückfallquote attestierte wie Weissen.[176]

Die Unschuldsvermutung beinhaltet, dass jede angeschuldigte Person bis zu ihrer Verurteilung als unschuldig gilt, dass es die Aufgabe der Strafverfolgungsbehörde ist, die Schuld zu beweisen und dass die Richterinnen und Richter einen Fall unvoreingenommen beurteilen müssen. Da bei Predictive Policing lediglich eine Risikoeinschätzung in Bezug auf eine allfällige zukünftige Straftat und keine Vorverurteilung wegen einer vergangenen Straftat vorliegt, dürfte die Unschuldsvermutung nicht verletzt sein.[177]

Schliesslich stellt sich die Frage, ob eine automatisierte Risikoeinschätzung die Grundlage für eine Präventivhaft (Art. 221 Abs. 2 StPO) sein könnte. Diese ist gemäss Art. 5 Abs. 1 Bst. c EMRK dann zulässig, wenn eine konkrete Gefahr besteht, dass eine Person ihre Drohung, ein schweres Verbrechen zu begehen, wahrmachen wird und die Vorschrift nur begrenzt zur Anwendung kommt.[178]

Schlussfolgerungen und Empfehlungen

Damit beim Einsatz einer automatischen Risikobewertung die Grund- und Menschenrechte gewahrt bleiben, müssen verschiedene Aspekte beachtet

175 Thouvenin/Früh/George, Automatisierte Entscheidungen, 2018, Rz. 9.

176 NZZ, Algorithmen unter Rassismusverdacht, 2016.

177 Camavdic, Predictive Policing in der Schweiz, 2019, Rz. 14.

178 Schmid/Jositsch, Kommentar zu Art. 221 StPO, 2018, N. 14; Hug/Scheidegger, Kommentar zu Art. 221 StPO, 2014, N. 40 ff.

werden: Zum einen benötigen automatisierte Behördenentscheide wie das Predictive Policing eine gesetzliche Grundlage. Derzeit wird die Berechtigung zu diesem Vorgehen häufig mit der allgemeinen Pflicht der Polizei begründet, die Begehung von Straftaten zu verhindern, der sogenannten polizeilichen Generalklausel. Damit das Diskriminierungsverbot nicht verletzt wird, muss der dem Algorithmus zugrunde liegende Trainingssatz zudem genügend divers und transparent ausgestaltet sein (→ **Fallbeispiel Algorithmus entscheidet über Bewerbungen 1.1** und → **Fallbeispiel KI und Big Data in der Diagnostik 2.2**).[179]

Weiterführende Hinweise

In der Schweiz werden Software vermehrt zur Vorhersage und Verhinderung schwerer Gewalttaten eingesetzt: Hierfür wird mit Menschen, die bestimmte wissenschaftlich belegte Warnsignale für das Begehen von zukünftigen Straftaten aufweisen, ein Gespräch geführt. Ergebnisse dieses Gesprächs und weitere Informationen, zum Beispiel aus vorhandenen Akten, werden daraufhin in eine Software eingegeben. Ein Algorithmus errechnet schliesslich das Risiko einer zukünftigen Straftat. Das Programm trifft in diesen Fällen eine erste Einschätzung. Die endgültige Entscheidung, ob die betroffene Person als sogenannter «Gefährder» oder «Gefährderin» eingestuft wird, trifft die zuständige Behörde.[180]

179 Braun Binder, Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, 2019, S. 473.

180 Simmler/Brunner/Schedler, Smart Criminal Justice, 2020, S. 14 ff.; Bundesrat, Bedrohungsmanagement, 2017, S. 5 ff.

3.4 Microtargeting im Abstimmungskampf

Frau I. möchte sich im Internet zu den anstehenden Abstimmungen informieren. Sie stösst nach einer kurzen Suche auf die Website einer Partei und liest dort die Erläuterungen zu den verschiedenen Vorlagen. Beim Öffnen der Website hat sie im auftauchenden Kasten ein Häkchen angebracht und sich mit der Cookie-Setzung einverstanden erklärt. Kurze Zeit später entdeckt Frau I. beim Öffnen ihres Facebook-Accounts eine Anzeige zu einer anstehenden Abstimmung – von der Partei, deren Website sie eben besucht hatte. Sie fühlt sich in unangenehmer Weise beobachtet.

Betroffene Grund- und Menschenrechte

- Meinungsfreiheit
- Politische Rechte (insb. freie Willensbildung)
- Recht auf Privatsphäre
- Recht auf Datenschutz

Rechtliche Fragestellung

Wie ist Microtargeting im Vorfeld von Wahlen und Abstimmungen aus grund- und menschenrechtlicher Sicht zu beurteilen? War die Weiterleitung der Daten von Frau I. an Facebook zulässig?

Rechtliche Beurteilung

Politische Kampagnen werden nicht nur in der analogen, sondern auch in der digitalen Welt geführt. Soziale Medien ermöglichen einen unkomplizierten Austausch und tragen so wesentlich zur politischen Meinungsbildung bei. Digitale Kampagnen können aber auch verschiedene Grund- und Menschenrechte beeinträchtigen. Werden im Abstimmungskampf Inhalte mittels Microtargeting (→ **Grundlagen Kapitel 1.1**) verbreitet, tangiert dies insbesondere die Meinungsfreiheit und die freie politische Willensbildung. Das Sammeln und Auswerten der Daten zur Identifizierung der Zielgruppen wirft Fragen im Zusammenhang mit dem Recht auf Privatsphäre und dem Recht auf Datenschutz auf.

Die Meinungsfreiheit beinhaltet unter anderem das Recht, die eigene politische Meinung frei zu bilden, zu äussern und zu verbreiten. Microtargeting stellt somit eine von zahlreichen zulässigen Methoden dar, wie politische Parteien und Interessengruppen ihre Ansichten und Botschaften verbreiten können. Gemäss Bundesgericht darf die Meinungsfreiheit im politischen Kontext nur in Ausnahmefällen eingeschränkt werden.[181] Dies wäre beispielsweise dann der Fall, wenn mittels Microtargeting rassistische Äusserungen verbreitet würden.

Die Bundesverfassung verlangt, dass Abstimmungs- und Wahlergebnisse den freien Willen der Stimmberechtigten zuverlässig und unverfälscht zum Ausdruck bringen. Eine Voraussetzung dafür ist, dass die Stimmberechtigten im Vorfeld von Wahlen und Abstimmungen sowohl durch Behörden als auch durch Private korrekt und ausgewogen informiert werden.[182] Die freie Willensbildung könnte also durch eine besonders aggressive Kommunikationsstrategie mittels Microtargeting, die auf sozialen Medien gezielt einseitige Informationen zu einer Vorlage verbreitet, beeinträchtigt werden. In diesen Fällen müssten die Behörden mit korrigierenden Informationen in den Abstimmungskampf eingreifen. Nur in Ausnahmefällen käme die Aufhebung einer Abstimmung in Frage.[183]

Bei Microtargeting werden weiter grosse Mengen an Personendaten gesammelt und ausgewertet, was das Recht auf Privatsphäre und das Recht auf Datenschutz tangiert. Zu beachten ist, dass nicht der Staat die Daten bearbeitet, sondern Private (Parteien, spezialisierte Unternehmen), die nicht direkt an die Grund- und Menschenrechte gebunden sind. In dieser Konstellation schützt aber das Datenschutzgesetz die Betroffenen (→ **Grundlagen Kapitel 2.2.7**).

Die Stimmberechtigten haben einen datenschutzrechtlichen Anspruch darauf, nachvollziehen zu können, aufgrund welcher digitaler Bearbeitungsmethoden und Technologien sie angesprochen und politisch beeinflusst werden. Informationen über politische Tätigkeiten und Interessen gehören zu den besonders schützenswerten Personendaten. Werden solche Daten erhoben und weitergeleitet, muss dies für die betroffene Person klar erkenn-

181 BGE 131 IV 23 E. 3.1.
182 BGE 121 I 138 E. 3.
183 BGE 135 I 292 E. 4.

bar sein, und sie muss dazu ihre ausdrückliche Einwilligung geben (Art. 4 Abs. 5 DSG; Art. 6 Abs. 6 und 7 Rev-DSG). Werden also beispielsweise beim Besuch der Website einer politischen Partei Daten erhoben, dürfen diese zur Profilbildung für Microtargeting nur dann weitergeleitet und mit anderen Daten verbunden werden, wenn die betroffene Person darüber ausreichend informiert wurde und ausdrücklich und selbstbestimmt eingewilligt hat. Diese Einwilligung kann beispielsweise so erteilt werden, dass neben der grundsätzlichen Einwilligung zur Setzung eines Cookies ein separates Häkchen angeklickt werden muss. Das generelle Akzeptieren der allgemeinen Nutzungsbedingungen reicht nicht aus. Die Information über die beabsichtigte Datenbearbeitung muss leicht verständlich und vollständig sein. Zudem besteht eine Informationspflicht darüber, ob die gesammelten Daten mit Daten aus sozialen Medien verknüpft werden. Auch muss die betroffene Person jederzeit die Möglichkeit haben, ihre Einwilligung zu widerrufen und die Löschung der Daten zu verlangen.[184]

Schlussfolgerungen und Empfehlungen

Microtargeting im Vorfeld von Wahlen und Abstimmungen tangiert verschiedene Grund- und Menschenrechte. Aus Sicht der Meinungsfreiheit und der politischen Rechte ist diese Methode der politischen Kommunikation grundsätzlich zulässig. Da aber grosse Mengen an Daten gesammelt und ausgewertet sowie spezifische Persönlichkeitsprofile erstellt werden, liegt ein Eingriff in das Recht auf Privatsphäre und das Recht auf Datenschutz vor. Unter welchen Voraussetzungen die Datenbearbeitung zwecks Microtargeting zulässig ist, ergibt sich wie oben ausgeführt aus dem Datenschutzgesetz.

