sui generis

HANDELN

Digitales Verwaltungshandeln

Rechtliche Aspekte der Digitalisierung in der öffentlichen Verwaltung

Roger Plattner

Roger Plattner

Digitales Verwaltungshandeln

Rechtliche Aspekte der Digitalisierung in der öffentlichen Verwaltung

Hinweise zur digitalen Fassung dieses Buches:

— Die digitale Fassung (Open Access) ist sowohl auf der Webseite des Verlags (www.suigeneris-verlag.ch), auf Google Books als auch direkt über den Digital Object Identifier (DOI) zugänglich. Der DOI zum vorliegenden Buch ist im Impressum angegeben.
— Sämtliche Gesetzesartikel sowie alle frei zugänglichen Gerichtsurteile und Behördenentscheidungen sind in der digitalen Fassung verlinkt.
— Häufig verwenden die AutorInnen in ihrem Manuskript Links auf weitere Quellen. Diese werden in den Büchern nicht abgedruckt, aber in der digitalen Fassung den entsprechenden Textstellen hinterlegt.
— Für die Verlinkung werden Permalinks eingesetzt. Es handelt sich dabei um Links auf eine archivierte Version der Webseiten im Zeitpunkt der Linksetzung. Die Links sind beständig, d.h. sie funktionieren auch dann noch, wenn die Originalseite nicht mehr zugänglich ist und ihr Inhalt ändert nicht, wenn sich die Originalseite ändert.

Roger Plattner

Digitales Verwaltungshandeln

Rechtliche Aspekte der Digitalisierung in der öffentlichen Verwaltung

sui generis, Zürich 2021

Für meine Eltern

Vorwort

Die vorliegende Arbeit wurde am 30. September 2020 von der Rechtswissenschaftlichen Fakultät der Universität Zürich als Dissertation angenommen. Die Digitalisierung der Verwaltung ist rasanten Entwicklungen und Wandlungen unterworfen. So war etwa zum Zeitpunkt der Fertigstellung des Manuskripts dieser Arbeit noch nicht absehbar, wie die Stimmbevölkerung über das Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz) abstimmen würde, welches Grundregeln für staatlich anerkannte elektronische Identitäten definieren soll und als wichtiger Mosaikstein für die digitale Leistungserbringung durch die Verwaltung angesehen wird. Zum Zeitpunkt der Publikation der Monographie ist hingegen der Ausgang dieser Referendumsabstimmung bereits bekannt. Dieser stetige Wandel macht das Thema hochinteressant, bringt aber auch Tücken mit sich. Das Manuskript dieser Arbeit wurde im Juli 2020 fertiggestellt. Daher konnten Entwicklungen in Lehre, Rechtsprechung und technologischer Natur nach diesem Zeitpunkt nur noch punktuell berücksichtigt werden.

Mein Dank gilt zuallererst meinem Doktorvater Prof. Dr. Tilmann Altwicker. Er hat meinen Arbeitsprozess mit grossem Interesse an diesem auch für ihn wichtigen Thema unterstützt und stand mir für Fragen und mit Hinweisen stets zur Verfügung. Von meiner Tätigkeit im Team der SNF-Förderungsprofessur und seinen Inputs auch ausserhalb der rein rechtlichen Betrachtungsweisen habe ich über die fast drei Jahre sehr viel profitiert. Daneben möchte ich auch Prof. Dr. Andreas Glaser für die zügige Erstellung des Zweitgutachtens und die wertvollen Hinweise danken.

Ein grosser Dank gilt auch dem gesamten Lehrstuhlteam der SNF-Förderungsprofessur, welches mir ebenfalls wertvolle Anregungen und teilweise auch willkommene Ablenkung im Rahmen der «Pflichtpausen» mitgab. Vielen Dank daher an: Martin Cattaneo, Frederic Fitzi, Florian «Empirical Flo» Geering, Daniel Gerber (danke für den «latte macchiato»), Zoé Gianocca, Alexandra Hansen und Andrea Vuksic.

Für die kritische Durchsicht und die wertvollen Hinweise danke ich zudem Ado Kaiser, Flavia Berger und meinem Bruder Matthias Plattner. Für die Konzeption des Titelbilds danke ich meinem Bruder Joël Plattner. Auch allen anderen, welche hier nicht namentlich genannt sind und mir auf dem Weg mit Rat und Tat oder einem offenen Ohr zur Seite standen, möchte ich an dieser Stelle danken

Der grösste Dank gilt aber meinen Eltern Denise Steinmann Plattner und Roland Plattner-Steinmann. Sie haben mich im Laufe meiner gesamten

Ausbildung und insbesondere in der Ausarbeitung dieser Dissertation bedingungslos unterstützt und immer wieder bestärkt. Ohne sie wäre diese Arbeit nie entstanden. Ihnen sei diese Schrift gewidmet.

Basel, März 2021
Roger Plattner

Inhaltsübersicht

Inhaltsverzeichnis

Literatur- und Materialienverzeichnis

Literaturverzeichnis

AEBI-MÜLLER REGINA / GÄCHTER THOMAS / ALIOTTA MASSIMO, Observationen im Sozialversicherungsrecht – Voraussetzungen und Schranken, in: Personen-Schaden-Forum 2011, Zürich, 2011, S. 179 ff.

ALBERTINI MICHELE, Der verfassungsmässige Anspruch auf rechtliches Gehör im Verwaltungsverfahren des modernen Staates, Eine Untersuchung über Sinn und Gehalt der Garantie unter besonderer Berücksichtigung der bundesgerichtlichen Rechtsprechung, Diss., Bern, 1999.

ALFTER BRIGITTE, Denmark, in: Automating Society – Taking Stock of Automated Decision-Making in the EU, Berlin, Januar 2019, S. 45 ff.

ALSTON PHILIP, Amicus brief in the case of NJCM c.s./De Staat der Nederlanden (SyRI): Implications of the use of digital technologies in welfare states, New York, 26. September 2019.

ALTWICKER TILMANN
- Transnationale Direktanfragen im Kontext des Übereinkommens über Cyberkriminalität des Europarats, in: Migration, Datenübermittlung und Cybersicherheit, Baden-Baden, 2016, S. 105 ff.
- Statistikbasierte Argumentation im Verwaltungsrecht, ZBl, 2018, S. 619 ff.
- International Legal Scholarship and the Challenge of Digitalization, Chinese Journal of International Law, 2019, S. 217 ff.

ANTONOPOULOS ANDREAS M., Mastering Bitcoin, Sebastopol, 2015.

ARNOLD CHRISTIAN, Die Gerichtsstandsklausel in den AGB von Facebook aus schweizerischer Sicht, SZIER, 2012, S. 613 ff.

ARNTZ MELANIE / GREGORY TERRY / ZIERAHN ULRICH, The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis, OECD Social, Employment and Migration Working Papers No. 189, 16. Juni 2016.

ARTIKEL-29-DATENSCHUTZGRUPPE
- Opinion 1/2010 on the concepts of "controller" and "processor", 16. Februar 2010.

– Opinion 5/2014 on Anonymisation Techniques, 10. April 2014 (= Artikel-29-Datenschutzgruppe, Opinion 5/2014).
– Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3. Oktober 2017 (= Artikel-29-Datenschutzgruppe, Guidelines ADM).

ATZORI MARCELLA, Blockchain Technology and Decentralized Governance: Is the State Still Necessary?, 1. Dezember 2015.

AUER ANDREAS / ARX NICOLAS VON, La légitimité des procédures de vote: les défis du e-voting, AJP, 2002, S. 491 ff.

Auer Christoph / Müller Markus / Schindler Benjamin / Altmann Rahel (Hrsg.), Kommentar zum Bundesgesetz über das Verwaltungsverfahren, 2. Aufl., Zürich, 2019 (zit. VwVG-Kommentar).

Bader Johann / Ronellenfitsch Michael (Hrsg.), Verwaltungsverfahrensgesetz, Mit Verwaltungsvollstreckungsgesetz und Verwaltungszustellungsgesetz: Kommentar, 47. Aufl., München, 2020 (zit. Kommentar VwVfG-D).

BAERISWYL BRUNO, Wenn die Rechtsauslegung «nebulös» wird, digma, 2019, S. 118 ff.

Baeriswyl Bruno / Pärli Kurt (Hrsg.), Datenschutzgesetz (DSG), Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG), Bern, 2015 (zit. SHK-DSG).

BANSAK KIRK / FERWERDA JEREMY / HAINMUELLER JENS / DILLON ANDREA / HANGARTNER DOMINIK / LAWRENCE DUNCAN / WEINSTEIN JEREMY, Improving refugee integration through data-driven algorithmic assignment, Science, 2018, S. 325 ff.

BARTH ARMIN P., Algorithmik für Einsteiger, Für Studierende, Lehrer und Schüler in den Fächern Mathematik und Informatik, 2. Aufl., Wiesbaden, 2013.

BASIN DAVID, Risikofolgenabschätzung zur Verwendung der AHV-Nummer als Personenidentifikator, Gutachten zuhanden des Bundesamts für Justiz (BJ) und des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), 27. September 2017.

BECHTOLF HANS / VOGT NIKLAS, Datenschutz in der Blockchain – Eine Frage der Technik, Technologische Hürden und konzeptionelle Chancen, ZD, 2018, S. 66 ff.

BERGER ARIANE, Der automatisierte Verwaltungsakt. Zu den Anforderungen an eine automatisierte Verwaltungsentscheidung am Beispiel des § 35a VwVfG, NVwZ, 2018, S. 1260 ff.

BERGHOFF CHRISTIAN / GEBHARDT UTE / LOCHTER MANFRED / MASSBERG SARAH, Blockchain sicher gestalten, Konzepte, Anforderungen, Bewertungen, Bonn, März 2019.

Bergmann Jan / Dienelt Klaus / Bauer Ina (Hrsg.), Ausländerrecht, Aufenthaltsgesetz, Freizügigkeitsgesetz/EU und ARB 1/80 (Auszug), Grundrechtecharta und Artikel 16a GG, Asylgesetz / Kommentar, 12. Aufl., München, 2018 (zit. Beck-Komm. Ausländerrecht-D).

BERRYHILL JAMIE / BOURGERY THÉO / HANSON ANGELA, Blockchains Unchained: Blockchain Technology and its use in the Public Sector, OECD Working Papers on Public Governance No. 28, Juni 2018.

Biaggini Giovanni (Hrsg.), BV Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft, 2. Aufl., Zürich, 2017 (zit. OFK BV).

BIRYUKOV ALEX / KHOVRATOVICH DMITRY / PUSTOGAROV IVAN, Deanonymisation of clients in Bitcoin P2P network, Proceedings of the 2014 ACM SIGSAC Conference, S. 15 ff.

BITKOM E. V.
- Künstliche Intelligenz, Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung, Berlin, 2017.
- Blockchain und Datenschutz, Faktenpapier, Berlin, 5. April 2018 (= Bitkom e. V., Blockchain-Studie).

BOEHME-NESSLER VOLKER
- Unscharfes Recht, Überlegungen zur Relativierung des Rechts in der digitalisierten Welt, Habil., Berlin, 2008.
- Wer formt den digitalen Code?, Rechtssetzung in der digitalisierten Gesellschaft, ZG, 2009, S. 74 ff.

BOLFING ANTON / HEINSER BERNHARD / GIUDICE GIANFRANCO / RITTER PETRA, Schweizer Accessibility Studie 2016, Zürich, 2016.

BOLLIGER CHRISTIAN / FÉRAUD MARIUS, Der Austausch von Personendaten zwischen Bundes-, Kantons- und Gemeindebehörden, Studie im Auftrag des Bundesamtes für Justiz, Bern, Februar 2010.

Bovay Benoît (Hrsg.), Mélanges en l'honneur de Pierre Moor, Professeur à la Faculté de droit de l'Université de Lausanne, Théorie du droit; droit administratif; organisation du territoire, Bern, 2005 (zit. FS Moor).

BRÄNDLI BEAT, Prozessökonomie im schweizerischen Recht, Grundlagen, bundesgerichtliche Rechtsprechung und Auswirkungen im schweizerischen Zivilprozess, Diss., St. Gallen, 2013.

BRAUN NADJA, Stimmgeheimnis, Eine rechtsvergleichende und rechtshistorische Untersuchung unter Einbezug des geltenden Rechts, Diss., Bern, 2006.

BRAUN BINDER NADJA
- Vollautomatisierte Verwaltungsverfahren im allgemeinen Verwaltungsverfahrensrecht?, NVwZ, 2016, S. 960 ff.
- Auf dem Weg zum vollautomatisierten Besteuerungsverfahren in Deutschland, Jusletter IT, 25. Mai 2016.
- Künstliche Intelligenz und automatisierte Entscheidungen in der öffentlichen Verwaltung, SJZ, 2019, S. 467 ff.
- Vollautomatisierte Verwaltungsverfahren, vollautomatisiert erlassene Verwaltungsakte und elektronische Aktenführung, in: Digitalisierte Verwaltung – Vernetztes E-Government, Berlin, 2019, S. 311 ff.

BREITENMOSER STEPHAN / HOFMANN ROLAND, Akten-Digitalisierung und elektronischer Rechtsverkehr, Justice – Justiz – Giustizia, 2019.

BRITZ GABRIELE, § 26 Elektronische Verwaltung, in: Grundlagen des Verwaltungsrechts, München, 2012, S. 435 ff.

BROSCH CHRISTOPHER, Nutzungspflicht für das besondere elektronische Anwaltspostfach?, NJW, 2015, S. 3692 ff.

BRÜESCH CAROLINE / MERTES ALEXANDER / FLICK WITZIG MARTINA / GIGER MARC-ANDRÉ / STEINBRECHER MARKUS, Digitale Verwaltung, Eine Studie des Institutes für Verwaltungs-Management (IVM) und KPMG Schweiz, Winterthur, 2017.

BRUNNER STEPHAN C.
- Vom Öffentlichkeitsprinzip zur transparenten Verwaltung, in: Das Öffentlichkeitsgesetz des Bundes, St. Gallen, 2006, S. 75 ff.
- Persönlichkeitsschutz bei der behördlichen Information der Öffentlichkeit von Amtes wegen: Ein Leitfaden, ZBl, 2010, S. 595 ff.

Brunner Stephan C. / Mader Luzius (Hrsg.), Öffentlichkeitsgesetz, Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung vom 17. Dezember 2004 (BGÖ), Bern, 2008 (zit. SHK BGÖ).

BUCHLI MARTIN / FRIEDRICH UELI, Handbuch Informationsaustausch unter Behörden Kanton Bern, Bern, 2012.

BUESS MICHAEL / ISELIN MILENA / BIERI OLIVER, Nationale E-Government-Studie 2017, E-Government in der Schweiz aus Sicht der Bevölkerung, der Unternehmen und der Verwaltung, Adligenswil/Luzern, 2017.

BUESS MICHAEL / RAMSDEN ALMA / BIERI OLIVER, Nationale E-Government-Studie 2019, E-Government in der Schweiz aus Sicht der Bevölkerung, der Unternehmen und der Verwaltung, Adligenswil/Luzern, 2019.

BÜHLMANN LUKAS / REINLE MICHAEL, Extraterritoriale Wirkung der DSGVO, digma, 2017, S. 8 ff.

BUNDESKARTELLAMT, Fallbericht Facebook; Konditionenmissbrauch gemäß §19 Abs.1 GWB wegen unangemessener Datenverarbeitung, 15. Februar 2019.

BUNDESVERBAND DIGITALE WIRTSCHAFT (BVDW) E.V., Social Media Kompass 2012/2013, Düsseldorf, 2012.

BUSCH CHRISTOPH, Algorithmic Accountability, Gutachten im Rahmen des ABIDA Projekts, Osnabrück, 2018.

CAMAVDIC BENJAMIN, Predictive Policing in der Schweiz, Jusletter IT, 26. September 2019.

CHATZIATHANASIOU KONSTANTIN, Der hungrige, ein härterer Richter? Zur heiklen Rezeption einer vielzitierten Studie, JZ, 2019, S. 455 ff.

CIOLA-DUTOIT SOPHIE / COTTIER BERTIL, Le droit de la personnalité à l'épreuve des blogs, medialex, 2008, S. 72 ff.

CUENI RAPHAELA, Falsche und irreführende Informationen im Verfassungsrecht der Schweiz, ex ante, 2019, S. 3 ff.

DANZIGER SHAI / LEVAV JONATHAN / AVNAIM-PESSO LIORA, Extraneous factors in judicial decisions, PNAS, 2011, S. 6889 ff.

DAPP MARCUS M./BALTA DIAN / KRCMAR HELMUT, Blockchain – Disruption der öffentlichen Verwaltung?, Eine Technologie zur Neugestaltung der Verwaltungsprozesse, Berlin, Juni 2017.

DATENSCHUTZBEAUFTRAGTER DES KANTONS BASEL-STADT, Merkblatt zur Anwendbarkeit der EU-Datenschutzgesetzgebung, Basel, 22. Januar 2019.

DEGRANDI BENNO, Die automatisierte Verwaltungsverfügung, Diss., Zürich, 1977.

DIETRICH SABRINA / MÜLLER LENA-SOPHIE / AKKAYA TÜRKAVCI CIGDEM / KRCMAR HELMUT / BOBERACH MICHAEL / EXEL STEFANIE, eGovernment Monitor 2017, Nutzung und Akzeptanz digitaler Verwaltungsangebote – Deutschland, Österreich und Schweiz im Vergleich, Berlin, München, 2017.

DIGITALE GESELLSCHAFT, Stellungnahme zur Mitwirkungspflicht im Asylverfahren: Überprüfungsmöglichkeit bei Mobiltelefonen, 4. Juni 2020.

DOVAS MARIA-URANIA, Automatisierte Einzelentscheidungen, digma, 2017, S. 98 ff.

DREYER STEPHAN, Predictive Analytics aus der Perspektive von Menschenwürde und Autonomie, in: Big Data – Regulative Herausforderungen, Baden-Baden, 2018, S. 135 ff.

DREYER STEPHAN / SCHULZ WOLFGANG, Was bringt die Datenschutz-Grundverordnung für automatisierte Entscheidungssysteme?, Gütersloh, April 2018.

DRUEY JEAN NICOLAS, Information als Gegenstand des Rechts, Entwurf einer Grundlegung, Zürich, 1995.

EBERHARD JACOB / TAI STEFAN, On or Off the Blockchain? Insights on Off-Chaining Computation and Data, ESOCC (European Conference on Service-Oriented and Cloud Computing), 2017, S. 3 ff.

EGGEN MIRJAM, Chain of Contracts, Eine privatrechtliche Auseinandersetzung mit Distributed Ledgers, AJP, 2017, S. 3 ff.

Ehmann Eugen / Selmayr Michael (Hrsg.), DS-GVO, Kommentar, 2. Aufl., München, 2018 (zit. Ehmann/Selmayr DSGVO).

Ehrenzeller Bernhard / Schindler Benjamin / Schweizer Rainer J./Vallender Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar BV, 3. Aufl., Zürich, 2014 (zit. SG Komm. BV).

EICHENBERGER SARAH / PRIBNOW VOLKER, Rentengrundlage Facebook-Profil?, HAVE, 2017, S. 275 ff.

ENGELER MALTE, Der staatliche Twitter-Auftritt, Rechtliche Hürden und mögliche Lösungen, MMR, 2017, S. 651 ff.

EPINEY ASTRID, Datenschutzrechtliche Rahmenbedingungen – Zu den datenschutzrechtlichen Vorgaben für öffentliche Organe des Bundes und der Kantone, in: Jahrbuch 2010, Bern, 2011, S. 5 ff.

EPINEY ASTRID / CIVITELLA TAMARA / ZBINDEN PATRIZIA, Datenschutzrecht in der Schweiz, Eine Einführung in das Datenschutzgesetz des Bundes, mit besonderem Akzent auf den für Bundesorgane relevanten Vorgaben, Freiburg, 2009.

Epping Volker / Hillgruber Christian (Hrsg.), Grundgesetz, Beck OK, 42. Aufl., München, 2020 (zit. Beck OK Grundgesetz).

ERBGUTH JÖRN, Datenschutz auf öffentlichen Blockchains, Jusletter IT, 22. Februar 2018.

ERNST CHRISTIAN, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ, 2017, S. 1026 ff.

EUROPEAN COMMISSION, eGovernment Benchmark 2017, Luxemburg, 2017.

EUROPEAN DATA PROTECTION BOARD (EDPB), Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), März 2018.

EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM, Legal and regulatory framework of Blockchains and Smart Contracts, Brüssel, September 2019.

FASCHING JOACHIM, Anwendungsbereiche und ausgewählte Rechtsfragen der Blockchain-Technologie, Master-Thesis, Wien, 2017.

FAVROD-COUNE PASCAL, Crowdfunding, Analyse de droit suisse du financement participatif, Diss., Lausanne, 2018.

FELFERING ALEXANDER / STETTINGER MARTIN / WUNDARA MANFRED / STANIK CHRISTOPH, Künstliche Intelligenz in der öffentlichen Verwaltung, in: Handbuch E-Government, Wiesbaden, 2019, S. 491 ff.

FINCK MICHÈLE, Blockchains and Data Protection in the European Union, EDPL, 2018, S. 17 ff.

FRAEFEL MARIANNE / KUHN FABIENNE / NEURONI ALESSIA / RIEDL REINHARD / SCHMID MARCEL, Open Government Data – Grundlagenstudie Schweiz 2013, Bern, Juni 2013.

FRAEFEL MARIANNE / SELZAM THOMAS / HUNZIKER ALEXANDER, E-Government Schweiz nachhaltig organisieren, Bern, 24. April 2012.

FRECH PHILIPP, Zivilrechtliche Haftung von Internet-Providern bei Rechtsverletzungen durch ihre Kunden, Eine rechtsvergleichende Untersuchung des schweizerischen, des amerikanischen und des deutschen Rechts unter besonderer Berücksichtigung des Urheber- und Markenrechts, Diss., Zürich, 2009.

FREI ANDREAS, Die Risikoeinschätzung von schwerwiegender häuslicher Gewalt anhand des computerisierten Prognoseinstrumentes DyRiAS – Eine Evaluationsstudie anhand von Fällen aus der Schweiz, in: Bedrohungsmanagement in der Schweiz, Frankfurt am Main, Im Erscheinen.

FREIBURGHAUS DIETER, E-Justice – etwas weniger Hektik bitte…, Justice – Justiz – Giustizia, 2018.

FREY FLORIAN / ROGG JÜRGEN / SCHMID CHRISTIAN, Digitale Verwaltung Schweiz, Wie gelingt der Aufstieg zur Spitze?, Zürich, Juni 2017.

FRÖHLICH WIEBKE / SPIECKER GENANNT DÖHMANN INDRA, Können Algorithmen diskriminieren?, VerfBlog, 26.12.2018.

GÄCHTER THOMAS, Schnell, schwammig, schlecht. Zugespitztes zu Art. 43a und Art. 43b ATSG, HAVE, 2018, S. 216 ff.

Geiser Thomas / Fountoulakis Christiana (Hrsg.), Zivilgesetzbuch I, Art. 1-456 ZGB, 6. Aufl., Basel, 2018 (zit. BSK ZGB I).

GERTH JULIANE / ROSSEGGER ASTRID / SINGH JAY P. / ENDRASS JÉRÔME, Assessing the Risk of Severe Intimate Partner Violence : Validating the DyRiAS in Switzerland, Archives of Forensic Psychology, 2015, S. 1 - 15.

GIGER ANGELA / HANGARTNER SENA, Identitätsdiebstahl in der digitalen Welt – die Gefahren des Missbrauchs persönlicher Daten und Prävention, Neuntes Zürcher Präventionsforum, S&R, 2017, S. 121 ff.

GILES JIM, Internet encyclopaedias go head to head, Nature, 2005, S. 900 f.

GISLER MICHAEL
- Einführung in die Begriffswelt des E-Government, in: eGovernment, Bern etc., 2001, S. 13 ff.
- Zum Beispiel eGovernment, Anwendungen der ICT in der Verwaltung, medienheft, 2003, S. 43 ff.

GLASER ANDREAS
- Der elektronisch handelnde Staat, ZSR, 2015, S. 259 ff.
- Einflüsse der Digitalisierung auf das schweizerische Verwaltungsrecht, SJZ, 2018, S. 181 ff.

GLASER ANDREAS / EHRAT MARCO, E-Government-Gesetzgebung durch die Kantone – Integration in die Verfahrenskodifikation oder Auslagerung in Spezialerlasse?, LeGes, 2019.

GLATTHAAR MATTHIAS, Robot Recruiting, SZW, 2020, S. 43 ff.

GOLLIEZ ANDRÉ / ASCHWANDEN CÉCILE / BRETSCHER CLAUDIA / BERNSTEIN ABRAHAM / FARAGO PETER / KRÜGEL SYBIL / FREI FELIX / LAUX CHRISTIAN / BUCHER BRUNO / NEURONI ALESSIA / RIEDL REINHARD, Open Government Data Studie Schweiz, Juni 2012.

GORDON CLARA-ANN/LUTZ TANJA, Haftung für automatisierte Entscheidungen – Herausforderungen in der Praxis, SZW, 2020, S. 53 ff.

GOTTLIEB DUTTWEILER INSTITUTE, Die Zukunft der vernetzten Gesellschaft, Rüschlikon, 2014.

GRAF DAMIAN K., Strafverfolgung 2.0: Direkter Zugriff der Strafbehörden auf im Ausland gespeicherte Daten?, Jusletter IT, 21. September 2017.

GRAF VON WESTPHALEN FRIEDRICH, Digitale Charta – Erweiterung der europäischen Grundrechte für das digitale Zeitalter, BB, 2018, S. 899 ff.

Griffel Alain / Kölz Alfred/Bosshart Jürg / Röhl Martin (Hrsg.), Kommentar zum Verwaltungsrechtspflegegesetz des Kantons Zürich (VRG), 3. Aufl., Zürich, 2014 (zit. Komm. VRG ZH).

GUCKELBERGER ANNETTE, Öffentliche Verwaltung im Zeitalter der Digitalisierung, Analysen und Strategien zur Verbesserung des E-Governments aus rechtlicher Sicht, 1. Aufl., Baden-Baden, 2019.

GUGGENBERGER NIKOLAS, Datenschutz durch Blockchain – eine große Chance, ZD, 2017, S. 49 f.

GÜNDÜZ ALI ASKER / METTLER TOBIAS / SCHEDLER KUNO, Smart Government – Partizipation und Empowerment der Bürger im Zeitalter von Big Data und personalisierter Algorithmen, HMD, 2017, S. 477-487.

GUNNING DAVID / AHA DAVID, DARPA's Explainable Artificial Intelligence (XAI) Program, AI Magazine, 2019, S. 44 ff.

HÄFELIN ULRICH / MÜLLER GEORG / UHLMANN FELIX, Allgemeines Verwaltungsrecht, 7. Aufl., Zürich, St. Gallen, 2016.

HÄNER ISABELLE
- Die Feststellung des rechtserheblichen Sachverhalts, in: Das erstinstanzliche Verwaltungsverfahren, Zürich, 2008, S. 33 ff.
- Anwaltsrevue, 2009, S. 174 ff.
- Digitalisierung des Verwaltungsverfahrens, in: Jahrbuch 2017/2018, Bern, 2018, S. 23 ff.
- Justizia 4.0 – Folgen für den Verwaltungsprozess, Justice – Justiz – Giustizia, 2018.

HANSJAKOB THOMAS, Überwachungsrecht der Schweiz, Kommentar zu Art. 269 ff. StPO und zum BÜPF, Zürich, Basel, Genf, 2018.

HARASGAMA REHANA, Erfahren – Wissen – Vergessen, Zur zeitlichen Dimension des staatlichen Informationsanspruches, Diss., Zürich, 2017.

HÄRTEL INES, Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren, LKV, 2019, S. 49 ff.

HÄRTING NIKO / GÖSSLING PATRICK, Gemeinsame Verantwortlichkeit bei einer Facebook-Fanpage, NJW, 2018, S. 2523 ff.

HEMMERT-HALSWICK MAXIMILIAN, EuGH: Urteil zu Facebook-Fanpages, MMR-Aktuell, 2018.

HERBERGER MAXIMILIAN, «Künstliche Intelligenz» und Recht, NJW, 2018, S. 2825 ff.

HESS MARTIN / LIENHARD STEPHANIE, Übertragung von Vermögenswerten auf der Blockchain, Jusletter, 4. Dezember 2017.

HETTICH PETER, Kapitel 20: Handlungsformen, in: Fachhandbuch Verwaltungsrecht, Zürich, 2015, S. 823 ff.

HEUSSER PIERRE, ATSG goes TKKG: Sozialdetektive sind unnötig, systemwidrig und unverhältnismässig, HAVE, 2018, S. 206 ff.

HILL HERMANN, Was bedeutet Künstliche Intelligenz (KI) für die Öffentliche Verwaltung?, VM, 2018, S. 287 ff.

HOCHRANGIGE EXPERTENGRUPPE KI, A definition of AI: Main capabilities and scientific disciplines, 2019.

HOFFMANN CHRISTIAN / SCHULZ SÖNKE E. / BRACKMANN FRANZISKA, Die öffentliche Verwaltung in den sozialen Medien?, Zulässigkeit behördlicher Facebook-Fanseiten, ZD, 2013, S. 122 ff.

HOFFMANN-RIEM WOLFGANG
- Regulierungswissen in der Regierung, in: Wissensregulierung und Regulierungswissen, Weilerswist, 2014, S. 135 ff.
- Rechtliche Rahmenbedingungen für und regulative Herausforderungen durch Big Data, in: Big Data – Regulative Herausforderungen, Baden-Baden, 2018, S. 11 ff.

HOHLFELD RALF / GORDULLA ALEXANDER, Das Phänomen der Sozialen Medien, in: Rechtshandbuch Social Media, Heidelberg Germany, 2015, S. 11 ff.

HOLL JÜRGEN / KERNBEISS GÜNTER / WAGNER-PINTER MICHAEL, Das AMS-Arbeitsmarktchancen-Modell, Dokumentation zur Methode, Wien, Oktober 2018.

HOLZNAGEL BERND, Phänomen «Fake News» – Was ist zu tun?, MMR, 2018, S. 18 ff.

HORNER SUSANNE / KAULARTZ MARKUS, Haftung 4.0, InTeR, 2016, S. 22 ff.

HORSCHIK MATTHIAS, Datenschutz und Einsatz von Privatdetektiven, in: Datenschutz im Arbeits-, Versicherungs- und Sozialbereich: Aktuelle Herausforderungen, St. Gallen, 2012, S. 81 ff.

HÖSLI PETER, Auf dem Weg zu fast papierlosen amtlichen Publikationsorganen im Kanton Zürich, LeGes, 2013, S. 157 ff.

IMBODEN MAX / RHINOW RENÉ, Schweizerische Verwaltungsrechtsprechung, Die Rechtsgrundsätze der Verwaltungspraxis, erläutert an Entscheiden der Verwaltungsbehörden und Gerichte, 5. Aufl., Basel, Stuttgart, 1976.

INFANGER ROLAND, Darf ein Richter googeln?, Justice – Justiz – Giustizia, 2017.

ISLER MICHAEL, Datenschutz auf der Blockchain, Jusletter, 4. Dezember 2017.

IVANOV DANIELA, Die Veröffentlichung von Materialien in den Kantonen, LeGes, 2013, S. 105 ff.

JACCARD GABRIEL, L'identité digitale et la création du surhomme 2.0, Jusletter, 30. April 2018.

JENSEN BJORNAR / KOCH MARKUS, Mensch und Maschine: Roboter auf dem Vormarsch?, Auswirkungen der Automatisierung auf den Schweizer Arbeitsmarkt, Zürich, 9. November 2015.

JÖRGER ANDREAS, Aktenführungspflicht und Modalitäten der Akteneinsichtnahme im Verwaltungsverfahrensrecht, Anwaltsrevue, 2019, S. 479 ff.

KAHL WOLFGANG, Kodifizierung des Verwaltungsverfahrensrechts in Deutschland und in der EU, JuS, 2018, S. 1025 ff.

KÄLIN WALTER / LIENHARD ANDREAS / WYTTENBACH JUDITH, Auslagerung von sicherheitspolizeilichen Aufgaben, Basel, 2007.

KALSCHEUER FIETE / HORNUNG CHRISTIAN, Das Netzwerkdurchsetzungsgesetz – Ein verfassungswidriger Schnellschuss, NVwZ, 2017, S. 1721 ff.

KALSCHEUER FIETE / JACOBSEN ANNIKA, Das digitale Hausrecht von Hoheitsträgern, Unter welchen Voraussetzungen darf der Staat Twitter-Nutzer blockieren?, NJW, 2018, S. 2358-2362.

KAPLAN ANDREAS / HAENLEIN MICHAEL, Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence, Business Horizons, 2019, S. 15 ff.

KAULARTZ MARKUS, Die Blockchain-Technologie, CR, 2016, S. 474 ff.

KAULARTZ MARKUS / HECKMANN JÖRN, Smart Contracts – Anwendungen der Blockchain-Technologie, CR, 2016, S. 618 ff.

KAYE DAVID
- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/32/38, 11. Mai 2016.
- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/HRC/38/35, 6. April 2018 (= Kaye, Report April 2018).

Kettiger Daniel (Hrsg.), Kommentar zum Publikationsgesetz des Bundes, Bern, 2011 (zit. Komm. PublG).

KETTIGER DANIEL, Die Haftung des Staates für seine Geodaten, in: Jahrbuch 2016/2017, Bern, 2017, S. 104 ff.

KIENER REGINA / RÜTSCHE BERNHARD / KUHN MATHIAS, Öffentliches Verfahrensrecht, 2. Aufl., Zürich, St. Gallen, 2015.

Kieser Ueli (Hrsg.), Kommentar zum Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts ATSG, 4. Aufl., Zürich, Basel, Genf, 2020 (zit. SK ATSG).

KITTLAUS HANS-BERND, Geschäftsmodelle, in: Handbuch Cloud Computing, Köln, 2014, S. 29 ff.

KLAFKI ANIKA / WÜRKERT FELIX / WINTER TINA, Digitalisierung und Öffentliches Recht, in: Digitalisierung und Recht, Hamburg, 2017, S. 1 ff.

KNEBEL SOPHIE VICTORIA, Unmittelbare Grundrechtsbindung von Facebook bei Löschentscheidungen, MMR, 2019, S. 56 ff.

KNOBLOCH TOBIAS, Vor die Lage kommen: Predictive Policing in Deutschland, Chancen und Gefahren datenanalytischer Prognosetechnik und Empfehlungen für den Einsatz in der Polizeiarbeit, Gütersloh, 2018.

KÖLZ ALFRED / HÄNER ISABELLE / BERTSCHI MARTIN, Verwaltungsverfahren und Verwaltungsrechtspflege des Bundes, 3. Aufl., Zürich, 2013.

KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN, Europa verbinden: Die Bedeutung der Interoperabilität für elektronische Behördendienste (eGovernment-Dienste), Brüssel, 2003.

KRCMAR HELMUT / MÜLLER LENA-SOPHIE / SCHEIBER PATRICIA / EXEL STEFANIE / MOTZET KERSTIN / BASTIN MELANIE, eGovernment Monitor 2019, Berlin, München, 16. Oktober 2019.

KROLL JOSHUA A./HUEY JOANNA / BAROCAS SOLON / FELTEN EDWARD W. / REIDENBERG JOEL R. / ROBINSON DAVID G. / YU HARLAN, Accountable Algorithms, PENN LAW REVIEW, 2017, S. 633 ff.

Kühling Jürgen / Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung/ BDSG, Kommentar, 2. Aufl., München, 2018 (zit. Beck-Komm. DSGVO).

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

LATZER MICHAEL / JUST NATHASCHA / METREVELI SULKHAN / SAURWEIN FLORIAN, Internet-Anwendungen und deren Nutzung in der Schweiz. Themenbericht aus dem World Internet Project, Zürich, 2012.

LAUX CHRISTIAN, Haftung der Stadt Zürich für Open Government Data, Gutachten, Zürich, 18. Mai 2012.

LEESE MATTHIAS, Predictive Policing in der Schweiz: Chancen, Herausforderungen, Risiken, in: Bulletin 2018 zur schweizerischen Sicherheitspolitik, Zürich, 2018, S. 57 ff.

LEWINSKI KAI VON, Regulierungsbedarf und Regulierungsfelder von algorithmischen Systemen, InTeR, 2018, S. 168-176.

LINS SEBASTIAN / SUNYAEV ALI, Klassifikation von Cloud-Services, in: Management sicherer Cloud-Services, Wiesbaden, 2018, S. 7 ff.

LUCKE JÖRN VON, Transparenz 2.0 – Transparenz durch E-Government, in: Transparenz, Wiesbaden, 2010, S. 396 ff.

LUCKE JÖRN VON / REINERMANN HEINRICH, Speyerer Definition von Electronic Government, in: Electronic government in Deutschland, Speyer, 2002.

LUHMANN NIKLAS, Recht und Automation in der öffentlichen Verwaltung, Eine verwaltungswissenschaftliche Untersuchung, 1. Aufl., Berlin, 1966.

LUMB RICHARD / TREAT DAVID / JELF OWEN, Editing the uneditable Blockchain, Why distributed ledger technology must adapt to an imperfect world, 2016.

LUMMEL FRIEDERIKE / FENSKE THOMAS / BOYN HEINER, Das besondere elektronische Anwaltspostfach (beA), Jusletter IT, 25. Februar 2016.

MADER LUZIUS
- Das Öffentlichkeitsgesetz des Bundes – Einführung in die Grundlagen, in: Das Öffentlichkeitsgesetz des Bundes, St. Gallen, 2006, S. 9 ff.
- Rechtliche Schranken staatlicher Öffentlichkeitsarbeit, in: St. Galler Tagung zur Öffentlichkeitskommunikation des Staates, St. Gallen, 2010.

MALGIERI GIANCLAUDIO, Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" for Algorithmic Decisions in the EU National Legislations, Computer Law & Security Review, 2019, S. 1 ff.

MARTINI MARIO
- Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz, in: Die digitale Lebenswelt gestalten, Baden-Baden, 2015, S. 97 ff.
- Algorithmen als Herausforderung für die Rechtsordnung, JZ, 2017, S. 1017.
- Transformation der Verwaltung durch Digitalisierung, in: Verwaltungspraxis und Verwaltungswissenschaft, Baden-Baden, 2018, S. 11 ff.

– Blackbox Algorithmus – Grundfragen einer Regulierung Künstlicher Intelligenz, Berlin, 2019 (= Martini, Blackbox).

MARTINI MARIO / NINK DAVID, Wenn Maschinen entscheiden … – vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz, NVwZ-Extra, 2017, S. 1 ff.

MATTER LIVIA, Gesichtserkennung auf dem Vormarsch, digma, 2019, S. 14 ff.

MATTHIAS ANDREAS, Automaten als Träger von Rechten, Diss., Berlin, 2008.

MAUME PHILIPP, Bestehen und Grenzen des virtuellen Hausrechts, MMR, 2007, S. 620.

Maurer-Lambrou Urs / Blechta Gabor Paul (Hrsg.), Datenschutzgesetz, Öffentlichkeitsgesetz. Basler Kommentar, 3. Aufl., Basel, 2014 (zit. BSK DSG/BGÖ).

MELL PETER / GRANCE TIM, The NIST Definition of Cloud Computing, Washington, September 2011.

MELLOULI SEHL / LUNA-REYES LUIS F. / ZHANG JING, Smart government, citizen participation and open data, IP, 2014, S. 1 ff.

MÉTILLE SYLVAIN, L'utilisation de l'informatique en nuage par l'administration publique, AJP, 2019, S. 609 ff.

MEYER CHRISTIAN, Die Mitwirkungsmaxime im Verwaltungsverfahren des Bundes, Ein Beitrag zur Sachverhaltsfeststellung als arbeitsteiligem Prozess, Diss., Luzern, 2019.

MEYER LILIANE, Sprachanalysen zur Herkunftsbestimmung im Asyl- und Ausländerbereich, Ein Neues Gebiet der forensischen Linguistik, Kriminalistik. Unabhängige Zeitschrift für die kriminalistische Wissenschaft und Praxis, 2006, S. 708 ff.

MEYER STEPHAN, Künstliche Intelligenz und die Rolle des Rechts für Innovation, ZRP, 2018, S. 233 ff.

MEYER STEPHAN / SCHUPPLI BENEDIKT, «Smart Contracts» und deren Einordnung in das schweizerische Vertragsrecht, recht, 2017, S. 204 ff.

Meyer-Ladewig Jens / Nettesheim Martin / Raumer Stefan von (Hrsg.), EMRK – Europäische Menschenrechtskonvention, Handkommentar, 4. Aufl., Basel, 2017 (zit. Meyer/Ladewig EMRK).

MILKER JENS, Die Polizei auf Twitter – Brauchen wir ein Social-Media-Gesetz für staatliche Stellen?, NVwZ, 2018, S. 1751 ff.

MÜLLER HENNING, Fristwahrender Eingang elektronischer Dokumente bei Gericht trotz Umlauten und Sonderzeichen in Dateinamen, NZA, 2019, S. 1120 ff.

MÜLLER JÖRG PAUL / SCHEFER MARKUS, Grundrechte in der Schweiz, Im Rahmen der Bundesverfassung, der EMRK und der Uno-Pakte, 4. Aufl., Bern, 2008.

NATIONAL INTEROPERABILITY FRAMEWORK OBSERVATORY (NIFO)
- eGovernment Factsheet Denmark.
- eGovernment Factsheet Austria.
- eGovernment Factsheet Estonia.
- eGovernment Factsheet UK.

NAVES JEROEN / AUDIA BENEDETTA / BUSSTRA MARJOLEIN / HARTOG KOEN LUKAS / VAN HEUKELOM-VERHAGE SANDRA, Legal Aspects of Blockchain, Innovations Technology Governance Globalization, 2019, S. 88 ff.

Niggli Marcel Alexander / Ackermann Jürg-Beat / Wiprächtiger Hans (Hrsg.), Strafrecht, 4. Aufl., Basel, 2018 (zit. BSK Strafrecht).

Niggli Marcel Alexander / Uebersax Peter / Wiprächtiger Hans / Kneubühler Lorenz / Aemisegger Heinz (Hrsg.), Bundesgerichtsgesetz, 3. Aufl., Basel, 2018 (zit. BSK BGG).

NOIZAT PIERRE, Blockchain Electronic Vote, in: Handbook of digital currency, Amsterdam, 2015, S. 453 ff.

OECD, Artificial intelligence in society, 2. Aufl., Paris, 11. Juni 2019.

OPIELA NICOLE / MOHABBAT KAR RESA / THAPA BASANTA / WEBER MIKE, Exekutive KI 2030 – Vier Zukunftsszenarien für Künstliche Intelligenz in der öffentlichen Verwaltung, München, 2018.

OSZE, Joint declaration on freedom of expression and "fake news", disinformation and propaganda, 3. März 2017.

Paal Boris P. / Pauly Daniel A. (Hrsg.), Datenschutz-Grundverordnung, 1. Aufl., München, 2017 (zit. Paal/Pauly DSGVO).

PÄRLI KURT, Datenschutz und Datenaustausch in der Interinstitutionellen Zusammenarbeit (IIZ), digma, 2014, S. 18 ff.

PASSADELIS NICOLAS, Rechtsanwendung bei internationaler Datenbearbeitung durch Private, in: Datenschutzrecht, Basel, 2015, S. 167 ff.

PEDUZZI ROBERTO, Die elektronische Eröffnung von Verfügungen im Bundesverwaltungsverfahren, Anwaltsrevue, 2009, S. 187 ff.

PENNER KRISTINA, European Union, in: Automating Society – Taking Stock of Automated Decision-Making in the EU, Berlin, Januar 2019, S. 17 ff.

PIESBERGEN JENS, Justitia 4.0 – Digitalisierung und Transformation der Justiz, Justice – Justiz – Giustizia, 2018.