Das Weiterleiten der Daten von Frau I. an Facebook war im vorliegenden Fall nicht zulässig. Sie war über die beabsichtigte Abgleichung ihrer Daten mit Daten aus sozialen Netzwerken nicht ausreichend informiert und konnte somit in diese auch nicht ausdrücklich einwilligen (zum Beispiel mit einem separaten Häkchen). Ihr generelles Einverständnis zur Setzung von Cookies war nicht ausreichend. Grundsätzlich kann Frau I. die Löschung derjenigen Daten verlangen, die ohne ihr Einverständnis weitergeleitet wurden. Dies ge-

184 EDÖB/Privatim, Datenschutzrecht Wahlen und Abstimmungen, 2019.

staltet sich in der Praxis jedoch oft schwierig. Zusätzlich kann sie sich, wie bei allen Fragen zum Datenschutz, durch das Büro des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten beraten lassen.

Weiterführende Hinweise

Das Fallbeispiel ist der Situation vor den eidgenössischen Wahlen 2019 nachgebildet. Damals sammelten verschiedene Parteien die Daten der Besucherinnen und Besucher ihrer Websites und leiteten diese teilweise ohne deren Einwilligung an Facebook weiter. In der Folge erhielten die betroffenen Personen gezielte Werbung der jeweiligen Parteien. Nachdem dies bekannt wurde, haben die Parteien die Datenweiterleitung und die Einwilligung dazu transparenter gestaltet.[185]

Ausführliche Erläuterungen zu Microtargeting im Vorfeld von Wahlen und Abstimmungen finden sich im Leitfaden der Datenschutzbehörden von Bund und Kantonen.[186]

185 SRF, CVP verschweigt digitalen Datenspion, 2019.

186 EDÖB/Privatim, Datenschutzrecht Wahlen und Abstimmungen, 2019.

3.5 Staatliche Videoüberwachung mit Gesichtserkennung im öffentlichen Raum

Frau J. engagiert sich in der Klimajugend und nimmt regelmässig an friedlichen Kundgebungen teil. In verschiedenen Medien liest sie, wie im Ausland bei grossen Menschenmengen (zum Beispiel Demonstrationen oder Sportveranstaltungen) Videoüberwachung mit Gesichtserkennung eingesetzt wird. Frau J. fragt sich, wie die Situation in der Schweiz aussieht und welche Konsequenzen sie als Teilnehmerin an bewilligten Kundgebungen zu gewärtigen hätte.

Betroffene Grund- und Menschenrechte

- Versammlungsfreiheit
- Meinungsfreiheit, insb. Meinungsäusserungsfreiheit
- Bewegungsfreiheit
- Recht auf Privatsphäre
- Recht auf Datenschutz

Rechtliche Fragestellung

Wie ist Videoüberwachung mit Gesichtserkennung (→ **Grundlagen Kapitel 1.4**) im öffentlichen Raum aus grund- und menschenrechtlicher Sicht zu beurteilen? Ist eine Videoüberwachung mit Gesichtserkennung in der Schweiz zulässig?

Rechtliche Beurteilung

Die Meinungsäusserungsfreiheit und die Versammlungsfreiheit garantieren unter anderem, dass jede Person an friedlichen Demonstrationen teilnehmen und dort ihre Meinung kundtun kann. Die Teilnahme an Kundgebungen sagt oft etwas über die jeweilige politische Einstellung oder über persönliche Merkmale wie beispielsweise die sexuelle Orientierung aus. Gleichzeitig garantiert die Menschenmasse eine gewisse Anonymität. Wird nun aber der öffentliche Raum, in dem eine Kundgebung stattfindet, mit Video überwacht und werden die Teilnehmenden möglicherweise mit Gesichtserkennungssoftware identifiziert, fällt dieses Gefühl von Anonymität und dem damit verbundenen Schutz weg. Dies wiederum kann dazu führen, dass verschiedene

Personen auf eine Teilnahme verzichten, weil sie nicht möchten, dass Daten, beispielsweise über ihre politische Einstellung, gesammelt werden. Aufgrund dieses Verzichts auf die Teilnahme an einer Demonstration infolge der Überwachungssituation würden die Meinungsäusserungs- und Versammlungsfreiheit indirekt eingeschränkt (sogenannter Chilling Effect).[187]

In ähnlicher Weise kann die Videoüberwachung mit Gesichtserkennung indirekt auch die Bewegungsfreiheit einschränken. Zwar hindert die Überwachung die einzelne Person nicht direkt daran, sich weiterhin frei im öffentlichen Raum zu bewegen. Wenn sie aber an einem bestimmten Ort nicht gefilmt und identifiziert werden möchte, muss sie diesen meiden.[188]

Schliesslich stellt der Einsatz von Gesichtserkennungssoftware im öffentlichen Raum auch einen Eingriff in das Recht auf Privatsphäre und das Recht auf Datenschutz dar. Grundsätzlich hat jede Person das Recht, sich unbeobachtet im öffentlichen Raum aufzuhalten. Filmt die Polizei Menschen und ihre Tätigkeiten, werden grosse Mengen an Personendaten gesammelt. Aus grund- und menschenrechtlicher Sicht benötigt der Einsatz von Gesichtserkennungssoftware somit zwingend eine gesetzliche Grundlage, er muss im öffentlichen Interesse liegen und verhältnismässig sein.

Würde Gesichtserkennung im öffentlichen Raum breitflächig eingesetzt, handelte es sich hierbei um eine Massenüberwachung. Es würden Daten von zahlreichen unbeteiligten Personen präventiv und ohne konkreten Verdacht gegen eine bestimmte Person gesammelt, was aus grund- und menschenrechtlicher Sicht nicht zulässig ist. Gerade wenn Daten darüber erhoben werden, wer sich wann an welchem Ort aufgehalten und eine bestimmte Tätigkeit ausgeführt hat, birgt dies ein erhebliches Risiko für das Recht auf Privatsphäre, die Meinungsfreiheit und die Versammlungsfreiheit.[189] So kann es zwar durchaus sein, dass die Aufzeichnung zum aktuellen Zeitpunkt der betroffenen Person unproblematisch erscheint. Bei dauerhafter Abspeicherung dieser Daten besteht aber die Gefahr, dass beispielsweise der Auf-

187 UNO-Hochkommissariat für Menschenrechte, New technologies in the context of assemblies, 2020, Rz. 34.

188 Schweizer, Kommentar zu Art. 10 BV, 2014, N. 35.

189 Weydner-Volkmann/Feiten, Vertrauensstiftende Videoüberwachung?, 2019, S. 218.

enthalt an einem bestimmten Ort zu einem späteren Zeitpunkt problematisch wird, weil Behörden diesen Ort mit einer bestimmten politischen Einstellung in Verbindung bringen.

Schlussfolgerungen und Empfehlungen

Die staatliche Videoüberwachung des öffentlichen Raums mit Gesichtserkennung ist zum aktuellen Zeitpunkt in der Schweiz nicht zulässig. Hierfür wäre ein neues Gesetz erforderlich, das spezifisch diese Überwachungsmethode regelt. Es müsste in detaillierter Weise die wichtigen Punkte wie den Zweck der Überwachung und die Löschung der erhobenen Daten regeln. Auch müsste immer überprüft werden, ob die Überwachung mittels Gesichtserkennung verhältnismässig ist.

Weiterführende Hinweise

Verschiedene Staaten setzen im öffentlichen Raum Gesichtserkennungssoftware ein: So beispielsweise die Polizei Hamburg zur Aufklärung von Straftaten anlässlich der Proteste gegen den G20-Gipfel 2017[190] und die Polizei in South Wales.[191]

In der Schweiz setzt die Grenzpolizei Gesichtserkennungssoftware am Flughafen Zürich bei der automatischen Passkontrolle von Personen aus dem EU/EFTA-Raum ein. Dort geht es aber nicht darum, unbekannte Personen zu identifizieren. Vielmehr kontrolliert die Software, ob es sich bei der einreisenden Person auch tatsächlich um die Person handelt, deren Pass vorgewiesen wird. Die Überprüfung findet anhand der biometrischen Daten des Passes statt. Daten werden keine gespeichert.[192]

190 Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, G20-Ermittlungen, 2020.

191 Urteil des Court of Appeal, R. gegen Chief Constable of South Wales Police, 11.8.2020 (Fallnummer C1/2019/2670).

192 Kamasa, Grenzkontrollen in Europa, 2019.

4 Internetnutzung

4.1 Hasskommentare im Internet

Frau K. engagiert sich bei einer Initiative, die Vorurteile gegenüber dem Islam abbauen will. Sie ist auch in den sozialen Medien aktiv und veröffentlicht regelmässig kurze Texte, in denen sie Vorurteile gegenüber Menschen muslimischen Glaubens im alltäglichen Leben aufzeigt. Ihre Postings werden rege kommentiert und geteilt. Einzelne Kommentare sind rassistisch und enthalten Gewaltandrohungen.

Betroffene Grund- und Menschenrechte

- Meinungsfreiheit
- Menschenwürde
- Diskriminierungsverbot
- Glaubens- und Gewissensfreiheit

Rechtliche Fragestellung

Wie kann rechtlich gegen Hassreden im Internet vorgegangen werden?

Rechtliche Beurteilung

Gemäss einer gängigen Definition fallen unter den Begriff der Hassrede rassistische, antisemitische und andere auf Intoleranz beruhende hasserfüllte Kommentare.[193] Kommentare im Internet sind in der Regel von der Meinungsfreiheit geschützt. Jede Person hat grundsätzlich das Recht, ihre Meinung frei zu äussern. Die Meinungsfreiheit gilt aber nicht absolut. Hasskommentare beeinträchtigen die Menschenwürde, das Diskriminierungsverbot und die Glaubens- und Gewissensfreiheit. Die Meinungsfreiheit kann deshalb zum Schutz der Grund- und Menschenrechte anderer Personen eingeschränkt werden.[194]

193 Europarat Ministerkommitee, Hassrede, 1997.
194 Hart, Hate-Speech, 2018, S. 20.

Kommentare, die öffentlich zu Hass oder zu Diskriminierung gegen Personen wegen ihrer «Rasse»,[195] Ethnie, Religion oder sexueller Orientierung aufrufen, sind strafbar. Ebenso strafbar ist die gegen die Menschenwürde verstossende Herabsetzung oder Diskriminierung aufgrund eines dieser Merkmale (Art. 261bis StGB). Hasskommentare in sozialen Medien gelten normalerweise als öffentlich und fallen somit unter dieses Verbot.