PRIVATIM
- Zusammenfassung der Stellungnahme von privatim zum Vernehmlassungsentwurf für ein totalrevidiertes Datenschutzgesetz des Bundes, 9. März 2017.
- Stellungnahme zum E-ID-Gesetz im Rahmen des Vernehmlassungsverfahrens, 2. Mai 2017, abrufbar: Bundesgesetz über elektronische Identifizierungsdienste, Weitere Stellungnahmen.
- Merkblatt Cloud-spezifische Risiken und Massnahmen, 17. Dezember 2019 (= privatim, Merkblatt Cloud-Computing).

RADEMACHER TIMO, Predictive Policing im deutschen Polizeirecht, AöR, 2017, S. 366.

RAINER BÖHME / PAULINA PESCH, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, DuD, 2017, S. 473 ff.

RALL RENÉ, Im Fokus des Vorstands SAV: Die Weichen für Justitia 4.0 sind gestellt, Anwaltsrevue, S. 147 f.

RAUER NILS / ETTIG DIANA, Rechtskonformer Einsatz von Cookies, ZD, 2018, S. 255 ff.

RECHSTEINER DAVID, Der Algorithmus verfügt, Verfassungs- und verwaltungsrechtliche Aspekte automatisierter Einzelentscheidungen, Jusletter, 26. November 2018.

REGIERUNGSRAT DES KANTONS BASEL-STADT, Ratschlag zum Gesetz über ein zentrales elektronisches Behördenportal (Behördenportalgesetz), Basel, 27. September 2016.

REGIERUNGSRAT DES KANTONS SCHWYZ, Gesetz über das E-Government Bericht und Vorlage an den Kantonsrat, Beschluss Nr. 1371/2008, Schwyz, 2008.

REGIERUNGSRATES DES KANTONS ZÜRICH, Antrag Nr. 5134 vom 22. Oktober 2014 zur Änderung des Publikationsgesetzes, ABl 2014-11-07, Zürich, 22. Oktober 2014.

REID FERGAL/HARRIGAN MARTIN, An Analysis of Anonymity in the Bitcoin System, 2011.

REINSEL DAVID / GANTZ JOHN / RYDNING JOHN, Data Age 2025, The Digitization of the World: From Edge to Core, Framingham, November 2018.

RHYNER MARKUS, Kantonsübergreifende Gerichte: sinnvoll für die Gerichtsorganisation bevölkerungsarmer Kantone?, Justice – Justiz – Giustizia, 2019.

RINGEISEN PETER / BERTOLOSI-LEHR ANDREA / DEMAJ LABINOT, Automatisierung und Digitalisierung in der öffentlichen Verwaltung, Digitale Verwaltungsassistenten als neue Schnittstelle zwischen Bevölkerung und Gemeinwesen, Swiss Yearbook of Administrative Sciences, 2018, S. 51 ff.

RIZVI SALI / LENEL BEAT / RISI SIMONA, E-Government – Kaleidoskop aus Digitalisierungselementen, Interaktionskonzept zwischen Verwaltungsbehörden und zwischen der Einwohnerschaft und der Verwaltung, speziell erläutert am Beispiel des Kantons St. Gallen, Jusletter IT, 26. September 2018.

ROON MICHA, Schlichtung und Blockchain, Anwaltsrevue, 2016, S. 359 ff.

ROSENTHAL DAVID
- Personendaten ohne Identifizierbarkeit, digma, 2017, S. 198 ff.
- Der Vorentwurf für ein neues Datenschutzgesetz: Was er bedeutet, Jusletter, 20. Februar 2017.
- Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter, 17. Juni 2019.

Rosenthal David (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, DSG, 2. Aufl., Zürich, 2018 (zit. Handkommentar DSG).

ROSSNAGEL ALEXANDER, Das De-Mail-Gesetz, Grundlage für mehr Rechtssicherheit im Internet, NJW, 2011, S. 1473 ff.

ROTH DAVID, Cloud-basierte Dienstleistungen im Licht der DSGVO, AJP, 2020, S. 68 ff.

ROTH MARIUS, Aktuelle Anforderungen an amtliche Sammlungen, LeGes, 2013, S. 33-62.

ROTH SIMON
- Die grenzüberschreitende Edition von IP-Adressen und Bestandesdaten im Strafprozess, Jusletter 17. August 2015.
- Die automatisierte Einzelentscheidung, digma, 2017, S. 104 ff.

RUCKENSTEIN MINNA / VELKO JULIA, Finland, in: Automating Society – Taking Stock of Automated Decision-Making in the EU, Berlin, Januar 2019, S. 56 ff.

RUDIN BEAT
- Verfassungswidrige Anwendbarkeit des Bundesdatenschutzgesetzes, SJZ, 2009, S. 1 ff.
- Datenschutz- Pendenzen bei OGD, digma, 2012, S. 62 ff.
- Überholte Ausnahmen beim Geltungsbereich, digma, 2016, S. 122 ff.

Rudin Beat / Baeriswyl Bruno (Hrsg.), Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG), Zürich, 2014 (zit. PK IDG BS).

SAFFERLING CHRISTOPH / RÜCKERT CHRISTIAN, Telekommunikationsüberwachung bei Bitcoins, MMR, 2015, S. 788 ff.

Sägesser Thomas (Hrsg.), Regierungs- und Verwaltungsorganisationsgesetz (RVOG), Bern, 2007 (zit. SHK RVOG).

SAXER URS, Einführung und rechtsstaatliche Grundlagen, in: St. Galler Tagung zur Öffentlichkeitskommunikation des Staates, St. Gallen, 2010, S. 1 ff.

SCHAAR PETER, Brauchen wir regulatorische Leitplanken der Digitalisierung?, in: Digitalisierung und Recht, Hamburg, 2017, S. 29 ff.

SCHEDLER KUNO, eGov und neue Servicequalität, in: eGovernment, Bern etc., 2001, S. 30.

SCHEDLER KUNO / SUMMERMATTER LUKAS / SCHMIDT BERNARD, Electronic Government einführen und entwickeln, Von der Idee zur Praxis, Bern, 2003.

SCHEFER MARKUS / HESS-KLEIN CAROLINE, Behindertengleichstellungsrecht, Bern, 2014.

SCHEFFLER JAN / VAN SPYK BENEDIKT, Rechtsverbindliche Publikation von Erlassen im Internet, in: Recht im digitalen Zeitalter, Zürich, 2015, S. 587 ff.

SCHEJA KATHARINA, Schutz von Algorithmen in Big Data Anwendungen, Wie Unternehmen aufgrund der Umsetzung der Geschäftsgeheimnis-Richtlinie ihre Algorithmen wie auch Datenbestände besser schützen können, CR, 2018, S. 485–492.

SCHERER MATTHEW U., Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies, Harvard Journal of Law & Technology, 2016, S. 354 ff.

SCHERER MAXI, Artificial Intelligence and Legal Decision-Making: The Wide Open?, Study on the Example of International Arbitration, Queen Mary University of London, School of Law, Legal Studies Research Paper, 2019, S. 1 ff.

SCHLATT VINCENT / SCHWEIZER ANDRÉ / URBACH NILS / FRIDGEN GILBERT, Blockchain: Grundlagen, Anwendungen und Potenziale, WHITE PAPER, Bayreuth, 2016.

SCHLEISS YVONNE, Zur Durchführung des EU-Rechts in Bundesstaaten, Ausgewählte Aspekte der Umsetzung der Dienstleistungsrichtlinie in Deutschland und Österreich, Diss., Freiburg, 2014.

SCHLIESKY UTZ / HOFFMANN CHRISTIAN, Die Digitalisierung des Föderalismus – Der Portalverbund gem. Art. 91c Abs. 5 GG als Rettung des E-Government?, DÖV, 2018, S. 193 ff.

SCHLUND ALBERT / PONGRATZ HANS, Distributed-Ledger-Technologie und Kryptowährungen – eine rechtliche Betrachtung, DStR, 2018, S. 598 ff.

SCHNEIDER HEUSI CLAUDIA, Vergaberecht, Zürich, 2013.

SCHREY JOACHIM / THALHOFER THOMAS, Rechtliche Aspekte der Blockchain, NJW, 2017, S. 1431 ff.

SCHRÖDER GEORG F., Datenschutzrecht für die Praxis, 3. Aufl., München, 2019.

SCHULER CARLO, Justitia 4.0: Alle Fragen offen, plädoyer, 2019, S. 12 ff.

SCHWARZENEGGER CHRISTIAN / THOUVENIN FLORENT / STILLER BURKHARD / GEORGE DAMIAN, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Anwaltsrevue, 2019, S. 25 ff.

SCHWEGLER IVO, Datenschutz im Polizeiwesen von Bund und Kantonen, Bern, 2001.

Schweizer Rainer J. / Druey Jean Nicolas (Hrsg.), Festschrift für Jean Nicolas Druey zum 65. Geburtstag, Zürich, 2002 (zit. FS Druey).

SECUNET AG, Technische Analyse und Konzeptprüfung des beA, Abschlussgutachten im Auftrag der Bundesrechtsanwaltskammer, Berlin, 18. Juni 2018.

SCHWEIZERISCHE FLÜCHTLINGSHILFE, Parlamentarische Intitative 17.423: Vernehmlassungsantwort der Schweizerischen Flüchtlingshilfe, Bern, 27. Mai 2020 (zit SFH, Stellungnahme Rev. AsylG).

Siegel Thorsten
- Automatisierung des Verwaltungsverfahrens – zugleich eine Anmerkung zu §§ 35a, 24 I 3,41 IIa VwVfG, DVBl, 2017, S. 24 ff.
- Auf dem Weg zum Portalverbund – Das neue Onlinezugangsgesetz (OZG), DÖV, 2018, S. 185 ff.

SIEGMUND ALEXANDER, Das beA von A bis Z, NJW, 2017, S. 3134 ff.

Simitis Spiros / Hornung Gerrit / Spiecker Döhmann Indra (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden, 2019 (zit. Nomos Komm. DSGVO).

SIMMCHEN CHRISTOPH, Blockchain (R)Evolution, MMR, 2017, S. 162 ff.

SIMMLER MONIKA / MARKWALDER NORA, Roboter in der Verantwortung?, Zeitschrift für die gesamte Strafrechtswissenschaft, 2017, S. 20 ff.

SINGLENSTEIN THOMAS, Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, NStz, 2018, S. 1 ff.

SÖBBING THOMAS, Der Datenskandal bei Facebook und die rechtliche Zulässigkeit von künstlicher Intelligenz (KI) zur Beeinflussung der politischen Willensbildung (sog. Microtargeting), InTeR, 2018, S. 182 ff.

SP SCHWEIZ, Vernehmlassungsantwort zum Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID), 29. Mai 2017.

SPICHIGER ANDREAS, Was taugt die Blockchain für die Registerführung?, Die Volkswirtschaft, 2019, S. 23 ff.

SPIELKAMP MATTHIAS, Automating Society – Taking Stock of Automated Decision-Making in the EU, 1. Aufl., Berlin, Januar 2019.

STADT ZUG / LUXOFT / FH ZENTRALSCHWEIZ INFORMATIK, Auswertung der Blockchain-Konsultativabstimmung in der Stadt Zug, November 2018.

STAFFLER LUKAS, Gesetzesinitiative gegen Fake News made in Italy, MMR-Aktuell, 2017, S. 387090.

STANOEVSKA-SLABEVA KATARINA, Web 2.0 - Grundlagen, Auswirkungen und zukünftige Trends, in: Web 2.0, Baden-Baden, 2008, S. 11 ff.

STEIGER MARTIN, Rechtskonforme Cookies auf Websites nach europäischem und schweizerischem Recht, Anwaltsrevue, 2015, S. 18 ff.

STENGEL CORNELIA / AUS DER AU ROMAN, Blockchain: Eine Technologie für effektiven Datenschutz?, sic!, 2018, S. 439 ff.

STIEMERLING OLIVER, «Künstliche Intelligenz» – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge, CR, 2015, S. 762 ff.

Sutter Patrick / Schweizer Rainer J. (Hrsg.), Selbstbestimmung und Recht, Festgabe für Rainer J. Schweizer zum 60. Geburtstag, Zürich, 2003 (zit. FS Schweizer).

SWAN MELANIE, Blockchain, Blueprint for a new economy, Beijing, 2015.

SZABO NICK, Formalizing and Securing Relationships on Public Networks, First Monday, 1997.

TAPSCOTT DON / TAPSCOTT ALEX, Blockchain revolution, How the technology behind Bitcoin is changing money, business, and the world, New York, New York, 2016.

THOUVENIN FLORENT / FRÜH ALFRED / GEORGE DAMIAN, Datenschutz und automatisierte Entscheidungen, Jusletter, 26. November 2018.

THURNHERR DANIELA, Geltung und Tragweite der Verfahrensgarantien bei Realakten – zum unausgeschöpften Potenzial von Art. 29 BV, recht, 2014, S. 241 ff.

TÖNDURY ANDREA MARCEL, Intervention oder Teilnahme? Möglichkeiten und Grenzen staatlicher Kommunikation im Vorfeld von Volksabstimmungen, ZBl, 2011, S. 341 ff.

TREUTHARDT DANIEL / LOEWE-BAUR MIRJAM / KRÖGER MELANIE, Der Risikoorientierte Sanktionenvollzug (ROS) – aktuelle Entwicklungen, SZK, 2018, S. 24 ff.

TRÜEB HANS RUDOLF / ZOBL MARTIN, Steuerdaten in der Cloud?, digma, 2016, S. 102 ff.

TSCHANNEN PIERRE, Amtliche Warnungen und Empfehlungen, ZSR, 1999, S. 353 ff.

TSCHANNEN PIERRE / ZIMMERLI ULRICH / MÜLLER MARKUS, Allgemeines Verwaltungsrecht, 4. Aufl., Bern, 2014.

TSCHÜMPERLIN PAUL, Die Justiz auf dem Weg zum elektronischen Dossier, Eine Standortbestimmung, SJZ, 2018, S. 313 ff.

UHLMANN FELIX
- Die Einleitung eines Verwaltungsverfahrens, in: Das erstinstanzliche Verwaltungsverfahren, Zürich, 2008, S. 1 ff.
- Regelungsgegenstand und Möglichkeiten, in: St. Galler Tagung zur Öffentlichkeitskommunikation des Staates, St. Gallen, 2010, S. 47 ff.
- Schweizerisches Staatshaftungsrecht, Zürich/St. Gallen, 2017 (= Uhlmann, Staatshaftungsrecht).

UHLMANN FELIX / STOJANOVIC JASNA, Vertrauen im Finanzmarktrecht aus öffentlich-rechtlicher Sicht, SZW, 2017, S. 732 ff.

UKROW JÖRG, Singapur: Gesetz gegen Fake News geplant, MMR-Aktuell, 2019.

UN SECRETARY-GENERAL'S HIGH-LEVEL PANEL ON DIGITAL COOPERATION, The age of digital interdependence, Report of the UN Secretary-General's High-level Panel on Digital Cooperation, Juni 2019.

UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN, Tätigkeitsbericht 2019, Kiel, 2019.

UNITED NATIONS, United Nations Activities on Artificial Intelligence (AI), 2019.

VETTER MEINRAD / PEYER DANIEL, Bekannte Tatsachen – unter besonderer Berücksichtigung des Internets, Eine zivilprozessuale Analyse, in: Recht im digitalen Zeitalter, Zürich, 2015, S. 759 ff.

VOLLERY LUC, Publication de la législation: vers la primauté de la version électronique, RFJ, 2014, S. 101 ff.

VOSHMGIR SHERMIN, Blockchains, Smart Contracts und das dezentrale Web, Berlin, 2016.

WACHTER SANDRA / MITTELSTADT BRENT / FLORIDI LUCIANO, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, 2017, S. 76 ff.

WACHTER SANDRA / MITTELSTADT BRENT / RUSSELL CHRIS, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, Jolt, 2018, S. 841 ff.

WAGNER ALEXANDER F. / WEBER ROLF H., Corporate Governance auf der Blockchain, SZW, 2017, S. 59 ff.

Waldmann Bernhard / Belser Eva Maria / Epiney Astrid (Hrsg.), Bundesverfassung, Basler Kommentar, Basel, 2015 (zit. BSK BV).

WALDMANN BERNHARD / SCHNYDER VON WARTENSEE ZENO, Funktion und Bedeutung der amtlichen Gesetzessammlungen heute, LeGes, 2013, S. 11 ff.

Waldmann Bernhard / Weissenberger Philippe (Hrsg.), Praxiskommentar Verwaltungsverfahrensgesetz (VwVG), 2. Aufl., Zürich, 2016 (zit. PK VwVG).

WALPORT MARK, Distributed Ledger Technology: beyond Blockchain, London, 2015.

WANGER RALPH / JOHANN LAURA, Liechtenstein, in: Blockchain and cryptocurrency regulation, London, 2019, S. 372 ff.

WATTER ROLF / KÄGI URS, Öffentliche Informationen über Verfahren und Entscheide in der Finanzmarktaufsicht, AJP, 2005, S. 39 ff.

WEBER ROLF H.
- Outsourcing von Informatik-Dienstleistungen in der Verwaltung, ZBl, 1999, S. 97 ff.
- Big Data: Herausforderungen für das Datenschutzrecht, in: Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, Zürich, 2015, S. 1 ff.
- Regulatory Environment of the Ledger Technology. Taking a closer look at regulatory initiatives and challenges, CRi, 2017, S. 1 ff.
- Blockchain als rechtliche Herausforderung, Jusletter IT, 18. Mai 2017.
- Leistungsstörungen und Rechtsdurchsetzung bei Smart Contracts, Jusletter, 4. Dezember 2017.

WEBER ROLF H. / FERCSIK SCHNYDER ORSOLYA, Was für 'ne Sorte von Geschöpf ist euer Krokodil?, Zur datenschutzrechtlichen Qualifikation von IP-Adressen, sic!, 2009, S. 577 ff.

WEBER ROLF H. / HENSELER SIMON, Regulierung von Algorithmen in der EU und in der Schweiz : Überlegungen zu ausgewählten Regulierungsthemen EuZ 2020, EuZ, 2020, S. 28 ff.

WEBER ROLF H. / LAUX CHRISTIAN / OERTLY DOMINIC, Datenpolitik als Rechtsthema, Agenda für Open Government Data, Zürich, 2016.

WELZEL CHRISTIAN / ECKERT KLAUS-PETER / KIRSTEIN FABIAN / JACUMEIT VOLKER, Mythos Blockchain: Herausforderung für den öffentlichen Sektor, Kompetenzzentrum Öffentliche IT, München, 2017.

WERMELINGER AMEDEO, Informationelle Amtshilfe: Verunmöglicht Datenschutz eine effiziente Leistungserbringung durch den Staat?, ZBl, 2004, S. 173 ff.

WEWER GÖTTRIK, Darf der Staat Facebook und Twitter nutzen?, ZRP, 2016, S. 23 ff.

WIDMER BARBARA, Auftragsdatenbearbeitung – zum Dritten, digma, 2014, S. 112 ff.

Widmer Lüchinger Corinne / Oser David (Hrsg.), Obligationenrecht I, Art. 1 – 529 OR, 7. Aufl., Basel, 2019 (zit. BSK OR I).

WIEDERKEHR RENÉ, Transparenz als Grundsatz rechtsstaatlichen Handelns (Art. 5 BV), ZBl, 2007, S. 521 ff.

WIEDMER ANNE / SEIBERTH CORINNA, OGD Schweiz Konzept: Rechtliche Rahmenbedingungen zur Publikation von Daten als Open Government Data (OGD), 13. März 2015.

WILSCH HARALD, Die Blockchain-Technologie aus der Sicht des deutschen Grundbuchrechts, DNotZ, 2017, S. 761 ff.

WISCHMEYER THOMAS, Regulierung intelligenter Systeme, AöR, 2018, S. 1 ff.

WISCHMEYER THOMAS, Predictive Policing – Nebenfolgen der Automatisierung von Prognosen im Sicherheitsrecht, in: Der Terrorist als Feind?, Tübingen, 2020, S. 189 ff.

WÖLFLE RALF, Digitale Transformation, Eine begriffliche Standortbestimmung im Jahr 2016, Basel, 2016.

WROBEL STEFAN / JOACHIMS THORSTEN / MORIK KATHARINA, Maschinelles Lernen und Data Mining, in: Handbuch der Künstlichen Intelligenz, München, 2013, S. 405 ff.

ZANOL JAKOB / CZADILEK ALEXANDER / LEBLOCH KASPAR, Self-Sovereign Identity und Blockchain, Jusletter IT, 22. Februar 2018.

ZOOG SAMUEL, Bitcoin als Rechtsobjekt, recht, 2019, S. 95 ff.

ZÜND ANDREAS / ERRASS CHRISTOPH, Privatisierung von Polizeiaufgaben, S&R, 2012, S. 162-184.

ZYSKIND GUY / NATHAN OZ / PENTLAND ALEX, Decentralizing privacy: using blockchain to protect personal data, IEEE security and privacy workshops, 2015, S. 180 ff.

Materialienverzeichnis

Änderung des Gesetzes über die Information und den Datenschutz (Informations- und Datenschutzgesetz, IDG) – Anpassung an das geänderte europäische Datenschutzrecht (zit. Vorlage Rev. IDG BL).

Austausch personenbezogener Daten zwischen Behörden des Bundes und der Kantone. BBl, 2011, S. 645 ff. (zit. Bericht Lustenberger).

Bericht Informationstätigkeit des Bundesrates und der Bundesverwaltung in ausserordentlichen Situationen vom 29. Mai 1997. BBl, 1997 III, S. 1568 (zit. Bericht Informationstätigkeit).

Bericht vom 17. August 2018 (zit. Bericht Zukunft).

Bericht vom Juni 1997 für eine Informationsgesellschaft in der Schweiz zuhanden des Schweizerischen Bundesrats (zit. Bericht Informationsgesellschaft 1997).

Botschaft zur Änderung des Fernmeldegesetzes (FMG) vom 12. November 2003. BBl, 2003, S. 7951 (zit. Botschaft Rev. FMG).

Botschaft betreffend den Beitritt zum Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 13. November 1996. BBl, 1997 I, S. 717 ff. (zit. Botschaft Beitritt SEV 108).

Botschaft zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 27. Februar 2013. BBl, 2012 (zit. Botschaft BÜPF).

Botschaft zum Bundesgesetz über den Datenschutz (DSG) vom 23. März 1988. BBl, 1988 I, S. 413 (zit. Botschaft DSG).

Botschaft zum Bundesgesetz über die Ausweise für Schweizer Staatsangehörige vom 28. Juni 2000. BBL, 2000, S. 4751 ff. (zit. Botschaft Ausweisgesetz).

Botschaft zum Bundesgesetz über die Öffentlichkeit der Verwaltung (Öffentlichkeitsgesetz, BGÖ) vom 12. Februar 2003. BBl, 2003, S. 1963 ff. (zit. Botschaft BGÖ).

Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017. BBl, 2017, S. 6941 ff. (zit. Botschaft Rev. DSG 2017).

Botschaft zum Bundesgesetz über elektronische Identifizierungsdienste vom 1. Juni 2018. BBl, 2018, S. 3915 ff. (zit. Botschaft BGEID).

Botschaft zum Bundesgesetz über Geoinformation. BBl, 2006, S. 7817 (zit. Botschaft GeoIG).

Botschaft zum Bundesgesetz über Lebensmittel und Gebrauchsgegenstände vom 25. Mai 2011. BBl, 2011, S. 5571 (zit. Botschaft LMG).

Botschaft zum Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (ZertES) vom 3. Juli 2001. BBl, 2001, S. 5679 (zit. Botschaft ZertES).

Botschaft zur Änderung des Bundesgesetzes über den Datenschutz (DSG) und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 19. Februar 2003. BBl, 2003, S. 2101 ff. (zit. Botschaft Rev. DSG 2003).

Botschaft zur Änderung des Publikationsgesetzes (Primatwechsel von der gedruckten zur elektronischen Version der amtlichen Veröffentlichungen) vom 28. August 2013. BBl, 2013, S. 7057 ff. (zit. Botschaft Rev. PublG).

Botschaft zur Revision des Ausländergesetzes (AuG) (Verfahrensnormen und Informationssysteme) vom 2.März 2018. BBl, 2017, S. 1685 ff. (zit. Botschaft Rev. AuG 2018).

Botschaft zur Revision des Bundesgesetzes über die Bekämpfung übertragbarer Krankheiten des Menschen (Epidemiengesetz, EpG). BBl, 2011, S. 311 (zit. Botschaft Rev. EpG).

Botschaft zur Totalrevision der Bundesrechtspflege vom 28. Februar 2001. BBl, 2001, S. 4202 ff. (zit. Botschaft Rev. Bundesrechtspflege).

Botschaft zur Totalrevision des Asylgesetzes sowie zur Änderung des Bundesgesetzes über Aufenthalt und Niederlassung der Ausländer vom 4. Dezember 1995. BBl, 1996 II, S. 1 (zit. Botschaft Rev. AsylG 1996).

Botschaft zur Volksinitiative «Gleiche Rechte für Behinderte» und zum Entwurf eines Bundesgesetzes über die Beseitigung von Benachteiligungen behinderter Menschen vom 11. Dezember 2000. BBl, 2000, S. 1715 ff. (zit. Botschaft VI Gleiche Rechte).

Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz): Bericht über das Ergebnis des Vernehmlassungsverfahrens, 5. Juni 2020 (zit. Vernehmlassungsbericht BGEID).

Bundesgesetz über elektronische Identifizierungsdienste (Geschäft Nr. 18.049) (zit. Stellungnahme BGEID).

Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register: Erläuternder Bericht zur Vernehmlassungsvorlage, 22. März 2019 (zit. Bericht Rechtsanpassung DLT).

Checkliste: Datenschutzrechtliche Zulässigkeit der Veröffentlichung von Daten über das OGD-Portal, 27. Januar 2017 (zit. Checkliste OGD).

Die EU-DSGVO und ihre Auswirkungen auf die Schweiz, November 2018 (zit. EDÖB Auswirkungen).

Die zivilrechtliche Verantwortlichkeit von Providern (zit. Bericht Provider).

Digitale Kompetenzen, Schutz der Privatsphäre und Online-Bildung: die Schweiz im internationalen Vergleich, 29. Mai 2018 (zit. BFS).

E-Government Strategie Schweiz 2020–2023 (zit. E-Government Schweiz).

Einführung des elektronischen Rechtsverkehrs (zit. Bericht Bischof).

Empfehlungen des Rats der OECD zu künstlicher Intelligenz, 22. Mai 2019 (zit. Empfehlungen des Rats der OECD zu künstlicher Intelligenz).

Erläuternder Bericht vom Februar 2018 zur Übernahme und Umsetzung der EES-Verordnung und der Änderungen des SGK (Smart Borders), «Weiterentwicklungen des Schengen-Besitzstands» (zit. Bericht Smart Borders).

Erläuternder Bericht zum Vernehmlassungsverfahren zum Bundesgesetz über elektronische Verfahren im Steuerbereich vom 21. Juni 2019 (zit. Bericht Rev. Steuerbereich).

Erläuternder Bericht zur Übernahme und Umsetzung des Reformpakets zum Schengener Informationssystem (SIS) «Weiterentwicklungen des Schengen-Besitzstands» und Eingabe der Landesverweisungen im ZEMIS und Erstellung einer erweiterten Statistik im Rückkehrbereich, Februar 2019 (zit. Bericht SIS).

Erläuterungen zu Webtracking (zit. Erläuterungen).

Geschäftsbericht des Bundesgerichts 2019.

Herausforderungen der künstlichen Intelligenz (zit. Bericht IDAG KI).

Leitfaden betreffend Anpassungsbedarf bei den kantonalen (Informations- und) Datenschutzgesetzen aufgrund der EU-Datenschutzreform und der Modernisierung der Europaratskonvention 108, 2. Februar 2017 (zit. Leitfaden).

Merkblatt für Online-Portale der öffentlichen Verwaltung (zit. Merkblatt Online-Portale).

Motion 07.3338, Noser Ruedi (zit. Bundesrat).

Motion 16.3999, Pardini Corrado (zit. 16).

Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022 vom 8. Dezember 2017. BBl, 2018 (zit. Strategie SKI).

Normkonzept zur Revision des Datenschutzgesetzes, 29. Oktober 2014 (zit. Bericht Normkonzept).

Parlamentarische Initiative 17.423, Rutz Gregor (zit. Parlamentarische Initiative 17.423 Rutz).

Parlamentarische Initiative Gesetzliche Grundlage für die Überwachung von Versicherten: Bericht der Kommission für soziale Sicherheit und Gesundheit des Ständerates vom 7. September 2017. BBl, 2017, S. 7421 (zit. Bericht PI Überwachung).

Parlamentarische Initiative Mitwirkungspflicht im Asylverfahren. Überprüfungsmöglichkeit bei Mobiltelefonen: Vorentwurf und erläuternder Bericht der Staatspolitischen Kommission des Nationalrates vom 14. Februar 2020 (zit. Vernehmlassungsbericht Mitwirkung Asyl).

Rechtliche Basis für Social Media: Bericht des Bundesrates in Erfüllung des Postulats Amherd 11.3912 vom 29. September 2011, 09.10.2013 (zit. Bericht Social Media 2013).

Rechtliche Basis für Social Media: Erneute Standortbestimmung, 10. Mai 2017 (zit. Bericht Social Media 2017).

Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz: Eine Auslegeordnung mit Fokus auf dem Finanzsektor (zit. Bericht DLT).

Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen. VPB 1/2012, 22. Dezember 2011 (zit. Rechtsgrundlagen IKT-Zusammenarbeit).

Referendum gegen das Bundesgesetz vom 27. September 2019 über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID): Zustandekommen. BBl, 2020, S. 1285 (zit. Mitteilung über das Zustandekommen des Referendums BGEID, BBl 2020 1285.).

Revision PublG ZH (zit. Antrag Rev. PublG ZH).

Situationsanalyse zum Stand von eGovernment in der Schweiz, 2005 (zit. Situationsanalyse E-Government).

Statusbericht: Erleichterter Datenaustausch zwischen Bundes- und Kantonsbehörden, 9. Mai 2012 (zit. Statusbericht Datenaustausch).

Stellungnahme zum Referentenentwurf vom 20.2.2017 (zit. Stellungnahme).

Strategie für eine Informationsgesellschaft in der Schweiz 2006. BBl, 2006, S. 1877 ff. (zit. Strategie Informationsgesellschaft 2006).

Strategie Digitale Schweiz. BBl, 2016, S. 3985 ff. (zit. Strategie Digitale Schweiz 2016).

Strategie für eine Informationsgesellschaft in der Schweiz vom 18. Februar 1998. BBl, 1998 III, S. 2387 ff. (zit. Strategie Informationsgesellschaft 1998).

Strategie für offene Verwaltungsdaten in der Schweiz 2019–2023 (OGD-Strategie. BBl, 2019, S. 879 (zit. OGD-Strategie 2019).

Bundesamt für Kommunikation: Wie Social-Media-Anbieter ihre AGBs auf den Schweizer Markt ausrichten, 19. November 2013 (zit. BAKOM Social Media).

Zielbild des Bundesrats für die digitale Transformation in der Bundesverwaltung und den Aufbau der digitalen Infrastrukturen, Januar 2019 (zit. Zielbild).

Abkürzungsverzeichnis

a.M.	anderer Meinung / am Main
AB N/S	Amtliches Bulletin der Bundesversammlung, Nationalrat/ Ständerat
ABl	Amtsblatt des Kantons Zürich
Abs.	Absatz
AG	(Kanton) Aargau
AGB	Allgemeine Geschäftsbedingungen
AI Magazine	AI Magazine (Palo Alto, California, U.S)
AiG	Bundesgesetz über die Ausländerinnen und Ausländer und über die Integration vom 16. Dezember 2005 (Ausländer- und Integrationsgesetz, SR 142.20)
AJP	Aktuelle Juristische Praxis (Zürich / St. Gallen)
Anwaltsrevue	Anwaltsrevue / Revue de l' Advocat (Bern)
AöR	Archiv des öffentlichen Rechts (Tübingen)
Art.	Artikel
AS	Amtliche Sammlung des Bundesrechts
AsylG	Asylgesetz vom 26. Juni 1998 (SR 142.31)
AsylG D	Asylgesetz Deutschland
ATSG	Bundesgesetz über den Allgemeinen Teil des Sozialversicherungsrechts vom 6. Oktober 2000 (SR 830.1)
Aufl.	Auflage
Az.	Aktenzeichen
BAKOM	Bundesamt für Kommunikation
BB	Betriebsberater (Frankfurt a.M.)
BBl	Bundesblatt
Bd./Bde.	Band/Bände
BE	(Kanton) Bern
BehiG	Bundesgesetz über die Beseitigung von Benachteiligungen von Menschen mit Behinderungen vom 13. Dezember 2002 (Behindertengleichstellungsgesetz, SR 151.3)
BFH	Bundesfinanzhof Deutschland
BFS	Bundesamt für Statistik
BGE	Entscheidungen des Schweizerischen Bundesgerichts, Amtliche Sammlung
BGEID	Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID)
BGer	Schweizerisches Bundesgericht

BGG	Bundesgesetz über das Bundesgericht vom 17. Juni 2005 (Bundesgerichtsgesetz, SR 173.110)
BGH	(Deutscher) Bundesgerichtshof
BJ	Bundesamt für Justiz
BSK	Basler Kommentar
BSK BGG	Niggli Marcel Alexander / Uebersax Peter / Wiprächtiger Hans (Hrsg.), Bundesgerichtsgesetz, Basler Kommentar, 2. Aufl., Basel 2011
BSK BV	Waldmann Bernhard / Belser Eva Maria / Epiney Astrid (Hrsg.), Bundesverfassung, Basler Kommentar, Basel 2015
BSK StGB	Niggli Marcel Alexander / Wiprächtiger Hans (Hrsg.), Strafrecht, Basler Kommentar, 3. Aufl., Basel 2013
BSK StPO	Niggli Marcel Alexander / Heer Marianne / Wiprächtiger Hans (Hrsg.), Schweizerische Strafprozessordnung, Basler Kommentar, 2. Aufl., Basel 2014
BÜPF	Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (SR 780.1)
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (SR 101)
BVerfG	Bundesverfassungsgericht der Bundesrepublik Deutschland
BVGer	Schweizerisches Bundesverwaltungsgericht
bzw.	beziehungsweise
ca.	circa
CR	Computer und Recht (Köln)
D	Deutschland
DBG	Bundesgesetz über die direkte Bundessteuer vom 14. Dezember 1990 (SR 642.11)
ders.	derselbe
d.h.	das heisst
Die Volkswirtschaft	— Die Volkswirtschaft – Plattform für Wirtschaftspolitik (Bern)
digma	Zeitschrift für Datenrecht und Informationssicherheit (Zürich)
Diss.	Dissertation
DLT	Distributed Ledger Technologie
DNotZ	Deutsche Notar-Zeitschrift (München)
DÖV	Die Öffentliche Verwaltung (Stuttgart)
DSG	Bundesgesetz über den Datenschutz vom 19. Juni 1992 (SR 235.1)

DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung)
DStR	Das deutsche Steuerrecht (München)
DuD	Datenschutz und Datensicherheit (Wiesbaden)
DVBl	Deutsches Verwaltungsblatt (Köln)
E.	Erwägung(en)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDPB	European Data Protection Board
EDPL	European Data Protection Law Review (Berlin)
E-DSG	Entwurf eines totalrevidierten Datenschutzgesetzes
EFTA	Europäische Freihandelsassoziation (European Free Trade Association)
EGMR	Europäischer Gerichtshof für Menschenrechte
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 (Europäische Menschenrechtskonvention, SR 0.101)
EpG	Bundesgesetz über die Bekämpfung übertragbarer Krankheiten des Menschen vom 28. September 2012 (Epidemiengesetz, SR 818.101)
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
Ex ante	Zeitschrift der juristischen Nachwuchsforscher (Zürich)
f./ff.	und folgende
fedpol	Bundesamt für Polizei
Fn.	Fussnote(n)
FS	Festschrift
GeoIG	Bundesgesetz über Geoinformation vom 5. Oktober 2007 (Geoinformationsgesetz, SR 510.62)
Gever	Geschäftsverwaltungssystem
GGG ZH	Gastgewerbegesetz (des Kantons Zürich) vom 1. Dezember 1996 (LS 935.11)
gl.M.	gleicher Meinung
grds.	grundsätzlich
HAVE	Haftung und Versicherung (Zürich)
HMD	HMD Praxis der Wirtschaftsinformatik (Wiesbaden)
HK	Handkommentar

HK EMRK	Meyer-Ladewig Jens / Nettesheim Martin / von Raumer Stefan (Hrsg.), Europäische Menschenrechtskonvention, Handkommentar, 4. Aufl., Baden-Baden 2017
Hrsg.	Herausgeber
IaaS	Internet as a Service
IDG BL	Gesetz (des Kantons Basel-Landschaft) über die Information und den Datenschutz vom 10. Februar 2011 (SGS 162)
IDG BS	Gesetz (des Kantons Basel-Stadt) über die Information und den Datenschutz vom 9. Juni 2010 (SG 153.260)
IDG ZH	Gesetz (des Kantons Zürich) über die Information und den Datenschutz vom 12. Februar 2007 (LS 170.4)
IMPuls	Zeitschrift IMPuls (St. Gallen)
InTeR	Zeitschrift zum Innovations- und Technikrecht (Frankfurt a.M.)
insb.	insbesondere
IP	Internet Protocol / Information Polity (Zeitschrift, Amsterdam)
IPRG	Bundesgesetz über das Internationale Privatrecht vom 18. Dezember 1987 (SR 291)
ISB	Informatiksteuerungsorgan des Bundes
i.S.v.	im Sinne von
i.V.m.	in Verbindung mit
Jolt	Harvard Journal of Law & Technology (Cambridge, Massachusetts)
Journalism Practice	— Journalism Practice (Abingdon-on-Thames, UK)
JZ	JuristenZeitung (Tübingen)
KdK	Konferenz der Kantonsregierungen
KI	Künstliche Intelligenz
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
Komm.	Kommentar
LeGes	Mitteilungsblatt der Schweizerischen Gesellschaft für Gesetzgebung und der Schweizerischen Evaluationsgesellschaft (Bern)
LG	(deutsches) Landgericht
lit.	litera(e)
LKV	Landes- und Kommunalverwaltung (Baden-Baden)
LMG	Bundesgesetz über Lebensmittel und Gebrauchsgegenstände vom 20. Juni 2014 (SR 817.0)
LS	Gesetzessammlung ZH

LugÜ	Übereinkommen über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen (Lugano-Übereinkommen, SR 0.275.12)
m.E.	meines Erachtens
medialex	Zeitschrift für Medienrecht / Revue de droit de médias (Bern)
m.H.	mit Hinweis(en)
MMR	Multimedia und Recht (München)
MVG	Bundesgesetz über die Militärversicherung vom 19. Juni 1992 (SR 833.1)
m.w.H.	mit weiteren Hinweisen
N	Note(n)
Nature	Zeitschrift «Nature» (London)
NJW	Neue Juristische Wochenschrift (München / Frankfurt a.M.)
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht (München)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (München)
NZA	Neue Zeitschrift für Arbeitsrecht (München)
OED	Oxford English Dictionary
OFK	Orell Füssli Kommentar
OLG	Oberlandesgericht (Deutschland)
OR	Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911 (SR 220)
Penn Law Review — University of Pennsylvania Law Review (Philadelphia)	
PI	Parlamentarische Initiative
PK	Praxiskommentar
plädoyer	plädoyer – Magazin für Recht und Politik (Zürich)
PNAS	Proceedings of the National Academy of Sciences of the United States of America (Washington D.C.)
PolG ZH	Polizeigesetz des Kantons Zürich vom 23. April 2007 (LS 550.1)
Pra	Die Praxis (Basel)
PublG	Bundesgesetz über die Sammlungen des Bundesrechts und das Bundesblatt vom 18. Juni 2004 (Publikationsgesetz, SR 170.512)
PublG ZH	Publikationsgesetz des Kantons Zürich vom 30. November 2015 (LS 170.5)
recht	Zeitschrift für juristische Weiterbildung und Praxis (Bern)
resp.	respektive
Rev.	Revision
RFJ	Freiburger Zeitschrift für Rechtsprechung (Freiburg)

Rs.	Rechtssache
Rspr.	Rechtsprechung
RV	Öffentlich-rechtliche Rahmenvereinbarung über die E-Government Zusammenarbeit in der Schweiz 2020
RVOG	Regierungs- und Verwaltungsorganisationsgesetz vom 21. März 1997 (SR 172.010)
Rz.	Randziffer(n)
S&R	Zeitschrift Sicherheit und Recht (Zürich)
S.	Seite(n)
Science	Zeitschrift «Science» (New York)
SEM	Staatssekretariat für Migration
SG	(Kanton) St. Gallen / Systematische Gesetzessammlung des Kantons Basel-Stadt
SGF	Systematische Gesetzessammlung des Kantons Freiburg
SG Komm.	St. Galler Kommentar
SG Komm. BV	Ehrenzeller Bernhard / Schindler Benjamin / Schweizer Rainer J. / Vallender Klaus A. (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Aufl., Zürich / Basel / Genf / St. Gallen 2014
SGS	Systematische Gesetzessammlung des Kantons Basel-Landschaft
SHK	Stämpfli Handkommentar
Sic!	Zeitschrift zum Immaterialgüter-, Informations- und Wettbewerbsrecht (Zürich)
SJZ	Schweizerische Juristen-Zeitung (Zürich)
SK	Stämpfli Kommentar
sog.	sogenannt
SR	Systematische Sammlung des Bundesrechts
SRL	Systematische Gesetzessammlung des Kantons Luzern
SRZS	Systematische Gesetzessammlung des Kantons Schwyz
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937 (SR 311.0)
StHG	Bundesgesetz über die Harmonisierung der direkten Steuern der Kantone und Gemeinden vom 14. Dezember 1990 (Steuerharmonisierungsgesetz, SR 642.14)
StPO	Schweizerische Strafprozessordnung vom 5. Oktober 2007 (SR 312.0)
SVA	Sozialversicherungsanstalt
SVVOR	Schweizerische Vereinigung für Verwaltungsorganisationsrecht

SZIER	Swiss Review of International and European Law (Basel)
SZK	Schweizerische Zeitschrift für Kriminologie (Zürich)
SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht (Zürich)
u.a.	unter anderem/n
URP	Umweltrecht in der Praxis (Winterthur)
usw.	und so weiter
UVG	Bundesgesetz über die Unfallversicherung vom 20. März 1981 (SR 832.20)
VBGÖ	Verordnung über das Öffentlichkeitsprinzip der Verwaltung vom 24. Mai 2006 (SR 152.31)
VDSG	Verordnung zum Bundesgesetz über den Datenschutz vom 14. Juni 1993 (SR 235.11)
VE	Vorentwurf
VeÜ-VwV	Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens vom 18. Juni 2010 (SR 172.021.2)
VG	Bundesgesetz über die Verantwortlichkeit des Bundes sowie seiner Behördemitglieder und Beamten vom 14. März 1958 (Verantwortlichkeitsgesetz, 170.32)
VGer	Verwaltungsgericht
vgl.	vergleiche
VlG	Bundesgesetz über das Vernehmlassungsverfahren vom 18. März 2005 (Vernehmlassungsgesetz, 172.061)
VM	Verwaltung & Management – Zeitschrift für moderne Verwaltung (Baden-Baden)
Vol.	Volume/Volumen
VPB	Verwaltungspraxis der Bundesbehörden (Bern)
VPG/LU	Gesetz über die Verwaltungsrechtspflege vom 3. Juli 1972 (SRL 40)
z.B.	zum Beispiel
ZBJV	Zeitschrift des Bernischen Juristenvereins (Bern)
ZBl	Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht (Zürich)
ZD	Zeitschrift für Datenschutz (München)
ZertES	Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate vom 18. März 2016 (SR 943.03)
ZG	Zeitschrift für Gesetzgebung (München) / Zollgesetz vom 18. März 2005 (SR 631.0)

ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907 (SR 210)
ZH	(Kanton) Zürich
Ziff.	Ziffer(n)
zit.	zitiert (als)
ZRP	Zeitschrift für Rechtspolitik (München)
ZSR	Zeitschrift für Schweizerisches Recht (Basel)

«Nichts ist so beständig wie der Wandel.»
HERAKLIT VON EPHESOS (ca. 520 bis 460 v. Chr.)

Einleitung

Der technologische Wandel verändert die Welt, in welcher wir leben, in teil- 1
weise beängstigendem Tempo. Studien und Untersuchungen überbieten sich mit Prognosen, wie die Digitalisierung die Welt verändern und wie diese in zwanzig oder dreissig Jahren aussehen könnte. Die Voraussagen reichen dabei von dystopischen Visionen wie in George Orwells «1984», wo ein totalitärer Überwachungsstaat die Privatsphäre der Bürger weitgehend abgeschafft hat und deren Bewegungen und Gedanken kontrolliert, bis hin zu einer Welt, in der alle Menschen in einer selbstbestimmten Freiheit leben, in welcher sie über freien Zugang zu Wissen, digitale Bildung und dezentrale Produktionsmittel verfügen.[1] Die Wahrheit wird wohl irgendwo zwischen diesen Prognosen liegen. Unstreitig dürfte sein, dass die Digitalisierung unsere Welt verändern wird und dies auch die öffentliche Verwaltung betrifft. So gehen verschiedene Studien davon aus, dass viele Routinetätigkeiten automatisiert werden und somit Berufsbilder sich verändern werden.[2]

In einer Zeit, in der man die meisten Aufgaben des Alltagslebens (z.B. Ein- 2
kauf, Kommunikation) am Computer oder am Mobiltelefon erledigen kann, entspricht es dem Zeitgeist, dass auch an die Verwaltung immer höhere Ansprüche bezüglich der Erreichbarkeit und Verfügbarkeit ihrer Dienstleistungen gestellt werden.[3] Daher wurden in den letzten Jahren unter dem Begriff des «E-Government» viele Verwaltungsdienstleistungen aufgrund neuer technologischer Möglichkeiten (etwa mobiles und schnelles Internet, billige Verfügbarkeit von Speicherplatz) digitalisiert. So können in vielen Gemeinwesen seit einiger Zeit Steuererklärungen digital ausgefüllt und eingesendet werden oder die Verwaltung informiert online über ihre Website und Social-Media-Plattformen wie «Facebook». Zudem ergeben sich neue Möglichkeiten, indem Informationen aus dem Internet oder der Social-Media-Auftritt einer Person durch die Behörden im Rahmen ihrer Abklärungen zum Erkenntnisgewinn verwendet werden können oder aufgrund von automatischer Datenauswertung aktueller und vergangener Wohnungseinbrüche vorhergesagt

1 Vgl. etwa GOTTLIEB DUTTWEILER INSTITUTE; OPIELA/MOHABBAT KAR/THAPA/WEBER.

2 Vgl. etwa: ARNTZ/GREGORY/ZIERAHN; JENSEN/KOCH. Ein auf einer entsprechenden Studie basierendes Internetprogramm gibt etwa an, dass sich die Hälfte der typischen Tätigkeiten eines Verwaltungsangestellten automatisieren lassen; vgl. den Futuromat des Instituts für Arbeitsamarkt und Berufsforschung.

3 RIZVI/LENEL/RISI, Jusletter IT, 26. September 2018, N. 5.

werden soll, wo weitere Delikte geschehen können, und somit entsprechend disponiert werden kann (sogenanntes «predictive policing»).[4] Der rasante technologische Fortschritt kann in Zukunft bisher noch unabsehbare Entwicklungen mit sich bringen, indem eines Tages «der Computer» sogar selbständig ohne Zutun des Menschen über Sachverhalte entscheiden können soll.

3 Mitten im Endbearbeitungszeitraum dieser Dissertation verbreitete sich mit COVID-19 eine hochansteckende und gefährliche Krankheit in Windeseile weltweit. Um die schnelle Verbreitung der Krankheit einzudämmen und das Gesundheitssystem zu entlasten, wurde in der Schweiz unter anderem zum «Social Distancing» aufgerufen, d.h., es sollten unnötige Sozialkontakte vermieden werden. Aus diesem Grund sollten Arbeiten falls möglich von zuhause aus (im «Home-Office») erledigt werden, und alle Ladengeschäfte, welche nicht Gegenstände des täglichen Gebrauchs verkauften, mussten vorübergehend ihre Türen schliessen. Diese Änderungen betrafen auch die öffentliche Verwaltung, welche vielerorts den Schalterbetrieb reduzierte oder gar einstellte und die Einwohner darauf verwies, wenn möglich die bereitgestellten Online-Lösungen zu nutzen.[5] Ein entsprechendes Vorgehen wäre vor zwanzig oder dreissig Jahren kaum vorstellbar gewesen und viele Dienstleistungen hätten nicht mehr im gewohntem Masse erbracht werden können.

4 Der Umgang der öffentlichen Verwaltung mit dieser Situation soll nicht Kernthema der vorliegenden Arbeit sein, aber dennoch an einigen Orten beispielhaft thematisiert werden, denn die Pandemie konnte somit auch als eine Art «Praxistest» verstanden werden, wie weit die Digitalisierung der Verwaltung in der Schweiz bereits fortgeschritten ist. Dabei zeigte sich, dass viele Dienstleistungen auch auf diese Weise auf gewohntem Niveau erbracht werden konnten, es wurden allerdings auch Unzulänglichkeiten offensichtlich.[6] Dies bestätigt das Bild diverser Studien zum Thema E-Government, in welchen die Schweiz zum Beispiel anhand der Verfügbarkeit verschiedener «Life Events» (z.B. Aufnahme eines Studiums, Familiengründung) und Schlüsselkriterien zwar nicht durchwegs schlecht bewertet wird, aber gerade im Vergleich mit anderen westlichen Industrienationen unterdurchschnittlich abschneidet.[7]

---

4 Vgl. dazu weiter unten Rz. 426 ff. und 467 ff.

5 Vgl. etwa die Kampagne der Stadt Zürich «Blib dihei, mach's online», welche das städtische Online-Portal bewarb.

6 So wurden etwa zur Übermittlung von Fallzahlen noch Faxgeräte genutzt, was zu Ungenauigkeiten führte, vgl. MÄDER, Die Bundesverwaltung bekommt einen «Mr. Digitalisierung», Neue Zürcher Zeitung, 15. April 2020.

7 FREY/ROGG/SCHMID, S. 3. EUROPEAN COMMISSION, S. 5 ff.

Alle diese neuen technologischen Entwicklungen sind für die Verwaltung und den Bürger durchaus mit Vorteilen verbunden. So verspricht man sich dadurch etwa mehr Effizienz, mehr Bürgernähe und sinkende Kosten.[8] Gerade dort, wo Maschinen Daten bearbeiten, wird eine fairere Behandlung von Fällen erhofft, da ein Rechner nur aufgrund derjenigen Daten und Regeln entscheiden kann, welche ihm vorliegen, und exogene Faktoren (wie Hunger oder Müdigkeit) keinen Einfluss auf seine Entscheidung haben.[9] Solche Verheissungen sind jedoch auch mit Gefahren für die Betroffenen verbunden. Deren Wahrnehmung wird nicht zuletzt befeuert durch Meldungen aus den Medien über technische Missgeschicke und Unzulänglichkeiten. So ist es dem Staat im Rahmen einer digitalisierten Welt möglich, auf einfache Weise Zugriff zu immer mehr Daten über seine Bürger zu erhalten, allenfalls gar ohne deren Kenntnis. Die Tatsache, dass er diese Daten auch zu seinen eigenen Zwecken bearbeiten kann, führt bei Bekanntwerden immer wieder zu grösseren Skandalen.[10] In diesem Zusammenhang stellen sich auch Fragen der Datensicherheit, wenn aufgrund eines Datenlecks teils hochsensible Benutzerdaten für jeden einsehbar sind oder von «Hackern» gestohlen werden.[11] Denkbar ist auch, dass durch einen Computer errechnete Resultate oder Wahrscheinlichkeiten aufgrund fehlerhafter Daten oder Grundannahmen falsch sind und unter Umständen ganze Bevölkerungsgruppen diskriminieren.[12] Schliesslich stellen sich auch Fragen danach, was mit Personen geschehen soll, welche keinen Internetzugang haben und auf diese Weise bedroht sind, von staatlichen Dienstleistungen ausgeschlossen zu werden.

8 Vgl. etwa die E-Government-Strategie Schweiz 2020–2023, S. 10.

9 Vgl. etwa die Studie von DANZIGER/LEVAV/AVNAIM-PESSO, PNAS, 2011, welche besagt, dass Richter vor der Mittagspause strenger entscheiden, als wenn sie nach dem Mittagessen wohl gesättigt sind. Kritische Auseinandersetzung dazu bei CHATZIATHANASIOU, JZ, 2019.

10 Als bekannteste Beispiele etwa der «Fichen»-Skandal oder der «NSA»-Skandal; vgl. für eine detailliertere Auseinandersetzung, HARASGAMA, S. 4 ff.

11 Vgl. etwa die unter dem Namen «Collection #1-5» veröffentlichten Benutzerdaten von Bund, Privaten und Armee, THELITZ, Hacker veröffentlichen Passwörter von Armee, Bund und Privaten, Neue Zürcher Zeitung, 7. März 2019.

12 Vgl. das in der USA eingesetzte COMPAS-System zur Bewertung von Rückfallgefahr, durch welches in den USA die Rückfallgefahr von schwarzen Gefängnisinsassen durchwegs höher bewertet wird als diejenige ihrer weissen Mithäftlinge, ANGWIN/LARSON/MATTU/KIRCHNER, Machine Bias. ProPublica, There's software used across the country to predict future criminals. And it's biased against blacks.

§1 Zielsetzung und Forschungsgegenstand

6 Nach dem soeben Ausgeführten hat die fortschreitende Digitalisierung der Verwaltung in verschiedenen Bereichen auch Auswirkungen auf die Rechtsstellung Privater. Das Thema der Verwaltungsautomatisierung beschäftigt die Rechtswissenschaft dabei schon überraschend lange.[13] Mit den stetig wachsenden technologischen Möglichkeiten hat indes auch die Anzahl an Publikationen zu damit verbundenen Themen zugenommen. Viele Werke befassen sich dabei in erster Linie mit spezifischen Bereichen wie künstlicher Intelligenz oder Datenbearbeitung durch die Verwaltung, während eine umfassende, systematische Darstellung des digitalen Verwaltungshandelns bisher in der Schweiz kaum vorgenommen wurde.[14] Die vorliegende Arbeit soll einen Beitrag leisten, um diese Lücke zu schliessen, und die Frage beantworten, wie die mit der Digitalisierung einhergehenden (bestehenden und künftig möglichen) Veränderungen im Bereich des Verwaltungshandelns rechtlich zu beurteilen sind.

7 Dabei soll in erster Linie im Rahmen einer normativ-analytischen Auseinandersetzung betrachtet werden, inwiefern sich bestehende und künftige technologische Entwicklungen in den bestehenden Rechtsrahmen einfügen. Betrachtet werden sollen dabei in erster Linie das Bundesrecht und die relevanten internationalen Rechtsquellen. Wo eine Notwendigkeit dazu besteht, wird auch kantonales Recht thematisiert. Gerade Computertechnologien entwickeln sich aktuell rasant weiter. Was heute aktuell ist, gilt oftmals bereits in fünf oder zehn Jahren als veraltet. Da Gesetzgebungsprozesse jeweils eine gewisse Zeit benötigen, ist es offensichtlich, dass das Recht der Technologie immer bis zu einem gewissen Grad hinterherhinkt.[15] Es ist daher davon auszugehen, dass gewisse Regelungslücken betreffend neu auftretende Technologien bestehen. Daher soll thematisiert werden, wie mit diesen Lücken umgegangen wird bzw. werden soll.

8 Die vorliegende Arbeit wird sich dabei auf Technologien und Phänomene beschränken, welche im Handeln der öffentlichen Verwaltung häufig eingesetzt werden. Dies umfasst sowohl das Handeln innerhalb (erstinstanzlicher) Verwaltungsverfahren als auch Verwaltungshandeln ausserhalb des Verfahrensrahmens (insbesondere die Information der und die Kommunikation mit der Bevölkerung). Dabei sollen in erster Linie diejenigen Bereiche

13 LUHMANN; DEGRANDI.

14 Vgl. aber immerhin etwa GLASER, ZSR, 2015. Vgl. dagegen für Deutschland etwa: GUCKELBERGER; SECKELMANN.

15 Vgl. etwa BOEHME-NESSLER, ZG, 2009, S. 85; GUCKELBERGER, S. 382.

betrachtet werden, welche eine direkte Aussenwirkung für die betroffenen Privaten haben. Die Arbeit ist als Überblick über vorhandene Phänomene der Digitalisierung zu verstehen und soll weniger auf konkrete Softwarelösungen und deren Detailprobleme eingehen. Hinsichtlich der zukünftigen Einsatzbereiche sollen sich abzeichnende, künftige Entwicklungen aufgezeigt und im Hinblick auf mögliche rechtliche Probleme kritisch untersucht werden. Da die Digitalisierung generell ein sich schnell wandelndes Feld darstellt und nicht vorausgesagt werden kann, welche Technologien sich in der Praxis auch durchsetzen werden, soll eine Beschränkung auf Themen stattfinden, zu welchen entweder in der Schweiz bereits konkrete Gesetzesvorhaben geplant sind oder welche in anderen Ländern bereits eingesetzt werden. Nicht oder nur am Rande Teil dieser Arbeit werden Fragestellungen in Bereichen wie «E-Voting»[16] oder «E-Justice»[17] sein.

§ 2 Aufbau

Die vorliegende Arbeit ist in vier Teile gegliedert. Im ersten Teil werden die 9
allgemeinen Grundlagen des Themas dargestellt. Dabei werden die relevanten Begriffe definiert und für diese Arbeit umschrieben. Dies ist im vorliegenden Zusammenhang von spezieller Bedeutung, da in der untersuchten Thematik oft mit «Buzzwords» (d.h. prägnanten Schlagwörtern, die Aufmerksamkeit erzeugen sollen) gearbeitet wird, die nicht immer einheitlich definiert werden. Zudem soll, wo dies für Rechtsfragen notwendig ist, ein grober technischer Überblick über die Funktionsweise der Technologien gegeben werden (§ 1). Zudem werden die aktuell wichtigsten gesetzlichen Grundlagen und Rechtsquellen im Bereich Digitalisierung der Verwaltung und E-Government mit Fokus auf die Bundesebene, aber auch unter Beachtung internationaler und kantonaler Erlasse dargestellt (§ 2).

Im zweiten Teil sollen bereits bestehende technologische Möglichkeiten 10
hinsichtlich ihrer Vereinbarkeit mit den geltenden Rechtsgrundlagen überprüft werden. Diese Untersuchung findet dabei viergeteilt statt: In einem ersten Teil werden massgebliche Veränderungen hinsichtlich des Verwaltungshandelns ausserhalb von Verfahren, insbesondere im Rahmen der Information der und Kommunikation mit der Bevölkerung betrachtet und auf

16 Darunter zu verstehen ist die Möglichkeit zur elektronischen Stimmabgabe etwa im Rahmen von Volksabstimmungen, vgl. weiterführend zum Thema etwa: AUER/ARX, AJP, 2002; BRAUN.

17 Damit wird der elektronische Rechtsverkehr im Zusammenhang mit Verfahren vor Gerichten verstanden, vgl. weiterführend: GLASER, ZSR, 2015; BRÄNDLI, N.F., 794.

ihre Vereinbarkeit mit der Rechtsordnung überprüft (§ 3). Danach wird betrachtet, inwiefern sich die Digitalisierung auf das Verwaltungshandeln innerhalb von (erstinstanzlichen) Verwaltungsverfahren ausgewirkt hat und wie diese Änderungen rechtlich zu bewerten sind. Der Fokus soll hierbei insbesondere auf den Möglichkeiten des elektronischen Rechtsverkehrs liegen (§ 4). Daneben gibt es verschiedene Phänomene, welche sowohl innerhalb als auch ausserhalb von Verfahren relevant sind und daher separat behandelt werden sollen. Dabei geht es einerseits um die Erkenntnisquellen, welcher sich die Verwaltung bedient und welche etwa durch das Internet und soziale Medien mit neuen Möglichkeiten ergänzt wurden (§ 5). Im Weiteren geht es um die Automatisierung in der Verwaltung durch Computerprogramme zur Entscheidungsunterstützung (§ 6)

11 Im dritten Teil sollen absehbare Entwicklungen im Bereich der Informations- und Kommunikationstechnologien im Rahmen des verfassungs- und gesetzesrechtlichen Kontexts betrachtet werden. Auch hier findet eine Unterscheidung zwischen dem Einsatz innerhalb und ausserhalb geregelter Verwaltungsverfahren statt. Ausserhalb von Verwaltungsverfahren wird unter anderem der Frage nachgegangen, wie dies zu beurteilen ist, wenn Information und Kommunikation der Verwaltung mit den Bürgern nur noch online stattfinden soll (§ 7). Innerhalb von Verwaltungsverfahren werden insbesondere mögliche Verbesserungen im Bereich des elektronischen Rechtsverkehrs (§ 8) beleuchtet. Auch zukünftig denkbare und sich abzeichnende neue Erkenntnisquellen hinsichtlich der Bearbeitung von Sachverhalten sollen kritisch betrachtet werden (§ 9). Durch die Fortschritte im Bereich der Automatisierung ist es zudem zumindest technisch bereits absehbar, dass die «Maschine» künftig ganz ohne menschlichen Einfluss rechtlich relevante Entscheide fällen kann. Diese Art der Entscheidungsfindung soll ebenfalls auf ihre rechtlichen Auswirkungen untersucht werden (§ 10). Eine weitere Technologie, welche potenziell sowohl inner- als auch ausserhalb von Verfahren einsetzbar sein könnte und sich daher nicht in dieses binäre Schema einfügen lässt, stellt die «Blockchain»- oder «Distributed Ledger»-Technologie (DLT) dar. Mithilfe dieser Technologie ist es möglich, gewisse Daten dezentral und unveränderlich zu speichern.[18] Wie sich diese Technologie in den geltenden Rechtsrahmen einfügen kann, wird daher separat untersucht (§ 11).

12 Abgeschlossen wird die Arbeit durch den vierten Teil, in welchem die wichtigsten Erkenntnisse zusammengefasst und kritisch gewürdigt werden (§ 12 und 13).

18 Eine genauere Definition sogleich in Teil I, Rz. 43 ff.

In dieser Arbeit wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.

Teil 1: Grundlagen

§ 1 Begriffserklärungen und technische Erläuterungen

Wie einleitend ausgeführt, kann der technologische Fortschritt auch für die öffentliche Verwaltung viele neue Möglichkeiten eröffnen. Immer wieder tauchen dabei neue Technologien und Begriffe wie «Blockchain» oder «künstliche Intelligenz» auf. Wie sich herausstellen wird, existiert nicht zuletzt aufgrund ihrer vergleichsweisen Neuheit für viele dieser Begriffe keine allgemeingültige Definition. Dies hat mit dazu geführt, dass gewisse Begriffe als Synonym oder überlappend verwendet werden. Somit ist es unter Umständen nicht gegeben, dass zwei Personen, welche von «künstlicher Intelligenz» sprechen, dasselbe Verständnis dieses Begriffs haben. Ebenfalls können verschiedene Ausgestaltungen der jeweiligen Phänomene bestehen, welche eine korrekte Verständigung erschweren. Die folgenden Ausführungen sollen dazu dienen, entsprechende Begriffe zu gruppieren und eine Definition dafür zu finden, wie diese Begriffe im Rahmen der vorliegenden Arbeit verstanden werden sollen. Im Weiteren basieren gewisse dieser Technologien, wie etwa die Blockchain, auf komplexen Verfahren. Daher soll im Folgenden auch eine kurze technische Einführung in die Funktionsweise der jeweiligen Technologien erfolgen. 13

I. Digitalisierung und E-Government

Die Digitalisierung bestimmt in zahlreichen Facetten zunehmend über unser Leben. Unter diesen Vorzeichen erstaunt es, dass es schwierig ist, etwa im Bundesrecht eine allgemeine Definition des Wortes «digital» oder der «Digitalisierung» als Phänomen zu finden.[19] Auch in der rechtswissenschaftlichen 14

19 Das Wort «digital» erzielt in der Systematischen Sammlung des Bundes zum Zeitpunkt der Fertigstellung dieser Arbeit 114 Treffer und die «Digitalisierung» kommt siebenmal als Begriff im schweizerischen Recht vor, jedoch findet sich in keiner dieser Bestimmungen eine allgemeingültige Definition des Begriffes; vgl. eine selbst getätigte Abfrage in der Onlineversion der systematischen Rechtssammlung des Bundesrechts (SR) am 15. Juni 2020.

Literatur befassen sich zahlreiche Publikationen mit verschiedenen Formen der Digitalisierung und ihren Chancen, Risiken und Auswirkungen, doch eine Auseinandersetzung mit der Terminologie findet nur selten statt. Häufig wird dabei auf das intuitive Sprachverständnis des jeweiligen Autors abgestützt, was zu einer Unschärfe des Begriffes der Digitalisierung führt.[20]

A. Digitalisierung

15 Das Wort «digital» hat seinen etymologischen Ursprung im lateinischen Wort «digitus» für Finger. Im heutigen Verständnis wird digital in erster Linie in Abgrenzung zum Begriff «analog» etwa hinsichtlich der Darstellung von Ziffern gebraucht.[21] Als Digitalisierung ist nach diesem Verständnis die Umwandlung von Daten von analoger zu digitaler Form zu verstehen. Neben dieser technischen Bedeutungsdimension hat der Begriff auch eine kulturelle Dimension, welche allerdings weniger klar umrissen ist.[22] Die englische Sprache unterscheidet diese beiden Dimensionen begrifflich. Der Begriff «Digitization» stellt die technische Dimension der Digitalisierung («The conversion of text, pictures, or sound into a digital form that can be processed by a computer») dar.[23] «Digitalization» steht dagegen für die wirtschaftlichen und gesellschaftlichen Entwicklungen, welche sich aus der computergestützten Datenverarbeitung ergeben.[24] Es wird festgestellt, dass durch die zunehmende Verbreitung des Internets und den Zugang dazu immer mehr Lebensbereiche von Informationstechnologie durchdrungen werden.[25] Durch diese Durchdringung ergeben sich neue Handlungsmöglichkeiten, welche sich auf die Strukturen zahlreicher Lebensbereiche auswirken. Auf diese Weise kann die Digitalisierung die Lebensbedingungen von Menschen verändern, was wiederum gesellschaftliche Dynamik und neue Herausforderungen mit sich bringen kann. Diese Veränderungsdynamik wird teilweise auch als «digitale Transformation» bezeichnet.[26] Auch wenn die gesellschaftliche Dimension in der Rechtsordnung kaum präsent ist, messen der Bund und die Kantone der Durchdringung der Gesellschaft mit Informationstechnologie und insbesondere deren gesellschaftlichen Auswirkungen eine hohe Bedeutung

20 KLAFKI/WÜRKERT/WINTER, in: Digitalisierung und Recht, S. 3.

21 Vgl. für eine Definition in der Onlineversion des Oxford English Dictionary: «digital, n. and adj.», zum Ganzen auch: KLAFKI/WÜRKERT/WINTER, in: Digitalisierung und Recht, S. 4.

22 BOEHME-NESSLER, Unscharfes Recht, S. 35.

23 «digitization, n.» Definition in der Onlineversion des Oxford English Dictionary.

24 ALTWICKER, Chinese Journal of International Law, 2019, S. 218.

25 FROMM/HOEPNER/WEBER/TIEMANN/WELZEL/GOLDACKER/STEMMER/WEIGAND/OPIELA/HENCKEL, S. 99.

26 Vgl. zum Ganzen: WÖLFLE, S. 10.

zu. So haben sich etwa verschiedene Bundesstellen damit befasst, welche Auswirkungen die Digitalisierung oder Teilphänomene wie «künstliche Intelligenz» auf die Gesellschaft haben und wie den sich daraus ergebenden Herausforderungen zu begegnen ist.[27]

Auch wenn das technische Verständnis des Begriffs «Digitalisierung» 16
durchaus von Relevanz ist, soll im Rahmen dieser Arbeit die Digitalisierung in Anlehnung an die soeben angestellten Überlegungen in erster Linie als die Durchdringung von Lebensbereichen mit Informationstechnologie verstanden werden. Um dennoch nicht auszuufern, werden in der vorliegenden Arbeit nicht sämtliche Lebensbereiche abgedeckt, sondern sie beschränkt sich lediglich auf die Auswirkungen der Digitalisierung auf die öffentliche Verwaltung. In diesem Zusammenhang fällt oft auch der Begriff «E-Government», welcher im Folgenden genauer zu betrachten ist.

B. E-Government

Die zunehmende Verbreitung des Internets und die sich daraus ergebende 17
Durchdringung aller Lebensbereiche durch die Informationstechnik macht auch vor dem Kontakt des Einzelnen mit der Verwaltung nicht halt. Die öffentliche Hand muss sich der Frage stellen, wie sie die Technologie einsetzen kann, um die damit verbundenen Anforderungen zu erfüllen. Das Phänomen, dass die digitale Technologie in der öffentlichen Verwaltung genutzt werden soll, wurde ab dem Ende der 1990er-Jahre rasch in Anlehnung an die bereits vorhandenen Begriffe wie «E-Commerce» unter dem Namen «E-Government» subsumiert.[28]

In der Folge wird ein kurzer Überblick gegeben, was dieser Begriff in der 18
vorliegenden Arbeit bedeuten soll. Auch in diesem Bereich gibt es in der Literatur je nach Blickwinkel und Herangehensweise eine beachtliche Menge an Definitionen.[29] Im Folgenden wird in erster Linie auf die Begriffserklärung der nationalen E-Government-Strategie 2015 aufgebaut. Gemäss dieser Strategie bedeutet E-Government den «Einsatz der Informations- und Kommunikationstechnologien (IKT) in öffentlichen Verwaltungen in Verbindung mit organisatorischen Änderungen und neuen Fähigkeiten (…), um öffentliche Dienste und demokratische Prozesse zu verbessern und die Gestaltung und Durchführung staatlicher Politik zu erleichtern»[30].

27 Vgl. anstatt vieler etwa die Strategie «Digitale Schweiz» vom September 2018 oder spezifischer zur KI den Bericht IDAG KI.

28 SCHEDLER, in: eGovernment, S. 35.

29 LUCKE/REINERMANN, in: Electronic government in Deutschland, S. 2.

30 E-Government-Strategie Schweiz 2015, S. 2.

19 Ein Hauptmerkmal des E-Government ist, den Zugang möglichst aller Bürger zu öffentlichen Dienstleistungen unter Verwendung neuer Informations- und Kommunikationstechnologien zu vereinfachen.[31] Die Dienste sollen so bereitgestellt werden, dass sie ohne besondere Kenntnisse von behördlichen Zuständigkeiten und ohne technisches Spezialwissen genutzt werden können.[32] Das E-Government soll auch dazu beitragen, Vorgänge und Entscheidungen in Politik, Verwaltung und Justiz «von aussen» (d.h. für den Bürger) nachvollziehbar zu gestalten und damit für ein transparentes Verwaltungshandeln zu sorgen.[33] Ein weiteres grosses Ziel, dessen Erreichung man sich von E-Government verspricht, ist die Steigerung der Effizienz und Effektivität staatlichen Handelns.[34] Durch die Optimierung von Prozessen und die elektronische Abwicklung von Behördengeschäften soll der Aufwand für alle Beteiligten reduziert werden.[35] Dies kann nicht zuletzt dadurch erreicht werden, dass der Bürger in einem gewissen Mass selber Aufgaben der Verwaltung übernimmt, in dem er z.B. ein Meldeformular eigenständig ausfüllt. Neben den Einsparungen, welche dies der Verwaltung bringt, sollen dadurch auch die Einflussmöglichkeiten des Bürgers auf das Verwaltungshandeln erhöht werden.[36]

1. Mittel

20 Nach der oben genannten Definition bedient sich das E-Government der Informations- und Kommunikationstechnologien, um die Dienste der öffentlichen Verwaltung zu verbessern. Auch darüber, was Informations- und Kommunikationstechnologien darstellen, besteht keine allgemeingültige Definition. Gemäss einer neueren Definition umfasst der Begriff alle technischen Medien, die für die Handhabung von Informationen und zur Unterstützung der Kommunikation eingesetzt werden; als Beispiele werden hierzu unter anderem Computer- und Netzwerkhardware sowie die zugehörige Software genannt.[37] Der Begriff Informations- und Kommunikationstechnologie, kann somit den Einsatz von Office- und E-Mail-Anwendungen am Verwaltungsarbeitsplatz oder sogar inzwischen veraltete Technologien wie Speicherdisketten ebenso umfassen wie aktuelle und kommende, technisch komplexe Lösungen wie «Cloud Computing» oder «Blockchain». Im Rahmen der vorliegenden Arbeit wird für eine weite Interpretation des Gegenstands Informations- und Kom-

31 GÜNDÜZ/METTLER/SCHEDLER, HMD, 2017, S. 478.
32 E-Government-Strategie Schweiz 2016, S. 6.
33 LUCKE, in: Transparenz; GÜNDÜZ/METTLER/SCHEDLER, HMD, 2017, S. 478.
34 GÜNDÜZ/METTLER/SCHEDLER, HMD, 2017, S. 478; SCHEDLER/SUMMERMATTER/SCHMIDT.
35 E-Government-Strategie Schweiz 2016, S. 6.
36 BOEHME-NESSLER, Unscharfes Recht, S. 398.
37 Vgl. Eurostat-Glossar, Informations- und Kommunikationstechnologien.

munikationstechnologie plädiert, welcher technologieoffen auch Raum für zukünftige Entwicklungen lässt.[38] Der Begriff soll indes auch simple und etablierte Lösungen wie die Verwendung von Textverarbeitungs- oder E-Mail-Programmen umfassen. Auch wenn etwa der Einsatz von E-Mail-Programmen auf den ersten Blick unkritisch erscheint, können sich dabei rechtliche Fragestellungen ergeben.[39]

2. Umfang

Zentral für den Begriff des E-Government ist, dass diese Informations- und 21
Kommunikationstechnologien eingesetzt werden, um damit die Dienstleistungen der öffentlichen Verwaltung zu verbessern und zu erleichtern. E-Government wird hier in einem weiten Sinne verstanden, welcher alle Geschäfte im Zusammenhang mit dem «Regieren und Verwalten» umfassen soll.[40] Das E-Government als solches soll sich an alle Ebenen und Gewalten der öffentlichen Verwaltung[41] und an den gesamten öffentlichen Sektor, bestehend aus Legislative, Exekutive und Judikative, richten.[42] Durch den Einsatz von Informations- und Kommunikationstechnologien können sowohl die Abläufe innerhalb der Verwaltung als auch die Beziehungen zwischen der Verwaltung und der Bevölkerung (als «Kunden») betroffen sein.[43] Die vorliegende Arbeit bezieht sich in erster Linie auf die Beziehung zwischen der Verwaltung und der Bevölkerung, da in diesem Bereich am ehesten Auswirkungen für die Betroffenen zu erwarten sind. Jedoch können auch Veränderungen in den Abläufen zwischen verschiedenen Amtsstellen durchaus Auswirkungen auf die Rechtsstellung von Privaten haben, etwa wenn Personendaten über sie an eine andere Amtsstelle neu in einem automatisierten Abrufverfahren bekanntgegeben werden können.[44]

Zu erwähnen bleibt weiter, dass das hier verwendete Verständnis von 22
E-Government nicht nur die technologischen Entwicklungen umfasst, sondern dass auch organisatorische Änderungen damit verbunden werden, d.h., dass im Rahmen des Einsatzes von neuen Technologien auch bestehende Prozesse auf ihre Zeitgemässheit überprüft und angepasst werden sollen.[45]

38 Ähnlich auch bei GISLER, in: eGovernment, S. 30.

39 Etwa hinsichtlich der Datensicherheit entsprechender Programme, siehe dazu weiter unten Rz. 329.

40 LUCKE/REINERMANN, in: Electronic government in Deutschland, S. 2.

41 GISLER, in: eGovernment, S. 21.

42 LUCKE/REINERMANN, in: Electronic government in Deutschland, S. 2.

43 GISLER, medienheft, 2003 S. 44.

44 Siehe dazu weiter unten Rz. 417.

45 Vgl. E-Government-Strategie Schweiz 2015, S. 2, vgl. BRÜESCH/MERTES/FLICK WITZIG/GIGER/STEINBRECHER, S. 24.

Zu beachten ist zudem, dass für die Nutzung einer neuen Technologie unter Umständen auch die rechtlichen Rahmenbedingungen geschaffen bzw. angepasst werden, was oftmals als sogenannte E-Governance definiert wird.[46] Da dieser Aspekt im vorliegenden Kontext – insbesondere hinsichtlich zukünftiger Entwicklungen[47] – ebenfalls von gewisser Relevanz ist, wird er im Rahmen dieser Arbeit ebenfalls behandelt.

3. Abgrenzungen und Unterformen

23 Der Begriff des E-Government wird im Rahmen dieser Arbeit somit grundsätzlich weit verstanden. Einige Themata sollen hier aufgrund des Fokus der Arbeit dennoch ausgespart werden. So kann nach dem bisherigen Verständnis unter dem Begriff auch die Möglichkeit subsumiert werden, dass dem Einzelnen durch die Verwendung von Technologien einseitig Partizipationsmöglichkeiten im Staat und bei der Vorbereitung bzw. Durchführung demokratischer Entscheidungsverfahren (wie Wahlen oder Abstimmungen) eingeräumt werden.[48] Prominentestes Beispiel dafür ist die bereits seit langer Zeit geführte Debatte über die Möglichkeit, online verbindlich wählen und abstimmen zu können, also das sogenannte «E-Voting». Zu nennen ist auch die elektronische Sammlung von Unterschriften für Initiativen und Referenden.[49] Diese Möglichkeiten werden von der Lehre unter den Begriff «E-Democracy» subsumiert.[50]. Eine dem Thema gerecht werdende Behandlung der sich daraus ergebenden Rechtsfragen würde den Rahmen dieser Arbeit sprengen. Ebenfalls immer öfter genannt wird der Begriff der «E-Justice». Auch hierbei handelt es sich letztlich um einen blossen Teilbereich des E-Government. «E-Justice» umfasst jenen Teil der Kommunikation mit Behörden, welcher sich auf den elektronischen Rechtsverkehr im Zusammenhang mit Verfahren vor Gerichten beschränkt.[51] Auch dieser Bereich wird in der vorliegenden Arbeit nur insofern thematisiert, als sich daraus Auswirkungen für das vorangehende Verwaltungsverfahren ergeben.[52]

24 Ebenfalls eine Unterform des E-Government stellt das «Smart Government» dar. Hier sollen der Verwaltung durch extensives Nutzen moderner,

46 RIZVI/LENEL/RISI, Jusletter IT, 26. September 2018, N. 5 ff.

47 Damit Dokumente online eingereicht werden können, muss zuerst eine entsprechende rechtliche Grundlage geschaffen werden (E-Governance). Erst danach können die entsprechenden Kommunikationskanäle für die Bürger geöffnet und von ihnen genutzt werden, vgl. GISLER, in: eGovernment, S. 15.

48 SCHEDLER, in: eGovernment, S. 37.

49 GLASER, ZSR, 2015, S. 270.

50 Vgl. GISLER, in: eGovernment, S. 23.

51 GLASER, ZSR, 2015, S. 309.

52 Vgl. dazu weiter unten Rz. 569 ff.

insbesondere datengetriebener Technologien wie «Künstliche Intelligenz» oder «Big Data»[53] neue Möglichkeiten der Leistungserbringung eröffnet werden. Mithilfe moderner Technologien kann etwa die physische öffentliche Infrastruktur (z. B. Abfallcontainer, Ampeln, Parkplatzschranken, Stromzähler) vernetzt werden, und es können dadurch automatische Daten, z.B. über deren Nutzung, gewonnen werden, was zur ständigen Verbesserung des jeweiligen Dienstes beiträgt.[54] Beispiele für Smart Government lassen sich bisher vor allem im Bereich der Infrastruktur von Gemeinden finden. So existieren in verschiedenen Schweizer Städten etwa intelligente Strassenlaternen, welche die Annäherung von Personen erkennen und auf diese Weise die Intensität der Strassenbeleuchtung anpassen, oder es können via Smartphone oder Parkkarte freie Parkplätze angezeigt oder Parkplätze bezahlt werden.[55]

4. Fazit

Im Rahmen der vorliegenden Arbeit soll E-Government nach der oben vorgestellten Definition in der E-Government-Strategie 2015 verwendet werden als der Einsatz von Informations- und Kommunikationstechnologien in der Verwaltung, in Verbindung mit organisatorischen Änderungen und neuen Fähigkeiten (…), um öffentliche Dienste und demokratische Prozesse zu verbessern und die Gestaltung und Durchführung staatlicher Politik zu erleichtern. E-Government soll also, grob ausgeführt, die Auswirkungen der Digitalisierung als Prozess auf die Verwaltung abbilden. Dabei soll keine weitere Eingrenzung hinsichtlich der verwendeten Mittel stattfinden, um eine möglichst breite Auseinandersetzung zu ermöglichen. 25

II. Soziale Medien

Mit dem Aufkommen des Internets bildete sich eine Vielzahl von Netzwerken heraus, über die Personen miteinander kommunizieren und Inhalte austauschen können. Diese Netzwerke werden zusammengefasst als «soziale Medien» oder «Social Media» bezeichnet. In der vorliegenden Arbeit sollen diese beiden Begriffe synonym verwendet werden. Bekannte Social-Media-Plattformen wie «Facebook» oder «Twitter» verfügen weltweit über mehr als eine Milliarde aktive Benutzerkonten. In der Schweiz allein gibt es mehr als 3,5 Millionen Facebook-Konten.[56] Es erstaunt daher nicht, dass auch die öffentliche 26

53 MELLOULI/LUNA-REYES/ZHANG, IP, 2014, zur Definition dieser Begriffe siehe weiter unten Rz. 32 ff.

54 Vgl. zum Ganzen: GÜNDÜZ/METTLER/SCHEDLER, HMD, 2017, S. 481.

55 GÜNDÜZ/METTLER/SCHEDLER, HMD, 2017, S. 480.

56 Vgl. für aktuelle Nutzungszahlen etwa : STATISTA, Facebook-Nutzer in der Schweiz 2020

Verwaltung zunehmend die Möglichkeiten von sozialen Medien für ihre Arbeit entdeckt und etwa über diese Kanäle mit der Bevölkerung interagiert. Diese zunehmende Bedeutung rechtfertigt eine eingehendere Behandlung des Phänomens im Rahmen dieser Arbeit und eine Definition an dieser Stelle. Gemäss Duden handelt es sich bei sozialen Medien um die «Gesamtheit der digitalen Technologien und Medien wie Weblogs, Wikis, soziale Netzwerke und Ähnliches, über die Nutzerinnen und Nutzer miteinander kommunizieren und Inhalte austauschen können».[57]

27 Durch das Aufkommen sozialer Medien wurden die bestehenden Informations- und Kommunikationsmittel in verschiedener Weise modifiziert. Während bestehende Internetangebote (wie Websiten) eine primär einseitige Interaktion ermöglichen, erlauben diese neuen Erscheinungsformen in vermehrtem Masse die Partizipation, d.h., dass auch die Benutzenden den Dialog mitbestimmen und gestalten können.[58] Die Interaktion ist dabei nicht nur mit den jeweiligen Informationsträgern oder Plattformtreibern, sondern auch mit anderen Nutzenden möglich.[59] Im Gegensatz zu bestehenden Kommunikationsformen – wie Telefon, Briefpost und E-Mail – sind dabei keine vorbestimmten Adressaten oder bestehenden Kontakte mehr notwendig, sondern es ist auch eine Kommunikation mit einer unbestimmten, unbekannten Menge an Empfängern möglich, indem die jeweiligen Inhalte beispielsweise allen Angehörigen einer Gruppe oder allen Nutzenden der Plattform zugänglich gemacht werden können.[60] Im Weiteren können die Kommunikationsinhalte als Text vermehrt mit anderen medialen Formen wie Bildern, Audiodateien oder Videos kombiniert werden.[61]

28 Dabei besteht eine schier unermessliche Vielzahl an anderen Angeboten, deren Fokus jeweils auf verschiedenen Zielgruppen und angebotenen Inhalten liegt.[62] Gemeinsam ist diesen Plattformen generell, dass sie interaktiv und partizipativ ausgerichtet sind und Kommunikation vereinfachen und multiplizieren sollen.[63] Die vorliegende Arbeit geht von einem weiten Verständnis des Begriffs Social Media aus, um die rechtlichen Auswirkungen des Phänomens grundsätzlich so offen wie möglich untersuchen zu können. Es ist festzustellen, dass gewisse Plattformen von der Verwaltung für die Erfüllung ihrer (Informations- und Kommunikations-)Aufgaben vordergründig genutzt und

57 Vgl. etwa die Definition von «Social Media» in der Online-Version des Duden.

58 HOHLFELD/GORDULLA, in: Rechtshandbuch Social Media, N. 1.

59 STANOEVSKA-SLABEVA, in: Web 2.0, S. 11 ff.

60 LANGER, AJP, 2014, S. 948.

61 Vgl. etwa: BUNDESVERBAND DIGITALE WIRTSCHAFT (BVDW) E.V., S. 138.

62 Vgl. Bericht Social Media 2017, S. 6.

63 LANGER, AJP, 2014, S. 948.

entsprechende Auftritte unterhalten werden.[64] Diese Plattformen werden daher oft als Beispiele angeführt. Zu beachten ist auch, dass die Social-Media-Welt einem ständigen Wandel unterliegt und Plattformen, welche heute omnipräsent sind, in fünf oder zehn Jahren vielleicht nicht mehr existieren.[65]

III. Cloud Computing

Bereits der einleitende kursorische Überblick über mögliche Anwendungen 29
der Digitalisierung in der Verwaltung hat gezeigt, dass es viele denkbare Einsatzbereiche moderner Informatik- und Kommunikationstechnologien gibt. Entsprechende Softwarelösungen müssen jedoch immer auch programmiert und betrieben werden. Die nötigen Fachkenntnisse dazu sind wohl selten in der jeweiligen Organisation bereits vorhanden. Zudem stellen sich diverse Aufgaben bei anderen Gemeinwesen oder auch bei privatwirtschaftlichen Betrieben in ähnlicher Weise, womit es Sinn macht, auf bereits bestehende Lösungen zurückzugreifen. Oftmals werden daher ganze IT-Dienstleistungen extern eingekauft und/oder auf den Servern eines anbietenden Unternehmens betrieben. In diesem Zusammenhang werden oft die Begriffe des «Outsourcing» oder «Cloud Computing» verwendet.[66] Diese sollen daher an dieser Stelle kurz erläutert werden.