Nicht als Aufruf zu Hass im Sinne des Strafrechts gelten Hasskommentare aus anderen Gründen, zum Beispiel gegen Frauen oder ältere Menschen. Diese werden aber von anderen Strafbestimmungen (zum Beispiel Beschimpfung, Bedrohung oder Nötigung) erfasst.

Schlussfolgerungen und Empfehlungen

Frau K. und jede andere Person, die einen Hasskommentar im Internet sieht, haben die Möglichkeit, einen Strafantrag bei der Polizei zu stellen. Polizei und Staatsanwaltschaft werden in der Folge eine Strafuntersuchung durchführen und überprüfen, ob der Kommentar gegen Art. 261bis StGB oder eine andere Bestimmung des Strafrechts verstösst. Auch kann Frau K. die Löschung der rassistischen Kommentare verlangen (→ **Fallbeispiel Cybermobbing 4.2**).

Weiterführende Hinweise

Es ist nicht immer einfach zu entscheiden, ob verletzende Kommentare im Internet unter den Begriff der Hassrede fallen. Auf der Webseite der Eidgenössischen Kommission gegen Rassismus ist eine Sammlung von Entscheiden und Urteilen zu Art. 261bis StGB veröffentlicht. Unter dem Stichwort Tatmittel «Elektronische Kommunikation» finden sich Praxisbeispiele zu Hassreden im Internet.

195 Der Begriff «Rasse» wird im Strafgesetzbuch und in der Bundesverfassung verwendet. Da es sich beim Begriff um ein rassismusbegründendes Konstrukt handelt, soll er gemäss Empfehlungen der Eidgenössischen Kommission gegen Rassismus bei der Verwendung in Anführungszeichen gesetzt werden.

4.2 Cybermobbing

L. ist eine siebzehnjährige Schülerin. Sie wird in der Schule regelmässig Opfer von Beleidigungen und Belästigungen. Diese verlagern sich bald auch in die sozialen Netzwerke, wo die Täterinnen und Täter unter anderem private Fotos von L. veröffentlichen. Die Situation ist für L. unerträglich.

Betroffene Grund- und Menschenrechte

- Recht auf geistige Unversehrtheit
- Meinungsfreiheit

Rechtliche Fragestellung

Was kann gegen Cybermobbing unternommen werden?

Rechtliche Beurteilung

Wird eine Person über längere Zeit systematisch über das Handy oder im Internet beleidigt, bedroht oder belästigt, handelt es sich um Cybermobbing. Im Unterschied zu Beleidigungen und Bedrohungen in der analogen Welt sind im Internet veröffentlichte Äusserungen oftmals auf unbestimmte Zeit gespeichert und zugänglich. Zudem ist der Kreis der Personen, die solche Äusserungen lesen können, wesentlich grösser.[196] Cybermobbing kann das Recht auf geistige Unversehrtheit tangieren. Entsprechende Äusserungen werden somit normalerweise von der Meinungsfreiheit nicht geschützt.[197]

Im Schweizer Strafrecht existiert kein spezifisches Verbot von Cybermobbing. Die Kommentare gegen L. werden aber von verschiedenen, ursprünglich für die analoge Welt geschaffenen Strafbestimmungen erfasst. In Frage kommen beispielsweise die üble Nachrede (Art. 173 StGB), Beschimpfung (Art. 177 StGB), Drohung (Art. 180 StGB) oder die Nötigung (Art. 181 StGB). Einige der Straftaten werden erst auf Antrag der betroffenen Person untersucht (Antragsdelikt; zum Beispiel üble Nachrede). Andere müssen von

196 Brun, Cyberbullying, 2016, S.101 f.

197 Zum Spannungsfeld zwischen der Meinungsfreiheit und dem Schutz der geistigen Unversehrtheit und anderer Grundrechte: → **Fallbeispiel Hasskommentare im Internet 4.1**.

der Polizei und der Staatsanwaltschaft verfolgt werden, sobald diese davon Kenntnis haben, unabhängig davon, ob eine Strafanzeige vorliegt oder nicht (Offizialdelikt; zum Beispiel Nötigung).

Weiter liegt bei Cybermobbing oftmals auch eine Persönlichkeitsverletzung (Art. 28 ZGB ff.) vor. Für L. bedeutet dies, dass sie die Löschung der beleidigenden oder drohenden Kommentare und der privaten Fotos in den sozialen Medien sowie je nach Situation auch Schadenersatz/Genugtuung verlangen kann.

Schlussfolgerungen und Empfehlungen

Bei Cybermobbing bieten verschiedene Stellen erste Beratung und Unterstützung (zum Beispiel Schulen, Pro Juventute, Opferhilfestellen). Mit diesen kann L. das geeignete Vorgehen besprechen. Grundsätzlich hat sie die Möglichkeit, innerhalb von drei Monaten einen Strafantrag bei der Polizei einzureichen.

Oft ist für eine betroffene Person aber nicht nur die strafrechtliche Verurteilung, sondern auch die Löschung der verletzenden Kommentare wichtig. Wenn L. dies nicht mithilfe der Betreiberin der sozialen Netzwerke erreicht, kann sie beim Zivilgericht an ihrem Wohnsitz Klage einreichen.

Weiterführende Hinweise

Weiterführende Informationen und Tipps gegen Cybermobbing finden sich in einem Ratgeber der Schweizerischen Kriminalprävention[198] und auf der Webseite von Pro Juventute.

198 Schweizerische Kriminalprävention, Cybermobbing, 2017.

5 Bildung und Forschung

5.1 Online-Unterricht in der Schule

M. ist 13 Jahre alt. Während der vorübergehenden Schulschliessung in der Corona-Pandemie lernte er wie alle anderen schulpflichtigen Kinder zu Hause. Regelmässig fanden Schulstunden per Videokonferenz statt. Im Englischunterricht musste er zudem Aufträge in der Online-Version seines Lehrmittels erledigen. Die Eltern von M. besitzen einen älteren Laptop. Diesen teilte er sich mit seinen Geschwistern, welche ebenfalls Online-Unterricht erhielten. Deshalb konnte M. in den Wochen während der Schulschliessung nur an etwa zwei Drittel aller Online-Lektionen teilnehmen und zahlreiche Aufträge nicht erledigen.

Betroffene Grund- und Menschenrechte

- Recht auf Bildung
- Anspruch auf ausreichenden Grundschulunterricht

Rechtliche Fragestellung

Welchen Einfluss hat die Digitalisierung auf das Recht auf Bildung? Kann der grundrechtliche Anspruch auf Grundschulunterricht mittels Online-Unterricht gewährleistet werden? Hätte M. aufgrund seiner erschwerten Situation einen Anspruch auf Unterstützung gehabt?

Rechtliche Beurteilung

Digitale Technologien haben ein grosses Potenzial, den Bereich der Bildung positiv zu beeinflussen und damit das Recht auf Bildung zu stärken. So können Lehrpersonen digitale Lehrmittel nutzen, um die Qualität im Präsenzunterricht zu erhöhen oder um den Unterricht komplett digital und damit ortsunabhängig durchzuführen. Die zunehmende Digitalisierung im Bildungsbereich kann aber auch ein Risiko für die Chancengleichheit sein, wenn Schülerinnen und Schülern die notwendige Infrastruktur wie ausreichender Internetzugang, Computer, das nötige technische Vorwissen oder

das unterstützende soziale Umfeld fehlt, um am Online-Unterricht teilzunehmen.[199] So hat die Erhebung des Schulbarometers für Deutschland, Österreich und die Schweiz ergeben, dass es während der Schulschliessung in der Corona-Pandemie im Frühling 2020 eine beträchtliche Zahl von Schülerinnen und Schülern gab, die für ihre Lehrpersonen digital gar nicht erreichbar waren. Zudem haben etwa zehn Prozent der befragten Kinder und Jugendlichen angegeben, dass sie Schwierigkeiten gehabt hätten, dem digitalen Unterricht zu folgen, weil ihnen die dafür notwendigen Geräte fehlten.[200]

Der UNO-Kinderrechtsausschuss hat sich mit den menschenrechtlichen Fragen der Digitalisierung der Schule und der dafür notwendigen Infrastruktur befasst. Demnach sind Staaten verpflichtet sicherzustellen, dass alle Kinder Zugang zu den digitalen Technologien haben, die für ihre Schulbildung notwendig sind. Kinder ohne ausreichenden Zugang zur notwendigen Technik und/oder die dafür notwendige Unterstützung durch ihre Eltern müssen durch die Lehrpersonen ausreichend (anderweitig) unterstützt werden.[201]

In Bezug auf das Fallbeispiel stellt sich die Frage, ob der Anspruch von M. auf ausreichenden Grundschulunterricht trotz der Einschränkungen gewahrt blieb. Jedes Kind in der Schweiz hat einen gerichtlich einklagbaren Anspruch auf ausreichenden und unentgeltlichen Grundschulunterricht vom Kindergarten bis zur neunten Klasse. Aus der bisherigen Rechtsprechung des Bundesgerichts ergibt sich nicht eindeutig, ob dieser Minimalanspruch eingeschränkt werden darf. Jedenfalls erachtet es temporäre Schulausschlüsse aus disziplinarischen Gründen als zulässig.[202] Der Grundschulunterricht dient der Verwirklichung der Chancengleichheit. Alle Kinder in der Schweiz sollen mindestens so viel Bildung erhalten, dass sie sich entfalten und später im Alltag ein selbstverantwortliches Leben führen können. Der Grundschulunterricht ist dann nicht ausreichend, wenn dem Kind Inhalte

199 UNO-Sonderberichterstatter zum Recht auf Bildung, Right to education in the digital age, 2016, Rz. 26 ff. und 31 ff.

200 Huber/Günther/Schneider et al., COVID-19 Herausforderungen in Schule und Bildung, 2020, S. 25 f. und S. 83 f.

201 UNO-Kinderrechtsausschuss, General Comment Nr. 25, 2021, Rz. 102 ff.; UNO-Kinderrechtsausschuss, COVID-19 pandemic, 2020, Rz. 3.

202 BGE 129 I 12.

nicht beigebracht werden, die aus gesellschaftlicher Sicht unverzichtbar sind, und die Chancengleichheit zwischen den Kindern nicht mehr gewahrt ist.[203]

Schlussfolgerungen und Empfehlungen

Der Anspruch von M. auf ausreichenden Grundschulunterricht ist dann gewährleistet, wenn die Einschränkung aufgrund der fehlenden Infrastruktur nicht dazu führt, dass ihm in der Zukunft wesentliche Inhalte fehlen, so dass er gegenüber seinen Mitschülerinnen und Mitschülern benachteiligt wird und seine Chancengleichheit nicht mehr gewahrt ist. Dem kann mit verschiedenen Massnahmen entgegengewirkt werden: Entweder hätte die Schule M. einen Laptop oder ein Tablet zur Verfügung stellen müssen. Oder aber die Lehrperson hätte ihm die Lerninhalte in Papierform und mittels Erklärungen am Telefon zukommen lassen müssen. Allfällige Lernrückstände müssten zudem mittels zusätzlicher Unterstützungsangebote nach Wiedereröffnung der Schulen aufgeholt werden.

Weiterführende Hinweise

Die Ausstattung der Schülerinnen und Schüler mit den notwendigen Geräten und deren Finanzierung sind zentrale Themen im Zusammenhang mit der Digitalisierung im Bildungsbereich. Dies hat auch die Schweizerische Konferenz der Kantonalen Erziehungsdirektoren erkannt. Sie beabsichtigt, in naher Zukunft Empfehlungen zur Ausstattung der Schülerinnen und Schüler mit den notwendigen Geräten zu erarbeiten.[204]

203 BGE 129 I 12 E. 4.1 f.

204 EDK, Massnahmen zur Digitalisierungsstrategie, 2019, S. 4 f.

5.2 Veröffentlichung einer wissenschaftlichen Studie

Frau N. ist bei einer Universität angestellt und arbeitet an einer wissenschaftlichen Studie zum Thema Fremdplatzierung von Kindern. Für ihre Untersuchung führt sie Interviews mit betroffenen Kindern und deren Eltern durch, die sie anschliessend auswertet. Die Studie wird vom Schweizerischen Nationalfonds finanziell unterstützt. Eine Bedingung dafür ist, dass Frau N. ihre Forschungsergebnisse und ihre Forschungsdaten (in anonymisierter Form) öffentlich zugänglich macht.

Betroffene Grund- und Menschenrechte

- Forschungsfreiheit
- Recht auf Teilhabe am wissenschaftlichen Fortschritt
- Recht auf Privatsphäre
- Schutz der Kinder und Jugendlichen
- Recht auf Datenschutz

Rechtliche Fragestellung

Welche besonderen Vorgaben sind in Bezug auf die erhobenen Daten zu beachten, wenn die Forschungsdaten und -ergebnisse für alle öffentlich zugänglich gemacht werden müssen?

Rechtliche Beurteilung

Der Schweizerische Nationalfonds und der Verband Swissuniversities haben 2017 in ihrer nationalen Open-Access-Strategie beschlossen, dass alle Forschungsergebnisse, die mit Unterstützung von öffentlichen Geldern finanziert werden, online uneingeschränkt und gratis zugänglich sein müssen.[205] Die Publikation der Ergebnisse soll demnach beispielsweise als Artikel in einer Open-Access-Zeitschrift oder als Open-Access-Buch erfolgen. Zudem sollen auch die der Forschung zugrundeliegenden Daten in einer digitalen und den FAIR-Pinciples (Findable, Accessible, Interoperable und Reusable) entsprechenden Datenbank der Öffentlichkeit zugänglich gemacht werden (Open Research Data).

205 SNF, Reglement Open-Access, 2017.

Die frei zugängliche Veröffentlichung von wissenschaftlicher Forschung im Internet steht im Spannungsfeld zwischen verschiedenen Grund- und Menschenrechten: Open Access stärkt die Forschungsfreiheit. Forschende können ohne Einschränkungen auf frühere Arbeiten innerhalb oder ausserhalb ihres Fachgebiets zurückgreifen und darauf aufbauen. Der damit geförderte Austausch unter den Forschenden erhöht zudem auch die Qualität der Forschung. Auch wird das Recht jeder einzelnen Person gestärkt, an den Errungenschaften des wissenschaftlichen Fortschritts teilzuhaben. So kann sich beispielsweise jede und jeder selbstständig über den aktuellen Stand der Forschung zu einem bestimmten Bereich informieren und Stellung nehmen.

Bei Personen, die als Probandinnen und Probanden an Studien teilnehmen, stellt sich hingegen die Frage, wie ihr Recht auf Privatsphäre und ihr Recht auf Datenschutz gewahrt werden können. Trotz Anonymisierung der Daten besteht nämlich grundsätzlich ein gewisses Risiko, dass sie aufgrund der im Internet veröffentlichten Studiendaten und Ergebnisse identifiziert werden können. Dies gilt insbesondere für Datensätze mit qualitativen Daten (zum Beispiel Audiodateien oder Protokolle von Interviews), bei denen eine Veröffentlichung der Originaldaten meist unvereinbar ist mit den ethischen Vorgaben zur Anonymisierung.[206]

Zum Schutz der Daten der Probandinnen und Probanden haben die Forschenden daher zahlreiche Regeln zu beachten. Zum einen müssen Forschende, die an einer Schweizer Hochschule oder in einem öffentlichen Spital tätig sind, sich an die jeweiligen kantonalen Datenschutzgesetze halten. Für andere Forschende und Mitarbeitende der ETH/EPFL gilt das eidgenössische Datenschutzgesetz. Für Forschende, die an «Horizon»-Programmen der EU beteiligt sind, finden zusätzlich die Vorschriften der DSGVO Anwendung. Weitere Vorschriften ergeben sich im Zusammenhang mit einer allfälligen finanziellen Unterstützung. So verlangt der Schweizerische Nationalfonds für unterstützte Forschungsprojekte zwar grundsätzlich eine Veröffentlichung der Datensätze, sieht aber auch Ausnahmen vor, unter anderem zum Schutz von besonders schützenswerten Personendaten. Ausserdem sind die Forschenden verpflichtet, in einem detaillierten Plan (Data Management Plan) aufzuzeigen, wie die Daten erhoben, dokumentiert und wo sie gespeichert werden. Dies verlangt das im DSG festgelegte Prinzip der Erkennbarkeit.[207]

206 Rocher/Hendrickx/de Montjoye, Re-identifications, 2019.

207 Thouvenin, Forschung, Big Data und Datenschutzrecht, 2017, S. 42 f.

Zudem müssen sie erklären, wie mit allfälligen ethischen Bedenken zur Veröffentlichung der Daten umgegangen wird, sowie wo und in welcher Form die Daten schliesslich veröffentlicht werden. Je nach Forschungsgegenstand müssen Forschende zudem die Bewilligung durch eine der verschiedenen Ethikkommissionen der Kantone oder Universitäten einholen.

Schlussfolgerungen und Empfehlungen

Der Schutz von Daten im Rahmen der Wissenschaft stellt eine Herausforderung für die Forschenden dar. Dies gilt umso mehr, wenn sie Daten und Ergebnisse öffentlich zugänglich machen müssen. Sie haben sich hierfür mit Vorgaben des Datenschutzrechtes sowie den Vorschriften ihrer Institute und finanziellen Förderer auseinanderzusetzen. An den Universitäten und Fachhochschulen gibt es dafür spezialisierte Stellen, welche die Forschenden zum Umgang mit ihren Forschungsdaten beraten.

Weiterführende Hinweise

Weitere Informationen zum Umgang mit Forschungsdaten im Allgemeinen und im Zusammenhang mit Open Access bzw. Open Research Data finden sich auf den Webseiten des EDÖB, der kantonalen Datenschutzbeauftragten sowie der Hochschulen.

6 Wirtschaft

6.1 Digitalisierter Laden

Herr O. betritt an einem Bahnhof einen Einkaufsladen und wundert sich, dass kein Kassenpersonal anwesend ist. Stattdessen legt die Kundschaft ihre Waren in eine Box mit Sensoren, die die Ware automatisch scannen. Vor dem erstmaligen Besuch des Ladens registrieren sich die Kundinnen und Kunden, indem sie ihr Gesicht scannen lassen und eine Online-Verbindung zu ihrem Bankkonto erstellen. Am Ende jedes Einkaufs wird das Gesicht erneut gescannt, und der Betrag der ausgewählten Waren wird dem jeweiligen Konto belastet.

Betroffene Grund- und Menschenrechte

- Recht auf Privatsphäre
- Recht auf Datenschutz

Rechtliche Fragestellung

Wie ist der digitalisierte Laden aus Sicht des Datenschutzgesetzes zu beurteilen?

Rechtliche Beurteilung

Die Betreiberin des digitalen Ladens sammelt und speichert verschiedene Daten ihrer Kundschaft: Zum einen den Namen, E-Banking-Angaben, evtl. Adresse und die eingekauften Produkte, zum anderen die mit dem Gesichtsscanner erhobenen biometrischen Daten. Bei biometrischen Daten handelt es sich um besonders schützenswerte Personendaten.

Im vorliegenden Fall bearbeitet nicht der Staat, sondern ein Unternehmen verschiedene Daten seiner Kundschaft. Das Datenschutzgesetz sorgt dafür, dass in solchen Konstellationen das Recht auf Privatsphäre und das Recht

auf Datenschutz gewahrt bleiben (→ **Grundlagen Kapitel 2.2.7**). Dieses legt fest, unter welchen Voraussetzungen Privatpersonen und Unternehmen Daten anderer Privater bearbeiten dürfen (Art. 26 ff. DSG; Art. 30 ff. Rev-DSG).