Beim «Outsourcing» handelt es sich um den Rückgriff auf die Ressourcen 30
verwaltungsexterner Dritter, welche im Auftrag des Gemeinwesens bestimmte Produkte herstellen oder Dienstleistungen erbringen.[67] Entsprechende Dienstleistungen werden meist im vollen Rahmen vom jeweiligen Hersteller auf dafür zur Verfügung gestellten Servern übernommen. Oftmals werden diese Lösungen für mehrere Bezüger gemeinsam bereitgestellt, welche im Rahmen ihrer Bedürfnisse darauf zurückgreifen.[68] In vermehrtem Masse werden die Ressourcen für die Datenbearbeitung dabei dynamisch zur Verfügung gestellt, so dass sich nicht mehr unbedingt sagen lässt, wo genau sich die Daten im Internet gerade befinden und bearbeitet werden.[69] In diesem Zusammenhang wird mittlerweile von der «Cloud» oder dem «Cloud Computing» gesprochen. Dabei handelt es sich um ein Modell, das eine flexible und bedarfsorientierte Verwendung aus einem gemeinsam genutzten Pool

64 Insb. Facebook und Twitter, vgl. etwa: KOBEL JÜRG, So nutzen die Schweizer Kantone Social Media.

65 Vgl. LANGER, AJP, 2014, S. 948.

66 BAERISWYL, SHK-DSG, Art. 10a, N. 7 f.

67 Vgl. etwa bereits: WEBER, ZBl, 1999, S. 97 ff.

68 Vgl. zum Ganzen: ROTH, AJP, 2020, S. 69.

69 PRIVATIM, Merkblatt Cloud-Computing, S. 1.

von konfigurierbaren IT-Ressourcen ermöglicht, welche grundsätzlich jederzeit und von überall im Netzwerk abgerufen werden können.[70]

31 Dabei gibt es verschiedene Ausgestaltungen von «Cloud Computing». Bei «Infrastructure as a Service» (IaaS) stellt der Anbieter dem Gemeinwesen die IT-Infrastruktur (z.B. in Form von Speicherplatz oder Bandbreite) zur Verfügung. Bei «Platform as a Service» (PaaS) stellt der Anbieter eine Plattform zur Verfügung, gestützt auf welche mit den Benutzenden kommuniziert werden kann und gegebenenfalls auch eigene Softwarelösungen erstellt werden können. «Software as a service» (SaaS) vereint als weitestgehende Form die anderen Ausgestaltungen, indem der Anbieter ein Gesamtpaket zur Verarbeitung von Daten (teils gar mittels Internetbrowser) zur Verfügung stellt. Dabei erfolgt weder eine lokale Installation noch eine lokale Speicherung der Daten.[71] Unterscheiden lassen sich diese Cloud-Dienstleistungen auch nach dem Bereitstellungsmodell. Hierbei gibt es «Private Clouds», welche nur von einer einzelnen Organisation (z.B. einer Dienststelle) genutzt und von dieser selbst oder einem Dritten betrieben werden. Eine «Community Cloud» wird hingegen von einer Gruppe von Organisationen mit ähnlichen Anforderungen gemeinsam betrieben. «Public Clouds» werden schliesslich für die ganze Öffentlichkeit bereitgestellt, wobei jeder Benutzer oder jede Organisation nur jeweils ihre eigenen Daten sieht.[72]

IV. Künstliche Intelligenz

32 Im Zusammenhang mit den neuen Möglichkeiten der Digitalisierung wird immer wieder auch der Begriff der «Künstlichen Intelligenz» (oder kurz KI) verwendet, welcher sinnbildlich für eine Vielzahl an Verheissungen durch Computertechnologie steht. Der Begriff begegnet uns auch im Alltag vermehrt, sei es etwa beim Sprachassistenten auf dem Mobiltelefon, welcher aufgrund der Nutzereingaben dazulernt, oder bei Haushaltgeräten, welche sich mit dem Internet verbinden, um selbständig neue Waren zu bestellen, um nur einige Beispiele zu nennen. Nicht zuletzt aufgrund dieser vielen Einsatzmöglichkeiten besteht keine allgemeingültige und akzeptierte Definition des Begriffs «Künstliche Intelligenz».[73] Der Begriff wird in Definitionsversuchen oftmals in Relation zur menschlichen Intelligenz gesetzt.[74] So wird es etwa als

70 MELL/GRANCE, S. 2; LINS/SUNYAEV, in: Management sicherer Cloud-Services, S. 7, N. 8.

71 KITTLAUS, in: Handbuch Cloud Computing, S. 29 ff.

72 Vgl. ROTH, AJP, 2020, S. 70.

73 Bericht IDAG KI, S. 9; Für eine Übersicht über verschiedene Definitionen, siehe OECD, S. 24.

74 Bericht IDAG KI, S. 19.

künstliche Intelligenz betrachtet, wenn Maschinen Aufgaben erledigen können, die – falls sie von Menschen erledigt werden müssten – Intelligenz benötigen würden.[75]

Unterschieden wird dabei oftmals zwischen starker und schwacher 33
künstlicher Intelligenz. Die schwache KI kann den Menschen bei der Lösung einzelner, klar definierter Probleme zu unterstützen.[76] Eine starke KI wäre dagegen in der Lage, bereichsübergreifend menschenähnlich zu denken und zu handeln und unter Umständen den Menschen dabei gar zu übertreffen.[77] Zum jetzigen Zeitpunkt handelt es sich bei der starken KI noch um «Science Fiction», sämtliche aktuell diskutierten KI-Systeme sind der schwachen KI zuzuordnen.[78] Zwar kann die Lösung der sich stellenden Probleme – etwa im Bereich der selbstfahrenden Autos – sehr komplex sein, und die Maschine kann den Menschen im entsprechenden Bereich gar übertreffen.[79] Jedoch ist die jeweilige Anwendung nur für diesen Bereich gedacht und scheitert, sobald sie eine nicht definierte Aufgabe lösen muss.[80]

Dieser Begriff der künstlichen Intelligenz bringt allerdings einige Charak- 34
teristiken mit, welche ihn für die vorliegende Arbeit ungeeignet erscheinen lassen. Sofern die künstliche Intelligenz sich per definitionem auf die menschliche Intelligenz bezieht, müsste zuerst klar sein, wie die menschliche Intelligenz definiert wird.[81] Indes handelt es sich bei der menschlichen Intelligenz um ein Konzept, welches zwar bereits vielfach und von vielen verschiedenen Forschungsrichtungen untersucht wurde, aber ebenfalls mehrdeutig und kaum genau definierbar bleibt. Auch wird der Begriff, sofern er denn definiert wird, immer auf menschliche Charakteristiken bezogen.[82] Auch wenn Maschinen diese bis zu einem gewissen Grad abbilden können, sind die Fähigkeiten nicht mit dem menschlichen Pendant vergleichbar.[83] Aufgrund dieser Vagheit könnte etwa vertreten werden, dass der Begriff praktisch alle IT-Anwendungen, also auch z.B. simple Taschenrechner, umfasst.[84] Dies würde im Kontext der vorliegenden Arbeit zu weit gehen.

75 SCHERER, Harvard Journal of Law & Technology, 2016, S. 362.

76 BRAUN BINDER, SJZ, 2019, S. 468.

77 BITKOM E. V., KI Gipfelpapier, S. 11; HOCHRANGIGE EXPERTENGRUPPE KI, A definition of AI: Main capabilities and scientific disciplines, S. 7.

78 BRAUN BINDER, SJZ, 2019, S. 468.

79 WISCHMEYER, AöR, 2018, S. 15.

80 BITKOM E. V., KI Gipfelpapier, S. 11.

81 Bericht IDAG KI, S. 19.

82 Vgl. zum Ganzen SCHERER, Harvard Journal of Law & Technology, 2016, S. 359.

83 Bericht IDAG KI, S. 19.

84 HERBERGER, NJW, 2018, S. 2826.

35 Einige Definitionen grenzen daher die «Künstliche Intelligenz» weiter ein, in dem sie gewisse Kernfähigkeiten, wie Wahrnehmen, Verstehen, Handeln und Lernen, in deren Zentrum stellen[85] oder lediglich das Lösen komplexer Aufgaben als «Künstliche Intelligenz» einordnen.[86] Damit stellt sich indes das Problem, dass auch diese Begriffe wieder definiert und eingegrenzt werden müssen, da sie nicht für sich selber sprechen.[87] Auch der Bericht der interdepartementalen Arbeitsgruppe (IDAG) «Künstliche Intelligenz» an den Bundesrat, welcher sich mit den «Herausforderungen der künstlichen Intelligenz» befasst, grenzt die «Künstliche Intelligenz» entsprechend den Charakteristiken ein, welche in KI-Anwendungen aktuell zum Einsatz kommen. Gemäss diesem Bericht sind KI-Systeme «in der Lage (1) Daten in Komplexität und Menge in einer Form auszuwerten, die mit anderen Technologien nach heutigem Stand nicht möglich wäre, (2) Vorhersagen als wesentliche Grundlage für (automatisierte) Entscheidungen zu erstellen, (3) dadurch Fähigkeiten nachzubilden, die mit menschlicher Kognition und Intelligenz in Verbindung gebracht werden und (4) auf dieser Basis weitgehend autonom zu agieren».[88]

36 Auch diese Eingrenzung kann indes nicht vollends überzeugen und lässt Raum für weitere Definitionsschwierigkeiten. Daher soll der Begriff «Künstliche Intelligenz» in dieser Arbeit zurückhaltend benutzt werden. Die obige Definition der IDAG soll indes als Ausgangspunkt verwendet werden, um einige weitere Begriffe einzuführen, welche mit dem Phänomen der «Künstlichen Intelligenz» in engem Zusammenhang stehen und im Rahmen dieser Arbeit verwendet werden.

A. Big Data: Verarbeitung von Daten in grossen Mengen und von grosser Komplexität

37 Es ist nicht neu, dass Daten genutzt und ausgewertet werden. Während der Staat und Unternehmen schon früher augenscheinlich über eine grosse Menge an Daten verfügten (und diese immer grösser wird)[89], war es ihnen meist aufgrund technischer Einschränkungen nicht möglich, diese wirtschaftlich sinnvoll auszuwerten. Moderne Rechner können indes grosse Mengen an Daten innerhalb kurzer Zeit auswerten und somit die Daten quasi in Echtzeit analysieren.[90] Ebenfalls eine neue Dimension stellt die Absicht dar, Daten aus

85 BITKOM E. V., KI Gipfelpapier, S. 29.

86 KAPLAN/HAENLEIN, Business Horizons, 2019, S. 15 ff.

87 Bericht IDAG KI, S. 19.

88 Bericht IDAG KI, S. 19.

89 REINSEL/GANTZ/RYDNING gehen für das Jahr 2016 von einer täglichen Datenmenge von 16,6 Zettabyte (eine 1 mit 21 Nullen) aus, welche sich bis 2026 ca. verzehnfachen wird.

90 Vgl. MARTINI, in: Die digitale Lebenswelt gestalten, S. 103.

unterschiedlichen Quellen miteinander zu verknüpfen, um auf diese Weise neue Erkenntnisse zu gewinnen oder Zusammenhänge zu erkennen.[91] In diesem Zusammenhang wird oft der Begriff «Big Data» genannt. Darunter verstanden wird etwa der Zugriff auf gewaltige Mengen von Daten unterschiedlicher Qualität, Herkunft und Art und deren Verarbeitung mit hoher Geschwindigkeit.[92]

B. Verfahren der Datenverarbeitung:

Verwaltungen sehen sich nach dem gerade Ausgeführten einer immer grösseren und komplexeren Menge an Daten gegenüber, welche von Menschen oftmals nicht mehr innert nützlicher Zeit gesichtet und verarbeitet werden. Daher benötigt die Auswertung dieser Daten technologische Unterstützung. Neue Analysemethoden sollen dabei den Erkenntnisgewinn aus den Daten verbessern beziehungsweise erst ermöglichen.[93] In diesem Zusammenhang ist etwa von Algorithmen oder maschinellem Lernen die Rede. Diese Begriffe haben dabei gemein, dass es sich grundsätzlich um Verfahren handelt, mit denen grosse Mengen von Daten verarbeitet werden können. Im Folgenden sollen diese Termini eingehender dargestellt und voneinander abgegrenzt werden. 38

1. Algorithmen und Expertensysteme

Computer können eine grosse Menge an Daten verarbeiten, dazu brauchen sie aber Anweisungen, wie sie vorzugehen haben. Diese Anweisungen werden als Algorithmen bezeichnet. Bei Algorithmen handelt es sich grob gesagt um Regeln, die bestimmte Aufgaben nach definierten Einzelschritten lösen.[94] Ein Algorithmus funktioniert somit wie ein Kochrezept, indem er verschiedene Zutaten (Input-Daten) und Anweisungen (Regeln) vorgibt, um damit ein Gericht (Resultat/Output) zu kreieren.[95] Als konkretes Beispiel werden etwa die Daten einer Person, die Sozialhilfeansprüche geltend macht (Alter, Einkommen, unterstützungsbedürftige Kinder im Haushalt), in das System eingegeben, und dieses berechnet aufgrund der Vorgaben, ob ein entsprechender Anspruch besteht. Der Begriff Algorithmus ist dabei kein grundsätzliches Phänomen des Computerzeitalters und kann dementsprechend auch weit verstanden werden.[96] Im Zusammenhang mit der vorliegenden Thematik 39

91 SCHAAR, in: Digitalisierung und Recht, S. 31.

92 HOFFMANN-RIEM, in: Big Data – Regulative Herausforderungen, S. 19.

93 MARTINI, in: Die digitale Lebenswelt gestalten, S. 7

94 HOFFMANN-RIEM, in: Big Data – Regulative Herausforderungen, S. 14.

95 Vgl. etwa ERNST, JZ, 2017, S. 1026 ff.

96 BARTH, S. 10.

wird der Begriff jedoch oft auf Verfahren eingegrenzt, in welchen mithilfe von IT-Systemen grosse Mengen an Daten ausgewertet werden und welche im Ergebnis zu nicht trivialen Entscheidungen führen.[97]

40 Die ersten Algorithmen im soeben genannten Sinn traten vor allem in den 80er- und 90er-Jahren in der Form sogenannter Expertensysteme (oder regelbasierter Systeme) auf.[98] Diese beruhten auf der vom Programmierer vorgegebenen Wissensbasis und konnten mithilfe der (vom Anwender eingegebenen) Inputs aufgrund von sogenannten Wenn-dann-Beziehungen auf ein bestimmtes Ergebnis schliessen. Dabei war aufgrund der im Vorneherein gesetzten Regeln stets ersichtlich, welcher Input zu welchem Output führen wird.[99] Durch die Programmierung haben und hatten diese Expertensysteme indes auch klar definierte technische Grenzen.[100]

2. Maschinelles Lernen und Deep Learning

41 Bei komplexer werdenden Datenbeständen stösst der Mensch mit der Definition entsprechender Regeln indes an seine Grenzen.[101] Deshalb soll ausgenutzt werden, dass Algorithmen mittlerweile das Potenzial haben, Bedeutungszusammenhänge in Datenbeständen zu erkennen (sogenanntes «maschinelles Lernen»).[102] Dies kann auf verschiedene Arten geschehen. Das System kann etwa mithilfe eines Trainingsdatensatzes darauf trainiert werden, welche Werte zu welchem Ergebnis führen sollen, und diese Erkenntnis inskünftig selber anwenden (sogenanntes «Überwachtes Lernen»).[103] Eine Weiterentwicklung davon stellt dar, dass selbständig aus den Datenbeständen Zusammenhänge und Kategorien erkannt und diese auf die zu entscheidenden Sachverhalte angewendet werden («Unüberwachtes Lernen»).[104] In einem letzten Entwicklungsschritt sollen diese Systeme in der Lage sein, sich selber unabhängig von der menschlichen Programmierung zu entwickeln (sog. «Deep Learning»).[105]

97 Vgl. etwa WISCHMEYER, AöR, 2018, S. 4, N. 9.
98 BITKOM E. V., KI Gipfelpapier, S. 35.
99 Vgl. MATTHIAS, S. 23 ff.
100 BITKOM E. V., KI Gipfelpapier, S. 35.
101 WISCHMEYER, AöR, 2018, S. 12.
102 STIEMERLING, CR, 2015, S. 2.
103 STIEMERLING, CR, 2015, S. 2.
104 WROBEL/JOACHIMS/MORIK, in: Handbuch der Künstlichen Intelligenz, S. 405 f.
105 HOFFMANN-RIEM, in: Big Data – Regulative Herausforderungen, S. 15.

C. Verwendung: Entscheidungsunterstützung und automatisierte Einzelfallentscheidung

Nach der oben genannten Definition sollen Systeme der künstlichen Intelligenz Vorhersagen als wesentliche Grundlage für (automatisierte) Entscheidungen erstellen. Sämtliche der vorher genannten Verfahren (vom regelbasierten Expertensystem bis hin zu «Deep Learning») können dabei auf zwei verschiedene Weisen eingesetzt werden. Einerseits können sie die Auswertung der Daten nach den vor- oder selbstdefinierten Regeln vornehmen und basierend darauf eine Entscheidungsempfehlung geben. Die Entscheidungsgewalt verbleibt in diesem Fall beim Menschen, während der Algorithmus lediglich der Unterstützung dient. Denkbar ist anderseits auch, dass die Maschine selbständig eine mit Rechten und Pflichten für den Privaten verbundene Entscheidung trifft, ohne dass eine inhaltliche Bewertung oder darauf gestützte Entscheidung durch eine natürliche Person stattfindet. Hierfür wird oftmals der Begriff der «automatisierten Einzel(fall)entscheidung» (oder das englische Äquivalent «automated decision-making») verwendet.[106] Dabei gibt es durchaus Abgrenzungsschwierigkeiten in der Frage, wann noch ein relevanter menschlicher Einfluss vorliegt, was im weiteren Verlauf dieser Arbeit eingehend thematisiert wird.[107] 42

V. Blockchain

Eine weitere Technologie, welche immer wieder als nächste grosse technische Revolution angepriesen wird, ist die sogenannte «Blockchain».[108] Da es sich auch hier um eine vergleichsweise neue Technologie handelt, ist es nicht verwunderlich, dass sich bisher noch keine einheitliche Definition dazu durchgesetzt hat, was eine Blockchain ist.[109] Grob gesagt ist die Blockchain ein «verteiltes, dezentrales Register, das Transaktionen in chronologischer Reihenfolge unveränderbar und nachvollziehbar speichert und miteinander verkettet»[110]. Die Daten werden dabei in Blöcken gruppiert, welche gemeinsam bestätigt werden, wobei ein Block mittels einer kryptographischen Hashfunktion auf den jeweils vorherigen verweist. Beim «Hashwert» handelt es sich um eine längere Zahlen- und Buchstabenreihenfolge, die sich aus der Kombination der im Block enthaltenen Transaktionsdaten und dem Ergebnis einer 43

106 Botschaft Rev. DSG 2017, S. 7056.

107 Siehe dazu unten Rz. 615 ff.

108 Vgl. etwa SWAN, TAPSCOTT/TAPSCOTT.

109 SCHLATT/SCHWEIZER/URBACH/FRIDGEN S. 7.

110 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 7.

komplizierten mathematischen Aufgabe ergibt, welche für jeden Block immer einzigartig ist.[111] Würde ein Block nachträglich bearbeitet, so würde dadurch, dass sich auch dieser «Hashwert» verändert, die Kette quasi aufgebrochen. Dieser Funktionsweise verdankt die Blockchain auch ihren Namen.[112]

44 Gegenüber herkömmlichen Datenbanken zeichnet sich die Blockchain einerseits dadurch aus, dass die Datenbank nicht zentral an einem Ort, sondern dezentral in einem Netzwerk gespeichert ist, in welchem alle teilnehmenden Rechner miteinander verbunden sind.[113] Anderseits kann die Blockchain aufgrund der oben beschriebenen Referenzierung der Blöcke auch nicht nachträglich verändert werden.[114] Durch diese Eigenschaften ist die Blockchain als Technologie vor allem dort interessant, wo es heute im Rechtsverkehr vertrauensstiftende Intermediäre wie Banken braucht, um eine Tatsache (z.B. eine Transaktion) zu garantieren. Die Blockchain verspricht durch ihre unveränderbare und dezentrale Natur, diese Intermediäre überflüssig zu machen.[115]

45 Ihren grössten und bisher bekanntesten Anwendungsbereich hat die Blockchain im Bereich der Kryptowährungen wie «Bitcoin».[116] Dabei handelt es sich um eine Art digitales Zahlungssystem, welches elektronische Zahlungen zwischen zwei Parteien ermöglicht, ohne dass dafür eine kontoführende Drittpartei notwendig ist.[117] Der Bitcoin stellt nur einen möglichen Anwendungsbereich der Blockchain dar.[118] Mit der Zeit öffneten sich indes auch andere Bereiche und Anwendungsmöglichkeiten für den Einsatz der Blockchain, indem es etwa möglich wurde, nicht nur Daten auf der Blockchain zu speichern, sondern diese auch zu verändern und Programmcode darüber auszuführen.[119] Mit der Zeit kamen immer mehr Einsatzbereiche und technische Ausgestaltungen (etwa in der Form neuer Konsensmechanismen zum Formen von Blöcken[120]) hinzu, so dass der Begriff der Blockchain sich als zu eng erwies. In diesem Zusammenhang ist daher oftmals auch von «Distributed Ledger»-Technologie (DLT) die Rede.[121] Ein «Distributed Ledger» ist dabei

111 SCHREY/THALHOFER, NJW, 2017 S. 1432.

112 Bericht DLT, S. 18.

113 BECHTOLF/VOGT, ZD, 2018, S. 67.

114 SCHREY/THALHOFER, NJW, 2017 S. 1432.

115 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 7.

116 Vgl. etwa WAGNER/WEBER, SZW, 2017 S. 61 f.

117 Bericht DLT, S. 18.

118 Vgl. etwa WEBER, Jusletter IT, 18. Mai 2017, N. 6.

119 ROON, Anwaltsrevue, 2016. S. 359, siehe für Anwendungsbereiche insb. hinsichtlich der öffentlichen Verwaltung weiter unten Rz. 659 ff.

120 Dazu sogleich Rz. 47.

121 Bericht DLT S. 18.

auf Deutsch übersetzt nichts anderes als ein «verteiltes Kontenbuch», welches sich von aus der Buchhaltung bekannten Kontenbüchern durch die Verteilung der Kontenführung auf verschiedene Rechner unterscheidet.[122] Problematisch ist dabei, dass diese Begriffe oftmals synonym verwendet werden, was zusätzlich zur Verwirrung beitragen kann. Die Blockchain stellt indes nur eine mögliche technische Lösung einer «Distributed Ledger» dar.[123]

A. Technische Erklärung

Hinsichtlich des Begriffs der Blockchain ist es für den Fortgang der Arbeit wichtig, zumindest in groben Zügen deren technologische Funktionsweise zu kennen, damit diese rechtlich eingeordnet werden kann. Dabei kann unterschieden werden zwischen der Datenstruktur (also quasi der dezentralen Datenbank, welche der Blockchain zugrunde liegt) und dem dazugehörigen, auf Kryptographie basierenden Verwaltungssystem, welches die Transaktionen verwaltet.[124] 46

1. Die Blockchain als dezentrales Register

Die Blockchain zeichnet sich wie erwähnt einerseits dadurch aus, dass jeweils die Gesamtheit der Daten nicht zentral an einem Ort, sondern dezentral auf allen beteiligten Rechnern gespeichert ist. Die Rechner stellen somit sogenannte «Nodes» oder Knoten dar.[125] Die beteiligten Rechner bilden ein sogenanntes «Peer-to-Peer-Netzwerk» (P2P), in welchem sie miteinander kommunizieren. Diese Art von Netzwerken zeichnet sich dadurch aus, dass es keinen zentralen Server gibt, auf welchem sämtliche Daten gespeichert sind und über welchen die Rechner kommunizieren. Viel mehr sind alle Rechner gleichberechtigte Teilnehmer des Netzwerks und fungieren gleichzeitig sowohl als Teilnehmer (Client) als auch als Server. Die Daten einer Blockchain sind somit komplett auf jedem einzelnen teilnehmenden Rechner abgebildet. Jeder Teilnehmer, welcher den Software-Client der jeweiligen Blockchain-Lösung installiert hat, speichert die gesamte Transaktionshistorie der Blockchain und fungiert darüber hinaus als Netzwerkserver.[126] Dies bringt mit sich, dass der Ausfall eines einzelnen Rechners (oder «Nodes») keinen Einfluss auf das Funktionieren des Systems hat. Da der gesamte Transaktionsverlauf auf jedem Rechner gespeichert ist, wird auf diese Art einem Verlust von Daten vorgebeugt, während bei einem klassischen Client-Server-System der Ausfall des 47

122 SCHLUND/PONGRATZ, DStR, 2018, S. 598.

123 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 31.

124 SCHLATT/SCHWEIZER/URBACH/FRIDGEN, S. 7.

125 BECHTOLF/VOGT, ZD, 2018 S. 67.

126 Vgl. etwa: SAFFERLING/RÜCKERT, MMR, 2015, S. 790; BECHTOLF/VOGT, ZD, 2018, S. 67.

Servers ohne entsprechende Massnahmen (z.B. Backups) zu Ausfällen oder irreversiblen Datenverlusten führen kann.[127]

48 Die im Rahmen dieses Netzwerks getätigten Transaktionen werden dabei in Blöcken gespeichert. Sobald ein Block sein Fassungsvermögen erreicht hat, wird der nächste Block beschrieben. Dieser Block verweist dann jeweils auf den vorherigen Block, so dass eine Kette von Datenblöcken (oder englisch eben eine «Blockchain») entsteht.[128]

2. Das Verwaltungssystem der Blockchain

49 Das Peer-to-Peer-Netzwerk stellt nur den Unterbau der Blockchain dar, es muss noch mit Transaktionen gefüllt werden. Damit die Teilnehmer Transaktionen tätigen können, benötigen sie ein Konto, in welchem sie digitale Werte speichern können. Dieses Konto kann man sich wie eine Brieftasche vorstellen, weswegen sie in vielen Anwendungsfällen, wie etwa bei der Kryptowährung Bitcoin, auch «Wallet» genannt wird.[129] Mit dieser «Wallet» erhält der Teilnehmer einen öffentlichen Schlüssel («public key») und einen privaten Schlüssel («private key»). Der private Schlüssel ist nur dem jeweiligen Benutzer bekannt. Er dient ihm dazu, seine Nachrichten zu signieren und authentifizieren. Dies erhöht die Sicherheit der Transaktion für ihren Auslöser. Der öffentliche Schlüssel dagegen ist den anderen Teilnehmern der Blockchain oder zumindest dem Empfänger der Transaktion bekannt, da er vorgängig mitgeteilt wurde oder auf der Blockchain abgespeichert ist.[130] Dieser öffentliche Schlüssel dient den anderen Teilnehmern zur Verifizierung des Absenders der Transaktion.[131] Da bei der Blockchain auf vertrauensstiftende Intermediäre (wie z.B. eine Bank, welche überprüft, ob die Voraussetzungen wie der richtige Empfänger oder genügende Kontodeckung auch vorliegen[132]) verzichtet wird, dient diese Prozedur dazu, Vertrauen zwischen den Parteien zu schaffen.

50 Aufgrund des Fehlens eines Intermediäres, welcher die Transaktionen prüft und freigibt oder verweigert, kann grundsätzlich nicht verhindert werden, dass durch Verzögerungen bei der Übermittlung oder durch bösartige Einflüsse (etwa das mehrfache Versenden derselben Werte, sog. «double

127 SCHLATT/SCHWEIZER/URBACH/FRIDGEN, S. 7.

128 SCHREY/THALHOFER, NJW, 2017, S. 1432; WEBER, Jusletter IT, 18. Mai 2017, N. 1 ff.

129 BECHTOLF/VOGT, ZD, 2018, S. 67.

130 Vgl. zum Ganzen: KAULARTZ, CR, 2016, S. 475.

131 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 7. Dabei werden jedoch keine Klarnamen, sondern nur ein Pseudonym gespeichert. Dies hat den Vorteil, dass auch anonyme Transaktionen über die Blockchain möglich sind; vgl. BECHTOLF/VOGT, ZD, 2018, S. 68 f.

132 KAULARTZ, CR, 2016, S. 476 f.

spending») ungültige oder ungewollte Transaktionen in die Blockchain aufgenommen werden. Zu diesem Zweck soll ein Konsensmechanismus zwischen den Beteiligten eingesetzt werden. Bei der Blockchain besitzt neben der oben beschriebenen Kopie der gesamten Blockchain jeder Teilnehmer des Netzwerks einen Zwischenspeicher, welcher die Transaktionsoutputs der Blockchain enthält, die noch nicht für neue Transaktionen weiterverwendet wurden, und eine Datenbank mit unbestätigten Transaktionen. Bei jeder eingehenden Transaktion wird mit dem Zwischenspeicher abgeglichen, ob die in der Transaktion referenzierten Werte noch nicht für andere Transaktionen verwendet wurden und ob die digitalen Signaturen gültig sind.[133] Ist dies der Fall, wird die betreffende Transaktion an weitere Knoten weitergeleitet. Nur wenn genügend Rechner die Transaktion bestätigen, kann diese in der Blockchain aufgenommen werden.[134]

Damit die unbestätigten Transaktionen in die Blockchain aufgenommen 51
werden, muss der gesamte Block validiert werden. Dies geschieht, indem Benutzer den «Hashwert» des jeweiligen Blocks errechnen (sog. «Mining»). Der Miner, welcher die Lösung als erster herausfindet, übermittelt sie als «proof of work» an das restliche Netzwerk und erhält dafür eine Belohnung.[135] Auf diese Weise entsteht ein neuer Block, welcher auf den vorherigen Block verweist und somit die namensgebende Kette bildet.[136] Jeder Block enthält zudem einen einzigartigen «Hashwert» sämtlicher im Block enthaltenen Transaktionen sowie die Informationen zu sämtlichen Transaktionen.[137] Würde nun versucht, eine Transaktion nachträglich zu ändern, würde sich der Hashwert ändern und die bestehenden Verweise zu den anderen Blöcken würden nicht mehr funktionieren, womit die Blockchain aufgebrochen würde. Dies führt dazu, dass die Blockchain praktisch nicht veränderbar ist.[138] Alle Transaktionen sind verlässlich auf der Blockchain gespeichert und einsehbar. Durch die Speicherung auf vielen verschiedenen Rechnern bringt die Blockchain auch ein hohes Mass an Fälschungssicherheit mit sich.[139] Neben

133 Vgl. zum Ganzen: SCHLATT/SCHWEIZER/URBACH/FRIDGEN, S. 8 ff.

134 SCHREY/THALHOFER, NJW, 2017, S. 1432.

135 BECHTOLF/VOGT, ZD, 2018, S. 67.

136 SCHREY/THALHOFER, NJW, 2017, S. 1431 f.

137 Vgl. BECHTOLF/VOGT, ZD, 2018, S. 67.

138 Eine erfolgreiche nachträgliche Änderung ist nur möglich, wenn der betreffende Hacker mehr als 50 % der Rechenleistung des jeweiligen Blockchain-Netzwerkes kontrolliert, da er auf diese Weise im Rahmen des Proof-of-Work alle anderen Versionen überstimmen könnte, vgl. SCHREY/THALHOFER, NJW, 2017, S. 1432. Zudem müsste für bereits abgeschlossene Blöcke eine aufwendige Rückberechnung stattfinden, vgl. BECHTOLF/VOGT, ZD, 2018, S. 73 ff.

139 SCHREY/THALHOFER, NJW, 2017, S. 1432.

dem soeben genannten «proof of work» gibt es inzwischen verschiedene weitere Möglichkeiten, wie dieser Konsens zwischen den verschiedenen Speicherorten hergestellt werden kann.[140]

B. Arten der Blockchain

52 Bei der Blockchain gibt es verschiedene Arten, welche sich insbesondere in den Berechtigungen unterscheiden. Dabei kann unterschieden werden zwischen öffentlichen (public) und geschlossenen (private) Blockchains. Bei einer öffentlichen Blockchain darf jeder in jeder beliebigen Rolle teilnehmen (z.B. als Miner, als Nutzer).[141] Bekanntestes Beispiel hierfür ist die Bitcoin-Blockchain. Bei einer geschlossenen Blockchain ist der Benutzerkreis von vorneherein auf eine bestimmte Anzahl oder Gruppe beschränkt.[142] Eine weitere Unterscheidung ist danach möglich, ob das Verwalten der Blockchain, also das Veranlassen von Transaktionen, von einer Berechtigung abhängig ist. Ist dies, wie etwa bei der Bitcoin-Blockchain bewilligungsfrei möglich, handelt es sich um eine sogenannte «permissionless blockchain».[143] Andernfalls, also wenn diejenigen Nutzer, welche die Validierung durchführen dürfen, vorab von einer zentralen Autorität festgelegt wurden, handelt es sich um eine genehmigungsbasierte («permissioned») Blockchain.[144]

C. Weitere relevante Begriffe

53 Im Zusammenhang mit der Blockchain werden auch immer wieder weitere Begriffe genannt, etwa wenn es um deren Einsatzmöglichkeiten oder konkrete Funktionsweisen geht. Einige wichtige dieser Begriffe werden an dieser Stelle daher ebenfalls kurz beschrieben.

1. Coin oder Token

54 Die auf einer Blockchain abgelegte Information wird oft als «Coin» oder «Token» bezeichnet.[145] Deren Inhalte können sich je nach dem Verwendungszweck unterscheiden und viele verschiedene Gestalten annehmen.[146]

140 Z.B. den «proof of space» oder den «proof of stake», vgl. WAGNER/WEBER, SZW, 2017, S. 61.

141 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 14.

142 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 15; zudem gibt es noch sogenannte konsortiale Blockchains, welche mehreren Unternehmen oder Organisationen gemeinsam offenstehen; vgl. BITKOM E. V., Blockchain-Studie, S. 10 ff. Deren Eigenheiten gegenüber den vorgestellten Arten sind im vorliegenden Zusammenhang indes nicht relevant.

143 BECHTOLF/VOGT, ZD, 2018, S. 67.

144 SCHLATT/SCHWEIZER/URBACH/FRIDGEN, S. 11.

145 Bericht DLT, S. 18.

146 HESS/LIENHARD, Jusletter, 4. Dezember 2017, N. 36 ff.

2. Kryptowährungen

Die früheste und bekannteste Einsatzmöglichkeit der Blockchain ist die Verwendung als sogenannte Kryptowährungen, wie etwa «Bitcoin». Dabei werden in den jeweiligen Blöcken in erster Linie Transaktionsdaten gespeichert, also etwa die Übertragung eines Bitcoins von Person A an Person B.[147] Eine Kryptowährung kann als eine Art digitales Bargeld verstanden werden.[148] Durch das dezentrale Wesen der Blockchain sind die jeweiligen Transaktionen nicht nur an einem Ort gesichert und durch die kryptografische Ausgestaltung des Systems nur mit hohem Aufwand veränderbar.[149] Im Rahmen der vorliegenden Arbeit ist der Einsatz von Blockchains als Kryptowährung lediglich von untergeordneter Bedeutung und wird daher nur am Rande thematisiert. 55

3. Smart Contract

Gerade im privatrechtlichen Vertragswesen ist das Vertrauen zwischen Vertragspartnern ein wichtiger Pfeiler. Kennen sich zwei Vertragsparteien nicht oder haben sie kein genügendes Vertrauen, dass die Gegenpartei ihre vertraglichen Pflichten einhält, so schliessen sie keinen Vertrag ab oder beauftragen einen Intermediär (z.B. eine Bank), welcher die Ausführung des Vertrags überwacht. Letzteres führt jedoch stets zu zusätzlichen Kosten. Aus diesem Grund wurde bereits in den 90er-Jahren des vergangenen Jahrhunderts das Prinzip von «Smart Contracts» diskutiert.[150] Gemäss diesem Konzept sollten Verträge so dargestellt werden, dass Leistungen und Gegenleistungen automatisch durch ein Programm abgewickelt werden können.[151] Ein Beispiel, welches oft zur Illustration angeführt wird, ist die Vermietung einer Wohnung, bei welcher die Zutrittskontrolle über ein Chipkartensystem funktioniert. Beim Betreten der Wohnung überprüft die Softwarelösung im Lesegerät, ob der Mietzins fristgerecht bezahlt wurde und öffnet danach die Tür oder eben nicht.[152] Ein «Smart Contract» benötigt dementsprechend ein Ereignis, welches sich digital überprüfen lässt und entweder wahr oder falsch ist (in unserem Beispiel die Bezahlung des Mietzinses), einen Programmcode, welcher das Ereignis verarbeitet, und eine rechtlich relevante Handlung, welche auf der Grundlage des Ereignisses ausgeführt wird, wie das Öffnen 56

147 ZOOG, recht, 2019, S. 97.

148 Bericht DLT, S. 14.

149 Vgl. zum Ganzen, SCHREY/THALHOFER, NJW, 2017, S. 1431.

150 Vgl. SZABO, First Monday, 1997.

151 KAULARTZ/HECKMANN, CR, 2016,S. 618.

152 SCHREY/THALHOFER, NJW, 2017, S. 1431.

der Zimmertür des Mietobjekts.[153] Aufgrund ihrer Eigenschaften wird die Blockchain als geeignetes Mittel angesehen, um «Smart Contracts» auszuführen. Wie weiter oben beschrieben, wird eine Transaktion auf der Blockchain erst validiert, wenn geklärt ist, ob der Absender zu deren Durchführung berechtigt war. Die entsprechende Transaktion kann auch vom Eintritt weiterer Bedingungen abhängig gemacht werden. Die Prüfung des Bedingungseintritts wird dabei von den im P2P-Netzwerk beteiligten Rechnern ausgeführt, ohne dass es eines Zutuns der Vertragsparteien bedarf.[154]

§ 2 Rechtsgrundlagen der Digitalisierung

57 Die Digitalisierung betrifft mittlerweile verschiedenste Bereiche unseres Lebens, und es ist folgerichtig, dass sie auch das Recht nicht unbeeinflusst lässt.[155] Das vorliegende Kapitel dient dazu, den Rechtsrahmen für die vorliegende Arbeit abzustecken und die relevantesten Erlasse im Bereich der Digitalisierung des Verwaltungshandelns vorzustellen. Die Digitalisierung macht dabei nicht vor Landesgrenzen halt. Immer öfter ergeben sich aus Sachverhalten internationale Anknüpfungspunkte, etwa wenn Daten über eine Person ins Ausland transferiert werden. Daher ist es unumgänglich, bestehende Regulierungen und Regulierungsvorhaben auf internationaler und supranationaler Ebene zu betrachten, welche im vorliegenden Zusammenhang Auswirkungen auf die Schweiz haben. Der Fokus soll indes auf den Regelungen auf Bundesebene liegen, welche das Handeln der Verwaltung hierzulande wesentlich prägen. Neben Gesetzen und Verordnungen spielen gerade hinsichtlich der Digitalisierung auch andere Instrumente wie interkantonale Vereinbarungen oder Strategien eine gewisse Rolle. Diese sollen ebenfalls betrachtet und die Frage beantwortet werden, ob sie Rechtsquellen im eigentlichen Sinne darstellen. Aufgrund des Fokus der Arbeit werden darüber hinaus in erster Linie verwaltungsrechtliche Quellen vorgestellt. Da auch auf kantonaler Ebene das Thema E-Government in den letzten Jahren immer stärker thematisiert wurde und die Kantone in dieser Hinsicht auch eigenständig tätig wurden, soll die kantonale Ebene in einem eigenen Kapitel ebenfalls einer Betrachtung unterzogen werden.

153 Beispiel entnommen aus: KAULARTZ/HECKMANN, CR, 2016, S. 618.

154 Vgl. zum Ganzen: KAULARTZ/HECKMANN, CR, 2016, S. 618 f.

155 Vgl. etwa den Schweizerischen Juristentag 2015, welcher das Thema aus vielen verschiedenen Blickwinkeln behandelte: GSCHWEND/HETTICH/MÜLLER-CHEN/SCHINDLER/WILDHABER.

I. Internationale und supranationale Ebene

A. Internationale Ebene

Es ist unbestritten, dass die Grundrechte, welche durch verschiedene internationale oder supranationale Regelwerke (etwa den UNO-Pakt I oder II oder die EMRK) garantiert sind, auch im digitalen Raum Geltung entfalten.[156] Indes wurden diese Regelwerke oft in einer vordigitalen Zeit erschaffen, und es ist daher aktuell noch genauer zu bestimmen, welche Auswirkungen sich für die jeweiligen Grundrechtspositionen durch die Digitalisierung ergeben können.[157] An dieser Stelle soll eine detaillierte Auseinandersetzung mit der Auswirkung der Digitalisierung auf verschiedene Grundrechte unterbleiben und dies lediglich dort thematisiert werden, wo für die Arbeit relevante Aspekte betroffen sind. 58

Da neue Technologien Staaten und Privaten schier unermessliche Möglichkeiten zur Überwachung von Bürgern geben, wird insbesondere das «right to privacy», welches etwa in Art. 17 UNO-Pakt II geregelt ist, als besonders gefährdet betrachtet.[158] Daher hat die UN-Generalversammlung im Laufe der letzten Jahre mehrere Resolutionen verabschiedet, in welchen sie die Staaten aufforderte, dieses Recht zu beachten und in relevanten Bereichen (etwa bei der Überwachung von Telekommunikation) effektive Aufsichts- und Rechtsschutzmechanismen vorzusehen.[159] Die UNO befasst sich auch in anderen Bereichen durchaus mit den Auswirkungen der Digitalisierung auf die Menschenrechte, etwa betreffend den Einsatz von künstlicher Intelligenz.[160] Oftmals lassen indes unterschiedliche Auffassungen zu einem Thema keinen breit abgestützten Konsens für den Erlass bindender neuer Regelungen zu.[161] 59

156 Vgl. dazu etwa die Antwort des Bundesrats auf die 16.

157 Vgl. UN SECRETARY-GENERAL'S HIGH-LEVEL PANEL ON DIGITAL COOPERATION, S. 23; s. dazu die Diskussion um eine Charta der digitalen Grundrechte der Europäischen Union; s. etwa: GRAF VON WESTPHALEN, BB, 2018, für die Schweiz siehe dazu sogleich Rz. 66.

158 UN SECRETARY-GENERAL'S HIGH-LEVEL PANEL ON DIGITAL COOPERATION. S. 26.

159 Vgl. etwa Resolution der UN-Generalversammlung 71/199: Das Recht auf Privatheit im digitalen Zeitalter, verabschiedet am 19. Dezember 2016.

160 Vgl. UN SECRETARY-GENERAL'S HIGH-LEVEL PANEL ON DIGITAL COOPERATION, S. 26; für eine detaillierte Übersicht der Anstrengungen der UN vgl. UNITED NATIONS.

161 Vgl. hierzu die Anstrengungen um eine Anpassung der Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons zur Regelung von LAWs (Lethal Autonomous Weapons Systems, d.h. tödliche autonome Waffensysteme), s. die Arbeit des Office for Disarmement Affairs.

B. Supranationale Ebene

60 Im vorliegenden Bereich relevanter und auch bereits konkreter sind Regulierungsvorhaben auf europäischer Stufe. Zu nennen ist in erster Linie die «Tallinn Declaration on eGovernment». Im Rahmen dieser Deklaration sind 32 Mitgliedsländer von EU und EFTA übereingekommen, E-Government international zu fördern. Zu diesem Zweck werden die Länder ebenso wie die Kommissionen und Institutionen der EU aufgerufen, gewisse Massnahmen zur Zielerreichung zu treffen.[162] So soll es etwa möglich werden, dass Menschen dieselben Daten der Verwaltung nur einmal übermitteln müssen und diese im Rahmen der Datenschutzvorschriften intern mehrmals verwendet werden, um den Bürger zu entlasten («once only»).[163] Im Weiteren sollen Systeme vermehrt interoperabel werden. Dies bedeutet, dass sie standardmässig ohne Hindernisse über (Landes-)Grenzen Daten austauschen und gemeinsam funktionieren können.[164] Wie sich bereits aus dem Wortlaut der Massnahmen («we will in our countries …») ergibt, handelt es sich dabei in erster Linie um Absichtserklärungen. Die Vertragsparteien werden in erster Linie dazu aufgefordert, gesetzgeberisch gewisse Massnahmen in das nationale Recht zu überführen. Für die Bürgerinnen und Bürger ergeben sich aus den Bestimmungen keine justiziablen Rechte und Pflichten.[165] Damit Bürger aus den Vorgaben der Deklaration einen Anspruch ableiten können, müssten entsprechende Regelungen daher im nationalen Recht umgesetzt werden.

61 Auch der Fluss von Informationen und Personendaten macht keinen Halt an den Ländergrenzen. Daher existieren in vielen bi- oder multilateralen Staatsverträgen Bestimmungen, welche eine Datenbekanntgabe in andere Länder vorsehen.[166] Die jeweiligen Rechtsnormen stellen dabei eine gesetzliche Grundlage zur Datenbekanntgabe im Sinne der Datenschutzgesetzgebung dar.[167] Durch die Schaffung einer Gesetzesgrundlage alleine kann jedoch nicht zwingend garantiert werden, dass die jeweiligen Daten auch im anderen Land im selben Rahmen geschützt sind. Daher bestehen internationale Bestrebungen, ein möglichst übergreifendes, hohes Datenschutzniveau bei gleichzeitiger Gewährleistung des freien grenzüberschreitenden

162 Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU on 6 October 2017, S. 3.