Wenn ein Unternehmen Personendaten erhebt, speichert und auswertet, darf es die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen. Das wäre insbesondere dann der Fall, wenn für die Datenbearbeitung eine Einwilligung notwendig ist und diese fehlt. Eine Einwilligung ist erst dann gültig, wenn sie gestützt auf ausreichende Information zur Datenbearbeitung und freiwillig gegeben wurde. In einem digitalisierten Einkaufsgeschäft muss die Kundschaft der Datenerhebung zustimmen, um überhaupt einkaufen zu können. Sofern mit den biometrischen Daten auch besonders schützenswerte Daten erhoben werden, muss die Einwilligung ausdrücklich erfolgen. Insbesondere reicht es hierfür nicht aus, dass die Kundinnen und Kunden bereits vorgesetzte Häkchen in Checkboxen wieder abwählen. Stattdessen müssen sie diese Haken aktiv selber setzen, um in die Datenschutzbestimmungen einzuwilligen.[208]

Je mehr Dienstleistungen digitalisiert werden, desto fraglicher wird, ob eine Einwilligung in die Datenbearbeitung überhaupt «freiwillig» erfolgen kann. Dies hängt unter anderem davon ab, ob die Einwilligung ohne Ausübung von Druck erteilt wurde.[209] Wenn bestimmte Dienstleistungen nur noch digital und im Gegenzug zur Bekanntgabe von persönlichen Daten in Anspruch genommen werden können, haben die Konsumentinnen und Konsumenten keine echte Wahlfreiheit mehr, was gerade bei essenziellen Dienstleistungen aus Sicht des Datenschutzes problematisch ist.

Weitere Vorschriften für die Bearbeitung von Personendaten sind: Die Bearbeitung muss nach Treu und Glauben erfolgen und verhältnismässig sein. Der mit der Erhebung verfolgte Zweck darf nur mithilfe von Daten erreicht werden, die dafür geeignet und erforderlich sind. Gleiches gilt für die Aufbewahrung der Daten.[210] Die Personendaten dürfen nur zu dem Zweck bearbeitet werden, über den beim Erheben der Daten informiert wurde, der allenfalls aus den Umständen ersichtlich war oder gesetzlich vorgesehen ist. Zudem soll die betroffene Person erkennen können, dass Personendaten

208 Keller, Datenschutz, 2019, S. 45.

209 Baeriswyl, Kommentar zu Art. 4 DSG, 2015, N. 65 f.

210 Baeriswyl, Kommentar zu Art. 4 DSG, 2015, N. 20 ff.

von ihr erhoben werden und zu welchem Zweck dies geschieht. Auch muss das Unternehmen die Richtigkeit der Daten überprüfen. Falsche Daten müssen berichtigt oder vernichtet werden. Schliesslich muss die Datensammlung gegen unbefugten Zugriff anderer gesichert sein. Ausserdem dürfen Personendaten nur dann gegen den Willen der betroffenen Person bearbeitet oder besonders schützenswerte Personendaten an Dritte weitergegeben werden, wenn ein Rechtfertigungsgrund vorliegt. Diese ergeben sich aus der bereits erwähnten Einwilligung der Betroffenen oder dem Vorliegen eines überwiegenden privaten oder öffentlichen Interesses (letzteres liegt zum Beispiel bei einer polizeilichen Ermittlung im Rahmen einer Strafverfolgung vor).

Schlussfolgerungen und Empfehlungen

Ob die Erhebung und Speicherung der Personendaten im digitalisierten Laden aus Sicht des Datenschutzes zulässig ist, hängt somit insbesondere davon ab, ob die Kundschaft bei der erstmaligen Registrierung ausreichend darüber informiert wird, welche Daten zu welchem Zweck erhoben, wie sie gespeichert und wie sie allenfalls weiterverwendet werden. Auch müsste die Kundschaft darüber informiert werden, ob die erhobenen Daten auch dafür verwendet werden, ihnen in Zukunft Produktvorschläge zu machen. Weil mit dem Gesichtsscanner biometrische Daten erhoben werden, müssten sie sich damit ausdrücklich einverstanden erklären.

Falls Daten von Kundinnen und Kunden unzulässigerweise gesammelt wurden, können diese vom Unternehmen die Berichtigung oder Löschung der Daten verlangen. Nötigenfalls kann dafür eine Klage beim Zivilgericht eingereicht werden (Art. 15 Abs. 1 DSG i.V.m. Art. 28 ZGB; Art. 32 Abs. 2 Rev-DSG).

Weiterführende Hinweise

2019 startete Migros im Hauptbahnhof Zürich ein Pilotprojekt, bei dem sich die Kundschaft mit einer App Zugang zum Laden verschafft und mit dieser auch selbstständig bezahlt. In anderen Ländern wird in digitalisierten Läden mit Gesichtserkennung gearbeitet.[211]

211 NZZ, Der kassenlose Laden kommt in die Schweiz, 2019.

6.2 Internetbasierte Geschäftsmodelle (Plattformökonomie)

Herr P. arbeitet als Kurier für einen Essenslieferdienst, der über eine digitale Plattform organisiert ist. Die Plattform informiert ihn über eine Handy-App, wenn das bestellte Essen in einem Restaurant zur Lieferung an die Kundschaft bereit ist. Herr P. wird von der Plattform auf Stundenbasis bezahlt. Als er wegen einer Grippe eine Woche lang nicht arbeiten kann, erhält er kein Geld.

Betroffene Grund- und Menschenrechte

- Wirtschaftsfreiheit
- Recht auf Arbeit zu angemessenen Bedingungen
- Recht auf soziale Sicherheit

Rechtliche Fragestellung

Geschäftsmodelle der sogenannten Plattformökonomie standen in jüngerer Vergangenheit teilweise wegen prekärer Arbeitsbedingungen der beschäftigten Personen in der Kritik: Die Kuriere würden von den Plattformbetreiberinnen fälschlicherweise als selbstständig Erwerbende behandelt (Scheinselbstständigkeit) und hätten dementsprechend arbeitsrechtliche und sozialversicherungsrechtliche Nachteile. Dürfen Plattformbetreibende frei darüber entscheiden, ob sie die beschäftigten Personen als Arbeitnehmende oder als selbstständig erwerbende «Partner» betrachten? Was kann Herr P. tun, wenn er sich gegen den Lohnausfall zur Wehr setzen möchte?

Rechtliche Beurteilung

Der oben beschriebene Lieferdienst arbeitet nach dem Geschäftsmodell der Plattformökonomie. Es bringt Anbietende und Interessierte auf einem digitalen Marktplatz zusammen. Im vorliegenden Beispiel verbindet die Plattform Kundinnen und Kunden, Restaurants und Kuriere miteinander: Die Kundschaft kann über eine von der Betreiberin bereitgestellte App Aufträge an bestimmte Restaurants erteilen, und die Plattform verteilt die Lieferaufträge über einen Algorithmus an die Kuriere. Dafür erhält die Betreiberin der Plattform bei jeder getätigten Bestellung eine Provision.

Die Betreiberinnen einer Plattform, über die Dienstleistungen wie die Essenslieferung vermittelt werden, können sich auf die Wirtschaftsfreiheit berufen. So steht es der Plattformbetreiberin grundsätzlich frei, wie sie ihr Geschäft organisiert und wie sie Verträge ausgestaltet. Sie kann die Kuriere als Arbeitnehmende anstellen oder aber als Selbstständige verpflichten. Die Wirtschaftsfreiheit gilt jedoch nicht absolut und kann beispielsweise zum Schutz der Arbeitnehmenden eingeschränkt werden.

Die Unterscheidung, ob eine Person angestellt oder als selbstständige «Partnerin» verpflichtet wird, ist deshalb wichtig, weil sie grosse Auswirkungen auf den arbeitsrechtlichen Schutz und die Sozialversicherungen hat: Das Obligationenrecht enthält verschiedene Vorschriften, welche die Arbeitnehmenden schützen, nicht aber selbstständig Erwerbende. So gibt es beispielsweise eine Kündigungsfrist, und bei Krankheit muss der Lohn für eine gewisse Zeit weiterbezahlt werden. Ein Vertrag mit einer selbstständig erwerbenden Person kann hingegen normalerweise ohne Kündigungsfrist jederzeit beendet werden, und es besteht kein Anspruch auf Bezahlung bei Krankheit. Auch bei den Sozialversicherungen sind Arbeitnehmende bessergestellt. So erfasst ein Teil der Versicherungen grundsätzlich nur Arbeitnehmende und keine selbstständig Erwerbenden (Arbeitslosenkasse, soziale Unfallversicherung, obligatorische Pensionskasse). Bei der AHV/IV zahlen Arbeitnehmende und Arbeitgebende die Versicherungsbeiträge hälftig. Selbstständig Erwerbende tragen ihre Beiträge alleine.

Ob eine Person als angestellte, unselbstständige Arbeitnehmende gilt, hängt insbesondere davon ab, ob sie in untergeordneter Stellung auf bestimmte oder unbestimmte Zeit Arbeit leistet, ohne ein wirtschaftliches Risiko zu tragen. Dabei spielt es keine Rolle, wie das Verhältnis im Vertrag definiert wird. Ob jemand als angestellt gilt, entscheidet die zuständige Ausgleichskasse. Sie beurteilt dafür jeden Fall einzeln und orientiert sich an den genannten Abgrenzungskriterien.[212]

Im obigen Beispiel wird Herr P. durch die Plattform benachrichtigt, wann und wo er Essen abholen und wohin liefern soll. Welcher der Kuriere mit einer konkreten Lieferung betraut wird, entscheidet der Algorithmus der Plattform. Ohne diese Benachrichtigung könnte Herr P. keine Kurierdienste wahrnehmen und würde somit auch nichts verdienen. Diese Abhängigkeit

212 Zentrale Ausgleichskasse, Sozialversicherungsrechtliche Stellung, 2017.

ist ein starkes Indiz dafür, dass es sich bei seiner Tätigkeit nicht um eine selbstständige Tätigkeit handelt, sondern dass Herr P. Arbeitnehmer der Plattformbetreiberin ist. Damit würde er von den arbeitsrechtlichen Schutzbestimmungen erfasst und hätte Anspruch auf Lohnfortzahlung während seiner Krankheit.[213]

Schlussfolgerungen und Empfehlungen

Die Abgrenzung zwischen selbstständiger und unselbstständiger Tätigkeit ist nicht immer ganz eindeutig. Sie hängt von der Organisation des jeweiligen Unternehmens ab. Auch die Durchsetzung der arbeitsrechtlichen Ansprüche, wie die Lohnfortzahlung während der Krankheit von Herrn P., kann in der Praxis schwierig sein. Betroffene Kuriere wie Herr P. können sich dazu beispielsweise bei den Rechtsauskunftsstellen der erstinstanzlichen Zivilgerichte in den Kantonen informieren.