163 EU eGovernment Action Plan 2016-2020, S. 3.

164 KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN S. 3 ff.

165 Vgl. Tallinn Declaration, S. 3 ff.

166 Vgl. als eines von zahlreichen Beispielen die Rechtsgrundlagen zur Nutzung des Schengener Informationssystems (SIS), siehe etwa: Bericht SIS., S. 4.

167 Vgl. Art. 17 DSG, s. dazu weiter unten Rz. 74.

Informationsaustausches sicherzustellen.[168] In diesem Zusammenhang ist insbesondere das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Übereinkommen SEV 108, SR 0.235.1) zu nennen. Dieses trat in der Schweiz per 1. Januar 1998 in Kraft und wurde seit seinem Inkrafttreten mehrfach überarbeitet. Zweck des Übereinkommens ist es, den Rechtsschutz der Betroffenen gegenüber der automatischen Verarbeitung ihrer Personendaten im privaten und im öffentlichen Sektor in allen Mitgliedstaaten bis zu einem gewissen Grad zu stärken und zu harmonisieren.[169] Zwar enthält auch dieses Übereinkommen keine unmittelbar anwendbaren Bestimmungen und in erster Linie Gesetzgebungsaufträge, doch ist eine Erfüllung dieser Vorgaben insbesondere darum wichtig, weil die Europäische Union die Bewertung, ob ein anderes Land über ein angemessenes Datenschutzniveau verfügt (sog. Angemessenheitsbeschluss), insbesondere auf die Ratifizierung des SEV-108-Übereinkommens stützt.[170] Die entsprechenden Vorgaben sollen im Rahmen der Datenschutzgesetzgebung umgesetzt werden.

62 Zu thematisieren ist an dieser Stelle zudem die Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgrundverordnung, DSGVO) vom 27. April 2016, welche eine Vereinheitlichung des Datenschutzrechts auf europäischer Ebene anstrebt.[171] Diese Verordnung ist für die Schweiz nicht direkt anwendbar, da sie nicht Teil des Schengen-Acquis darstellt.[172] Sie zeigt jedoch einerseits dadurch Auswirkungen auf das Rechtssystem dieses Landes, dass die Schweiz als Nicht-EU-Mitglied ein angemessenes Datenschutz-Niveau aufweisen muss, damit der grenzüberschreitende Verkehr von Daten nicht erschwert wird. Aus diesem Grund hat die DSGVO einen starken Einfluss auf die laufende Revision der schweizerischen Datenschutzgesetzgebung.[173] Anderseits kann sie unter gewissen Voraussetzungen für Schweizer Unternehmen extraterritorial anwendbar sein, falls diese eine Niederlassung in einem EU-Staat haben, Personen in der Union Waren oder Dienstleistungen anbieten oder das Verhalten betroffener Personen beobachten (Art. 3 DSGVO).[174] Während davon auszugehen ist, dass Behörden sich nicht in erster Linie an Personen in

168 Vgl. Botschaft Rev. DSG 2003, S. 2113.

169 Botschaft Beitritt SEV 108, S. 717.

170 Botschaft Rev. DSG 2017, S. 6970

171 Vgl. ZERDICK, Ehmann/Selmayr DSGVO, Art. 1 N. 2 f.

172 Botschaft Rev. DSG 2017, S. 6964.

173 Botschaft Rev. DSG 2017, S. 6994 ff.

174 Vgl. EDÖB Auswirkungen, S. 6.

anderen Staaten wenden oder gegenüber diesen Dienstleistungen erbringen,[175] ist es immerhin denkbar, dass die DSGVO für Behörden aufgrund der Beobachtung des Verhaltens betroffener Personen in der EU anwendbar ist, sofern staatliche Websites Tracking-Tools nutzen, die dem Beobachten der Internetaktivitäten einer natürlichen Person dienen.[176]

63 Im Laufe der vorliegenden Arbeit wird die DSGVO aufgrund dieser Ausführungen in erster Linie dort eingehend thematisiert, wo sie für Behörden auch relevant ist. Ansonsten wird sie lediglich herbeigezogen, wenn eine Regelung der DSGVO in massgeblicher Weise von der relevanten Schweizer Regelung abweicht oder wenn sie einen Lösungsansatz für ein Problem bietet, für welches das schweizerische Datenschutzrecht de lege lata keine befriedigende Lösung hat.

64 Erwähnt sei an dieser Stelle noch, dass zwischen der Schweiz und den Staaten der EU zudem eine Vielzahl an bereichsspezifischen Staatsverträgen etwa im Bereich der Verfolgung von Cyberkriminalität bestehen.[177]

II. Bundesebene

A. Bundesverfassung

65 Die neue Bundesverfassung der Schweiz trat per 1. Januar 1999 in Kraft und ist somit im Vergleich mit anderen Verfassungen eher neueren Datums. Jedoch hat gerade in den letzten zwanzig Jahren auch eine enorme technologische Entwicklung stattgefunden, welche damals noch nicht vollständig absehbar war. Die Digitalisierung und ihre Auswirkungen sind im Gegensatz etwa zu Deutschland, welches in Art. 91c GG eine *verfassungsrechtliche Grundlage für die Zusammenarbeit von Bund und Ländern auf dem Gebiet der Informationstechnik geschaffen hat*[178], in der Bundesverfassung nicht offensichtlich präsent.

175 DATENSCHUTZBEAUFTRAGTER DES KANTONS BASEL-STADT, Anwendbarkeit der EU-Datenschutzgesetzgebung auf Behörden, Einrichtungen und sonstige Stellen des Kantons Basel-Stadt, S. 3; es wird davon ausgegangen, dass behördliches Handeln nicht als Dienstleistung i.S. von Art. 3 DSGVO zu verstehen ist. Zu beachten ist auch, dass die Reichweite gewisser Regelungen der DSGVO noch nicht abschliessend geklärt ist und dass die Aufsichtsbehörden in der EU oder der Europäische Gerichtshof diesbezüglich zu anderen Schlüssen kommen könnten. Als eine erste Richtlinie können indes die Ausführungen des EDPB dienen, vgl. EUROPEAN DATA PROTECTION BOARD, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).

176 DATENSCHUTZBEAUFTRAGTER DES KANTONS BASEL-STADT, Anwendbarkeit der EU-Datenschutzgesetzgebung auf Behörden, Einrichtungen und sonstige Stellen des Kantons Basel-Stadt, S. 5, vgl. dazu weiter unten Rz. 175.

177 Vgl. etwa das Übereinkommen über die Cyberkriminalität vom 23. September 2001 (SR 0.311.43).

178 SUERBAUM, Beck OK Grundgesetz, Art. 91c, N. 3.

Eine explizite Nennung einer neuen Technologie findet lediglich im nach einer Volksabstimmung im Jahr 2012 geänderten Art. 106 BV betreffend die Kompetenzverteilung im Bereich der Geldspiele statt, welcher in Absatz 4 regelt, dass diese Bestimmung auch bei telekommunikationsgestützten Geldspielen zu gelten hat.

1. Grundprinzipien und Grundrechte

Relevant und zu beachten sind im vorliegenden Zusammenhang selbstverständlich die in der Verfassung geregelten Grundprinzipien und Grundrechte. Aus dem Legalitätsprinzip gemäss Art. 5 BV ergibt sich, dass jedes staatliche Handeln eine gesetzliche Grundlage benötigt. Auch wenn eine neue Technologie oder eine digitale Lösung eines bisher analogen Vorgangs (z.B. die Möglichkeit der rechtsverbindlichen digitalen Signatur) in der Verwaltung umgesetzt werden soll, müssen daher unter Umständen neue rechtliche Grundlagen geschaffen werden. Die Grundrechte gelten – wie bereits oben ausgeführt – auch im digitalen Raum. Auch in der Schweiz sind diverse Stimmen laut geworden, welche eine Anpassung des Grundrechtekatalogs an die veränderte digitale Wirklichkeit fordern und dabei auf die bereits erwähnte digitale Grundrechtecharta der EU Bezug nehmen. Der Bundesrat sieht hier indes bis anhin keinen Handlungsbedarf.[179] 66

2. Bundeskompetenz im Bereich der Digitalisierung des Verwaltungshandelns

Im Weiteren lässt sich anhand der Bundesverfassung die Frage thematisieren, inwiefern der Bund die Kompetenz hat, übergreifende Regulierungen zu Themen der Digitalisierung zu schaffen. Denkbar sind etwa Regelungen zur Förderung der elektronischen Verwaltung, wie sie in Deutschland (Gesetz zur Förderung der elektronischen Verwaltung [E-Government-Gesetz, E-GovG, in Kraft seit dem 1. August 2013]) oder Österreich (Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen [E-Government-Gesetz, E-GovG, vom 1. März 2004]) bestehen. Aufgrund der bundesstaatlichen Kompetenzordnung ist der Bund gemäss Art. 3 und Art. 42 BV nur dann zum Erlass von Vorschriften befugt, wenn er dazu eine genügende Grundlage hat, welche sich entweder explizit oder implizit aus der Verfassung ergibt.[180] So hat der Bund beispielsweise im Straf- oder Zivilverfahren eine umfassende Gesetzgebungskompetenz und kann in 67

179 Vgl. die Motion 16.399 Pardini «Grundrechte und Charta für eine demokratische Digitalisierung der Schweiz» und die Antwort des Bundesrats darauf.

180 Vgl. etwa BIAGGINI, BSK BV, Art. 42, N. 1 ff.

diesen Bereichen verbindliche technische und organisatorische Vorgaben für eine einheitliche elektronische Verwaltungslandschaft erlassen.[181]

68 Im Bereich des Verwaltungsverfahrens besteht indes keine umfassende entsprechende Grundlage in der Bundesverfassung. Teilweise wird versucht, diese aus der Bundeskompetenz in einem Sachbereich – etwa Art. 81 BV (Öffentliche Werke) oder Art. 92 Abs. 1 BV (Post- und Fernmeldewesen) – herzuleiten, was jedoch richtigerweise mehrheitlich abgelehnt wird.[182] Aus Art. 46 Abs. 1 BV ergibt sich zwar, dass der Bund den Kantonen bei der Umsetzung von Bundesrecht gewisse Umsetzungspflichten auferlegen kann, jedoch muss er sich auch hierbei auf eine Grundlage in Verfassung oder Gesetz stützen können, womit er im jeweiligen Bereich wiederum eine Kompetenz haben muss.[183] Daher kann der Bund lediglich in denjenigen Bereichen umfassende Vorgaben machen, in denen der Bund über umfassende oder fragmentarische Rechtsetzungskompetenzen verfügt. Dies ist jedoch gerade im Verwaltungsrecht in wichtigen Bereichen (z.B. Steuern, Bildung) nicht der Fall.[184] Zwar wird befürwortet, dass der Bund, zumindest in den Bereichen, in denen er kompetent ist, unter Umständen auch organisatorische Vorgaben, etwa das Verwenden einer bestimmten Software, vorsehen kann (allenfalls gar auf Verordnungsstufe). Zu beachten ist jedoch, dass gemäss Art. 46 Abs. 3 BV den Kantonen bei der Umsetzung des Bundesrechts eine möglichst grosse Gestaltungsfreiheit zu belassen ist. Insbesondere wenn in einem Kanton bereits eine Informatikinfrastruktur im entsprechenden Bereich aufgebaut ist, würde dies einen nicht unbedeutenden Eingriff in dessen Autonomie darstellen, was tendenziell zu unterlassen ist.[185]

69 Eine entsprechende Querschnittsregelung wie in Deutschland oder Österreich scheitert daher de lege lata an der fehlenden Kompetenz des Bundes. Eine diesbezügliche Kompetenz müsste auf dem Weg der Verfassungsänderung geschaffen werden.[186] Es ist jedoch fraglich, ob dies mit dem föderalistischen Staatsaufbau der Schweiz und dem auch in der Bundesverfassung präsenten Gedanken, dass die Kantone ihre Eigenständigkeit so weit als möglich bewahren, vereinbar wäre.[187] Zu beachten ist an dieser Stelle, dass mit dem zum Zeitpunkt der Ausarbeitung dieser Arbeit im Vernehmlassungsverfahren

181 Rechtsgrundlagen IKT-Zusammenarbeit, S. 7 f

182 Rechtsgrundlagen IKT-Zusammenarbeit, S. 7.

183 WALDMANN/BORTER, BSK BV, Art. 46, N. 20 ff.

184 Rechtsgrundlagen IKT-Zusammenarbeit, S. 10.

185 Vgl. zum Ganzen Rechtsgrundlagen IKT-Zusammenarbeit, S. 10.

186 Rechtsgrundlagen IKT-Zusammenarbeit, S. 14.

187 Vgl. etwa GLASER, SJZ, 2018, S. 186.

befindlichen Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben (EMBaG), welches zumindest im Bereich des Vollzugs von Bundesrecht vorsieht, dass der Bund Kantone zur Nutzung gewisser Dienste und zur Einhaltung gewisser Standards verpflichten kann (vgl. Art. 12–14 E-EMBaG), sowie mit dem Aufbau der Organisation «Digitale Verwaltung Schweiz» gewisse Anstrengungen in diese Richtung unternommen werden.[188]

B. Gesetzesebene

Wie soeben ausgeführt, gibt es mangels entsprechender Bundeskompetenz im Bereich des Verwaltungsverfahrens kein Gesetz, welches bereichsübergreifend Rechtsfragen regelt, die sich mit der Digitalisierung der Verwaltung stellen. Entsprechende Regelungen sind daher in erster Linie in den jeweils einschlägigen Fachgesetzen zu finden. Eine erschöpfende Behandlung des Umgangs mit der Digitalisierung in verschiedenen Rechtsbereichen der öffentlichen Verwaltung würde den Rahmen dieser Arbeit sprengen. Daher sollen vorliegend lediglich die wichtigsten Erlasse kurz vorgestellt werden, welche im weiteren Verlauf eine gewisse Rolle spielen. 70

1. Datenschutzgesetzgebung

Der Einsatz von neuen Informations- und Kommunikationstechnologien geht in zunehmendem Masse auch mit einer vermehrten Datenbearbeitung (insbesondere über Personen) und somit mit einer steigenden Gefahr von Persönlichkeitsverletzungen einher.[189] Gemäss dem Grundrecht der informationellen Selbstbestimmung, welches seit der Revision der BV in Art. 13 Abs. 2 BV statuiert ist, hat jede Person Anspruch auf den Schutz vor Missbrauch ihrer persönlichen Daten. Der durch die Bestimmung gewährte Schutz erstreckt sich über den engen Wortlaut hinaus grundsätzlich auf jede datenbezogene Tätigkeit des Staates hinsichtlich der Daten von Personen.[190] 71

Konkretisiert wird dieser Anspruch durch die Datenschutzgesetzgebung des Bundes und der Kantone. Das Bundesgesetz über den Datenschutz (DSG, SR 235.1) vom 19. Juni 1992 regelt den Schutz für das Bearbeiten von Personendaten durch Private und Bundesorgane (vgl. Art. 1 und Art. 2 DSG). Das Datenschutzgesetz des Bundes kommt gemäss Art. 2 Abs. 1 dann zur Anwendung, wenn Bundesorgane (oder Private) Personendaten bearbeiten, während die 72

188 Vgl. etwa: Bundesrat, Medienmitteilung vom 11. Dezember 2020: Vernehmlassungseröffnung EMBaG

189 Botschaft DSG, S. 414.

190 DIGGELMANN, BSK BV, Art. 13, N. 33.

jeweiligen kantonalen Gesetze die Datenbearbeitung durch Kantonal- und Kommunalbehörden – ausser Letztere sehen eigene Regelungen vor – regeln. Da viele dieser Gesetze später als das DSG erlassen wurden, können sie allenfalls Regelungen zu Problemen enthalten, welche das DSG nicht regelt. Auf die kantonalen Regelungen soll daher in erster Linie eingegangen werden, wenn sie über das DSG des Bundes hinausgehende oder davon abweichende Regelungen treffen.

73 Die Datenschutzgesetzgebung sieht unter anderem vor, unter welchen Voraussetzungen Personendaten bearbeitet und bekanntgegeben werden dürfen und welche Rechte Privaten hinsichtlich der Bearbeitung ihrer Daten zustehen. Hierbei handelt es sich um die Grundsätze der Datenbearbeitung, welche das «formelle Datenschutzrecht» bilden.[191] Diese Grundsätze sagen indes nichts darüber aus, welche Daten in einem konkreten Sachbereich an wen bekanntgegeben werden dürfen. Daher bedürfen sie regelmässig einer Konkretisierung im jeweiligen bereichsspezifischen Fachrecht. Dabei handelt es sich um das sogenannte «materielle Datenschutzrecht».[192] Dies führt dazu, dass viele andere Gesetze ebenfalls (materielle) Datenschutzbestimmungen enthalten. So ist zum Beispiel die Datenbearbeitung im Ausländer- und Asylrecht im AiG bzw. AsylG und den zugehörigen Verordnungen ausführlich geregelt.[193] Zudem wird die Datenschutzgesetzgebung durch diverse Verordnungen konkretisiert.

a) Wichtige Regeln zur Datenbearbeitung durch Bundesorgane

74 Inzwischen findet bei fast jeder Behördenhandlung auch eine Bearbeitung von Personendaten statt, zumal diese Begriffe nach dem soeben Ausgeführten weit zu verstehen sind. Da im Laufe der Arbeit wiederholt auf die damit verbundenen Bestimmungen des DSG eingegangen wird, werden hier quasi vor der Klammer die wichtigsten, einschlägigen Rechtsgrundlagen behandelt. Diese sollen später auf den jeweiligen Anwendungsfall übertragen und weiter konkretisiert werden.

75 Auf Bundesebene sieht Art. 2 Abs. 2 DSG gewisse Ausnahmen vor, in welchen das Gesetz nicht anwendbar ist. Insbesondere kommt es gemäss Art. 2 Abs. 2 lit. c DSG im Rahmen von hängigen Straf-, Zivil- und verwaltungsrechtlichen Verfahren nicht zur Anwendung, mit Ausnahme jedoch der hier insbesondere interessierenden erstinstanzlichen Verwaltungsverfahren.

191 Erstmals RUDIN, SJZ, 2009, S. 1 ff., RUDIN, PK IDG BS, Grundlagen, N. 43 ff. für das kantonale Recht.

192 Vgl. zum Ganzen: RUDIN, digma, 2016, S. 124.

193 Vgl. etwa Art. 97 ff. AIG

Als Personendaten im Sinne dieser Gesetzgebung haben dabei gemäss Art. 3 lit. a DSG sämtliche Angaben zu gelten, die sich auf eine bestimmte oder bestimmbare Person beziehen. Gewisse Personendaten sind aufgrund ihres Gehalts in besonderem Masse geeignet, eine Persönlichkeitsverletzung herbeizuführen. Diese sogenannten besonders schützenswerten Personendaten umfassen etwa Daten zu Religion oder Gesundheit (Art. 3 lit. c DSG).[194] Ebenfalls ein erhöhtes Schutzbedürfnis besteht bei Persönlichkeitsprofilen, verstanden als Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (Art. 3 lit. d DSG). Das Bearbeiten von Personendaten ist dabei in einem möglichst weiten Sinne zu verstehen[195], so dass jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln, darunter zu subsumieren ist (Art. 3 lit. e. DSG). Die Bekanntgabe von Personendaten umfasst in einem weiten Verständnis jede Aktivität, mit der Personendaten einer anderen Person zugänglich gemacht werden (Art. 3 lit. f DSG).[196] 76

Jegliche Bearbeitung von Daten benötigt nach Art. 17 DSG eine gesetzliche Grundlage. Grundsätzlich müssen in dieser Rechtsgrundlage Zweck, beteiligte Organe und Ausmass der Datenbearbeitung in den Grundzügen festgelegt sein. Allerdings stellt bereits die Botschaft klar, dass in der Regel aufgrund der Vielzahl möglicher Bearbeitungen keine allzu strengen formellen Anforderungen an diese Grundlage gestellt werden dürfen.[197] Besonders schützenswerte Personendaten oder Persönlichkeitsprofile benötigen gemäss Art. 17 Abs. 2 DSG grundsätzlich eine Regelung im formellen Gesetz. Ausnahmen davon bestehen, wenn dies für eine in einem Gesetz im formellen Sinn klar umschriebene Aufgabe unentbehrlich ist (Bst. a), der Bundesrat es im Einzelfall bewilligt, weil die Rechte der betroffenen Person nicht gefährdet sind (Bst. b), oder die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat (Bst. c). Die Bekanntgabe von Personendaten durch Bundesorgane ist in Art. 19 DSG geregelt. In erster Linie ist eine Bekanntgabe nur zulässig, wenn eine gesetzliche Grundlage im Sinne von Art. 17 DSG vorliegt. Zusätzlich statuiert jedoch auch Art. 19 DSG einige Ausnahmen, in denen keine entsprechende Grundlage notwendig ist. Findet eine Bekanntgabe ins Ausland statt, so muss gemäss Art. 6 DSG sichergestellt werden, dass damit keine zusätzliche Gefährdung der betroffenen Person verbunden ist, weil im Empfangsstaat eine 77

194 Vgl. RUDIN, SHK-DSG, Art. 3, N. 20 f. (kritisch zum Begriff).

195 Botschaft DSG, S. 447.

196 RUDIN, SHK-DSG, Art. 3 N. 40 ff.

197 Botschaft DSG 1988, S. 467.

Gesetzgebung fehlt, welche einen angemessenen Schutz gewährleistet. Spezielle Regeln gelten gemäss Art. 10a DSG auch, wenn das Bearbeiten von Personendaten durch Vereinbarung oder Gesetz an Dritte übertragen werden soll.

78 Das DSG statuiert zudem einige Grundsätze der Datenbearbeitung, welche in Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG verankert sind.[198] Diese Grundsätze gelten nicht absolut, sondern spezielle gesetzliche Grundlagen können explizit davon abweichen. Wo dies nicht der Fall ist, sind die entsprechenden Grundsätze indes zu beachten.[199] Aus diesen Bestimmungen ergibt sich etwa, dass Personendaten nur nach Treu und Glauben bearbeitet werden dürfen und ihre Bearbeitung verhältnismässig sein muss (Art. 4 Abs. 2 DSG). In diesem Sinne dürfen nur diejenigen Daten beschafft werden, welche für den jeweiligen Zweck explizit benötigt werden.[200] Weiter dürfen sie nur zu dem Zweck bearbeitet werden, welcher bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist (Art. 4 Abs. 3 DSG), und die Beschaffung sowie der Zweck müssen für die betroffene Person erkennbar sein (Art. 4 Abs. 4 DSG). In gewissen Fällen wird gemäss Art. 4 Abs. 5 eine Einwilligung der Person in die Bearbeitung verlangt, welche nur dann gültig ist, wenn sie freiwillig und nach angemessener Information erfolgt. Aus Art. 5 DSG ergibt sich, dass, wer Personendaten bearbeitet, sich über ihrer Richtigkeit zu vergewissern und Massnahmen dafür zu treffen hat, dass die Daten berichtigt oder vernichtet werden können. Aus Art. 7 DSG ergibt sich schliesslich, dass Personendaten durch angemessene technische oder organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen sind. Je nach Art der gespeicherten Daten sind die gewählten technischen und organisatorischen Massnahmen entsprechend anzupassen.[201]

79 Den Betroffenen stehen einige Ansprüche zu, mit denen sie die ihnen durch dieses Gesetz gewährten Rechte durchsetzen können. So haben sie gemäss Art. 8 DSG ein Recht, gegenüber dem Inhaber einer Datensammlung Auskunft zu verlangen, ob Personendaten über sie bearbeitet werden. Der Person müssen dabei die betreffenden Daten sowie allenfalls Zweck oder Rechtsgrundlagen der Bearbeitung mitgeteilt werden. Art. 25 DSG sieht zudem vor, dass bei einer widerrechtlichen Bearbeitung (etwa mangels gesetzlicher Grundlage) verlangt werden kann, dass das Bundesorgan das widerrechtliche Bearbeiten einstellt, dessen Folgen beseitigt oder dessen Widerrechtlichkeit feststellt.

198 Vgl. Dazu bereits den Wortlaut von Art. 12 Abs. 2 lit. a DSG:

199 EPINEY/CIVITELLA/ZBINDEN PATRIZIA, S. 22.

200 MAURER-LAMBROU/STEINER, BSK DSG/BGÖ, Art. 4 DSG, N. 11.

201 BAERISWYL, SHK-DSG, Art. 7, N. 18

b) Aktuelle Entwicklungen im Bereich des Datenschutzrechts

Das geltende Datenschutzgesetz des Bundes wurde Ende der 80er- und zu Beginn der 90er-Jahre erarbeitet. Die rasante technologische Entwicklung hat dabei Fragestellungen aktuell werden lassen, welche beim damaligen Erlass noch nicht absehbar waren (z.B. die in dieser Arbeit interessierenden Technologien wie Blockchain). Zudem erfuhr auch das Datenschutzrecht der Europäischen Union mit der Einführung der DSGVO einschneidende Veränderungen.[202] Aus diesen Gründen beschloss der Bundesrat, das DSG einer Totalrevision zu unterziehen. Durch diese Revision soll der Datenschutz gestärkt werden, indem etwa die Transparenz der Bearbeitung von Daten und die Kontrollmöglichkeiten der betroffenen Personen über ihre Daten verbessert werden.[203] Zudem soll die Aufsicht über die Anwendung und die Einhaltung der eidgenössischen Datenschutznormen verbessert werden, etwa indem dem Eidgenössischen Datenschutzbeauftragten zusätzliche Kompetenzen eingeräumt und Verletzungen stärker sanktioniert werden.[204] Die Revision des Datenschutzrechts befindet sich zum Zeitpunkt der Arbeit in der parlamentarischen Beratung.[205] Daher erfolgt die Behandlung datenschutzrechtlicher Fragen im Rahmen dieser Arbeit in erster Linie auf der Basis des geltenden DSG. Es soll indes auf im interessierenden Kontext relevante Neuerungen im Rahmen der Totalrevision hingewiesen werden. 80

2. Öffentlichkeitsgesetzgebung

Die Verwaltung verfügt nicht nur über immer mehr Personendaten, sondern hat auch einen immer grösseren «Datenschatz» an anderen Daten, an deren Offenlegung die Bevölkerung ebenfalls ein Interesse hat. Lange Zeit waren für die Öffentlichkeit nur diejenigen Informationen der Verwaltung zugänglich, welche aufgrund einer gesetzlichen Grundlage bekanntgegeben werden mussten oder welche die Behörden von sich aus freiwillig preisgaben.[206] Ab der Mitte des letzten Jahrhunderts setzte jedoch eine internationale Entwicklung ein, das Verwaltungshandeln öffentlicher zu machen und ein allgemeines Zugangsrecht auf Informationen der Verwaltung auf Gesuch hin anzuerkennen. Dies führte auch in der Schweiz zuerst in einigen Kantonen und schliesslich im Bund zu einem Paradigmenwechsel: Anstelle des Prinzips, 81

202 Für die Relevanz der DSGVO siehe im späteren Verlauf der Arbeit etwa Rz. 648 ff.

203 Botschaft Rev. DSG 2017, S. 6943.

204 Botschaft Rev. DSG 2017, S. 6973.

205 Vgl. zum aktuellen Stand.

206 Vgl. Botschaft BGÖ, S. 1964; BRUNNER/MADER, SHK BGÖ, Einleitung, N. 4.

dass alles geheim sein soll, was nicht explizit öffentlich ist, soll alles öffentlich sein, was nicht explizit geheim ist.[207] Dieses Öffentlichkeitsprinzip wurde auf Bundesebene nicht ausdrücklich in der Verfassung verankert. Es ist aber umfassend im per 1. Juli 2006 in Kraft getretenen BGÖ geregelt.[208] Das Gesetz gesteht jeder Person einen (einschränkbaren) Anspruch auf Zugang zu amtlichen Dokumenten ohne den Nachweis eines besonderen Interesses zu.[209] Durch die Information vonseiten der Verwaltung soll deren Transparenz erhöht und somit das Vertrauen der Bevölkerung gestärkt werden.[210] Das Gesetz wird in der Verordnung über das Öffentlichkeitsprinzip der Verwaltung (Öffentlichkeitsverordnung, VBGÖ; SR 152.31) vom 24. Mai 2006 konkretisiert. Auch in den meisten Kantonen gilt das Öffentlichkeitsprinzip, so dass diese ebenfalls eine entsprechende Gesetzgebung besitzen.[211]

3. Verfahrensgesetze und elektronischer Behördenverkehr

82 Ein wichtiger Teil dieser Arbeit ist den Auswirkungen der Digitalisierung auf das Verwaltungsverfahren gewidmet. Im Rahmen der erstinstanzlichen Verwaltungsverfahren ist dabei insbesondere das Bundesgesetz über das Verwaltungsverfahren (Verwaltungsverfahrensgesetz, VwVG, SR 172.021) vom 20. Dezember 1968 relevant. Das VwVG regelt gemäss Art. 1 das Verfahren in Verwaltungssachen, die durch Verfügungen von Bundesverwaltungsbehörden in erster Instanz oder auf Beschwerde hin zu erledigen sind. Es kommt (mit einigen in Art. 2 VwVG statuierten Ausnahmen) in sämtlichen Verwaltungsverfahren auf Bundesebene zur Anwendung. Zu Beginn der 2000er-Jahre erkannte der Gesetzgeber das Potenzial des «elektronischen Behördenverkehrs» und schaffte daher die Grundlagen dafür, dass gewisse Eingaben bei Verwaltungs- und Gerichtsbehörden auch elektronisch eingereicht werden können.[212] Konkretisiert werden diese Bestimmungen im Rahmen der Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV) vom 18. Juni 2010. Relevant ist in diesem Zusammenhang auch das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES, SR 943.03) vom 18. März 2016, welches vorgibt,

207 BRUNNER/MADER, SHK BGÖ, Einleitung, N. 8.

208 Vgl. MÜLLER, BSK BV, Art. 180, N. 8. Botschaft BGÖ, S. 2039.

209 GLASER, ZSR, 2015, S. 298.

210 Botschaft BGÖ, S. 1973.

211 Vgl. etwa die Kantonsübersicht des Vereins Öffentlichkeitgesetz.ch.

212 Botschaft Rev. Bundesrechtspflege, S. 4209.

unter welchen Voraussetzungen elektronische Signaturen mit handschriftlichen Unterschriften gleichgesetzt werden können.

C. Informatikstrategien

Die Digitalisierung betrifft – wie bereits ausgeführt wurde – potenziell eine Vielzahl verschiedener Rechtsbereiche und somit auch Akteure aus unterschiedlichen Hierarchiestufen. Eine übergreifende Querschnittsregelung im Sinne eines E-Government-Gesetzes ist dabei aus Kompetenzgründen zumindest de lege ferenda nicht möglich. Indes können sich die gleichen oder zumindest ähnliche Probleme in verschiedenen Bereichen oder Gemeinwesen stellen. Um zu verhindern, dass alle Akteure ihre eigenen Ziele auf eigene Weise verfolgen, was zweifelsohne zu Doppelspurigkeiten und Ineffizienz führen würde, ist eine gewisse Koordination des Vorgehens unerlässlich. Bereits im Jahr 1997 hatte sich eine vom Bundesrat berufene verwaltungsunabhängige «Groupe de réflexion» mit den Chancen und Risiken der Informationsgesellschaft und deren sozialen und ökonomischen Auswirkungen und Folgen auseinandergesetzt und dabei auf die Wichtigkeit einer politisch definierten Strategie für den Übergang in die Informationsgesellschaft für alle Ebenen der Verwaltung hingewiesen.[213] Gestützt auf den von dieser Groupe de réflexion vorgelegten Bericht legte der Bundesrat am 18. Februar 1998 eine «Strategie für eine Informationsgesellschaft Schweiz» vor.[214] Ziel dieser Strategie war, dass Informations- und Kommunikationstechnologien rasch und koordiniert zum Nutzen aller eingesetzt werden sollen[215], um von der fortschreitenden Digitalisierung in allen Lebensbereichen zu profitieren und die Wohlfahrt der Bevölkerung langfristig nicht nur zu sichern, sondern diese auch auszubauen.[216] Dazu wurden Grundsätze und – in besonders wichtigen Themenfeldern – Ziele für eine gewisse strategische Zeitperiode festgelegt. Zur Erreichung dieser Ziele wurden verschiedene Massnahmen, etwa die Ausarbeitung von Konzepten oder rechtlichen Grundlagen, festgesetzt. Die Strategie wurde in den Jahren 2006 und 2012 überarbeitet und im Jahr 2016 in eine Strategie «Digitale Schweiz» überführt, welche trotz des geänderten Namens als direkter Nachfolger der vorgenannten Strategien zu sehen ist.[217] 83

Der Bund erkannte früh, dass der elektronische Behördenverkehr (und somit E-Government) einen wichtigen Teil des Umgangs der Schweiz mit der 84

213 Bericht Informationsgesellschaft 1997, S. 8.

214 Strategie Informationsgesellschaft 1998, S. 2387.

215 Strategie Informationsgesellschaft 2006, S. 1877

216 Strategie Digitale Schweiz 2016, S. 3986.

217 Strategie Digitale Schweiz 2016, S. 3986.

Informationsgesellschaft darstellt.[218] Eine erste E-Government-Strategie auf Bundesebene wurde unter der Federführung des Informatikstrategieorgans des Bundes (ISB) im Jahr 2002 verabschiedet und verfolgte das Ziel, die Regierungs- und Verwaltungstätigkeit effizienter, flexibler und transparenter zu gestalten.[219] Im Rahmen einer Situationsanalyse von E-Government in der Schweiz kam das ISB im Jahr 2005 auf Basis von nationalen und internationalen Studien zum Schluss, dass die Schweiz in Bezug auf öffentliche Online-Dienstleistungen schlecht abschnitt.[220] Als Problem wurde insbesondere die fehlende Nutzung von Synergien erkannt, weswegen eine Koordination von E-Government-Aktivitäten im Rahmen einer konsensualen Gesamtstrategie entwickelt werden müsse, welche alle föderalen Ebenen einbeziehe.[221]

85 Die am 24. Januar 2007 verabschiedete E-Government-Strategie setzte sich daher als Hauptziel, dass sowohl die Wirtschaft als auch die Bevölkerung ihren wichtigen oder mit grossem Aufwand verbundenen Behördenverkehr elektronisch abwickeln können und Behörden verwaltungsintern untereinander elektronisch verkehren sollen. Zu diesem Zweck sah die Strategie weitreichende Neuerungen vor, etwa in der Form eines Katalogs priorisierter Vorhaben, welche schwerpunktmässig bearbeitet und laufend aktualisiert werden sollten.[222] Die Strategie wurde in der Folge mehrfach überarbeitet, wobei die aktuelle Version «E-Government-Strategie 2020–2023» Ende 2019 durch den Bundesrat, die Konferenz der Kantonsregierungen (KdK) und die Vorstände des Städte- und Gemeindeverbands unterzeichnet wurde.[223] Die Strategien sind dabei primär für die jeweiligen zuständigen Departemente des Bundes handlungsrelevant, da die Umsetzung in erster Linie durch diese vorzunehmen ist.[224] Private können daraus keine Rechte und Pflichten ableiten. Für die Behörden sehen die Strategien indes konkrete Handlungsvorgaben vor, an welchen sich diese auch messen lassen müssen.

86 Ein wichtiges Umsetzungswerkzeug der E-Government-Strategie ist auch der Katalog priorisierter Vorhaben sowie der Aktionsplan (RV 2011) bzw. der Schwerpunktplan (RV 2015). Darin werden die wichtigsten Projekte und die Massnahmen, um diese zu erreichen, sowie deren periodische Überprüfung

218 Bereits in der ersten Strategie im Jahr 1998 wurde festgehalten, dass die Rahmenbedingungen für einen elektronischen Geschäfts- und Behördenverkehr geschaffen werden sollen, vgl. Strategie Informationsgesellschaft 1998, S. 2389.

219 FRAEFEL/SELZAM/HUNZIKER, S. 22.

220 Vgl. Situationsanalyse E-Government und FRAEFEL/SELZAM/HUNZIKER, S. 23.

221 Situationsanalyse E-Government, S. 8.

222 E-Government-Strategie Schweiz 2007, S. 9 f.

223 Vgl. etwa: die E-Government Strategie 2020–2023. E-Government Schweiz.

224 Vgl. etwa Strategie Informationsgesellschaft 2006, S. 1884.

festgelegt. Die Rechtsnatur dieser Pläne ist ebenfalls nicht eindeutig. Die jeweiligen Vorhaben dienen indes in erster Linie als Orientierungshilfen, welche rechtlich nicht als verbindlich betrachtet werden. Sie sind somit als Realakte zu charakterisieren.[225] Behördliche Realakte sind diejenigen Verwaltungshandlungesn, welche nicht auf einen rechtlichen, sondern einen tatsächlichen Erfolg gerichtet sind. Als solche können sie auch keine Rechte und Pflichten für den Privaten begründen.[226] Entsprechend sind auch sie für den Einzelnen nicht verbindlich.

III. Kantonale Ebene

A. Interkantonale Regelungsansätze

Wie bereits ausgeführt, gibt es aus Kompetenzgründen keine Bundesgesetzgebung, welche die Digitalisierung im Verwaltungsverfahren übergreifend regelt. In allen Bereichen, in denen die Kantone mindestens eine parallele Gesetzgebungskompetenz haben, können sie daher das Verfahren selbständig regeln. Es hat sich indes im Laufe der letzten Jahre vermehrt gezeigt, dass sich in vielen Bereichen kantonsübergreifend ähnliche Probleme stellen und sich dadurch auch Doppelspurigkeiten (oder positiv ausgedrückt Synergien) ergeben können.[227] Die E-Government-Strategie Schweiz soll dazu dienen, die Bemühungen der Gemeinwesen der verschiedenen Stufen zu koordinieren. Deren Umsetzung verbleibt, wie ebenfalls weiter oben ausgeführt, in der Organisationsautonomie der Kantone. Bereits in der E-Government-Strategie von 2007 wurde daher als Ziel genannt, dass die Kantone gemeinsam mit ihren Gemeinden basierend auf dieser Strategie eigene E-Government-Strategien und -Massnahmen definieren.[228] Zum aktuellen Zeitpunkt verfügen praktisch alle Kantone über eine eigene E-Government-Strategie.[229] Um zumindest eine gewisse Kohärenz zwischen den Bemühungen des Bundes und der Kantone herzustellen, erarbeiteten der Bundesrat und die Konferenz der Kantonsregierungen (KdK) im Rahmen der E-Government-Strategie eine «Rahmenvereinbarung über die E-Government Zusammenarbeit in der Schweiz». Dabei handelt es sich um einen Vertrag zwischen den Kantonen.[230] 87

225 GLASER, ZSR, 2015, S. 299.

226 HÄFELIN/MÜLLER/UHLMANN, N. 1408 ff.

227 Vgl. FRAEFEL/SELZAM/HUNZIKER, S. 9.

228 E-Government-Strategie Schweiz 2008–2015, S. 5.

229 Über keine eigene Strategie verfügte per Ende 2019 lediglich der Kanton AI, vgl. E-Government Schweiz: Zahlen und Fakten.

230 Vgl. etwa Rechtsgrundlagen IKT-Zusammenarbeit, S. 15 oder GLASER, ZSR, 2015, S. 297.

Im Rahmen seiner Zuständigkeiten kann sich gemäss Art. 48 Abs. 2 BV auch der Bund an einem solchen Vertrag beteiligen.

88 Die Rahmenvereinbarung soll dazu dienen, die Zusammenarbeit von Bund und Kantonen in diesem Bereich (etwa hinsichtlich der Organisation und der Finanzierung) zu regeln (Art. 1 Rahmenvereinbarung [RV]). Diese legte etwa fest, dass Gemeinwesen anderen Gemeinwesen die Nutzung ihrer Daten oder Leistungen nicht unnötig erschweren (Art. 3 RV) oder dass international bzw. national erarbeitete Standards eingehalten werden sollen (Art. 4 RV). Zudem wurden gemeinsame Organe geschaffen, namentlich ein Steuerungsausschuss, ein beratender Expertenrat und eine im Informatiksteuerorgan des Bundes (ISB) angesiedelte und vom Bund finanzierte «Geschäftsstelle E-Government Schweiz» als Stabsorgan dieser beiden Gremien.[231] Darüber hinaus wurden Regelungen zur Trägerschaft und der Finanzierung von Projekten getroffen. Auch die Rahmenvereinbarung wurde in den letzten Jahren mehrfach überarbeitet und gilt in ihrer aktuellen Version bis ins Jahr 2023.

89 Die Rahmenvereinbarung sieht vor, dass die Kantone im Bereich des E-Government zusammenzuarbeiten haben, etwa indem sie Daten und Lösungen mehrfach nutzen (Ziffer 1.3 RV) oder gemeinsame Standards verwenden (Ziffer 1.4 RV). Zudem werden gewisse gemeinsame Organe, wie ein Steuerungs- und ein Planungsausschuss, geschaffen (Ziffer 2.1 RV). Im Weiteren statuiert Ziffer 1.7 RV, dass Rechtsetzung Sache der Kantone bzw. des Bundes bleibt, indem etwa Rechtsetzungsbedarf frühzeitig evaluiert wird und entsprechende Rechtsgrundlagen zeitgerecht geschaffen werden. Bei den Bestimmungen handelt es sich somit um Handlungsanweisungen an die Kantone, welche allenfalls entsprechende Gesetzesbestimmungen erlassen müssen. Für den Einzelnen schaffen die Bestimmungen indes keine Rechte und Pflichten und sind auch nicht genügend klar formuliert, um in einem Einzelfall direkt angewendet werden zu können. Eigenes Recht wird durch die Rahmenvereinbarung nicht gesetzt. Die vorliegende Rahmenvereinbarung stellt somit ebenfalls keinen unmittelbar anwendbaren Erlass dar, welcher Private verpflichten oder berechtigen würde. Vielmehr handelt es sich um ein rechtsgeschäftliches Konkordat, welches die Kantone untereinander und im Verhältnis zum Bund zur Einhaltung verpflichtet.[232] Allerdings geht auch die Ansicht, dass es sich bei der Rahmenvereinbarung nur um eine formale Absichtserklärung zur verstärkten Zusammenarbeit handle, welche indes keinen verpflichtenden Charakter habe[233], meines Erachtens fehl. Dafür spricht,

231 FRAEFEL/SELZAM/HUNZIKER, S. 24.

232 Vgl. zum Ganzen GLASER, ZSR, 2015, S. 297.

233 FRAEFEL/SELZAM/HUNZIKER, S. 24.

dass in den überarbeitenden Versionen der Rahmenvereinbarung die Bestimmung fehlt, den Kantonen würden keine finanziellen Verpflichtungen aus der Unterzeichnung der Rahmenvereinbarung erwachsen. Vielmehr können sie gar zu Finanzierungsbeiträgen verpflichtet werden.[234]

B. Kantonale Gesetze

Im Gegensatz zum Bund, welcher mangels Kompetenz keine einheitliche E-Government-Gesetzgebung erlassen hat, ist eine solche für die Kantone zumindest im Bereich ihrer Kompetenzen durchaus zulässig. Daher haben einige Kantone eigene E-Government-Gesetze erlassen.[235] In vielen Fällen beschränken sich die darin enthaltenen Regelungen allerdings darauf, als Rahmengesetzgebung die Zusammenarbeit zwischen Kanton, Bezirken und Gemeinden und wichtige Grundsätze zur Finanzierung, zu den Mitsprachemöglichkeiten und zur Entscheidungsfindung zu regeln.[236] Sie funktionieren somit ähnlich wie die soeben thematisierte Rahmenvereinbarung. Hervorzuheben ist hier die Lösung des Kantons Appenzell Ausserrhoden, welcher im Gesetz über E-Government und Informatik vom 4. Juni 2012 eine spezialgesetzliche Aktiengesellschaft «AR-Informatik AG» geschaffen hat, deren Zweck gemäss Art. 11 des Gesetzes die Erbringung von Dienstleistungen im Bereich der Informations- und Kommunikationstechnologie für den Kanton und die Gemeinden sowie die Unterstützung von Kanton und Gemeinden im Bereich E-Government ist. 90

Mittlerweile bieten praktisch alle Kantone gewisse Dienstleistungen online an. In einigen Kantonen können dabei verschiedene Angebote des jeweiligen Gemeinwesens über einen einzigen webbasierten Zugangskanal abgerufen werden (sog. Behördenportal).[237] Dabei wird in der Regel vorgesehen, dass den Benutzenden ein individuelles Konto zur Verfügung gestellt wird, welches zur Abwicklung der Geschäfte dient und gewisse Daten über sie speichert, damit diese nicht bei jedem Behördenkontakt erneut eingegeben werden müssen.[238] Verschiedene Kantone haben den Aufbau und die Funktion 91

234 Vgl. dazu etwa Art 2a bzw. 15 Rahmenvereinbarung 2011 und Art. 23 Rahmenvereinbarung 2015.

235 Zu nennen sind hier etwa: Gesetz über eGovernment und Informatik (Kanton Appenzell Ausserhoden, bGS 142.3) vom 4. Juni 2012, Verordnung über das Informatik- und Telekommunikationsmanagement in der Kantonsverwaltung Freiburg (SGF 112.96.11) vom 3. November 2015, Gesetz über das E-Government (Kanton Schwyz, SRZS 140.600) vom 22. April 2009.

236 Vgl. etwa für das E-Government Gesetz des Kantons Schwyz: REGIERUNGSRAT DES KANTONS SCHWYZ, S. 2.

237 REGIERUNGSRAT DES KANTONS BASEL-STADT, S. 5.

238 REGIERUNGSRAT DES KANTONS BASEL-STADT, S. 9.

entsprechender Portale in einem Spezialgesetz geregelt.[239] Einzelne Kantone oder Gemeinwesen bieten gar eigene digitale Identifikationslösungen an, welche den Benutzern dazu dienen, elektronische Dienstleistungen über ein Behördenportal zu beziehen, und teilweise auch im privatwirtschaftlichen Umfeld eingesetzt werden können.[240]

92 Wie auf Bundesebene gibt es auch auf kantonaler Ebene diverse weitere Erlasse, welche im Bereich der digitalen Verwaltung relevant sind. Eine umfassende Vorstellung dieser Rechtsquellen kann im Rahmen dieser Arbeit nicht geleistet werden. Zu beachten sind etwa die kantonalen Verfahrensgesetze, welche analog etwa zum VwVG die Möglichkeit von elektronischen Eingaben im kantonalen Verwaltungs- oder Verwaltungsgerichtsverfahren vorsehen können. Aktuell verfügen indes (noch) nicht alle Kantone über die gesetzlichen Grundlagen, um Verfahrenshandlungen im Verwaltungs- und Verwaltungsgerichtsverfahren auf elektronischem Wege zu ermöglichen.[241] Auch auf kantonaler Ebene werden im Behördenverkehr Personendaten über die Bevölkerung bearbeitet. Für die Bearbeitung von Personendaten durch kantonale Behörden ist nicht das Datenschutzgesetz des Bundes einschlägig, welches nur Bearbeitungen durch Bundesorgane und Private abdeckt. Daher muss jeder Kanton über eine eigene kantonale Datenschutzgesetzgebung verfügen, welche im Bereich E-Government ebenfalls zu beachten ist.

93 Insgesamt gilt es festzustellen, dass die Digitalisierung der Verwaltung in den Kantonen unterschiedlich weit fortgeschritten ist und unterschiedlich stark im Fokus steht. Daher unterscheidet sich auch die jeweils einschlägige Gesetzgebung derzeit noch stark voneinander. Während einige Kantone in einer Vielzahl von Gesetzen die jeweiligen Aspekte (z.B. Behördenportale, Identifikationslösungen) behandeln, verfügen andere über keinen entsprechenden rechtlichen Rahmen. Es ist trotz dieses unterschiedlichen Umgangs mit der Thematik festzuhalten, dass das Thema in fast allen Kanton Beachtung findet, sei dies anhand einer Strategie, eines Gesetzes oder sonstiger Anstrengungen.[242]

239 REGIERUNGSRAT DES KANTONS BASEL-STADT, S. 4.

240 Vgl.die eID+ des Kantons Schaffhausen.

241 Im Jahr 2016 waren es lediglich 11 von 26 Kantonen, vgl. Fischer, Elektronischer Behördenverkehr im Kanton Bern.

242 Vgl. BUESS/ISELIN/BIERI, S. 58; 90 % der Kantone bieten ihrer Bevölkerung ein Portal für die Abwicklung elektronischer Behördengeschäfte und Social-Media-Kanäle für die Kommunikation.

Teil 2: Auseinandersetzung mit den geltenden Rechtsgrundlagen

Die öffentliche Verwaltung bedient sich in einem zunehmenden Masse der Informations- und Kommunikationstechnologie. Viele Anwendungen dienen dabei in erster Linie der Vereinfachung interner Prozesse, etwa Geschäftsverwaltungslösungen, welche die Aktenführung digital abbilden sollen.[243] Doch können technologische Lösungen auch im Umgang des Staats mit Privaten vielfältig eingesetzt werden. Im vorliegenden Teil soll untersucht werden, ob die Rechtsfragen, welche sich durch die neuen Möglichkeiten der Digitalisierung stellen, mit den vorhandenen Regeln der Rechtsordnung gelöst werden können bzw. konnten oder ob Anpassungen notwendig sind, um eine mit dem übergeordneten Recht vereinbare Nutzung der bestehenden Technologien garantieren zu können. 94

Gemäss der Verwaltungsrechtslehre stehen den Behörden zur Erfüllung ihrer Aufgaben verschiedene Handlungsformen zur Verfügung.[244] Diese lassen sich etwa dadurch unterscheiden, ob sie auf einen tatsächlichen Erfolg oder auf einen rechtlichen Erfolg ausgerichtet sind. Das rechtliche Verwaltungshandeln ist immer auf die unmittelbare Gestaltung einer Rechtslage und somit auf einen rechtlichen Erfolg ausgerichtet.[245] Als wichtigstes Instrument des rechtlichen Verwaltungshandelns gilt die Verfügung.[246] Jedoch existieren durchaus auch andere denkbare Handlungsformen, etwa Pläne, aber auch privat- und verwaltungsrechtliche Verträge.[247] Aufgrund des Fokus der Arbeit soll vorliegend in erster Linie das Verwaltungsverfahren behandelt werden, welches im Erlass einer Verfügung endet und in den jeweiligen Verwaltungsverfahrensordnungen eingehend geregelt ist. Wie sogleich näher erläutert wird, haben Informations- und Kommunikationstechnologien bereits in verschiedener Form Eingang in diesen Bereich gefunden, sei es, indem es Privaten möglich ist, Verfahren oder Verfahrensschritte online zu erledigen, 95

243 Vgl. etwa JÖRGER, Anwaltsrevue, 2019, S. 481.

244 Vgl. etwa HETTICH, in: Fachhandbuch Verwaltungsrecht N. 20.1 ff.

245 Vgl. zum Ganzen: HETTICH, in: Fachhandbuch Verwaltungsrecht, N. 20.5.

246 MÜLLER, VwVG-Kommentar, Art. 5, N. 1.

247 Vgl. zum Ganzen HETTICH, in: Fachhandbuch Verwaltungsrecht, N. 20.1 ff.

oder indem sich Behörden des Internets oder anderer technologischer Fortschritte bedienen, um etwa einen Sachverhalt besser erfassen zu können.

96 Neben dem rechtlichen Verwaltungshandeln gibt es auch Handlungen der öffentlichen Verwaltung, welche unmittelbar einen Taterfolg herbeiführen und keine unmittelbaren Rechte und Pflichten bei Privaten begründen, etwa Auskünfte oder Empfehlungen der Behörden, aber auch direkte Vollzugshandlungen wie Strassenunterhalt oder Müllabfuhr. Hierbei handelt es sich um das sogenannte tatsächliche Verwaltungshandeln.[248] Es ist indes nicht ausgeschlossen, dass auch tatsächliches Verwaltungshandeln mittelbare Rechtswirkungen nach sich ziehen kann, etwa wenn Private gestützt auf die Auskunft einer Behörde weitere Dispositionen ergreifen.[249] Daher soll auch betrachtet werden, inwiefern das tatsächliche Verwaltungshandeln durch die Digitalisierung verändert wurde und welche rechtlichen Folgen dies für den Bürger hat. Dabei können zwar auch Vollzugshandlungen durch die Digitalisierung durchaus beeinflusst werden, indem etwa die Müllabfuhr im Rahmen des «Smart Government» aufgrund der Auswertung von Massendaten optimiert wird[250], direktere Auswirkungen hat das tatsächliche Verwaltungshandeln für den Bürger jedoch dort, wo die Verwaltung informell (ausserhalb von Verfahren) mit ihm interagiert, indem sie etwa über ihre Website über Sachverhalte informiert. Diese informelle Interaktion zwischen der Verwaltung und dem Bürger lässt sich unterteilen in Information und Kommunikation.[251]

97 Die Untersuchung soll im Folgenden anhand dieser Unterscheidungen durchgeführt werden, wobei einerseits das rechtliche Verwaltungshandeln und anderseits das tatsächliche Verwaltungshandeln betrachtet werden. Dabei werden bei Letzterem die Information und die Kommunikation separat behandelt, da sich unter Umständen unterschiedliche Rechtsfragen stellen.

Vorbemerkung: Outsourcing von Informatikdienstleistungen

98 Wie bereits einleitend erwähnt, werden gerade IT-Dienstleistungen häufig nicht direkt von den jeweiligen Behörden, sondern von externen Anbietern bereitgestellt. Dabei gibt es, wie weiter oben ausgeführt, verschiedene Arten

248 HÄFELIN/MÜLLER/UHLMANN, N. 1408.

249 HÄFELIN/MÜLLER/UHLMANN, N. 1408.

250 Siehe dazu oben Rz. 24.

251 Vgl. BRITZ, in: Grundlagen des Verwaltungsrechts, N. 21–25; als stärkste Form existiert schliesslich noch die Transaktion, wobei es sich hier um rechtsverbindliche Verwaltungshandlungen zwischen Bürger und Verwaltung handelt, welche wohl in der Regel dem rechtlichen Verwaltungshandeln zuzuordnen sind . In der Schweiz hat z.B. GLASER die entsprechende Einteilung teilweise übernommen, vgl. GLASER, ZSR, 2015, S. 299.

dieses «Outsourcing», welche in verschiedensten Anwendungsbereichen und in verschiedenem Umfang Datenbearbeitungen für den jeweiligen Anwender (vorliegend die öffentliche Hand) übernehmen.[252] Auch wenn der Anbieter dabei nur die Infrastruktur bereitstellt, um die Daten zu speichern (IaaS), kann es sich dabei um einen datenschutzrechtlich relevanten Vorgang handeln. Dies ist dann der Fall, wenn Personendaten bearbeitet werden, zumal der datenschutzrechtliche Begriff der Bearbeitung gemäss Art. 3 DSG – wie bereits ausgeführt – weit zu verstehen ist und bereits die Speicherung von Daten umfasst. Nicht relevant ist dabei, ob der Bearbeiter die Daten zur Kenntnis nimmt.[253] Es ist davon auszugehen, dass entsprechende Anwendungen in der Verwaltung inzwischen weit verbreitet sind.[254] Auch einige der Applikationen, die in dieser Arbeit betrachtet werden, erbringt die Verwaltung wohl in guten Teilen mithilfe von Drittanbietern, welche Speicherplatz oder Softwarelösungen zur Verfügung stellen. Daher soll an dieser Stelle das Outsourcing oder Cloud Computing durch die Verwaltung vorab rechtlich betrachtet werden.

Nach dem soeben Ausgeführten ist gut denkbar, dass es im Rahmen des 99
Outsourcings zu einer Bearbeitung von Personendaten kommt und die Datenschutzgesetzgebung somit einschlägig ist. Da die Daten dabei im vorliegenden Zusammenhang oft für die Zwecke der auftraggebenden staatlichen Stelle bearbeitet werden, ist dies regelmässig als Auftragsdatenbearbeitung im Sinne von Art. 10a DSG zu verstehen.[255] Auch bei der Auftragsdatenbearbeitung werden Daten über die Person an einen Dritten (den Auftragsbearbeitenden) bekanntgegeben, so dass die Vorgaben erfüllt sein müssen.[256] Der Auftragsdatenbearbeitende wird durch die Regelung von Art. 10a DSG daher privilegiert behandelt, indem etwa keine gesetzliche Grundlage benötigt wird. Dies insbesondere, weil die Dritten im Sinne von Art. 19 DSG im Gegensatz zu den Auftragsdatenbearbeitenden nach Art. 10a DSG die Daten für ihre eigenen Zwecke bearbeiten dürfen.[257]

Auch Art. 10a DSG macht den Auftraggebern indes einige Vorgaben. So 100
darf die Bearbeitung nur gestützt auf eine Vereinbarung oder ein Gesetz übertragen werden. Für Bundesorgane kann eine Grundlage entsprechend in einem Gesetz geregelt sein, die Übergabe ist aber auch erlaubt, wenn lediglich

252 Vgl. TRÜEB/ZOBL, digma, 2016, S. 102.

253 WIDMER, digma, 2014, S. 118.

254 Vgl. BAERISWYL, digma, 2019, S. 118, TRÜEB/ZOBL, digma, 2016, S. 102 f.

255 WEBER, ZBl, 1999 S. 115.

256 Siehe dazu oben Rz. 77.

257 TRÜEB/ZOBL, digma, 2016, S. 103.

eine Vereinbarung besteht. Eine solche ist grundsätzlich formlos möglich, sollte indes gerade zum Schutz des Auftraggebers schriftlich getroffen werden.[258] Weiter darf gemäss Art. 10a Abs. 1 lit. b DSG keine gesetzliche oder vertragliche Geheimhaltungspflicht eine Übertragung verbieten. In der Praxis ist hier etwa an das Amtsgeheimnis oder andere Spezialgeheimnisse der Verwaltung (wie das Steuergeheimnis) zu denken. Diese stehen indes einer Auslagerung der Datenbearbeitung nicht generell entgegen, die Geheimniswahrung ist aber an die Bearbeitenden zu überbinden.[259] Schliesslich dürfen die Bearbeitenden gemäss Art. 10a Abs. 1 lit. a. DSG die Daten nur so bearbeiten, wie der Auftraggeber dies selbst auch dürfte. Insbesondere dürfen die Daten nicht für eigene Zwecke des Auftragnehmers bearbeitet werden. Zu beachten ist im Weiteren, dass das öffentliche Organ bei der Auslagerung einer Datenbearbeitung für die Einhaltung der Vorschriften der Datenschutzgesetzgebung verantwortlich bleibt.[260] In diesem Sinne sieht Art. 10a Abs. 2 DSG vor, dass der Auftraggebende sich insbesondere zu vergewissern hat, dass der Dritte die Datensicherheit gewährleistet. Damit soll insbesondere sichergestellt werden, dass der Rechtsschutz des Betroffenen unabhängig davon nicht verschlechtert werden soll, ob das öffentliche Organ oder ein Dritter in seinem Auftrag die Daten bearbeitet.[261]

101 Das Outsourcing ist dabei von der Übertragung öffentlich-rechtlicher Aufgaben abzugrenzen, bei welcher die Erfüllung einer gesamten staatlichen Aufgabe durch Private aufgrund Gesetz stattfindet.[262] Beim Outsourcing wird hingegen regelmässig auf eine Dienstleistung zurückgegriffen, um eine staatliche Aufgabe selbst erfüllen zu können. Diese Abgrenzung ist relevant, da bei der Auftragsdatenbearbeitung das öffentliche Organ nach dem oben Geschriebenen für die Datenbearbeitung verantwortlich bleibt, während bei der Aufgabenübertragung der Dritte, welcher die staatliche Aufgabe erfüllen soll, Art. 3 lit. h DSG folgend selbst zum Bundesorgan i.S. des Datenschutzgesetzes wird und somit datenschutzrechtlich wie ein Bundesorgan zu behandeln ist.[263] Die Abgrenzung zwischen Datenbearbeitung im Auftrag und

258 BAERISWYL, SHK-DSG, Art. 10a, N. 19 f.

259 BAERISWYL, SHK-DSG, Art. 10a, N. 33 f. Hinsichtlich des Berufsgeheimnisses (insb. des Anwaltsgeheimnisses) wird in der Lehre kontrovers diskutiert, ob Datenbearbeitende als Hilfspersonen oder als Dritte zu qualifizieren sind, vgl. etwa Urteil des BGer 2C_1083/2017 4. Juni 2019, anstatt vieler MÉTILLE, AJP, 2019, 613 ff.; SCHWARZENEGGER/THOUVENIN/STILLER/GEORGE, Anwaltsrevue, 2019, S. 25.

260 BAERISWYL, SHK-DSG, Art. 10a, N. 2.

261 EPINEY, in: Jahrbuch 2010, Ziff. V.5.

262 Vgl. etwa BAERISWYL, SHK-DSG, Art. 10a, N. 7 ff.

263 RUDIN, SHK-DSG, Art. 3, N. 46.

Aufgabenübertragung kann dabei im Einzelfall durchaus mit Schwierigkeiten verbunden sein.[264]

§ 3 Digitalisierung des tatsächlichen Verwaltungshandelns

I. Behördeninformation

A. Grundlagen der Behördeninformation

Ein nicht unwesentlicher Teil des Verwaltungshandelns, gerade auch im Internet, spielt sich auf einer informellen Ebene ausserhalb von formalisierten Verfahren ab.[265] So verfügen sämtliche Kantone der Schweiz und auch der Bund über Internetauftritte (Websites), auf welchen sie etwa gewisse Informationen verbreiten. Einige Kantone und Gemeinden verfügen auch über Präsenzen in verschiedenen sozialen Medien wie Facebook oder Twitter, auf denen sie mit ihrer Einwohnerschaft in Kontakt treten können. Die rege Informationstätigkeit der Verwaltungsbehörden ist dabei nicht reiner Selbstzweck, sondern verfolgt verschiedene Ziele: Einerseits soll das staatliches Handeln für die Bürgerinnen und Bürger transparent und voraussehbar gemacht und sollen der Bevölkerung Grundlagen für die Meinungsbildung und demokratische Entscheidungsprozesse geliefert werden, anderseits kann die Information auch als politisches Führungsinstrument dienen.[266] Daher ist es wenig verwunderlich, dass die Verfassung bzw. das Gesetz Vorgaben an die Behörden enthalten, der Allgemeinheit gewisse Informationen zugänglich zu machen oder gar von sich aus zu informieren. 102

1. Aktive und passive Informationstätigkeit

Zu unterscheiden ist dabei zwischen der aktiven Informationstätigkeit, welche impliziert, dass die Behörde von sich aus über gewisse Angelegenheiten informieren muss («Bring-Prinzip»), und der passiven Informationstätigkeit, gemäss welcher die Behörde nur auf Anfrage Informationen zugänglich machen muss («Hol-Prinzip»). Diese beiden Informationsarten und ihre verfassungsrechtliche Verankerung sollen im Folgenden kurz präsentiert werden. 103

264 TRÜEB/ZOBL, digma, 2016, S. 103.

265 Vgl. etwa GLASER, ZSR, 2015, S. 297.

266 EHRENZELLER/SAXER/BRUNNER, SG Komm. BV, Art. 180, N. 30 ff.

a) Aktive Informationstätigkeit

104 Aus Art. 180 Abs. 2 BV ergibt sich, dass «der Bundesrat die Öffentlichkeit rechtzeitig und umfassend über seine Tätigkeit [informieren muss], soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen».[267] Gegenstand der Informationstätigkeit sind gemäss dem Wortlaut der Bestimmung alle Tätigkeiten des Bundesrats, unabhängig von Handlungsform und Zweck. Umfasst werden dabei nicht nur Handlungen des Bundesrats, sondern die Informationspflicht muss auch die Bundesverwaltung als Ganzes erfassen, deren Handlungen dem Bundesrat zugerechnet werden.[268] Die Informationspflicht wird durch Art. 10 RVOG konkretisiert. Gemäss dessen Absatz 2 hat der Bundesrat für eine einheitliche, frühzeitige und kontinuierliche Information über seine Lagebeurteilungen, Planungen, Entscheide und Vorkehren zu sorgen. Diese Aufzählung soll indes nur beispielhaft sein und deutlich machen, dass über alles Wichtige eine Information erfolgen muss.[269] Hinsichtlich der Modalitäten wird dem Bundesrat ein weiter Ermessensspielraum belassen.[270] Art. 180 Abs. 2 BV statuiert lediglich, dass diese Informationspflicht rechtzeitig und umfassend wahrgenommen wird. Die Lehre nennt indes weitere Grundsätze, welche sich implizit aus diesen Vorgaben sowie den allgemeingültigen Verfassungsprinzipien wie Treu und Glauben ergeben. So muss die Information etwa sachlich, einheitlich, verständlich, klar und transparent erfolgen.[271] In weiten Teilen ist der Bundesrat hinsichtlich der Ausgestaltung der Information frei, solange die Informationstätigkeit ihren Zweck zu erfüllen vermag.[272] Er kann selber informieren, aber die Informationstätigkeit auch an eine nachgeordnete Amtsstelle oder Behörde delegieren.[273] Die meisten Kantone verpflichten ihre Verwaltung ebenfalls per Verfassung oder Gesetz, die Öffentlichkeit über ihre Tätigkeit zu informieren.[274]

267 MÜLLER, BSK BV, Art. 180, N. 10.

268 BRUNNER/MADER, SHK BGÖ, Einleitung, N. 79, MÜLLER, BSK BV, Art. 180, N. 1.

269 SÄGESSER, SHK RVOG, Art. 10, N. 60; BRUNNER/MADER, SHK BGÖ, Einleitung, N. 81.

270 MÜLLER, BSK BV, Art. 180, N. 14.

271 BRUNNER/MADER, SHK BGÖ, Einleitung, N. 82; MÜLLER, BSK BV, Art. 180, N. 15 ff.

272 Vgl. EHRENZELLER/SAXER/BRUNNER, SG Komm. BV, Art. 180, N. 35.

273 BIAGGINI, OFK BV, Art. 180, N. 10; EHRENZELLER/SAXER/BRUNNER, SG Komm. BV, Art. 180, N. 37.

274 Für eine Übersicht, vgl. IVANOV, LeGes, 2013, S. 109 f.; NUSPLIGER, SHK BGÖ, Das Öffentlichkeitsprinzip in den Kantonen, S. 384.

b) Passive Informationstätigkeit

Während Art. 180 Abs. 2 BV eine objektive Handlungspflicht der Behörden vorsieht, statuiert die Bestimmung kein subjektiv einklagbares Recht auf Information in einer bestimmten Angelegenheit.[275] Im Rahmen der verfassungsrechtlichen und allenfalls spezialgesetzlichen Vorgaben sind die Behörden daher bei der Erfüllung ihrer Informationspflicht frei. Die passive Information wirkt hier gewissermassen komplementär und ergänzt die aktive Informationstätigkeit.[276] 105

Aus der in Art. 16 Abs. 3 BV verankerten Informationsfreiheit erwächst jeder Person das Recht, Informationen frei zu empfangen, aus allgemein zugänglichen Quellen zu beschaffen und zu verbreiten. Ob eine Information allgemein zugänglich ist, entscheidet sich dabei gemäss bundesgerichtlicher Rechtsprechung nach der «Umschreibung und Wertung durch den Verfassungs- und Gesetzgeber».[277] Dies heisst, dass es dem Gesetzgeber überlassen bleibt, eine Abwägung zwischen Einsichts- und Geheimhaltungsinteressen vorzunehmen.[278] Im Laufe der letzten Jahre sind immer mehr Gemeinwesen dazu übergegangen, das Verwaltungshandeln im Rahmen der Etablierung des Öffentlichkeitsprinzips öffentlicher zu machen und nur noch diejenigen Informationen vom Zugang durch die Bevölkerung auszunehmen, für welche dies explizit normiert ist. Das Öffentlichkeitsprinzip ist auf Bundesebene im BGÖ verankert.[279] Gemäss Art. 6 BGÖ hat jede Person auf Gesuch hin das Recht, amtliche Dokumente einzusehen und von den Behörden Auskünfte über deren Inhalt zu erhalten. Dieses Recht kann dabei ohne ein besonderes Interesse geltend gemacht und auch gegen den Willen der Verwaltung gerichtlich durchgesetzt werden.[280] Durch den Wechsel zum Öffentlichkeitsprinzip der Verwaltung und die explizite Regelung in Art. 6 BGÖ sind amtliche Dokumente als «allgemein zugängliche Quelle» im Sinne der Verfassungsbestimmung zu werten.[281] Das Öffentlichkeitsprinzip dient somit unmittelbar der Grundrechtsverwirklichung.[282] Zwar wurde der Schutzbereich der Informationsfreiheit durch das Öffentlichkeitsprinzip erweitert, jedoch können 106

275 Vgl. MÜLLER, BSK BV, Art. 180, N. 8.

276 EHRENZELLER/SAXER/BRUNNER, SG Komm. BV, Art. 180, N. 29.

277 Vgl. BGE 137 I 8, E. 2.3.1; BGE 127 I 145, E. 4c/aa.

278 KLEY/TOPHINKE, SG Komm. BV, Art. 16 N. 36.

279 Siehe zum Ganzen oben Rz. 81.

280 Vgl. BRUNNER/MADER, SHK BGÖ, Einleitung, N. 39 ff.

281 Vgl KLEY/TOPHINKE, SG Komm. BV, Art. 16, N. 36.

282 BRUNNER, FS Schweizer, Öffentlichkeit der Verwaltung und informationelle Selbstbestimmung: Von Kollisionen und Verkehrsregeln, S. 35.

immer noch gewichtige Ausnahmen vorgesehen werden.[283] Es ist daher aktuell von einem «Öffentlichkeitsprinzip mit Geheimhaltungsvorbehalt» auszugehen.[284] Dass auf Bundesebene trotz des Öffentlichkeitsprinzips viele Dokumente vom Schutzbereich der Informationsfreiheit ausgenommen sind, wird in der Lehre zunehmend kritisch gesehen.[285]

2. Allgemeine und spezielle Informationstätigkeit

107 Eine weitere Unterscheidung kann getroffen werden zwischen der allgemeinen und der speziellen Informationstätigkeit. Die allgemeine Informationstätigkeit bezieht sich auf sämtliche Tätigkeitsbereiche der Verwaltung und ergibt sich aus den oben genannten rechtlichen Grundlagen. In gewissen Bereichen sehen die einschlägigen Gesetze spezielle Informationspflichten vor, welche den generellen Regelungen vorgehen. Zu denken ist etwa an Informationspflichten im Umweltbereich, in Bereichen mit staatlicher Aufsicht oder bei öffentlichen Registern.[286] Spezielle Informationspflichten können dabei sowohl Teil der aktiven (etwa bei der Auflage von Plänen oder bei öffentlichen Ausschreibungen) als auch der passiven (z.B. Anspruch auf Auszüge aus dem Handelsregister oder dem Grundbuch) Informationstätigkeit sein.[287]

B. Aktive Informationstätigkeit der Verwaltung und Digitalisierung

108 In der Zeit vor der Verbreitung des Internets wurde der Verfassungsauftrag, die Bevölkerung aktiv zu informieren, in erster Linie über die Medien – anhand von Medienmitteilungen oder Medienkonferenzen – wahrgenommen.[288] Durch das Internet ist es den Behörden möglich geworden, die Bevölkerung ohne Zwischenschaltung eines weiteren Akteurs direkt zu erreichen. Es ist wenig verwunderlich, dass der Bund und die Kantone teils aufwendige und ausführliche Webauftritte gestaltet haben, auf denen sie der Bevölkerung Informationen zur Verfügung stellen.[289] Diese Angebote werden von der Bevölkerung augenscheinlich genutzt. So gaben gemäss der nationalen

283 Vgl. etwa die Ausnahmeregelungen im BGÖ, dass spezialgesetzliche Regelungen den Zugang verweigern können (Art. 4 BGÖ), dass nur fertiggestellte Dokumente als amtliche Dokumente gelten können (Art. 5 BGÖ) oder dass gegenüberstehende Interessen Dritter zu beachten sind (Art. 7 ff. BGÖ).

284 Vgl. etwa MADER, in: Das Öffentlichkeitsgesetz des Bundes, S. 15; BRUNNER, in: Das Öffentlichkeitsgesetz des Bundes, S. 76 f.

285 Vgl. etwa MÜLLER/SCHEFER, S. 523 und 537 f. m.w.H.

286 NUSPLIGER, SHK BGÖ, Das Öffentlichkeitsprinzip in den Kantonen, N. 77.

287 Vgl. zum Ganzen NUSPLIGER, SHK BGÖ, Das Öffentlichkeitsprinzip in den Kantonen, N. 83 und 85.

288 Vgl. EHRENZELLER/SAXER/BRUNNER, SG Komm. BV, Art. 180, N. 10.

289 Vgl. etwa die Webseite des Bundes.

E-Government-Studie 2017 nur 14 % der Befragten an, nie eine Internetseite einer Behörde zur Suche nach Informationen genutzt zu haben.[290] Die Palette an auf den jeweiligen Internetsites verfügbaren Informationen ist dabei sehr breit, schliesslich soll gemäss Art. 180 Abs. 2 BV über alle behördliche Tätigkeit informiert werden.[291]

109 Die zunehmende Verbreitung internetfähiger Mobiltelefone und der Ausbau der Mobilfunkinfrastruktur hatten zur Folge, dass grundsätzlich von jedem beliebigen Ort zu jeder Zeit auf Internetinhalte zugegriffen werden kann. Dies führte mit zu einer Zunahme der Anforderungen an die öffentliche Verwaltung hinsichtlich Erreichbarkeit und Verfügbarkeit.[292] Zudem konnten vermehrt zusätzliche Programme von Drittanbietern auf den Telefonen installiert werden (im Rahmen dieser Arbeit wird der umgangssprachlich gebräuchliche Ausdruck «App» benutzt), welche sich die Vorzüge der Smartphones (z.B. GPS-Lokalisierung, eingebaute Kamera) zu Nutze machen. Telefone, welche diese zusätzlichen Möglichkeiten boten, wurden unter dem Namen «Smartphone» bekannt und verbreiteten sich rasch. Dieser Trend ist an der öffentlichen Verwaltung nicht spurlos vorbeigegangen, so dass durchaus ein strategisches Bestreben besteht, Dienstleistungen mobil anzubieten.[293] Dies führte dazu, dass im Laufe der letzten Jahre zahlreiche «Apps» von Bundesstellen, Kantonen oder kantonalen Dienststellen oder Gemeinden/Städten entstanden.[294]

110 Mit dem Aufkommen des Internets bildete sich unter dem Begriff der «Sozialen Medien» auch eine Vielzahl von Netzwerken heraus, über die Personen miteinander kommunizieren und Inhalte austauschen können. Die entsprechenden Netzwerke werden auch in der Schweiz von einem nicht unwesentlichen Teil der Bevölkerung genutzt und bieten der Bevölkerung neue Interaktionsmöglichkeiten mit der Verwaltung (etwa durch das Teilen oder «Liken» von Beiträgen).[295] Daher ist es nicht erstaunlich, dass immer mehr Kantonsverwaltungen (oder zumindest deren Ämter oder Dienststellen) und Gemeinden neben dem Betrieb einer Websites auch in den sozialen Medien aktiv sind. Auch eine grosse Anzahl an Bundesämtern bedient ein Konto auf mindestens einer entsprechenden Plattform.[296]

290 BUESS/RAMSDEN/BIERI, S. 20.

291 EHRENZELLER/SAXER/BRUNNER, SG Komm. BV, Art. 180, N. 44.

292 DIETRICH/MÜLLER/AKKAYA TÜRKAVCI/KRCMAR/BOBERACH/EXEL, S. 16 und 32.

293 Vgl. E-Government-Strategie Schweiz 2016-2019, S. 2 und 5.

294 Vgl. etwa: SRF, News-Beitrag vom 24.3.2016.

295 Siehe dazu bereits oben Rz. 26 ff.

296 Für eine (indes nicht ganz aktuelle) Übersicht vgl. Soziale Medien, Übersicht Kantone; Soziale Medien, Übersicht Bund.

111 Gemeinwesen sind dazu übergegangen, Daten, welche sie im Rahmen ihrer Aufgaben erheben müssen, in ihrer Rohform als sogenannte Open Government Data (OGD) zu publizieren. Als OGD werden offen zugängliche und frei wiederverwendbare Behördendaten, sofern durch diese nicht Datenschutz-, Urheberrechts- oder Informationsschutzbestimmungen verletzt werden, definiert.[297] Unter diesem Begriff werden auch Daten publiziert, welche neben dem Hauptprodukt der behördlichen Aufgaben anfallen.[298] Dies können etwa begleitende Statistiken oder Daten sein, welche zwar von einer Behörde erhoben, aber nicht komplett ausgewertet werden (etwa Wetterdaten). Die auf diese Weise publizierten Daten stehen explizit einer sekundären Nutzung durch die interessierte Bevölkerung offen, welche etwa durch die Verknüpfung mit anderen Datenbeständen neue Erkenntnisse daraus erzielen kann.[299] Die Schweiz ist in den vergangenen Jahren vermehrt bestrebt, den Zugang zu Behördendaten als «Open Government Data» zu vereinfachen.[300] In diesem Rahmen bietet etwa der Bund seit einigen Jahren ein einheitliches Portal für offene Behördendaten, auf welchem Bund, Kantone und Gemeinden Daten publizieren können.[301]

1. Generelle Zulässigkeit der Behördeninformation mithilfe neuer Technologien

112 Die neuen Technologien bringen – wie soeben beschrieben – dem Staat viele zusätzliche Möglichkeiten, wie er seine Öffentlichkeitsinformation effizienter machen und unter Umständen gewisse Zielgruppen besser erreichen kann. Der Staat ist indes beim Entscheid, ob und wie er diese Technologien nutzen möchte, nicht gänzlich frei. Auch im Rahmen des informellen Handelns ist er an gewisse Grundsätze des rechtsstaatlichen Handelns gebunden, welche in Art. 5 BV statuiert sind.[302] Insbesondere muss die Öffentlichkeitsinformation des Staates auf eine gesetzliche Grundlage gestützt sein, im öffentlichen Interesse liegen und verhältnismässig sein.[303] Ob der Einsatz neuer Technologien mit diesen Grundsätzen vereinbar ist, soll im Folgenden betrachtet werden.

297 Vgl. GOLLIEZ/ASCHWANDEN/BRETSCHER/BERNSTEIN/FARAGO/KRÜGEL/FREI/LAUX/BUCHER/NEURONI/RIEDL, S. 3.

298 Vgl. OGD-Strategie 2019, S. 881; WIEDMER/SEIBERTH, S. 4; WEBER/LAUX/OERTLY, S. 32.

299 Vgl. OGD-Strategie 2019, S. 883.

300 Vgl. etwa die Ziele der OGD-Strategie 2019. S. 884 ff.

301 Vgl. das OGD-Portal des Bundes.

302 Vgl. SAXER, in: St. Galler Tagung zur Öffentlichkeitskommunikation des Staates, S. 22; vgl. auch EPINEY, BSK BV, Art. 5, N. 33.

303 SAXER, in: St. Galler Tagung zur Öffentlichkeitskommunikation des Staates, S. 20.

a) Gesetzliche Grundlage

i) Generelle Ausführungen zur Informationstätigkeit im Internet

Die gesetzlichen Grundlagen der staatlichen Kommunikation müssen die Verwendung neuer Technologien vorsehen oder dürfen diese zumindest nicht verbieten. Wie weiter oben ausgeführt, ist die öffentliche Hand im Bund und vielen Kantonen per Verfassung oder zumindest gesetzlich zur aktiven Information der Bevölkerung verpflichtet. Die entsprechenden Grundlagen sind dabei oft sehr weit gefasst und statuieren etwa, dass «die Behörde die Öffentlichkeit über ihre Tätigkeit informiert».[304] Der jeweilige Informationsauftrag wird in der Regel im Rahmen einer Informationsgesetzgebung und auf Verordnungsstufe konkretisiert. Geregelt werden auf dieser Stufe insbesondere die Zuständigkeiten zur Information, wobei diese in der Regel parallel zur Sachzuständigkeit bestehen.[305] Weiter werden allgemeine Anforderungen an die Behördeninformation definiert, etwa dass diese in zeitlicher Hinsicht «frühzeitig» oder «rasch» erfolgen, im Umfang «umfassend» oder «vollständig» und inhaltlich «sachlich» oder «zutreffend» sein muss.[306] 113

Festzustellen bleibt, dass diese Regelungen oft sehr allgemein formuliert sind. Der Grund hierfür ist, dass die Informationsbedürfnisse in der Regel nicht im Detail vorhersehbar und die möglichen Konstellationen kaum überblickbar sind.[307] Es ergibt sich daraus, dass die Behörden bei der Ausgestaltung ihrer Informationstätigkeit in der Regel ein weites Ermessen geniessen. Gewisse Grenzen gesetzt sind der Informationstätigkeit durch gegenüberstehende private oder öffentliche Interessen, wie bereits der Wortlaut von Art. 180 Abs. 2 BV verdeutlicht. Wo durch die speziellen Gefahren der Veröffentlichung von Informationen über das Internet zusätzliche Risiken entstehen (etwa bei der Bekanntgabe von Personendaten), können allenfalls konkretere gesetzliche Grundlagen notwendig sein.[308] Zudem sind die Informationspflichten in gewissen Regelungsbereichen aufgrund ihrer Komplexität oder Relevanz in Spezialgesetzen geregelt, welche zusätzliche Vorgaben enthalten. 114

304 Die entsprechende Formulierung lässt sich in verschiedenen Verfassungen finden, vgl. UHLMANN, in: St. Galler Tagung zur Öffentlichkeitskommunikation des Staates, S. 58.

305 SAXER, in: St. Galler Tagung zur Öffentlichkeitskommunikation des Staates, S. 22.

306 Für eine Auflistung der jeweiligen Rechtsgrundlagen, vgl. BRUNNER, ZBl, 2010, S. 603 ff.

307 BRUNNER, ZBl, 2010, S. 609, m.w.H. Oft ist auch fraglich, ob sich diese überhaupt sinnvoll regeln lassen bzw. ob sich gute Kommunikation erzwingen lässt; vgl. auch UHLMANN, in: St. Galler Tagung zur Öffentlichkeitskommunikation des Staates, S. 47 ff. Es wurde etwa im Bundesgesetz für politische Rechte darauf verzichtet, eine Liste mit Informationsinstrumenten aufzunehmen, da diese kaum je vollständig geführt werden könnte, vgl. TÖNDURY, ZBl, 2011, S. 371 (kritisch).

308 Darauf soll weiter unten vertieft eingegangen werden, siehe Rz. 249 ff.

115 Die allgemeinen Regelungen zur Informationstätigkeit sehen in ihrer soeben beschriebenen Offenheit nicht vor, dass ein bestimmtes Medium benutzt werden muss.[309] Nur selten sind Regeln zu finden, die etwa von der kantonalen Verwaltung die Führung eines Internetauftritts verlangen und diesen umfassend regeln.[310] Wo nichts anderes geregelt ist, kann davon ausgegangen werden, dass die Verwaltung frei darüber bestimmen kann, über welche Kanäle sie die Öffentlichkeit informieren möchte. Der allgemeine Informations- und Kommunikationsauftrag wird als genügende gesetzliche Grundlage für die Information über alle denkbaren Kanäle erachtet.[311] Die Bedingung ist lediglich, dass die entsprechende Form auch geeignet ist, die Öffentlichkeit zu erreichen. Dies wäre wohl nicht gegeben, wenn der Staat über eine Social-Media-Plattform informieren würde, welche kaum aktive Benutzer hat. Unter Umständen kann es gar geboten sein, dass der Staat sich neuer Medien oder Mittel bedient, um adressatengerechte Kommunikation zu ermöglichen.[312] Nach dem soeben Geschriebenen kann die Informationstätigkeit des Staates gestützt auf die allgemeinen gesetzlichen Grundlagen der Behördeninformation grundsätzlich ohne Weiteres über das Internet oder «Apps» geführt werden.

ii) Social Media

116 Bedient sich der Staat im Rahmen seiner Informationstätigkeit einer Social-Media-Plattform, so ergeben sich daraus einige zusätzliche Fragestellungen. Problematisch ist dabei, dass die Benutzer von sozialen Netzwerken sich bei diesen in der Regel registrieren und dazu den Nutzungsbedingungen dieser Netzwerke zustimmen müssen. Dies gilt sowohl für den Staat als auch für den Privaten, welcher mit dem Staat über diese Plattformen interagieren möchte. Die derzeit wichtigsten Social-Media-Plattformen werden dabei von internationalen Anbietern betrieben und haben ihren Hauptsitz ausserhalb der Schweiz. Es ist daher die Frage zu stellen, inwiefern diese das Schweizer Recht überhaupt beachten müssen. Ein zweiter, vorab zu beleuchtender Punkt ist die Stellung des Staates, welcher einerseits als Nutzer des Netzwerkes auftritt, anderseits aber gegenüber seinen Einwohnern über diese Netzwerke eine öffentliche Aufgabe erfüllt. Es ist die Frage zu beantworten, welche Konsequenzen

309 Vgl. LANGER, AJP, 2014, S. 951.

310 Vgl. aber z.B. die Verordnung über die Information über die Tätigkeit des Staatsrats und der Kantonsverwaltung des Kantons Freiburg vom 14. Dezember 2010 (InfoV FR, SGF 122.0.51), welche mehrere Artikel zum Internet-Auftritt des Kantons enthält, oder Art. 15bis Informations- und Datenschutzverordnung vom 10. Dezember 2001 des Kantons Solothurn (InfoDV SO, BGS 114.2).

311 Vgl. LANGER, AJP, 2014, S. 951.

312 Vgl. MADER, in: St. Galler Tagung zur Öffentlichkeitskommunikation des Staates, S. 42 f.

sich aus dieser Doppelrolle ergeben und ob dies einen Einfluss darauf hat, dass bzw. wie der Staat soziale Medien zu seiner Informationstätigkeit nutzen darf.

aa) Vorfrage: Anwendbarkeit von Schweizer Recht

Die wichtigsten Social-Media-Plattformen werden in der Regel von grossen internationalen Unternehmen geführt, welche wiederum über Niederlassungen oder Tochtergesellschaften (etwa für einen gewissen geografischen Raum) verfügen.[313] Aus diesem Grund haben die Betreiber oftmals kein Interesse daran, in jedem Land dem dortigen Recht unterstellt zu sein und ihre Nutzungsbedingungen an die jeweilige Rechtsordnung anpassen zu müssen. Es erstaunt daher nicht weiter, dass die wichtigsten Anbieter in ihren Nutzungsbedingungen, welche vor der Registrierung von jedem Benutzer akzeptiert werden müssen, regelmässig auf das nationale bzw. lokale Recht am Sitz der Gesellschaft (oder einer Tochtergesellschaft) verweisen und die Zuständigkeit der staatlichen Gerichte an diesem Ort vorsehen.[314] Derartige Rechtswahlklauseln können unter Umständen den Regeln des internationalen Privatrechts widersprechen. Sowohl das IPRG als auch das Lugano-Übereinkommen sehen zum Schutz von Konsumenten vor, dass in Verbrauchersachen von der Zuständigkeit der Gerichte am Wohnsitz und der Anwendbarkeit von dessen Recht nicht im Vorneherein – etwa durch Allgemeine Geschäftsbedingungen – abgewichen werden kann (vgl. Art. 15 ff. LugÜ sowie Art. 114 und 120 IPRG).[315] 117

Das Unternehmen «Facebook» sah in seinen Nutzungsbedingungen lange Zeit einen Gerichtsstand in Kalifornien vor.[316] Nach dem soeben Geschriebenen muss der betroffenen Person aber ein Gerichtsstand im Heimatland zustehen, sofern sie die Verbrauchereigenschaft im Sinne des IPRG oder des LugÜ erfüllt. Dies ist nach Art. 15 Abs. 1 LugÜ etwa der Fall, wenn der Vertrag nicht zu einem gewerblichen oder beruflichen Zweck geschlossen wurde, wobei die Unentgeltlichkeit der Dienstleistung keine Rolle spielt. Gestützt auf diese Kollisionsnorm muss es privaten Nutzern der Plattform aus der Schweiz möglich sein, an Schweizer Gerichte zu gelangen und die Streitsache nach schweizerischem Recht beurteilen zu lassen.[317] 118

313 So hat Facebook etwa 71 Niederlassungen weltweit, vgl. die Company-Info Website von Facebook. Für europäische Kunden wird die Plattform durch die Facebook Ireland Limited mit Sitz in Irland bereitgestellt; vgl. die aktuellen Nutzungsbedingungen von Facebook.