Weiterführende Hinweise

Im Juni 2020 entschied das Genfer Verwaltungsgericht, beim Essenskurier «Uber Eats» handle es sich um einen Arbeitgeber, und sprach den Fahrerinnen und Fahrern die Eigenschaft als Arbeitnehmende zu.[214]

213 Gächter/Meier, Rechtsgutachten Uber-Fahrer, 2018, Rz. 40 und 113.

214 NZZ, Uber, 2020.

Fazit

Wie die Fallbeispiele aufzeigen, hat die Digitalisierung in den unterschiedlichsten Lebensbereichen einen grossen Einfluss auf die Grund- und Menschenrechte. Dessen müssen sich Unternehmen, staatliche Behörden und Privatpersonen bewusst sein, wenn sie digitale Technologien entwickeln, einsetzen, anwenden oder anderweitig damit in Kontakt kommen. Digitalisierung ist kein unkontrollierbarer Vorgang, sondern eine gesellschaftliche Entwicklung, die sich nicht nur beeinflussen, sondern auch gestalten lässt. Es ist daher von zentraler Bedeutung zu diskutieren, wie digitale Technologien von den beteiligten Akteuren ausgestaltet, eingesetzt und allenfalls reguliert werden müssen, damit sie nicht zu Grund- und Menschenrechtsverletzungen führen, sondern vielmehr zur Stärkung der Grund- und Menschenrechte jeder einzelnen Person beitragen.

Abkürzungsverzeichnis

AJP	Aktuelle Juristische Praxis (Zeitschrift)
Abs.	Absatz
ArGV 3	Verordnung 3 zum Arbeitsgesetz
Art.	Artikel
AVO	Verordnung über die Beaufsichtigung von privaten Versicherungsunternehmen
BAKOM	Bundesamt für Kommunikation
BGE	Bundesgerichtsentscheid
Bst.	Buchstabe
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft
DLT	Distributed-Ledger-Technologie
DSG	Bundesgesetz über den Datenschutz
DSGVO	Datenschutz-Grundverordnung der EU
E.	Erwägung
EBGB	Eidgenössisches Büro für die Gleichstellung von Menschen mit Behinderungen
EDK	Schweizerische Konferenz der kantonalen Erziehungsdirektoren
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EMRK	Europäische Menschenrechtskonvention
et al.	und andere
FAZ	Frankfurter Allgemeine Zeitung
GlG	Bundesgesetz über die Gleichstellung von Frau und Mann
GVP	Gerichts- und Verwaltungspraxis des Kantons Zug
Hrsg.	Herausgeberinnen und/oder Herausgeber
InTeR	Zeitschrift zum Innovations- und Technikrecht
IT	Informationstechnik

IoT	Internet of Things
KI	künstliche Intelligenz
NZZ	Neue Zürcher Zeitung
o.D.	ohne Datum
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OR	Obligationenrecht
Rev-DSG	Revidiertes Datenschutzgesetz
Rz.	Randziffer
SBFI	Staatssekretariat für Bildung, Forschung und Innovation
SECO	Staatssekretariat für Wirtschaft
SGB	Schweizerischer Gewerkschaftsbund
SJZ	Schweizerische Juristen-Zeitung
SKMR	Schweizerisches Kompetenzzentrum für Menschenrechte
SNF	Schweizerischer Nationalfonds
StGB	Schweizerisches Strafgesetzbuch
StPO	Schweizerische Strafprozessordnung
SZK	Schweizerische Zeitschrift für Kriminologie
SZW	Schweizerische Zeitung für Wirtschafts- und Finanzmarktrecht
UNO-Sozialpakt	Internationaler Pakt über wirtschaftliche, soziale und kulturelle Rechte
UNO-Zivilpakt	Internationaler Pakt über bürgerliche und politische Rechte
URG	Bundesgesetz über das Urheberrecht und verwandte Schutzrechte
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
ZBJV	Zeitschrift des Bernischen Juristenvereins
ZGB	Schweizerisches Zivilgesetzbuch
ZSR	Zeitschrift für Schweizerisches Recht
ZStR	Schweizerische Zeitschrift für Strafrecht

Literaturverzeichnis

ABEGG ANDREAS/BERNAUER CHRISTOF, Welchen neuen Regulierungsbedarf schaffen Airbnb, Uber & Co.?, AJP/PJA 1/2018, S. 82 ff.

ADAMSON ADEWOLE/SMITH AVERY, Machine Learning and Health Care Disparities in Dermatology, JAMA Dermatology 11/2018.

AKKAYA GÜLCAN, Grund- und Menschenrechte in der Sozialhilfe, Ein Leitfaden für die Praxis, Luzern 2015.

AKKAYA GÜLCAN/BELSER EVA MARIA/EGBUNA-JOSS ANDREA/JUNG-BLATTMANN JASMIN, Grund- und Menschenrechte von Menschen mit Behinderungen, Ein Leitfaden für die Praxis der sozialen Arbeit, Luzern 2016.

AMMANN ROBERT, Nutzen und Grenzen der robotergestützten Pflege, Krankenpflege/ Soins infirmiers 4/2019, S. 22 ff.

BAERISWYL BRUNO, Kommentar zu Art. 4 DSG, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz, Bern 2015.

BAISCH STEFANIE/KOLLING THORSTEN/RÜHL SASKIA ET AL., Emotionale Roboter im Pflegekontext, Empirische Analyse des bisherigen Einsatzes und der Wirkung von Paro und Pleo, Zeitschrift für Gerontologie und Geriatrie 1/2018, S. 16 ff.

BEZEMEK CHRISTOPH, The 'Filter Bubble' and Human Rights, in: Petkova Bilyana/Ojanen Toumas (Hrsg.), Fundamental Rights Protection Online, The Future Regulation of Intermediaries, Cheltenham 2020, S. 34 ff.

BIAGGINI GIOVANNI, BV Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft, 2. Auflage, Zürich 2017.

BITKOM E.V./DFKI, Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, Berlin 2017.

BRAUN BINDER NADJA, Als Verfügungen gelten Anordnungen der Maschinen im Einzelfall, Dystopie oder künftiger Verwaltungsalltag?, ZSR 139/2020, S. 253 ff.

BRAUN BINDER NADJA, Automatisierte Entscheidungen, Perspektive Datenschutzrecht und öffentliche Verwaltung, SZW 1/2020, S. 27 ff.

BRAUN BINDER NADJA, Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, SJZ 115/2019, S. 467 ff.

BREITENMOSER STEPHAN/SCHWEIZER RAINER J., Kommentar zu Art. 13 BV, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J. et al. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Auflage, Zürich 2014.

BRUN MARCEL, Cyberbullying – aus strafrechtlicher Sicht, recht – Zeitschrift für juristische Weiterbildung und Praxis 2/2016, S. 100 ff.

BÜCHLER ANDREA, Kommentar zu Art. 28 ff. ZGB, in: Kren Kostkiewicz Jolanta/Wolf Stephan/Amstutz Marc et al. (Hrsg.), ZGB Kommentar, 3. Auflage, Zürich 2016.

CAMAVDIC BENJAMIN, Predictive Policing in der Schweiz, Die Vereinbarkeit des Predictive Policing mit der schweizerischen Rechtsordnung, Jusletter IT, 26.9.2019.

CAVELTI URS JOSEF/KLEY ANDREAS, Kommentar zu Art. 15 BV, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J. et al. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Auflage, Zürich 2014.

DASTIN JEFFREY, Amazon scraps secret AI recruiting tool that showed bias against women, Reuters, 11.10.2018.

DIGGELMANN OLIVER, Kommentar zu Art. 13 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar Bundesverfassung, Basel 2015.

EGGEN MIRJAM, Home Smart Home, Eine privatrechtliche Einordnung von Lösungen für intelligentes Wohnen, AJP/PJA 9/2016, S. 1131 ff.

EGGEN MIRJAM/STENGEL CORNELIA, Wearables – Eine vertragsrechtliche Betrachtung, Jusletter, 19.11.2018.

EGGER, DREHER & PARTNER AG, Bestandesaufnahme aller arbeitsmarktlichen Massnahmen für über 50-jährige Stellensuchende in den Kantonen, 17.4.2019.

EGLI SANDRA/EGBUNA-JOSS ANDREA/GHIELMINI SABRINA/BELSER EVA MARIA/KAUFMANN CHRISTINE, Grundrechte im Alter, Ein Handbuch, Luzern 2019.

EGLI URS, Soziale Netzwerke und Arbeitsverhältnis, Über die Auswirkung von Facebook, Xing & Co. auf den betrieblichen Alltag, Jusletter, 17.1.2011.

ERRASS CHRISTOPH, Kommentar zu Art. 22 BV, in: Ehrenzeller Bernhard/Schindler Benjamin/ Schweizer Rainer J. et al. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Auflage, Zürich 2014.

FAZ ONLINE, Eine Blockchain für den Schwarzen Seehecht, 16.10.2019.

GÄCHTER THOMAS/MEIER MICHAEL E., Sozialversicherungsrechtliche Qualifikation von Uber-Fahrern, Rechtsgutachten zuhanden der UNIA Bern, Zürich 2018.