314 Vgl. BAKOM Social Media, S. 1.

315 Vgl. Bericht Social Media 2017, S. 67 f.

316 ARNOLD, SZIER, 2012, S. 615; BAKOM Social Media, S. 1.

317 ARNOLD, SZIER, 2012, S. 618 f. Ähnliches hat auch für die EU zu gelten; vgl. explizit das Urteil des EUGH C-498/16 vom 25. Januar 2018.

119 Inzwischen sehen die AGB von Facebook vor, dass für Verbraucher mit ständigem Wohnsitz in einem EU-Land eine Klage am Gerichtsstand des Wohnsitzes möglich ist. Für alle anderen Ansprüche sehen die Nutzungsbedingungen weiterhin die Zuständigkeit irischer Gerichte und die Anwendbarkeit irischen Rechts vor.[318] Schweizer Benutzer erhalten ebenfalls diese Version der Nutzungsbedingungen angezeigt. Falls man nun strikt nach dem Wortlaut geht, müssten also – da die Schweiz kein EU-Mitglied ist – Klagen gegen Facebook durch Betroffene aus der Schweiz in Irland eingereicht werden, was nach dem Geschriebenen als nicht zulässig erachtet werden kann. Es muss zumindest in Verbrauchersachen eine Anrufung von Schweizer Gerichten möglich bleiben. Indes bleibt festzustellen, dass für die Schweiz wohl oftmals keine eigene Regelung getroffen wird, da diese zumindest von aussen als Teil der EU oder als zu kleiner Markt erachtet wird, als dass man seine Nutzungsbedingungen komplett auch darauf ausrichten könnte.[319]

120 Auch wenn die Plattformen nach diesen Ausführungen im Rahmen ihrer Nutzungsbedingungen das Recht des jeweiligen Staats beachten müssen, so geschieht dies in der Praxis oft nur dann, wenn dies nicht anders möglich ist (z.B. aufgrund eines Gerichtsurteils).[320] Auch ein allfälliges Gerichtsurteil, welches in Anwendung von Schweizer Recht und mit der Zuständigkeit eines Schweizer Gerichts ergangen ist, garantiert noch nicht die Vollstreckbarkeit der Ansprüche im Ausland. Oft bieten die im internationalen Privatrecht vorgesehenen Verfahren zur Anerkennung von Entscheiden dem Anbieter die Möglichkeit, sich erneut gegen die Zuständigkeit des Schweizer Gerichts zu wehren, was zu weiteren Verzögerungen und Kostenfolgen für den Kläger führt. Entsprechende Ansprüche sind daher oftmals nur erschwert durchsetzbar und betroffene Private bis zu einem gewissen Grad auf den guten Willen der Plattformanbieter angewiesen.[321]

121 Fraglich ist indes, ob auch die Nutzung von sozialen Medien durch den Staat unter den Anwendungsbereich von Art. 15 LugÜ und Art. 114 und 120 IPRG fällt. Im Gegensatz zu privaten Benutzern nutzen juristische Personen Facebook oftmals auch für gewerbliche oder berufliche Tätigkeiten, etwa um neue Kunden zu gewinnen.[322] Facebook sieht für Personen des öffentlichen Lebens und privatrechtliche oder öffentlich-rechtliche juristische Personen

318 Vgl. die aktuellen Nutzungsbedingungen von Facebook. Dies erscheint zulässig, sofern damit keine anderen zwingenden Gerichtsstände verletzt werden.

319 a.M. indes BAKOM Social Media, S. 6.

320 Vgl. BAKOM Social Media, S. 6.

321 Vgl. Bericht Social Media 2017, S. 68.

322 Vgl. ARNOLD, SZIER, 2012, S. 618.

die Einrichtung sogenannter Fanseiten vor, welche sich von den Profilseiten normaler Nutzer unter anderem dadurch unterscheiden, dass eine Begrenzung der Freundesanzahl wegfällt.[323] Zudem werden den Betreibern gewisse statistische Informationen zu den Besuchern der jeweiligen Seite zur Verfügung gestellt und wird ihnen dadurch ermöglicht, das Nutzerverhalten zu analysieren.[324] Staatliche Stellen werden wohl oft entsprechende Fanseiten erstellen. Damit muss davon ausgegangen werden, dass sie nicht als Verbraucher im Sinne des IPRG und des LugÜ betrachtet werden können, weshalb zumindest ihnen gegenüber eine entsprechende Gerichtsstandsvereinbarung gültig sein könnte.

bb) Vorfrage: Doppelrolle des Staates als Nutzender und Anbieter

Die Behörden verfügen im vorliegend diskutierten Zusammenhang oft über eine Doppelrolle. Als Betreiber eines Profils müssen sie den Nutzungsbedingungen der jeweiligen Plattform ebenfalls zustimmen, welche ihnen dieselben Rechte und Pflichten einräumen wie einer Privatperson. Indes stehen Behörden, wie soeben ausgeführt, im Rahmen ihrer «Fanseiten» einige Zusatzfunktionen zur Verfügung. Wie ebenfalls bereits beschrieben, müssen die Behörden bei all ihrer Informationstätigkeit unabhängig vom Informationsmedium das übergeordnete Recht und insbesondere die Grundrechte beachten. Dies gilt selbstverständlich auch für behördliche Handlungen auf Social-Media-Plattformen. Die Behörden sind daher in ihrer Nutzung dieser Plattformen grundsätzlich eingeschränkter als Private.[325] 122

Nach dem soeben Geschriebenen könnten sich somit die Social-Media-Plattformen zumindest gegenüber dem Staat als Nutzendem auf entsprechende Gerichtsstandvereinbarungen berufen. Indes kann sich aus anderen Rechtsquellen dennoch eine Anwendbarkeit des jeweiligen Rechts auch dem Staat gegenüber ergeben.[326] Die Diskrepanz zwischen privaten Nutzenden und dem Staat als Nutzendem entsprechender Plattformen spielt somit für den vorliegenden Kontext keine wichtige Rolle. Der Aspekt soll im Rahmen der vorliegenden Arbeit nicht weiter vertieft werden, da diese in erster Linie die rechtlich relevanten Auswirkungen der staatlichen Social-Media-Nutzung auf die Privaten als Grundrechtsträger untersuchen soll. 123

323 LANGER, AJP, 2014, S. 956.

324 HOFFMANN/SCHULZ/BRACKMANN, ZD, 2013, S. 123.

325 LANGER, AJP, 2014, S. 950.

326 Vgl. etwa die Ausführungen zur internationalen Amtshilfe, siehe dazu unten Rz. 412 ff.

cc) Auswirkungen auf die Zulässigkeit

124 Hinsichtlich der Frage, ob unter diesen Umständen eine Nutzung von sozialen Medien durch den Staat zulässig ist, ist in erster Linie zu beachten, dass die öffentliche Verwaltung durch die Benutzung von Social-Media-Plattformen zur Erfüllung ihrer verfassungsrechtlichen Informationsaufgabe eine private Dienstleistung benutzt. Da die öffentliche Hand an verschiedenen Orten auf private Anbieter zurückgreifen muss, um ihre Aufgaben zu erfüllen (z.B. im Strassenbau), ist dies nicht grundsätzlich verboten. Dennoch bestehen im Rahmen des Beschaffungswesens umfassende Regelungen, welche dafür sorgen sollen, dass die entsprechenden Verfahren transparent ablaufen und keine Ungleichbehandlungen stattfinden.[327] Unter anderem werden gewisse Schwellenwerte festgelegt, oberhalb deren ein formales Verfahren durchlaufen werden muss, wenn der Staat eine Dienstleistung durch Private erledigen lässt.[328] Hierbei ist zu beachten, dass die Dienstleistungen der Plattformbetreiber von allen Benutzern (und somit auch von staatlichen Stellen) im vorliegenden Kontext unentgeltlich genutzt werden können. Die Betreiber lassen sich jedoch im Rahmen der Nutzungsbedingungen weitgehende Rechte an der Datennutzung zusichern und generieren Einnahmen mittels Werbung und der Daten der Benutzer, welche verarbeitet werden.[329] Der Wert der erbrachten Dienstleistung ist damit vorliegend nur schwer berechenbar, es ist jedoch davon auszugehen, dass er unter den vergaberechtlichen Vorgaben bleibt. Das Zutreffen dieser Prämisse vorausgesetzt, sind in dieser Hinsicht entsprechend keine weiteren Voraussetzungen (etwa in der Form eines formelle Vergabeverfahrens) zu erfüllen.[330]

125 Es stellt sich zudem die Frage, ob die öffentliche Verwaltung, wenn sie auf einer Plattform präsent ist, diese nicht gegenüber anderen bevorteilt.[331] Aus der in Art. 27 BV geregelten Wirtschaftsfreiheit ergibt sich, dass der Staat Konkurrenten grundsätzlich gleich behandeln muss.[332] Daraus kann jedoch nicht geschlossen werden, dass mit allen Konkurrenten ein Vertragsverhältnis eingegangen werden muss. Sachliche Gründe können es rechtfertigen, dass der Staat unterschiedliche Anbieter ungleich behandelt. Als sachlicher

327 Vgl. etwa SCHNEIDER HEUSI, S. 2.

328 Vgl. dazu die Bundes- und kantonalen Gesetze über das Beschaffungswesen und das Übereinkommen über das öffentliche Beschaffungswesen (GATT/WTO-Abkommen, SR 0.632.231.422).

329 WEWER, ZRP, 2016, S. 25; LANGER, AJP, 2014, S. 956.

330 LANGER, AJP, 2014, S. 956.

331 LANGER, AJP, 2014, S. 956.

332 Vgl. UHLMANN, BSK BV, Art. 27 N. 62 f.

Grund kann etwa die wesentlich grössere Verbreitung einer Plattform gelten.[333] Wer mit dem Staat auf einer dieser Plattformen interagieren will, benötigt wie bereits ausgeführt ebenfalls ein entsprechendes Konto. Die Social-Media-Angebote der Kantone (z.B. Facebook- oder Twitter-Konto) sind oft prominent auf der jeweiligen Website verknüpft, um auf sie aufmerksam zu machen. Die öffentliche Verwaltung macht somit, wenn auch allenfalls unbewusst, Werbung für die jeweilige Plattform.[334] Dies kann insofern problematisch sein, als durch die staatliche Nutzung der Plattformen suggeriert wird, dass Private diese unbedenklich nutzen können, zumal dem Staat eine gewisse Vorbilds- oder Vertrauensfunktion zuerkannt wird.[335] Zu beachten ist hierzu indes, dass viele Benutzende wahrscheinlich unabhängig von der Präsenz des Staates ein entsprechendes Konto besitzen und Letztere wohl selten das entscheidende Kriterium für eine Registrierung auf einer Plattform darstellt.

Trotz all dieser Einschränkungen und Vorbehalte stehen die verfassungs- 126
und gesetzesrechtlichen Anforderungen an die staatliche Informationstätigkeit einer Benutzung von Social Media im vorliegenden Kontext grundsätzlich nicht entgegen und der allgemeine Informationsauftrag kann dazu auch als genügende gesetzliche Grundlage betrachtet werden.[336]

iii) Spezielle Informationstätigkeit

Für gewisse Regelungsbereiche ist die Informationstätigkeit aufgrund der 127
Komplexität der Daten (z.B. bezüglich Vermessungsdaten)[337] oder ihrer besonderen Relevanz in einem Spezialgesetz geregelt. In diesen Bereichen können die jeweiligen spezialgesetzlichen Regelungen auch vorsehen, über welche Kanäle die Informationstätigkeit zulässig ist. Beispielhaft sei hier die Lebensmittelgesetzgebung des Bundes genannt. So sieht Art. 24 LMG vor, dass die zuständigen Behörden die Bevölkerung über ihre Tätigkeit und deren Wirksamkeit sowie über Lebensmittel und Gebrauchsgegenstände, bei denen ein hinreichender Verdacht besteht, dass sie ein Risiko für die Gesundheit mit sich bringen können, informieren. Letztere Pflicht wird in Art. 54 LMG konkretisiert. Während das Gesetz für die allgemeine Information über die Tätigkeit die Form von Jahresberichten oder eine andere geeignete Weise

333 Vgl. zum Ganzen: LANGER, AJP, 2014, S. 957.

334 WEWER, ZRP, 2016, S. 23.

335 So wird vom Staat etwa erwartet, dass er bei der Gleichstellung von Mann und Frau oder in der Umweltpolitik eine gewisse Vorreiterrolle einnimmt; vgl. etwa WEWER, ZRP, 2016, S. 23.

336 LANGER, AJP, 2014, S. 951.

337 Vgl. dazu KETTIGER, in: Jahrbuch 2016/2017, S. 104 ff.

genügen lässt[338], werden für den Fall der öffentlichen Warnungen in Art. 54 LMG konkrete Vorgaben gemacht, indem bei schwerwiegenden Gefährdungen davon auszugehen ist, dass die Öffentlichkeit breit (mithilfe der Medien) informiert werden muss, während bei geringeren Fällen allenfalls auch eine Information über die Website der Behörde ausreicht.[339]

128 Fehlt die Bezeichnung eines Mediums, so steht es der Behörde aufgrund des bisher Ausgeführten in der Regel frei, über welchen Kanal sie die Informationspflicht erfüllt. Wichtig bleibt immer, dass über das entsprechende Medium der Informationszweck erreicht werden kann.[340] Im Folgenden soll auf ausgewählte Bereiche der speziellen Informationstätigkeit und darauf, über welche Kanäle diese zulässig ist, vertieft eingegangen werden.

aa) Amtliche Publikationen

129 Gewisse Informationen der Behörden müssen aufgrund ihrer Funktion oder Wichtigkeit in einer bestimmten Weise publiziert werden. Zu gelten hat dies in erster Linie für die Publikation rechtsetzender Erlasse wie Gesetze und Verordnungen. Da diese Privaten Rechte und Pflichten auferlegen können, muss der Private in der Lage sein, diese Rechte und Pflichten auch zu kennen, um sich danach ausrichten zu können. Daher zählt die Publikation von Erlassen zu einer unabdingbaren Voraussetzung für deren Anwendbarkeit und Verbindlichkeit.[341] Auch individuell-konkrete Rechtsakte (wie Verfügungen) sind darauf ausgerichtet, beim Betroffenen Rechte oder Pflichten zu begründen. Diese werden in der Regel dem Adressaten persönlich eröffnet, jedoch kann es unter Umständen nicht effizient oder nicht realisierbar sein, die betroffenen Personen einzeln zu benachrichtigen, etwa aufgrund unbekannten Aufenthalts oder weil eine Vielzahl von Parteien involviert ist. Praktikabilitäts- und Effizienzüberlegungen legen es nahe, dass in derartigen Fällen eine alternative Möglichkeit gegeben sein muss, diese Personen zu erreichen.[342] Die sich aus dem Rechtsakt ergebenden Rechtswirkungen verlangen, dass auch in diesen Fällen den potenziell Betroffenen zumindest die Möglichkeit gegeben wird, die entsprechenden Informationen zur Kenntnis nehmen zu können.[343]

338 Botschaft LMG, S. 5613.

339 Botschaft LMG, S. 5633.

340 Siehe dazu bereits oben Rz. 115.

341 Vgl. etwa BGE 120 Ia 1, E. 4.a) m.w.H.

342 KNEUBÜHLER/PEDRETTI, VwVG-Kommentar, Art. 36, N. 1.

343 WEBER/LAUX/OERTLY, S. 32.

• *Vorgaben an die Publikation*

Während die Bundesverfassung und auch die kantonalen Verfassungen meist keine ausdrückliche Pflicht zur Veröffentlichung von Erlassen kennen, ergibt sich diese aus dem Legalitätsprinzip (Art. 5 Abs. 1 BV), dem Gebot der Rechtsgleichheit (Art. 8 BV) und dem Willkürverbot bzw. dem Grundsatz von Treu und Glauben (Art. 9 BV).[344] Art. 141 BV sieht immerhin implizit vor, dass es eine amtliche Veröffentlichung geben muss, indem das fakultative Referendum daran gebunden ist, dass 50'000 Stimmberechtigte oder acht Kantone innert 100 Tagen seit der Veröffentlichung des Erlasses dies verlangen.[345] Aufgrund dieser Vorgaben haben Rechtsprechung und Lehre gewisse verfassungsrechtliche Mindestanforderungen an die Publikation von Erlassen entwickelt. So muss diese schriftlich, in einem formellen Verfahren und einem offiziellen Publikationsorgan, innert angemessener Frist und einfach zugänglich erfolgen.[346] 130

Die rechtsgültige Publikation erfüllt dabei zwei verschiedene Funktionen. Einerseits muss sie das geltende Recht in seiner Gesamtheit abbilden, anderseits müssen aktuelle und bevorstehende Rechtsänderungen abgebildet werden können.[347] Ein einziges Publikationsorgan kann diese beiden Teilgehalte nicht gleichzeitig im selben Umfang erfüllen, daher kennen der Bund und fast alle Kantone mindestens zwei Arten von Publikationsorganen.[348] Die chronologische Publikation umfasst neue Rechtsvorschriften sowie Änderungen und Aufhebungen von Vorschriften in ihrer zeitlichen Reihenfolge.[349] Wird ein Gesetz abgeändert, umfasst die chronologische Publikation nur diejenigen Regelungen bzw. Artikel, welche geändert wurden. Dadurch bildet sie immer nur einen Teil des relevanten Rechts direkt ab, nämlich denjenigen, der sich verändert.[350] Daher besteht zudem eine konsolidierte Publikation, welche das gesamte geltende Recht zu einem bestimmten Zeitpunkt abbildet. Auf der Ebene des Bundes sind die chronologischen Erlasse in der «Amtlichen Sammlung» zu finden, während die konsolidierte Fassung in der «Systematischen Rechtssammlung» ersichtlich ist. 131

344 WALDMANN / SCHNYDER VON WARTENSEE, LeGes, 2013, S. 12.

345 SCHEFFLER / VAN SPYK, in: Recht im digitalen Zeitalter, S. 590.

346 SCHEFFLER / VAN SPYK, in: Recht im digitalen Zeitalter, S. 591 f. m.W.h.; WALDMANN, Komm. PublG, Die Publikation kantonalen Rechts, S. 98.

347 WALDMANN / SCHNYDER VON WARTENSEE, LeGes, 2013, S. 14.

348 WALDMANN / SCHNYDER VON WARTENSEE, LeGes, 2013, S. 16-18.

349 SCHEFFLER / VAN SPYK, in: Recht im digitalen Zeitalter, S. 587.

350 SCHEFFLER / VAN SPYK, in: Recht im digitalen Zeitalter, S. 594.

Viele Kantone kennen ein ähnliches System.[351] Aufgrund ihrer grösseren Übersichtlichkeit bedient sich die Bevölkerung in erster Linie der konsolidierten Sammlung.[352]

132 Für die Publikation von Verfügungen sieht Art. 36 VwVG auf Bundesebene vor, dass diese in einem «amtlichen Blatt» eröffnet werden müssen, wenn eine Partei unbekannten Aufenthalts oder im Ausland wohnhaft ist. Ebenfalls ist die amtliche Publikation möglich, wenn eine Vielzahl von Parteien in einem Verfahren involviert ist oder die Verfahrensparteien nur mit unverhältnismässigem Aufwand erreicht werden können. Diese Publikation zieht die unwiderlegbare Vermutung nach sich, dass die Verfügung den betroffenen Adressaten eröffnet wurde, und bewirkt die damit verbundenen Rechtsfolgen (etwa den Beginn eines Fristenlaufs).[353] Aufgrund der damit verbundenen Rechtswirkungen kann die Publikation nur in einem amtlichen Publikationsmittel rechtsgültig vorgenommen werden. Zu diesem Zweck müssen der Bund und die Kantone ein solches Publikationsorgan betreiben, welches in den Kantonen etwa «Amtsblatt» oder «Kantonsblatt» und beim Bund «Bundesblatt» genannt wird.[354]

• *Zulässigkeit elektronischer Publikation*

133 Im Rahmen der skizzierten Vorgaben haben der Bund und die Kantone ihre amtlichen Veröffentlichungen zu regeln. Für den Bund ist hierzu etwa das Bundesgesetz über die Sammlungen des Bundesrechts und das Bundesblatt vom 18. Juni 2004 (PublG, SR 170.512) einschlägig. Dieses umfasst gemäss Artikel 1 PublG die Sammlungen des Bundesrechts, also die Amtliche (chronologische) und die Systematische (konsolidierte) Sammlung sowie das Bundesblatt. Geregelt wird in den entsprechenden Erlassen etwa der Inhalt der jeweiligen Publikationen, aber auch die Form der Veröffentlichung.

134 Die Publikationsorgane wurden während langer Zeit im Wochenrhythmus den jeweiligen Abonnenten in gedruckter Form zugestellt und sind bzw. waren in Verwaltungsgebäuden (etwa Gemeindeverwaltungen) und zum Teil sogar Gastronomiebetrieben aufzulegen.[355] Insbesondere durch das

351 Für eine Übersicht vgl. WALDMANN / SCHNYDER VON WARTENSEE, LeGes, 2013, Anhang.

352 Vgl. WALDMANN / SCHNYDER VON WARTENSEE, LeGes, 2013, S. 29.

353 Vgl. UHLMANN/SCHILLING-SCHWANK, PK VwVG, Art. 36, N. 5.

354 Vgl. etwa das Bundesblatt. Nebenbei existieren etwa auch das Schweizerische Handelsamtsblatt oder das Publikationsorgan des IGE, vgl. KNEUBÜHLER/PEDRETTI, VwVG-Kommentar, Art. 36, Art. 36, N. 4.

355 Vgl. etwa Botschaft Rev. PublG, S. 7064. Für die Auflagepflicht von Gastronomiebetrieben im Kanton Zürich vgl. den inzwischen nicht mehr geltenden § 20 des Gastgewerbegesetzes vom 1. Dezember 1996 (GGG ZH, LS 935.11); vgl. HÖSLI, LeGes, 2013, S. 158.

Aufkommen des Internets ergaben sich neue Publikationswege, welche diese Publikationsweise in ihrer Übersichtlichkeit, Zugänglichkeit und hinsichtlich des möglichen Publikationsrhythmus übertreffen. Schon alleine aus Effizienzüberlegungen kamen daher Bund und Kantone fast nicht umhin, ihre Amtsblätter und Gesetzessammlungen auch online zu veröffentlichen.[356] Im Bereich der Erlasspublikation brachte dies weitere Vorteile mit sich, indem etwa Inhalte oder Erlasse miteinander verlinkt, nach bestimmten Worten durchsucht oder Erlasstexte direkt weiterverarbeitet werden können.[357] Aufgrund der erwähnten Vorteile liefen die Online-Versionen den gedruckten Ausgaben verständlicherweise schnell den Rang ab.[358]

Die obengenannten verfassungsrechtlichen Minimalvorgaben stehen einer Internetpublikation nicht entgegen, da auch auf diese Weise grundsätzlich eine allgemein zugängliche Information in angemessener Frist erfolgen kann. Dies bedingt indes, dass die jeweilige Publikationsplattform entsprechend ausgestaltet ist und reibungslos funktioniert sowie Vorkehrungen getroffen werden für den Fall, dass sie dies eben nicht tut.[359] Festzustellen ist, dass durch die Internetpublikation die Verfügbarkeit amtlicher Publikationen generell eher erhöht wird.[360] Spezifische Probleme im Gegensatz zur gedruckten Version können sich für die Online-Version allenfalls in erster Linie hinsichtlich ihrer Verlässlichkeit ergeben. So müssen auch bei einer Online-Publikation jederzeit die Authentizität und die Integrität gewahrt sein, indem Manipulationen durch Dritte, aber auch durch den Staat selbst nachhaltig ausgeschlossen werden.[361] 135

Für den Bund sieht Art. 1a PublG, welcher per 1. Januar 2016 in Kraft getreten ist, als gesetzliche Grundlage vor, dass die Veröffentlichungen der Bundeskanzlei (also das Bundesblatt sowie die Amtliche und die Systematische Sammlung) zentral über eine öffentlich zugängliche Plattform erfolgen sollen. Viele Kantone haben inzwischen die Online-Veröffentlichung von Gesetzen und Verordnungen oder des Amtsblatts ebenfalls in den Gesetzen oder Verordnungen explizit geregelt.[362] 136

356 WALDMANN / SCHNYDER VON WARTENSEE, LeGes, 2013, S. 15.

357 Vgl. etwa SCHEFFLER / VAN SPYK, in: Recht im digitalen Zeitalter, 599, ROTH, LeGes, 2013, S. 46.

358 Vgl. Botschaft Rev. PublG, S. 7061: 2'000 gedruckten Versionen des Bundesblatts stehen 1 Mio. Online-Zugriffe alleine auf das Bundesblatt gegenüber (20 Mio. Online-Zugriffe für AS, SR und BBl).

359 Botschaft Rev. PublG, S. 7088 f.

360 SCHEFFLER / VAN SPYK, in: Recht im digitalen Zeitalter, S. 597 f.

361 Vgl. ROTH, LeGes, 2013, S. 70.

362 Für eine Übersicht, s. WALDMANN / SCHNYDER VON WARTENSEE, LeGes, 2013, Anhang.

137 Besteht keine spezifische Regelung über die Publikationsform des Amtsblatts, so müsste nach den oben genannten Grundsätzen davon ausgegangen werden, dass zumindest eine zusätzliche Publikation über das Internet zulässig sein kann, wenn der Kanton einen generellen Informationsauftrag hat und der Online-Version keine Rechtskraft zukommt (siehe dazu sogleich im nächsten Absatz).[363] In der Lehre wird indes teilweise auch vertreten, dass aufgrund der mit dem Paradigmenwechsel von gedruckter zur elektronischer Version verbundenen technischen und organisatorischen Herausforderungen eine gesetzliche Grundlage im formellen Sinn zumindest in den Grundzügen notwendig wird.[364] Aus Gründen der Rechtssicherheit höchst fraglich ist in jedem Fall eine Lösung wie diejenige des Kantons Waadt, welcher ohne gesetzliche Regelung die Ablösung der Papierform durch die alleinige Publikation im Internet vornahm.[365] Ebenfalls nicht zulässig wäre eine Online-Publikation, wenn die gesetzliche Regelung explizit eine ausschliessliche Publikation in gedruckter Form vorsieht, was allerdings soweit ersichtlich in keinem Kanton der Fall ist.

- *Massgeblichkeit der Version*

138 Wie soeben ausgeführt bestehen oftmals Online- und Papierversion von amtlichen Publikationen nebeneinander. Bei der Erlasspublikation existieren zudem jeweils eine chronologische und eine konsolidierte Fassung. Bei einer derartigen Vielfalt muss – schon aus Gründen der Rechtssicherheit – festgelegt werden, dass die eine Version der anderen vorgeht, auch wenn es in der Praxis kaum je zu Divergenzen kommt.[366] Relevant ist eine entsprechende Prioritätenregelung etwa betreffend den massgeblichen Veröffentlichungszeitpunkt und somit die Auslösung eines Fristenlaufs, wenn die Veröffentlichung im Internet nicht zeitgleich mit der Papierfassung erfolgte (da z.B. das gedruckte Amtsblatt nur wöchentlich erscheint, das Internet-Amtsblatt aber täglich aktualisiert werden kann).[367] Da das Verfassungsrecht, wie weiter vorne angedeutet, kaum Vorgaben über die Ausgestaltung der Publikation macht, haben sich in der Schweiz verschiedene Modelle entwickelt, deren ausführliche Vorstellung hier unterbleiben soll.[368] Es hat jedoch im Laufe der letzten Jahre unter anderem angesichts des geänderten Nutzungsverhaltens

363 WALDMANN, Komm. PublG, Die Publikation kantonalen Rechts, S. 115.

364 SCHEFFLER/VAN SPYK, in: Recht im digitalen Zeitalter, S. 596.

365 Vgl. SCHEFFLER/VAN SPYK, in: Recht im digitalen Zeitalter, S. 606.

366 Vgl. VOLLERY, RFJ, 2014, S. 111; Antwort des Bundesrats auf die Bundesrat.

367 GLASER, ZSR, 2015, S. 289.

368 Vgl. zum Ganzen und mit weiteren Hinweisen zur Lage in den Kantonen, WALDMANN/SCHNYDER VON WARTENSEE, LeGes, 2013, S. 24.

eine Umstellung hin zur Verbindlichkeit der elektronischen Publikation stattgefunden.[369]

• *Fazit*

Die Mehrheit der Kantone ist inzwischen dazu übergegangen, amtliche Publikationen auch über das Internet zu veröffentlichen. Die verfassungsrechtlichen Minimalvorgaben stehen einer derartigen Publikation nicht entgegen. Eine gesetzliche Grundlage ist aufgrund der technischen Herausforderungen zu begrüssen und auch in den meisten Kantonen vorhanden. Sofern die gedruckte Version parallel weiterexistiert, ist dabei auch zu regeln, welche dieser Versionen massgeblich ist. Einige Kantone sind inzwischen dazu übergegangen, amtliche Publikationen nur noch in elektronischer Form zu publizieren.[370] Daraus ergeben sich weitere grundrechtliche Fragen, welche an späterer Stelle vertieft betrachtet werden.[371] 139

bb) Open Government Data

Open Government Data geht über die aktive Informationstätigkeit hinaus, indem neben der Information über die Tätigkeit der Behörden weitere Daten publiziert werden, die mit oder neben dem Hauptprodukt der behördlichen Aufgaben anfallen.[372] Auch wenn durch das Zurverfügungstellen von Behördendaten als OGD in erster Linie eine staatliche Leistung an Private erbracht wird, es sich also um ein Element der Leistungsverwaltung und nicht der Eingriffsverwaltung handelt, ist weitgehend unbestritten, dass für die Publikation der Daten eine gesetzliche Grundlage benötigt wird.[373] 140

Teilweise wird die Meinung vertreten, dass die Publikation von Open Government Data sich bereits aus der jeweiligen Staatsaufgabe ergibt, da praktisch bei jeder Aufgabe nutzbare Daten anfallen, welche gestützt auf das Öffentlichkeitsprinzip der Verwaltung auch der Publikation zugänglich sein müssen. Somit müsste keine gesonderte Gesetzesgrundlage geschaffen werden. Dagegen ist einerseits einzuwenden, dass die systematische Bereitstellung von Daten in maschinenlesbarer Form wohl das gesetzliche Aufgabenfeld der Verwaltung übersteigt. Anderseits ist ein wichtiger Pfeiler von Open Government Data auch die Weiterverarbeitung der Daten durch die Benutzenden. Diese 141

369 Botschaft Rev. PublG, S. 7058; vgl. Art. 15 Abs. 2 PublG, gemäss dem die auf der Publikationsplattform veröffentlichten Versionen der «Amtlichen Sammlung» (chronologische Fassung) als massgeblich zu gelten haben (in Kraft seit dem 1.1.2016).

370 Vgl. für den Kanton ZH: Art. 12 Abs. 1 PublV ZH.

371 Siehe dazu unten Rz. 216.

372 Vgl. OGD-Strategie 2019, S. 881; WIEDMER/SEIBERTH, S. 4; WEBER/LAUX/OERTLY, S. 32.

373 WIEDMER/SEIBERTH, S. 3; HÄFELIN/MÜLLER/UHLMANN, N. 39.

bringt etwa Fragestellungen urheberrechtlicher oder datenschutzrechtlicher Natur mit sich.[374] Es erscheint daher angezeigt, die Bereitstellung der Daten oder zumindest diese damit anfallenden Fragen in einer gesetzlichen Grundlage zu regeln.[375]

142 Denkbar sind dabei verschiedene Regelungsmöglichkeiten. Einerseits kann für jede Art von Informationen (z.B. Geoinformationen) im dazugehörigen Spezialgesetz geregelt werden, wie diese veröffentlicht werden sollen. Anderseits ist es denkbar, eine Querschnittsregelung im Sinne eines OGD-Gesetzes zu erstellen, welche die Nutzung von als OGD veröffentlichten Daten generell normiert.[376] Die Schweiz hat sich anders als etwa Deutschland für erstere Lösung entschieden. Wichtige Regelungen zu Open Government Data sind daher in den einschlägigen Fachgesetzen zu suchen.[377] Die einschlägigen Gesetze regeln etwa, welche Dateien durch die Behörden zu veröffentlichen sind, wobei hier ein wesentlicher Ermessensspielraum besteht. So können Bundesämter festlegen, welche Daten sie als für die Nutzung durch Dritte geeignet erachten. Dies führt mitunter dazu, dass Daten nicht publiziert werden, obwohl sie dazu geeignet wären.[378] Auch obliegt es der zuständigen Behörde zu entscheiden, ob sie ein Entgelt für die Daten verlangt. Die Prinzipien von OGD und ihnen nachfolgend auch die OGD-Strategie des Bundes setzen zwar das Ziel, dass offene Behördendaten gebührenfrei genutzt werden können. Ein umfassender Anspruch auf Gebührenfreiheit lässt sich daraus indes nicht ableiten.[379]

b) Öffentliches Interesse

143 Durch die Informationstätigkeit des Staates soll über das Internet die Transparenz erhöht werden. Die Transparenz des Verwaltungshandelns erfüllt eine wichtige rechtsstaatliche Funktion.[380] Somit ist das öffentliche Interesse an der Kommunikationstätigkeit über Internet evident.

374 Vgl. zum Ganzen die Diskussion bei: GOLLIEZ/ASCHWANDEN/BRETSCHER/BERNSTEIN/FARAGO/KRÜGEL/FREI/LAUX/BUCHER/NEURONI/RIEDL, S. 51, FN. 80.

375 Vgl. RUDIN, digma, 2012, 62 f.

376 WIEDMER/SEIBERTH, S. 2; RUDIN, digma, 2012, S. 62 f.

377 Vgl. GLASER, SJZ, 2018, S. 184. Hervorzuheben sind etwa das Bundesstatistikgesetz (BstatG, SR 431.01) vom 9. Oktober 1992 oder die jeweilige Bundesgesetzgebung über die Meteorologie und Klimatologie sowie über Geoinformationen; vgl. für eine Übersicht: WEBER/LAUX/OERTLY, S. 83 ff.; GOLLIEZ/ASCHWANDEN/BRETSCHER/BERNSTEIN/FARAGO/KRÜGEL/FREI/LAUX/BUCHER/NEURONI/RIEDL, S. 52; Für D vgl. § 12a Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz, EGovG).

378 Öffentlichkeitsgesetz.ch, ogd.

379 OGD-Strategie 2019, S. 884.

380 Vgl. EHRENZELLER/SAXER/BRUNNER, SG Komm. BV, Art. 180, N. 30; vgl. auch WIEDERKEHR, ZBl, 2007, S. 543.

c) Verhältnismässigkeit

Art. 5 Abs. 2 BV verlangt, dass staatliches Handeln verhältnismässig sein muss. 144
Die Verhältnismässigkeit setzt sich dabei zusammen aus den drei Elementen Geeignetheit, Erforderlichkeit und Verhältnismässigkeit im engeren Sinne (bzw. Angemessenheit oder Zumutbarkeit).[381]

Der Staat muss – wie weiter oben erwähnt – beachten, dass das gewählte 145
Informationsmittel für den jeweiligen Informationszweck geeignet ist, wobei die Informationstätigkeit bekanntlich verschiedene Ziele verfolgen kann.[382] Somit schränkt dieses Erfordernis den Staat bei der Wahl der Informationsmittel kaum ein. Unabhängig vom verfolgten Ziel muss es aber darum gehen, die Information möglichst schnell, verlässlich und effizient an die Bevölkerung weitergeben zu können. Aufgrund der augenscheinlich grossen Verbreitung des Internets kann die Publikation über dieses Medium eine geeignete Möglichkeit der Informationsverbreitung darstellen.[383] Es ist indes zu beachten, dass etwa der Unterhalt einer Internetpräsenz, die Entwicklung einer «App» oder das Bewirtschaften eines Social-Media-Auftritts beträchtliche personelle, finanzielle und zeitliche Ressourcen benötigen kann.[384] Es stellen sich daher die Fragen, ob die entsprechenden Ausgaben auch erforderlich sind oder ob die Behördeninformation auf althergebrachtem Weg als mildere Alternative ausreichen würde und ob die eingesetzten Mittel in einem vernünftigen Verhältnis zu ihrer Wirkung stehen.

i) Staatliche Internetpräsenz

Es ist nicht von der Hand zu weisen, dass eine Internetpräsenz mit gewissen 146
Kosten verbunden ist. Auf der anderen Seite bietet sie den Vorteil, dass dadurch Informationen weltweit und jederzeit erreichbar gemacht werden. In der Schweiz hat praktisch die gesamte Bevölkerung Zugriff auf das Internet und die meisten Personen benutzen dieses auch regelmässig.[385] Damit steht ihnen die Benutzung von behördlichen Webseiten grundsätzlich rund um die Uhr offen. Zudem erlaubt eine eigene Website einer Behörde die direkte Information der Bevölkerung ohne eine Zwischenschaltung der Medien als Intermediäre. Dadurch ist einerseits eine grössere Frequenz an Mitteilungen möglich, anderseits besteht auch keine Gefahr, dass die Information durch

381 EPINEY, BSK BV, Art. 5 N. 70 ff.
382 Vgl. EHRENZELLER/SAXER/BRUNNER, SG Komm. BV, Art. 180, N. 47.
383 BRUNNER, ZBl, 2010, S. 631.
384 Vgl. LANGER, AJP, 2014, S. 957 für Zahlen zum Webauftritt des Bundes.
385 Im Jahr 2017 hatten 93 % der Haushalte einen Internetzugang: BFS, S. 1.

die Medien allenfalls verändert und verfälscht wird. Nicht zuletzt kann durch die Publikation von Merkblättern im Internet proaktiv gehandelt werden. Nach dem Geschriebenen ist jedenfalls hinsichtlich des Kosten-Nutzen-Verhältnisses kein milderes Mittel zur effizienten und effektiven Information der Bevölkerung ersichtlich.[386] Unter Umständen kann eine adressatengerechte und wirksame Öffentlichkeitskommunikation gar verlangen, dass der Staat moderne Mittel wie das Internet für seine Informationstätigkeit einsetzt.[387]

ii) «Apps»

147 Internetfähige Mobiltelefone und Smartphones sind inzwischen in der Schweiz ebenfalls weit verbreitet.[388] Somit kann auch über das Anbieten von «Apps» grundsätzlich ein grosser Anteil der Bevölkerung erreicht werden. Die Bereiche, die durch «Apps» der öffentlichen Verwaltung abgedeckt werden, sind mannigfaltig, seien es etwa Daten zu Wetter und Naturgefahren, Abstimmungsinformationen oder Dienste der Polizei.[389] Das Ziel der «Apps» ist in der Regel, die im jeweiligen Bereich relevanten Informationen (z.B. polizeiliche Notrufnummern) in übersichtlicher Weise aufzubereiten. Noch eher selten bieten die «Apps» darüber hinausgehende Funktionalitäten (etwa das Einreichen von Formularen oder das Übermitteln von Fotos) an. Jedoch kann bereits durch die einfache und mobile Erreichbarkeit entsprechender Dienstleistungen und Informationen ein öffentliches Interesse bedient werden.

148 Indes sind auch die Entwicklung und der Unterhalt einer «App» kein billiges Unterfangen. Es wird daher bemängelt, dass gewisse «Apps» für den Betrag, welchen ihre Entwicklung gekostet hat, kaum einen wirklichen Zusatznutzen bieten.[390] Dies insbesondere, wenn sie lediglich eine Website mobil darstellen oder gewisse Dateien zur Verfügung stellen. Als kritisch betrachtet wird zusätzlich, dass oftmals keine behördenübergreifende Strategie besteht und viele Dienststellen oder Departemente ihre eigenen «Apps» anbieten.[391] Es lässt sich fragen, ob die Entwicklungskosten in solchen Fällen in einem angemessenen Verhältnis zum erbrachten Nutzen stehen. Die Behörden haben daher bei der Entwicklung einer «App» stets kritisch zu hinterfragen, ob diese ein sinnvolles Kosten-Nutzen-Verhältnis aufweist.

386 Im Ergebnis gleich: LANGER, AJP, 2014, S. 957 f.

387 MADER, in: St. Galler Tagung zur Öffentlichkeitskommunikation des Staates, S. 42.

388 So geben etwa 80 % der Befragten in einer Studie des BFS an, über ihr Mobiltelefon regelmässig auf das Internet zuzugreifen; vgl: BFS, Mobile Internetnutzung.

389 Vgl. SRF, News-Beitrag vom 24.3.2016.

390 SRF, News-Beitrag vom 24.3.2016.

391 Siehe etwa die umfangreiche Palette an «Apps» der Stadt Zürich.

Aktuelle Entwicklungen, etwa das kürzlich veröffentlichte «Zielbild für die digitale Transformation in der Bundesverwaltung und den Aufbau der digitalen Infrastrukturen» des Bundesrats, gehen hier einen Schritt in die richtige Richtung, indem sichere, einfach zu bedienende Ansprechstellen («single points of contact») oder einmalige Dateneingaben in Applikationen oder Websites thematisiert werden.[392] Es wäre durchaus wünschenswert, dass vermehrt über horizontale (Departements-) oder vertikale Grenzen hinweg zusammengearbeitet würde, um den Benutzern einen grösseren Mehrwert zu bieten. Ein positives Beispiel stellt hier etwa die von Bund und Kantonen gemeinsam lancierte «App» «VoteInfo» dar, welche Informationen und Ergebnisse zu Wahlen und Abstimmungen bietet.[393] Erstrebenswert ist in diesem Sinne auch, dass die «Apps» über die Umwandlung von blossen Internetinhalten hinaus einen Zusatznutzen bieten, welcher explizit auf die Möglichkeiten von Smartphones (z.B. mit deren Kameras) abgestimmt ist.[394] Ein Beispiel hierfür bietet die «App» «Züri wie neu», mithilfe welcher es möglich ist, Schäden an der Infrastruktur der Stadt Zürich direkt den Behörden zu melden.[395] Das Anbieten solcher Zusatzleistungen würde die Entwicklung solcher «Apps» sinnvoller und verhältnismässiger machen. 149

iii) Social Media

Hinsichtlich der Verhältnismässigkeit gilt es festzuhalten, dass etwa die Hälfte der Schweizer Bevölkerung mindestens einen Account auf einer der gängigen Social-Media-Plattformen unterhält. Dabei ist zu beachten, dass im Gegensatz zur generellen Internetnutzung ein wesentlich grösseres Ungleichgewicht zwischen «Jung» und «Alt» besteht.[396] Auch wenn aus der privaten Nutzung entsprechender Dienste nicht unbedingt geschlossen werden kann, dass die Angebote der Behörden genutzt werden, so steht den Benutzenden die entsprechende Möglichkeit zumindest offen.[397] Ob sie diese wahrnehmen, ist in diesem Rahmen nicht relevant. Zu beachten ist, dass der Zugriff auf die 150

392 Vgl. Zielbild. Die Eingabe von Personendaten bringt wieder andere Probleme mit sich, welche an späterer Stelle behandelt werden sollen, siehe unten Rz. 155 ff.

393 Vgl. etwa: SDA, Bund und Kantone lancieren Abstimmungs-App, Neue Zürcher Zeitung, 14. Januar 2019.

394 VOGT, Schweizer Mobile Government steckt in den Kinderschuhen.

395 STADT ZÜRICH, Züri wie neu, Webangebot Züri wie neu.

396 Vgl. etwa LATZER/JUST/METREVELI/SAURWEIN, S. 21; für aktuellere Zahlen auch den Media Use Index. Auch wenn sich der Trend inzwischen etwas aufweicht; vgl. Bernetblog.