GLATTHAAR MATTHIAS, Robot Recruiting, Datenschutzrechtliche Aspekte einer Automatisierung von Rekrutierungsentscheiden, SZW 1/2020, S. 43 ff.

GYARMATI NIKOLAUS, Phänomen Cybercrime und seine Bekämpfung, SZK 1/2019, S. 86 ff.

HAFNER PETER, Auswertung der E-Mails von Arbeitnehmern, AJP/PJA 11/2018, S. 1327 ff.

HART PATRICK, Hate-Speech, Ein sozialpsychologisches Phänomen im Zeitalter der Globalisierung, in: Grafl Christian/Klob Bernhard/Reindl-Krauskopf Susanne (Hrsg.), «Das wird man ja wohl noch sagen dürfen!» – Meinungsfreiheit und Strafrecht, Schriftenreihe Kriminalwissenschaften in Theorie und Praxis 12/2018, S. 13 ff.

HATTENHAUER RAINER, Das Computerlexikon für Einsteiger, Bonn 2019.

HUBER STEPHAN GERHARD/GÜNTHER PAULA SOPHIA/SCHNEIDER NADINE ET AL., COVID-19 – aktuelle Herausforderungen in Schule und Bildung, Erste Befunde des Schul-Barometers in Deutschland, Österreich und der Schweiz, Münster 2020.

HUG MARKUS/SCHEIDEGGER ALEXANDRA, Kommentar zu Art. 221 StPO, in: Donatsch Andreas/Hansjakob Thomas/Lieber Viktor (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung, Zürich 2014.

JANNES MARC/FRIELE MINOU/JANNES CHRISTIANE ET AL., Algorithmen in der digitalen Gesundheitsversorgung, Gütersloh 2018.

JIANG FEI/JIANG YONG/ZHI HUI ET AL., Artificial intelligence in healthcare, Past, present and future, Stroke and Vascular Neurology 2/2017, S. 230 ff.

JØRGENSEN RIKKE FRANK, Human Rights and Private Actors in the Online Domain, in: Land Molly K./Aronson Jay D. (Hrsg.), New Technologies for Human Rights Law and Practice, Cambridge 2018, S. 243 ff.

KÄGI-DIENER REGULA, Kommentar zu Art. 19 BV, in: Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J. et al. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Auflage, Zürich 2014.

KÄLIN WALTER/KÜNZLI JÖRG, Universeller Menschenrechtsschutz, Der Schutz des Individuums auf globaler und regionaler Ebene, 4. Auflage, Basel 2019.

KAMASA JULIAN, Neue Technologien für Grenzkontrollen in Europa, CSS Analysen zur Sicherheitspolitik 255/2019, S. 1 ff.

KELLER CLAUDIA, Datenschutz, Zürich 2019.

KIENER REGINA/KÄLIN WALTER/WYTTENBACH JUDITH, Grundrechte, 3. Auflage, Bern 2018.

KREIS JEANNE, Umsorgen, überwachen, unterhalten – sind Pflegeroboter ethisch vertretbar?, in: Bendel Oliver (Hrsg.), Pflegeroboter, Wiesbaden 2018, S. 213 ff.

LANGER LORENZ, Staatliche Nutzung von Social Media-Plattformen, AJP/PJA 7/2014, S. 946 ff.

MARKIĆ LUKA, Die elektronische Stimmabgabe im Lichte des Prinzips der Öffentlichkeit, E-Voting im Spannungsverhältnis zwischen dem Ruf nach mehr digitaler Demokratie und der Wahl- und Abstimmungsfreiheit, in: Dal Molin-Kränzlin Alexandra/Schneuwly Anne Mirjam/Stojanovic Jasna (Hrsg.), Digitalisierung – Gesellschaft – Recht, APARIUZ 2019, S. 125 ff.

MEIER-GUBSER STEFANIE, Mitarbeiterüberwachung, Rechte, Pflichten und Verbote, TREX 5/2020.

MÖHRING KATJA/NAUMANN ELIAS/REIFENSCHEID MAXIMILIANE ET AL., Die Mannheimer Corona-Studie, Schwerpunktbericht zu Erwerbstätigkeit und Kinderbetreuung, Mannheim 2020.

MÜLLER JÖRG PAUL, Verwirklichung der Grundrechte nach Art. 35 BV, Der Freiheit Chancen geben, Bern 2018.

NZZ, Algorithmen unter Rassismusverdacht, 24.5.2016.

NZZ, Die Diagnose kommt vom Computer, 26.7.2019.

NZZ, Der kassenlose Laden kommt in die Schweiz – wird bald auch Gesichtserkennung eingesetzt?, 27.8.2019.

NZZ, Uber muss nachgeben, In Genf haben die Food-Kuriere nun einen Arbeitsvertrag, 1.9.2020.

PÄRLI KURT, Kommentar zu Art. 328b OR, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Stämpflis Handkommentar zum Datenschutzgesetz, Bern 2015.

PELLASCIO MICHEL, Kommentar zu Art. 328 ff. OR, in: Kren Kostkiewicz Jolanta/Wolf Stephan/Amstutz Marc et al. (Hrsg.), OR Kommentar, 3. Auflage, Zürich 2016.

RASO FILIPPO/HILLIGOSS HANNA/KRISHNAMURTHY VIVEK ET AL., Artificial Intelligence & Human Rights, Opportunities & Risks, Berkman Klein Center Research Publication 6/2018.

RECHSTEINER DAVID, Der Algorithmus verfügt, Verfassungs- und verwaltungsrechtliche Aspekte automatisierter Einzelentscheidungen, Jusletter, 26.11.2018.

ROCHER LUC/HENDRICKX JULIEN M./DE MONTJOYE YVES-ALEXANDRE, Estimating the success of re-identifications in incomplete datasets using generative models, Nature Communications 10/2019, S. 1 ff.

RÜTSCHE BERNHARD, Was sind öffentliche Aufgaben?, recht – Zeitschrift für Weiterbildung und Praxis 4/2013, S. 153 ff.

SCHAFHEITLE SIMON/WEIBEL ANTOINETTE, HR Tech Survey, Pulse of people analytics in Switzerland 2020, St. Gallen 2020.

SCHMID NIKLAUS/JOSITSCH DANIEL, Praxiskommentar Schweizerische Strafprozessordnung, 3. Auflage, Zürich/St. Gallen 2018.

SCHWEIZER RAINER J., Kommentar zu Art. 10 BV, in: Ehrenzeller Bernhard/Schindler Benjamin/ Schweizer Rainer J. et al. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Auflage, Zürich 2014.

SCHWEIZERISCHE STIFTUNG ZUR BEHINDERTENGERECHTEN TECHNOLOGIENUTZUNG, Schweizer Accessibility-Studie, Bestandesaufnahme der Zugänglichkeit bedeutender Schweizer Internet-Angebote, Zürich 2016.

SGB, Dossier Nr. 125, Digitalisierung muss den Berufstätigen nützen, Analyse und Handlungsbedarf, Bern 2017.

SIMMLER MONIKA/BRUNNER SIMONE/SCHEDLER KUNO, Smart Criminal Justice, Eine empirische Studie zum Einsatz von Algorithmen in der Schweizer Polizeiarbeit und Strafrechtspflege, St. Gallen 2020.

SÖBBING THOMAS, Künstliche Intelligenz im HR-Recruiting-Prozess, Rechtliche Rahmenbedingungen und Möglichkeiten, InTeR 2/2018, S. 64 ff.

SPRECHER FRANZISKA, Datenschutzrecht und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, ZBJV 8/2018, S. 519 ff.

SRF, CVP verschweigt digitalen Datenspion, 26.6.2019.

SRF, Aargauer und Solothurner Polizei bleiben bei Autonummern-Scanner, 31.10.2019.

SRF, Wie soziale Roboter in Altersheimen helfen sollen, 15.10.2020.

STREIFF ULLIN/VON KAENEL ADRIAN/RUDOPLH ROGER, Arbeitsvertrag, Praxiskommentar zu Art. 319–362 OR, 7. Auflage, Zürich 2012.

TAGESANZEIGER, Lieferroboter der Post fahren nicht mehr, 4.3.2019.

THOUVENIN FLORENT, Forschung im Spannungsfeld von Big Data und Datenschutzrecht, Eine Problemskizze, in: Boehme-Nessler Volker/Rehbinder Manfred (Hrsg.), Big Data, Ende des Datenschutzes?, Gedächtnisschrift für Martin Usteri, Bern 2017, S. 27 ff.

THOUVENIN FLORENT/FRÜH ALFRED/GEORGE DAMIAN, Datenschutz und automatisierte Entscheidungen, Jusletter, 26.11.2018.

TSCHANNEN PIERRE, Kommentar zu Art. 33 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar Bundesverfassung, Basel 2015.

VALLONE VERA, Wenn sich Algorithmen absprechen, Wettbewerbsabreden durch künstliche Intelligenz, ex ante 2/2018, S. 35 ff.

WEBER ROLF H./THOUVENIN FLORENT (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014.

WEBER ROLF H./LAUX CHRISTIAN/OERTLY DOMINIC, Datenpolitik als Rechtsthema, Zürich 2016.

WEBER ROLF H., Blockchain als rechtliche Herausforderung, Jusletter, 18.5.2017.

WEBER ROLF H./THOUVENIN FLORENT, Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft?, ZSR 1/2018, S. 43 ff.

WEBER ROLF H., Digitalisierung und der Kampf ums Recht, in: Dal Molin-Kränzlin Alexandra/Schneuwly Anne Mirjam/Stojanovic Jasna (Hrsg.), Digitalisierung – Gesellschaft – Recht, APARIUZ 2019, S. 3 ff.

Weber Rolf H., Automatisierte Entscheidungen, Perspektive Grundrechte, SZW 1/2020, S. 18 ff.

Wermelinger Amédéo, Kommentar zu Art. 15 DSG, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Datenschutzgesetz (DSG), Bern 2015.

Weydner-Volkmann Sebastian/Feiten Linus, Vertrauensstiftende Videoüberwachung?, digma 4/2019, S. 218 ff.

Widmer Lüchinger Corinne, Digitale Innovation und ärztliche Sorgfalt, Life Science Recht – Juristische Zeitschrift für Pharma, Biotech und Medtech 2/2019, S. 77 ff.

Wildhaber Isabelle, Robotik am Arbeitsplatz, Robo-Kollegen und Robo-Bosse, AJP/PJA 2/2017, S. 213 ff.

Wirth Felix/Johns Marco/Meurers Thierry et al., Anonymisierung medizinischer Daten, Innovative medizinische Forschung benötigt qualitativ hochwertige Daten. Können diese sicher anonymisiert werden?, digma 2/2020, S. 74 ff.

Wohlers Wolfgang, Kommentar zu Art. 79b StGB, in: Wohlers Wolfgang/Godenzi Gunhild/Schlegel Stephan (Hrsg.), Handkommentar Schweizerisches Strafgesetzbuch, 4. Auflage, Bern 2020.

Zeit Online, Twitter-Nutzer machen Chatbot zur Rassistin, 24.3.2016.

Zeller Franz/Kiener Regina, Kommentar zu Art. 17 BV, in: Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar Bundesverfassung, Basel 2015.

Zuiderveen Borgesius Frederik, Discrimination, artificial intelligence and algorithmic decision-making, Strassburg 2018.

Materialienverzeichnis

BAKOM, Wie sich Privatpersonen gegen Verletzungen ihrer Persönlichkeits-Rechte durch Dritte auf Social Media Plattformen wehren können, 2013.

BRITISCHER NATIONALER KONTAKTPUNKT FÜR DIE OECD-LEITSÄTZE FÜR MULTINATIONALE UNTERNEHMEN, Privacy International & Gamma International UK Ltd, Final Statement, 2014.

BUNDESRAT, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6942, 15.9.2017.

BUNDESRAT, Bedrohungsmanagement, insbesondere bei häuslicher Gewalt, Bericht in Erfüllung des Postulates Feri 13.3441, 11.10.2017.

BUNDESRAT, Auswirkungen der Digitalisierung auf Beschäftigung und Arbeitsbedingungen – Chancen und Risiken, Bericht in Erfüllung der Postulate 15.3854 Reynard und 17.3222 Derder, 8.11.2017.

BUNDESRAT, Goldhandel und Verletzung der Menschenrechte, Bericht in Erfüllung des Postulats Recordon 15.3877, 14.11.2018.

BUNDESRAT, Civic Tech und Vereinfachung des Vernehmlassungsverfahrens, Entwicklungen und Massnahmen, Bericht in Erfüllung der Postulate 17.3149 Hausammann und 17.4017 Müller Damian, 8.5.2020.

BUNDESRAT, Strategie Digitale Schweiz, 2020.

DEUTSCHER BUNDESTAG, Menschenrechte im digitalen Zeitalter, WD2-3000-107/18, 3.8.2018.

EBGB, Leitfaden barrierefreie digitale Kommunikation, Version 2.0, 2018.

EBGB, Faktenblatt Leichte Sprache, Version 2.1, 2019.

EDK, Massnahmen zur Digitalisierungsstrategie der EDK, 27.6.2019.

EDÖB, Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz, Für die Privatwirtschaft, 2013.

EDÖB/PRIVATIM, Leitfaden der Datenschutzbehörden von Bund und Kantonen zur Anwendung des Datenschutzrechts auf die digitale Bearbeitung von Personendaten im Zusammenhang mit Wahlen und Abstimmungen in der Schweiz, 2019.

EDÖB, Erläuterungen zu Webtracking, 2014, abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/erlaeuterungen-zu-webtracking.html> (Stand 30.12.2020).

EDÖB, Erläuterungen zu Cloud Computing, o.D., abrufbar unter: <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing.html> (Stand 30.12.2020).

EUROPÄISCHE KOMMISSION, Künstliche Intelligenz für Europa, Mitteilung der Kommission an das Europäische Parlament, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, COM 237/2018, 25.4.2018.

EUROPARAT MINISTERKOMMITEE, Empfehlung Nr. R (97) 20 über Hassrede, 30.10.1997.

GEMEINDERAT STADT BERN, Online-Angebote, Effort für mehr Barrierefreiheit, Medienmitteilung, 16.8.2018.

HAMBURGISCHER BEAUFTRAGTER FÜR DATENSCHUTZ UND INFORMATIONSFREIHEIT, Polizei Hamburg löscht die im Zuge der G20-Ermittlungen erstellte biometrische Datenbank zum Gesichtsabgleich, 28.5.2020.

NATIONALRAT, Interpellation 18.3282, Entsolidarisierung in der Grundversicherung verhindern, 18.3.2018.

OECD, Going Digital, Shaping Policies, Improving Lives, 11.3.2019.

OECD, Is there a role for blockchain in responsible supply chains?, 11.9.2019.

REGIERUNGSRAT KANTON ZÜRICH, Impulsprogramm Digitale Verwaltung 2020, 1.4.2020.

SBFI, Herausforderungen der künstlichen Intelligenz, Bericht der interdepartementalen Arbeitsgruppe «Künstliche Intelligenz» an den Bundesrat, 13.12.2019.

SCHWEIZERISCHE KRIMINALPRÄVENTION, Cybermobbing, Alles, was Recht ist, 2. Auflage, 2017.

SECO, Wegleitung zu den Verordnungen 3 und 4 zum Arbeitsgesetz, Gesundheitsschutz, Plangenehmigung, 2020.

SNF, Reglement über die Open-Access-Publikationsförderung, 7.11.2017.

STÄNDERAT, Postulat 16.4169, Inklusives Arbeitsumfeld im Lichte der Digitalisierung, 16.12.2016.

UNO-AUSSCHUSS FÜR WIRTSCHAFTLICHE, SOZIALE UND KULTURELLE RECHTE, General Comment Nr. 25 on Science and Economic, Social and Cultural Rights, E/C.12/GC/25, 30.4.2020.

UNO-HOCHKOMMISSARIAT FÜR MENSCHENRECHTE, Human Rights in a New Era, Speech at the University of Geneva by UN High Commissioner for Human Rights Michelle Bachelet, 14.11.2018, abrufbar unter: <https://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23874&LangID=E> (Stand 30.12.2020).

UNO-HOCHKOMMISSARIAT FÜR MENSCHENRECHTE, Question of the realization of economic, social and cultural rights in all countries, the role of new technologies for the realization of economic, social and cultural rights, A/HRC/43/29, 4.3.2020.

UNO-Hochkommissariat für Menschenrechte, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protest, A/HRC/44/24, 24.6.2020.

UNO-Kinderrechtsausschuss, The Committee on the Rights of the Child warns of the grave physical, emotional and psychological effect of the COVID-19 pandemic on children and calls on States to protect the rights of children, 8.4.2020.

UNO-Kinderrechtsausschuss, General Comment Nr. 25, Children's rights in relation to the digital environment, 2.3.2021.

UNO-Sonderberichterstatter für Menschenrechte und extreme Armut, Digital Welfare State, A/74/48037, 11.10.2019.

UNO-Sonderberichterstatter über die Förderung der Meinungsfreiheit und das Recht auf freie Meinungsäusserung, Surveillance and human rights, A/HRC/41/35, 28.5.2019.

UNO-Sonderberichterstatter zu Menschenrechten und Terrorismusbekämpfung, Annual Report, A/HRC/34/61, 21.2.2017.

UNO-Sonderberichterstatter zum Recht auf Bildung, Right to education in the digital age, A/HRC/32/37, 6.4.2016.

Zentrale Ausgleichskasse, Sozialversicherungsrechtliche Stellung in der AHV/IV/EO, Merkblatt, 2017.

Autorinnen

Sabrina Ghielmini

MLaw, Rechtsanwältin, wissenschaftliche Mitarbeiterin am Kompetenzzentrum Menschenrechte, Universität Zürich, und beim Themenbereich Menschenrechte und Wirtschaft des SKMR.

Christine Kaufmann

Prof. Dr. iur., ordentliche Professorin für öffentliches Recht, Völker- und Europarecht und Vorsitzende Leitungsausschuss Kompetenzzentrum Menschenrechte, Universität Zürich, Themenbereichsleitung Menschenrechte und Wirtschaft des SKMR.

Charlotte Post

MLaw, wissenschaftliche Mitarbeiterin beim Themenbereich Menschenrechte und Wirtschaft des SKMR.

Tina Büchler

Dr. phil. nat., wissenschaftliche Mitarbeiterin am Interdisziplinären Zentrum für Geschlechterforschung, Universität Bern, und beim Themenbereich Geschlechterpolitik des SKMR.

Mara Wehrli

Hilfsassistentin am Interdisziplinären Zentrum für Geschlechterforschung, Universität Bern, Bereich Postkolonialismus.

Michèle Amacker

Prof. Dr., Assistenzprofessorin für Geschlechterforschung, Co-Leitung des Interdisziplinären Zentrums für Geschlechterforschung, Universität Bern, und Themenbereichsleitung Geschlechterpolitik des SKMR.

Die Digitalisierung hat ein grosses Potenzial, Grund- und Menschenrechte in ganz unterschiedlichen Lebensbereichen zu stärken. Gleichzeitig besteht die Gefahr, dass digitale Technologien zu neuen oder verschärften Formen von Grund- und Menschenrechtsverletzungen führen.
Die vorliegende Publikation, herausgegeben vom Schweizerischen Kompetenzzentrum für Menschenrechte (SKMR), gibt einen Überblick, wie sich digitale Technologien im Alltag auf die Grund- und Menschenrechte auswirken. In einem ersten Teil behandelt sie wichtige neue Technologien und Anwendungen sowie die relevanten rechtlichen Grundlagen. In einem zweiten Teil erläutern die Autorinnen anhand von ausgewählten Fallbeispielen, welche Grund- und Menschenrechte bei der Entwicklung und Anwendung von digitalen Technologien betroffen sind. Das Buch leistet damit einen Beitrag zur Diskussion, wie Grund- und Menschenrechte und Digitalisierung miteinander vereinbar sind.

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

buch & netz