397 Vgl. etwa KOBEL JÜRG, So nutzen die Schweizer Kantone Social Media. Auch aktuell bewegen sich die entsprechenden Abonenntenzahlen meist noch im vier- oder niedrigen fünfstelligen Bereich.

jeweiligen Angebote oftmals auch möglich ist, ohne dass man sich auf der jeweiligen Plattform registriert. In diesen Fällen bleiben lediglich gewisse Interaktionsmöglichkeiten (etwa das «Liken» oder Kommentieren von Beiträgen) verwehrt.

151 Auf der anderen Seite ist davon auszugehen, dass die Nutzung einer bestehenden Plattform kostengünstiger ist als der Unterhalt einer eigenen Web-Präsenz.[398] Wenn, wie weiter oben beschrieben, der Unterhalt einer Website zur Informationstätigkeit als verhältnismässig erachtet wird, erstaunt es nicht, dass die staatliche Nutzung von Social Media in der Schweiz kaum thematisiert oder grundsätzlich als unproblematisch beurteilt wird.[399]

152 Es versteht sich von selbst, dass auch bei der Nutzung von sozialen Medien zur Informationstätigkeit die allgemeinen Anforderungen an die staatliche Informationstätigkeit, wie Neutralität, Verlässlichkeit, Korrektheit und zeitliche Nähe zu beachten sind.[400] Zu erwähnen ist in diesem Zusammenhang, dass es auf Social-Media-Plattformen oft problemlos möglich ist, über die eigene Identität zu täuschen. So existieren z.B. zahlreiche inoffizielle Facebook-Seiten, welche in ihrer Aufmachung nicht von offiziellen Angeboten unterscheidbar sind.[401] Dies kann problematisch sein, da staatlicher Information ein grosses Mass an Zuverlässigkeit zugebilligt wird.[402] Diese Zuverlässigkeit kann auf Social-Media-Plattformen unter Umständen nicht auf die gleiche Weise gewährleistet werden. Einige Plattformen wie Facebook oder Twitter bieten den Benutzern immerhin die Möglichkeit, ihr Konto zu verifizieren, um nachzuweisen, dass die Marke oder das Unternehmen dahintersteckt, welche vorgegeben wird.[403]

153 Diese Massnahme verfehlt jedoch ihre Wirkung, wenn nicht alle Gemeinwesen sich verifizieren lassen und die Bedeutung des entsprechenden Symbols kaum bekannt ist.[404] Die Behörden müssen sich dieser Gefahr bewusst sein und gegen entsprechende «Fake Accounts» vorgehen. Die entsprechenden

398 LANGER, AJP, 2014, S. 957.

399 Vgl. die Berichte des Bundesrats: Bericht Social Media 2013 und Bericht Social Media 2017, wobei hier jeweils privatrechtliche Fragestellungen im Vordergrund stehen und kaum eine Auseinandersetzung mit Problemen der staatlichen Nutzung stattfindet.

400 Vgl., MILKER, NVwZ, 2018, S. 1755. So darf die Polizei z.B. nicht einer politischen Partei auf Facebook folgen.

401 Beispiele bei LANGER, AJP, 2014, S. 956.

402 Vgl. etwa TSCHANNEN, ZSR, 1999, S. 418.

403 Vgl. z.B. für Facebook: Was ist eine verifizierte Seite?. Ein entsprechendes Konto enthält z.B. einen blauen Haken auf der entsprechenden Seite, welcher die Verifizierung anzeigt.

404 Vgl. etwa die in der Werbewoche zitierte Studie, zu deren Zeitpunkt nur drei kantonale Verwaltungen ihre Konten verifiziert haben.

Konten können etwa dem jeweiligen Plattformbetreiber zur Löschung gemeldet werden und/oder es kann zivilrechtlich gegen die Betreiber vorgegangen werden.[405] Je nach Ziel des «Fake Accounts» ist auch eine strafrechtliche Verfolgung denkbar. Dies jedoch nur dann, wenn eine eigenständige strafbare Handlung, etwa unbefugte Datenbeschaffung (Art. 143 StGB) oder Ehrverletzung (Art. 173 StGB), damit begangen wird, da der Identitätsdiebstahl als solcher im Schweizer Recht zum jetzigen Zeitpunkt nicht strafbar ist.[406]

iv) Amtliche Publikation

Hinsichtlich der amtlichen Publikationen existieren teilweise vergleichende Kosten-Nutzen-Analysen zwischen dem analogen und dem digitalen Angebot. So hat etwa die gedruckte Version des Bundesblatts lediglich knapp 2'000 Abonnenten, während über eine Million Zugriffe pro Monat auf die jeweiligen Webangebote erfolgen.[407] Die Reichweite scheint hier klar dafür zu sprechen, dass die Online-Publikation eine verhältnismässige Alternative darstellt. Zwar sind die Einführung und Instandhaltung des jeweiligen Systems ebenfalls mit Kosten verbunden, diese können etwa durch die entfallenden Druckkosten aufgewogen werden. Oftmals wird daher gerade die Kostensenkung als Argument für den Wechsel von der gedruckten zur Online-Version aufgeführt.[408] Um die Online-Publikation verhältnismässig ausgestalten zu können, ist es indes wichtig, die oben genannten Mindestvorgaben, welche sich aus der Verfassung ableiten lassen, zu beachten. Dies hat insbesondere hinsichtlich der einfachen Zugänglichkeit zu gelten. Ein Online-Zugriff kann hier gewisse Vorteile bringen. Dazu muss jedoch die Authentizität auch im Rahmen des Online-Angebots gewährleistet werden können. Entsprechend muss etwa früheres Recht zugänglich bleiben und der Zugang benutzerfreundlich ausgestaltet sein. Zudem muss das Angebot kostenlos zugänglich sein.[409] 154

2. Informationelle Selbstbestimmung

Nach dem soeben Ausgeführten sind die gesetzlichen Grundlagen der Behördeninformation bewusst und notwendigerweise weit gefasst. Dennoch sind 155

405 Ein zivilrechtliches Vorgehen, z.B. gestützt auf Art. 29 Abs. 2 ZGB, scheitert jedoch oft an der Anonymität der Betreiber; vgl. GIGER/HANGARTNER, S&R, 2017, S. 136. Auch ein Vorgehen über den Betreiber bringt nicht immer den gewünschten Erfolg; vgl. das lange Warten auf die Deaktivierung des «Fake Accounts» von BR Ueli Maurer: NZZ, Bund versucht falschen Ueli Maurer zu stoppen, 8. April 2013.

406 Vgl. etwa die Motion 14.3288 Comte Raphaël: «Identitätsmissbrauch. Eine strafbare Handlung für sich» und die abschlägige Antwort des Bundesrats in dieser Angelegenheit.

407 Botschaft Rev. PublG, S. 7061.

408 Botschaft Rev. PublG, S. 7069 und 7094.

409 WALDMANN, Komm. PublG, Die Publikation kantonalen Rechts, S. 115.

gewisse Grenzen zu beachten. So sieht bereits Art. 180 Abs. 2 BV im Wortlaut der Bestimmung vor, dass der Bundesrat über seine Tätigkeit informiert, sofern nicht überwiegende öffentliche oder private Interessen entgegenstehen. Eine ähnliche Einschränkung kennen auch Art. 10 Abs. 3 RVOG und eine Vielzahl an kantonalen Informationsbestimmungen.[410] Denkbar sind dabei etwa private Interessen wie der Schutz der Privatsphäre sowie Berufs-, Geschäfts- oder Fabrikationsgeheimnisse, aber auch öffentliche Interessen, etwa der Schutz internationaler Beziehungen oder der freien Meinungs- und Willensbildung der Behörden. Es muss dabei im jeweiligen Einzelfall eine Abwägung zwischen dem öffentlichen Informationsinteresse und den gegenüberstehenden privaten oder öffentlichen Interessen vorgenommen werden.[411]

156 Für viele der soeben genannten entgegenstehenden Interessen hat sich durch die Digitalisierung nichts Wesentliches verändert. Gerade dort, wo jedoch Daten über Personen via das Internet bekanntgegeben werden, besteht für die Betroffenen eine grössere Gefahr, da die publizierende Behörde nach einer Publikation im Internet keine Kontrolle mehr darüber hat, wer die Information weiterverbreitet. Auf diese Weise können einmal publizierte Informationen erst recht nur schwer wieder aus dem Internet entfernt werden, zumal nicht bekannt ist, wo diese ebenfalls noch vorhanden sind.

157 Es ist offensichtlich, dass die Behördeninformation in gewissen Fällen Daten über eine Person enthalten muss, um Sinn zu ergeben, etwa bei der Bekanntgabe der zuständigen Fachperson in der Verwaltung. In einigen Fällen besteht jedoch z.B. die Gefahr, dass mehr Daten bekanntgegeben werden, als es eigentlich notwendig ist. Daher soll im Folgenden vertieft betrachtet werden, wie die Schweizer Rechtsordnung diese Gefahr beschränkt. Dabei ist insbesondere das Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV zu beachten, welches, wie bereits an früherer Stelle ausgeführt, vor dem Missbrauch persönlicher Daten einer Person schützt. Konkretisiert wird diese Grundrechtsbestimmung durch das einschlägige eidgenössische oder kantonale Datenschutzgesetz. In jüngerer Zeit sind zudem viele Gemeinwesen dazu übergegangen, bei jedem Besuch auf der Website bzw. bei jeder Benutzung der von ihnen veröffentlichten Apps gewisse Randdaten der jeweiligen Besuchenden aufzuzeichnen. Diese Daten sollen dazu dienen, die Nutzung der Website zu analysieren und das Web-Angebot auf diese Weise effizienter zu gestalten. Es stellt sich auch hier die Frage, ob dies mit der Schweizer Rechtsordnung und insbesondere mit dem Recht auf informationelle Selbstbestimmung vereinbar ist.

410 Vgl. z.B. Art. 18 IDG BL.

411 EHRENZELLER/SAXER/BRUNNER, SG Komm. BV, Art. 180, N 69 ff.

a) Bekanntgabe von Personendaten im Rahmen der Behördeninformation

i) Bearbeitung von Personendaten

Damit die Datenschutzgesetzgebung einschlägig ist, müssen – wie bereits an anderer Stelle ausgeführt – Daten bearbeitet oder bekanntgegeben werden, durch welche eine Person bestimmt oder bestimmbar ist (vgl. etwa Art. 3 DSG). Für die Bestimmbarkeit einer Person muss sich deren Identität nicht unmittelbar aus einem Datum ergeben, sondern es reicht aus, dass sich diese aus dem Kontext mit anderen Daten ohne unverhältnismässigen Aufwand ermitteln lässt.[412] In den meisten Fällen ist offensichtlich, ob im Rahmen der Behördeninformation Daten über eine Person bekanntgegeben werden. Auch amtliche Publikationen können Daten enthalten, durch welche Personen bestimmt oder bestimmbar sind. Zu denken ist hier etwa an die Publikation von Baugesuchen oder Gerichtsvorladungen einer Person mit unbekanntem Aufenthalt im Amtsblatt. Mithin kann es sich hier gar um Daten handeln, welche über administrative oder strafrechtliche Verfolgungen und Sanktionen einer bestimmten oder bestimmbaren Person Auskunft geben und somit als besondere Personendaten i.S. von Art. 3 lit. c. Abs. 4 DSG zu gelten haben.[413] 158

Nicht auf den ersten Blick ersichtlich ist indes, ob es sich bei der Publikation von «Open Government Data» um Personendaten handelt. Es ergibt sich aus der obenstehenden Definition, dass als Open Government Data nur Daten veröffentlicht werden sollen, welche keine Datenschutzbestimmungen verletzen.[414] Problemlos möglich ist aus datenschutzrechtlicher Warte eine Veröffentlichung von Datensätzen daher, wenn die entsprechenden Daten nie einen Personenbezug besassen, wenn es sich mithin um Sachdaten (etwa Wetter- oder Umweltdaten) handelt. 159

Bei Personendaten kann die Anonymisierung von Daten eine Möglichkeit darstellen, diese dennoch in geeigneter Form als OGD zu veröffentlichen. Dabei reicht es unter Umständen indes nicht aus, lediglich den Namen oder die Adresse wegzulassen, um den Personenbezug endgültig zu entfernen. Bei der Publikation ist nämlich in der Regel nicht absehbar, welche Datensätze später veröffentlicht oder mit dem betreffenden Datensatz verknüpft werden und wieder eine Identifizierungsmöglichkeit der jeweiligen Person schaffen können.[415] Illustrieren lässt sich dies etwa am folgenden Beispiel: Wenn statistische Daten (z.B. über das Einkommen eines Haushalts) parzellengenau 160

412 RUDIN, digma, 2012, S. 65.

413 Vgl. etwa SCHEFFLER / VAN SPYK, in: Recht im digitalen Zeitalter, S. 599.

414 Siehe oben Rz. 111.

415 Sog. Rückkoppelung, vgl. GOLLIEZ/ASCHWANDEN/BRETSCHER/BERNSTEIN/FARAGO/KRÜGEL/FREI/LAUX/BUCHER/NEURONI/RIEDL, S. 55.

veröffentlicht werden, kann man aus diesen zwar nicht direkt Personendaten ableiten, es ist aber möglich, mit der einfachen Abfrage des Eigentümers aus dem Grundbuch, Rückschlüsse über die dort wohnenden Personen zu ziehen.[416] Daher ist etwa gerade bei georeferenzierten Daten stets Vorsicht walten zu lassen.[417]

161 Bei der Publikation von OGD ist daher anzuregen, dass die zuständige Behörde auch zukunftsgerichtet überlegt, welche Daten allenfalls später mit den publizierten Daten verknüpft werden können, und nach der Veröffentlichung kontinuierlich Risikoanalysen in Bezug auf die veröffentlichten Daten vornimmt.[418] Dabei dürfte es sich zweifellos um ein anspruchsvolles Unterfangen handeln. Es ist hervorzuheben, dass die verantwortlichen Behörden sich der datenschutzrechtlichen Probleme in der Regel bewusst sind und von der Publikation von Personendaten absehen. Auch versuchen sie durch zusätzliche Einschränkungen, wie etwa den Verzicht auf parzellenscharfe Erhebungen oder eine Begrenzung der Anzahl möglicher Abrufe pro Tag, Missbrauch vorzubeugen.[419]

ii) Gesetzliche Grundlage

162 Bereits aus Art. 36 BV ergibt sich das Erfordernis einer gesetzlichen Grundlage für Grundrechtseingriffe. Werden Personendaten bekanntgegeben, so ist in diesem Zusammenhang auch die einschlägige Datenschutzgesetzgebung zu beachten, welche in Art. 19 DSG für jede Datenbekanntgabe grundsätzlich eine gesetzliche Grundlage fordert. Wie weiter oben beschrieben, sind die Rechtsgrundlagen über die aktive Behördeninformation aufgrund ihres weiten Anwendungsspektrums und der verschiedenen Kommunikationskanäle oftmals relativ weit formuliert und sprechen sich kaum darüber aus, ob in diesem Rahmen Personendaten bekanntgegeben werden dürfen.[420] Dies ist in Anbetracht der vielen denkbaren Kommunikationsszenarien nachvollziehbar. Lediglich dort, wo der Gesetzgeber spezielle Informationspflichten vorsieht, spricht er sich teilweise auch über die Bekanntgabe von Personendaten aus.[421]

416 Beispiele entnommen aus RUDIN, digma, 2012, S. 64.

417 Unter Georeferenzierung ist die die Zuweisung raumbezogener Referenzinformationen zu einem Datensatz zu verstehen; vgl. SWISSTOPO, Definition Georeferenzierung.

418 RUDIN, digma, 2012, S. 67, m.w.H.

419 Vgl. Checkliste OGD S. 2; so soll z.B. bei geografischen Angaben die Referenzierung (Strasse, Block) so gewählt werden, dass mindestens 20 (bzw. bei besonderen Personendaten mindestens 50) Einheiten umfasst sind.

420 Vgl. BRUNNER, ZBl, 2010, S. 609.

421 Vgl. Art. 50a Abs. 3 des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung; siehe dazu: BRUNNER, ZBl, 2010, S. 619.

Fehlt eine spezielle Gesetzesgrundlage, so ist gemäss Art. 19 Absatz 1bis DSG die Bekanntgabe von Personendaten im Rahmen der behördlichen Information zulässig, falls diese Daten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen und an deren Bekanntgabe ein überwiegendes öffentliches Interesse besteht. Auch die Kantone sehen oft ähnliche Regeln vor.[422] Findet diese Information über das Internet statt, gehen damit zusätzliche Risiken für die Persönlichkeit der Betroffenen einher. So kann die weitere Verbreitung einer Information und deren Kontext durch den ursprünglichen Absender nicht mehr kontrolliert werden und eine einmal publizierte Information kann unter Umständen nicht mehr entfernt werden («Das Internet vergisst nicht!»).[423] Auch im Lichte dieser Gefahren statuiert Art. 19 Abs. 3bis DSG, dass eine Publikation mittels automatisierter Informations- und Kommunikationsdienste nur zulässig ist, wenn eine Rechtsgrundlage diese vorsieht oder eine Bekanntgabe im Rahmen des oben genannten Absatz 1bis zulässig ist und die entsprechende Publikation entfernt wird, wenn kein öffentliches Interesse an deren Veröffentlichung mehr besteht. 163

Betreffend die amtliche Publikation rekapituliert auf Bundesebene Art. 16b PublG die Voraussetzungen des Datenschutzgesetzes. Auch hier ist die gesetzliche Grundlage der jeweiligen Publikation in den jeweiligen Spezialerlassen, also den Verfahrensgesetzen oder etwa den kantonalen Baugesetzen (für die Veröffentlichung von Baugesuchen), zu finden. Es wird dabei als ausreichende gesetzliche Grundlage betrachtet, wenn das jeweilige Gesetz die amtliche Publikation vorsieht, ohne sich explizit über die Veröffentlichung von Personendaten auszusprechen.[424] Dies, zumal es sich bereits aus Sinn und Zweck der Publikation regelmässig ergibt, dass Daten über eine Person mitveröffentlicht werden, da ansonsten für die Adressaten gar nicht bzw. höchst umständlich verifizierbar wäre, ob sie von der publizierten Verfügung betroffen sind. 164

Zu beachten ist an dieser Stelle zusätzlich, dass Daten, welche über das Internet publiziert werden, in der Regel auch für Personen im Ausland verfügbar sind. Gemäss Art. 6 DSG ist eine Datenbekanntgabe ins Ausland nicht zulässig, wenn dort eine Gesetzgebung fehlt, welche einen angemessenen Schutz für diese Personendaten bietet. Dieser angemessene Schutz liegt indes nicht in allen Ländern vor.[425] Dementsprechend wäre eine Publikation von Informationen mit Personendaten über das Internet aufgrund der potenziell 165

422 Vgl. etwa Art. 18 Abs. 1 lit. b IDG BL: «zur Erfüllung einer gesetzlichen Aufgabe notwendig».

423 Vgl. BRUNNER, ZBl, 2010, S. 631.

424 Vgl. Botschaft Rev. PublG, S. 7089.

425 Vgl. etwa die Staatenliste des EDÖB.

weltweiten Verfügbarkeit nicht mit dem Gesetz vereinbar. Art. 5 VDSG stellt indes klar, dass die Bekanntgabe von Personendaten mittels automatisierter Informations- und Kommunikationsdienste zur Information der Öffentlichkeit nicht als Übermittlung ins Ausland im Sinne der Gesetzesbestimmung gilt. Diese Einschränkung ist nicht zu beanstanden.

iii) Öffentliches Interesse und Verhältnismässigkeit

166 Es ist eine Vielzahl an öffentlichen Interessen denkbar, welche es rechtfertigen können, dass die Information durch eine Behörde Personendaten enthält. In Frage kommen etwa polizeiliche Interessen bei der Warnung vor einem entflohenen Straftäter. Bei der amtlichen Publikation wiederum ist das öffentliche Interesse an der Veröffentlichung dieser Daten darin zu sehen, dass allfällige Betroffene über laufende Verfahren oder beschlossene Gesetze informiert werden und es ihnen möglich ist, innert Frist einen Rechtsbehelf oder ein Rechtsmittel einzulegen oder zumindest bewusst darauf zu verzichten. Dieses Interesse besteht solange, als die entsprechende Frist zur Einsprache oder zur Ergreifung eines Rechtsmittels läuft.

167 Die Datenbekanntgabe muss auch verhältnismässig erfolgen, d.h. geeignet und erforderlich sowie verhältnismässig im engeren Sinn sein. Kaum Probleme bereiten hier die Geeignetheit und die Erforderlichkeit. Muss eine Person, deren Aufenthalt unbekannt ist, oder eine Vielzahl von unbestimmten Personen (z.B. im Rahmen der Veröffentlichung eines Baugesuchs) erreicht werden, so ist die Publikation geeignet, diese Personen zu erreichen, und es sind auch keine milderen Mittel ersichtlich, wie dies geschehen könnte.

168 Das Schlüsselelement für die Veröffentlichung von Personendaten ist nach dem soeben Ausgeführten und bereits aufgrund von Art. 19 Abs. 1bis DSG die Abwägung zwischen dem öffentlichen Interesse an der Information und dem privaten Interesse am Schutz der Personendaten im konkreten Einzelfall. Hat der Gesetzgeber eine spezialgesetzliche Grundlage geschaffen, so hat er diese Abwägung in genereller Weise bereits vorgenommen.[426] Ohne entsprechende Grundlage ist die Abwägung jedoch im Einzelfall zu treffen, wobei das öffentliche Interesse an der Publikation das private Interesse klar überwiegen muss.[427] Dies ist insbesondere deshalb wichtig, weil bei der aktiven Informationstätigkeit kein Verfahren statuiert ist, in welchem die Betroffenen ihre Rechte vorgängig geltend machen können, wie dies etwa im Rahmen der passiven Informationstätigkeit mit Art. 11 BGÖ vorgesehen ist. Wo eine vorgängige Konsultation der Betroffenen möglich ist, kann eine solche

426 BRUNNER, ZBl, 2010, S. 618.

427 Vgl. etwa WATTER/KÄGI, AJP, 2005, S. 51.

auch bei der aktiven Informationstätigkeit durchgeführt werden. Unter Umständen ist dies allerdings aufgrund des Zwecks der Information oder der zeitlichen Dringlichkeit nicht möglich.[428]

169 Bei der Güterabwägung ist insbesondere zu berücksichtigen, welche Personendaten bekanntgegeben werden sollen und welche Auswirkungen die Bekanntgabe auf die betroffene Person hat. Die Bekanntgabe, dass eine Person in eine Behörde gewählt wurde, hat eher geringe Auswirkungen und muss daher im Sinne der Transparenz der Verwaltung zulässig sein. Bei personenbezogenen Warnungen (etwa vor einem flüchtigen Gewaltverbrecher) sind aufgrund der bekanntzugebenden Daten die Grundrechtspositionen dieser Person stärker betroffen, jedoch ist auch das öffentliche Interesse an entsprechenden Warnungen – etwa hinsichtlich der öffentlichen Sicherheit – um einiges höher.[429]

170 Zu beachten ist auch, dass das Interesse an der Publikation dieser Daten mit der Zeit nachlässt, etwa wenn die dazugehörige Einsprache- oder Rechtsmittelfrist abgelaufen ist. Ab einem gewissen Zeitpunkt besteht in der Regel kein öffentliches Interesse mehr daran, dass die entsprechenden Personendaten weiterhin einsehbar sind, insbesondere im Internet mit seinen umfassenden Suchmöglichkeiten.[430] Eine zeitlich unbeschränkte Verfügbarkeit des gesamten Datenbestands kann grundsätzlich nicht als verhältnismässig angesehen werden.[431] Daher sind – wie in Art. 19 Abs. 3bis DSG vorgesehen – die betreffenden Daten wieder aus dem automatisierten Informations- und Kommunikationsdienst zu entfernen, sobald das öffentliche Interesse an der Zugänglichmachung nicht mehr besteht. Auch Art. 16b Abs. 2 PublG statuiert in diesem Sinne, dass Texte, die besonders schützenswerte Personendaten enthalten, online nicht länger öffentlich zugänglich sein und nicht mehr Informationen enthalten dürfen, als es ihr Zweck erfordert.[432] Unter Umständen können dabei auf Verordnungsstufe Zeiträume festgelegt werden, während welcher Daten abrufbar sind, wie dies etwa Art. 20 Abs. 2 PublG ZH vorsieht. Auf diese Weise kann bereits durch den Gesetzgeber eine Abwägung zwischen öffentlichem und privatem Interesse vorgenommen werden. Je nach Art der Personendaten und damit verbundenem Schutzbedarf können zudem die Zeiträume der Veröffentlichung variieren.[433]

428 Vgl. BRUNNER, ZBl, 2010, S. 609.

429 Vgl. zum Ganzen und für weitere Beispiele: BRUNNER, ZBl, 2010, S. 626 ff.

430 Vgl Antrag Rev. PublG ZH, S. 27.

431 Vgl. HÖSLI, LeGes, 2013, S. 161.

432 Vgl. Botschaft Rev. PublG, S. 7090.

433 Vgl. Verordnung über das Internet-Amtsblatt BL vom 26. Juni 2007 (SGS 106.12).

171 Nach Ablauf des Zeitraums sollten die jeweiligen Ausgaben (bzw. Bereiche) des Amtsblatts aus diesen Überlegungen aus dem Internet entfernt werden. Allfälligen berechtigten Anliegen Dritter soll dadurch Rechnung getragen werden, dass die Behörden ältere Ausgaben weiterhin offline zugänglich halten.[434] Das Publikationsgesetz des Bundes sieht in Art. 16b Abs. 3 PublG zudem vor, dass weitere technische Massnahmen getroffen werden sollen, um den Schutz der Personendaten sicherzustellen. Dabei denkt der Gesetzgeber etwa an schwierig entzifferbare Bild- oder Tonsequenzen (sog. «CAPTCHA») oder die Möglichkeit, die entsprechenden Seiten von der Auffindbarkeit durch Suchmaschinen auszunehmen[435], wobei soweit ersichtlich bisher keine dieser Massnahmen umgesetzt wurde.

b) Erhebung von Personendaten im Rahmen der Behördeninformation

172 Über ihre Websites oder Apps haben die staatlichen Behörden die Möglichkeit, Daten von den besuchenden Personen zu erheben. So können inzwischen – wie weiter oben ausgeführt – oft direkt auf der Website Formulare ausgefüllt werden, um z.B. Gesuche einzureichen oder mit der Verwaltung in Kontakt zu treten. Die sich damit hinsichtlich der informationellen Selbstbestimmungen ergebenden Probleme wurden dabei weiter oben bereits behandelt.[436] Unmittelbar mit dem Informationszweck der Websites verbunden ist auch, dass viele Verwaltungen dazu übergegangen sind, bei jedem Besuch auf der Website bzw. bei jeder Benutzung einer App gewisse Randdaten der jeweiligen Besuchenden aufzuzeichnen. Diese Daten sollen dazu dienen, die Nutzung der Website zu analysieren und das Web-Angebot auf diese Weise effizienter zu gestalten.[437]

173 Interagiert ein Benutzer über soziale Netzwerke mit der Behörde, so werden durch die jeweilige Plattform ebenfalls Daten über ihn erhoben. Bei der Registrierung in diesen Netzwerken überträgt der Benutzer den Betreibern mit dem Akzeptieren der Nutzungsbedingungen die Nutzungsrechte an einer Vielzahl eigener Daten. Die entsprechenden Daten dürfen durch den Plattformbetreiber dementsprechend etwa genutzt werden, um personalisierte Werbeangebote anzuzeigen, und gegebenenfalls auch an Drittparteien weitergegeben werden.[438] Der «Datenhunger» dieser Plattformen wurde immer wieder thematisiert, und es wurden bereits mehrfach Fälle publik, in denen

434 Vgl. Antrag Rev. PublG ZH, S. 27.

435 Vgl. Botschaft Rev. PublG, S. 7073.

436 Siehe weiter oben Rz. 321 ff.

437 Vgl. etwa die Erläuterungen des EDÖB zu Webtracking.

438 Vgl. SÖBBING, InTeR, 2018, S. 182 ff.

Daten von den Plattformbetreibern entgegen der Nutzungsbestimmung weitergegeben wurden. Erwähnt sei hier lediglich der «Cambridge Analytica»-Skandal, in dessen Zuge sich herausstellte, dass Facebook Benutzerdaten an eine Politberatungsfirma weitergegeben hatte, die von dieser für sogenanntes «Micro Targeting» im amerikanischen Präsidentschaftswahlkampf von 2016 benutzt wurden.[439] Die Frage stellt sich somit, ob staatliche Stellen die Privaten durch das Anbieten einer Social-Media-Präsenz allenfalls einem höheren Risiko des Missbrauchs ihrer Daten aussetzen. Auch wenn sich Benutzer nicht registrieren müssen, um die entsprechenden Inhalte angezeigt zu erhalten, können teilweise Daten über sie erhoben werden. So stellt Facebook den Inhabern von Fanseiten – wie diese auch oft von staatlichen Stellen geführt werden – unabdingbar und kostenlos das Tool «Facebook Insights» zur Verfügung, welches statistische Informationen zu den Besuchern der jeweiligen Seite offenlegt und dadurch ermöglicht, das Nutzerverhalten zu analysieren.[440]

In den soeben genannten Fällen besteht die Möglichkeit, dass die Behör- 174
den Personendaten über die Besuchenden oder die Benutzer sammeln und bearbeiten, womit ein Eingriff in die informationelle Selbstbestimmung vorliegen könnte und die Vorgaben der Datenschutzgesetzgebung zu beachten wären. Im Folgenden soll daher betrachtet werden, ob allfällige Datenbearbeitungen mit dem geltenden Recht vereinbar sind.

i) Websites und Apps

Zu den Daten, welche bei der Nutzung einer Website oder einer App in der 175
Regel erhoben und in Logfiles gespeichert werden, zählen etwa IP-Adresse, Datum und Uhrzeit des Zugriffs sowie der verwendete Webbrowser und das Betriebssystem.[441] Komplexere Trackingverfahren können Mausklicks oder Scroll-Verhalten von Nutzern zur Auswertung aufzeichnen.[442] Zu diesem Zweck wird auf dem Computer des Benutzers eine Datei abgespeichert, welche beim erneuten Aufruf der Seite vom Server abgefragt wird, ein sogenanntes «Cookie».[443] Aus dieser Datei können die oben genannten Daten ausgelesen und ausgewertet werden. Diese Auswertung kann durch die Informatikabteilung der jeweiligen Behörde vorgenommen werden, geschieht jedoch häufig auch durch eine Auslagerung an eine spezialisierte Firma.[444] Das Augenmerk

439 Vgl, SÖBBING, InTeR, 2018, S. 182.

440 HOFFMANN/SCHULZ/BRACKMANN, ZD, 2013, S. 123.

441 Vgl. etwa die entsprechenden Hinweise auf der Website des Bundes.

442 Vgl. Erläuterungen.

443 ROSENTHAL, digma, 2017, S. 198.

444 Siehe zum «Outsourcing bereits weiter oben Rz. 98. Viele Websites verwenden z.B. den Dienst «Google Analytics»; vgl. die Erläuterungen des EDÖB zu Webtracking.

liegt bei dieser Datensammlung nicht auf der Sammlung von Daten des Einzelnen, sondern in erster Linie in der Aufzeichnung allgemeiner Besucherströme. Dennoch können auf diese Weise Informationen über die Internetnutzung einer Person gewonnen werden. Es ist unter Umständen sogar möglich, ein Nutzungsprofil des jeweiligen Benutzenden zu erstellen.[445]

aa) IP-Adresse als Personendatum

176 Fraglich ist indes, ob es sich bei den gesammelten Daten überhaupt um Personendaten im Sinne der Datenschutzgesetzgebung handelt, das heisst um Angaben, durch die eine Person bestimmt oder bestimmbar ist. Die meisten in diesem Zusammenhang erhobenen Daten wie Datum und Uhrzeit des Zugriffs, Webbrowser und Betriebssystem oder auch das Nutzungsverhalten auf einer Site lassen ohne zusätzliche Angaben keine Rückschlüsse auf eine bestimmte Person zu. Bei der IP-Adresse handelt es sich indes um die einem Gerät[446] zugeordnete, eindeutige Adresse, welche dieses gegenüber anderen Teilnehmern in einem Netzwerk (wie dem Internet) ausweist. Diese Adressen können dem jeweiligen Gerät statisch zugewiesen werden, das heisst, sie bleiben bei jeder Internetnutzung gleich. Für Privatnutzer werden die IP-Adressen indes grundsätzlich dynamisch vergeben. Sie sind dem Benutzer nur für eine kurze Zeit zugeteilt, wobei diese Zuordnung in der Regel durch den Internetprovider geschieht. [447]

177 Das Bundesgericht hatte sich erst einmal mit der konkreten Einordnung der IP-Adresse als Personendatum zu befassen. Es führte dabei aus, dass nur anhand der konkreten Umstände beurteilt werden kann, ob aus der IP-Adresse Rückschlüsse auf die Personen dahinter gezogen und diese somit bestimmbar gemacht werden können.[448] Statische IP-Adressen sind in der Regel in öffentlichen Verzeichnissen abrufbar und dadurch mit verhältnismässig geringem Aufwand zuordenbar. Bei dynamischen IP-Adressen ist dagegen eine Identifikation von deren Trägern in der Regel nur mithilfe des Providers möglich, der die Adressen vergeben hat. Dynamische IP-Adressen stellen dementsprechend für den Betreiber eines Website-Trackingtools dann ein personenbezogenes Datum dar, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, den Nutzer anhand der Zusatzinformationen (die er etwa

445 Vgl. die Erläuterungen des EDÖB zum Einsatz von Webanalysetools für Bundesorgane.

446 Dabei kann es sich um einen einzelnen Computer handeln oder wohl im Regelfall um einen Router, an welchen wiederum mehrere Geräte angeschlossen sind, welche sich dieselbe IP-Adresse teilen.

447 Vgl. für eine weitergehende technische Beschreibung etwa WEBER / FERCSIK SCHNYDER, sic!, 2009, S. 577.

448 BGE 136 II 508, E. 3.5, mit Verweis auf WEBER / FERCSIK SCHNYDER, sic!, 2009, S. 579 f.

vom Internetzugangsanbieter erhält) bestimmen zu lassen. Dieses Tätigwerden eines Dritten schliesst eine Einordnung von IP-Adressen als Personendaten nicht per se aus. Lediglich wenn der Aufwand des Auftraggebers für die Bestimmung der betroffenen Person derart gross ist, dass nach der allgemeinen Lebenserfahrung nicht mehr damit gerechnet werden kann, dieser werde ihn auf sich nehmen, liegt kein Personendatum mehr vor.[449]

178 Im vor dem Bundesgericht beurteilten Fall war es gerade das Geschäftsmodell der Beschwerdegegnerin, dynamische IP-Adressen und andere Daten aufzuzeichnen, um diese entgeltlich an die Inhaber von Urheberrechten zur Verfolgung strafrechtlicher Schritte weiterzugeben. Dieser Rechteinhaber kann im Rahmen eines allfälligen Strafverfahrens die Identifizierung der Person hinter der IP-Adresse verlangen.[450] Der Europäische Gerichtshof geht in seiner Rechtsprechung ebenfalls davon aus, dass sich nur anhand der Umstände beurteilen lässt, ob eine IP-Adresse ein Personendatum darstellt. Er bejahte dies in einem Fall, in dem Einrichtungen des deutschen Staates diese speicherten, zumal in Deutschland für die Behörden Möglichkeiten bestehen, diese zu identifizieren, etwa im Rahmen der Strafverfolgung von Cyberattacken.[451]

179 Wenn nun Behörden im Rahmen ihrer Websites Daten über deren Nutzung erheben, so ist dies aufgrund der Umstände eher mit der dem EuGH vorgelegten Rechtssache als mit der durch das Bundesgericht beurteilten Streitigkeit vergleichbar. Auch im Schweizer Recht gibt es für Behörden Möglichkeiten, aus der IP-Adresse Rückschlüsse zu ziehen. Diese sind indes an strikte Vorgaben gebunden. So werden nach Art. 21 BÜPF die Anbieter von Fernmeldediensten – zu welchen auch die Internetdienstanbieter gehören – verpflichtet, gewisse Randdaten über ihre Kunden aufzubewahren. Diese Daten können der Identifizierung der betroffenen Personen etwa im Fall von Straftaten dienen und müssen unter Umständen dem Dienst für die Überwachung des Post- und Fernmeldeverkehrs weitergegeben werden.[452] Dieser Dienst kann sie wiederum an andere Behörden weitergeben, wenn diese eine Überwachungsmassnahme im Rahmen einer Strafuntersuchung[453] oder des Nachrichtendiensts[454] angefordert haben.

449 Vgl. zum Ganzen: BGE 136 II 508, E. 3.3 f.

450 BGE 136 II 508, E. 3.5.

451 Urteil des EuGH C-582/14 vom 19. Oktober 2016.

452 Vgl. zum Ganzen: Botschaft BÜPF, S. 2732 ff.

453 Vgl. Artikel 269 StPO.

454 Vgl Art. 26 Bundesgesetz über den Nachrichtendienst (Nachrichtendienstgesetz, NDG) vom 25. September 2015.

180 Die einschlägige Literatur ist in der Frage uneinig, ob IP-Adressen im Fall des Webtracking Personendaten darstellen. ROSENTHAL vertritt, dass durch die Speicherung der Daten in Cookies zwar eine Singularisierung vorliegt, sprich die Person von allen anderen unterschieden werden kann. Dies reiche jedoch nicht aus, um die Daten als bestimmbar zu erachten.[455] Andere Autoren gehen davon aus, dass es sich dennoch um Personendaten handelt, weil eine Identifizierbarkeit möglich bleibt.[456]

181 Beim Tracking auf Websites ist mittlerweile verbreitet, dass die IP-Adresse vor der Speicherung um den letzten Bestandteil (das letzte Byte) gekürzt und somit als anonymisiert betrachtet wird.[457] Das Datenschutzrecht kommt nur dann zur Anwendung, wenn es sich bei den erhobenen Daten um Personendaten i.S. von Art. 3 DSG handelt, das heisst um Angaben, durch die eine Person bestimmt oder bestimmbar ist. Die Identität muss sich nicht unmittelbar aus einem Datum ergeben, sondern es reicht aus, dass sich die Identität aus dem Kontext mit anderen Daten ohne unverhältnismässigen Aufwand feststellen lässt.[458] Werden Personendaten anonymisiert, so wird deren Personenbezug irreversibel aufgehoben, womit keine Rückschlüsse auf die betroffene Person mehr möglich sind, ohne dass dafür ein unverhältnismässiger Aufwand betrieben werden müsste. Von der Anonymisierung ist die Pseudonymisierung zu unterscheiden, bei welcher ein Schlüssel aufbewahrt wird, mit dem eine spätere Re-Identifikation möglich ist.[459] Sofern die Daten vor der Verwendung vollständig anonymisiert werden, stellen sie keine Personendaten im Sinne der Datenschutzgesetzgebung mehr dar und können ohne Beachtung von deren Vorgaben verwendet werden. Es ist indes zu beachten, dass auch bei vermeintlich anonymisierten Personendaten unter Umständen mithilfe anderer Daten wieder ein Personenbezug hergestellt werden kann.[460]

182 Nach der hier vertretenen Ansicht bleibt für Behörden eine Identifizierbarkeit von Personen über die IP-Adresse zumindest unter gewissen Umständen möglich, so dass diese als Personendaten betrachtet werden können. Die Tatsache, dass ein Dritter beigezogen werden muss, steht diesem Schluss – wie bereits ausgeführt wurde – nicht grundsätzlich im Weg. Eine Kürzung des letzten Bytes erschwert die Identifizierung auch für den Provider allerdings

455 ROSENTHAL, digma, 2017, S. 197.

456 DATENSCHUTZBEAUFTRAGTER DES KANTONS BASEL-STADT, Anwendbarkeit der EU-Datenschutzgesetzgebung auf Behörden, Einrichtungen und sonstige Stellen des Kantons Basel-Stadt; STEIGER, Anwaltsrevue, 2015, S. 18.

457 Vgl. etwa: die Nutzungsbedingungen der Website des Kantons Zürich, d.h. anstatt z.B. 130.60.184.132 wird nur noch 130.60.184 gespeichert.

458 Vgl. RUDIN, digma, 2012, S. 65.

459 RUDIN, SHK-DSG, Art. 3, N. 13.

460 HÄRTEL, LKV, 2019, S. 55.

in einem solchen Masse, dass sie nicht mehr mit vernünftigem Aufwand möglich ist. Bei diesem Vorgehen ist eher davon auszugehen, dass kein Personenbezug mehr vorhanden ist.

bb) Konsequenzen einer Qualifikation als Personendaten

Eine Qualifikation von IP-Adressen als Personendaten für Webtracking durch Bundes- und kantonale Organe hätte weitreichende Folgen. In erster Linie würde dies dazu führen, dass die Voraussetzungen des Bundes- oder des kantonalen Datenschutzrechts zu beachten sind.[461] Ist eine Person durch ihre IP-Adresse bestimmbar, so können auch die weiteren erhobenen Daten mit dieser Person verknüpft werden. Je nach Einstellung und Komplexität der Software lassen sich auf diese Weise detaillierte Benutzerprofile über die Nutzung der Webseite erstellen, womit gar das Vorliegen eines Persönlichkeitsprofils nach Art. 3 lit. c DSG in Betracht fallen könnte. 183

Wie bereits an verschiedenen Stellen ausgeführt, ist die Bearbeitung von Personendaten durch Bundesorgane nach Art. 17 DSG nur gestützt auf eine gesetzliche Grundlage zulässig, welche zumindest die Grundzüge der Datenbearbeitung regelt. Für die Bearbeitung von Persönlichkeitsprofilen wird grundsätzlich sogar eine ausdrückliche Grundlage in einem formellen Gesetz benötigt.[462] Soweit ersichtlich haben weder Bund noch Kantone eine entsprechende Grundlage geschaffen. Allenfalls könnte hierbei Art. 45c FMG beigezogen werden, gemäss welchem das Bearbeiten von Daten auf fremden Geräten durch fernmeldetechnische Übertragung erlaubt ist, wenn die Benutzerinnen und Benutzer über die Bearbeitung und ihren Zweck informiert und darauf hingewiesen werden, dass sie die Bearbeitung ablehnen können. Die entsprechende Gesetzesbestimmung wurde vor dem Hintergrund eingeführt, dass technische Vorgänge, wie das Speichern und Abrufen von «Cookies», sich unbemerkt zwischen Geräten abspielen, und soll diese Prozesse im Rahmen der oben genannten Voraussetzungen legalisieren.[463] 184

Es wird im Rahmen der soeben vorgestellten Bestimmung als der Informationspflicht genügend erachtet, wenn ein entsprechender Hinweis auf die Datenerhebung in der Datenschutzerklärung niedergeschrieben ist und sich die Speicherung der Cookies deaktivieren lässt. Das schweizerische Recht folgt damit dem «Opt-out»-Prinzip, während das Recht der EU aufgrund der 185

461 Vgl. Erläuterungen des EDÖB zum Einsatz von Webanalysetools für Bundesorgane.

462 Vgl. zum Ganzen: Erläuterungen des EDÖB zum Einsatz von Webanalysetools für Bundesorgane.

463 Botschaft Rev. FMG, S. 7987. Die Regelung gilt zumindest, insoweit die entsprechenden Cookies einen Personenbezug haben, was bei der IP-Adresse – wie soeben ausgeführt – bisher zumindest umstritten ist; vgl. ROSENTHAL, Handkommentar DSG, Art. 45c FMG, N. 7.

Richtlinie 2009/136/EG (sog. «Cookie-Richtlinie») die Verwendung von Cookies nur noch zulässt, wenn die Nutzenden ihre Einwilligung nach vorgängiger Aufklärung erteilen («Opt-in»).[464] Wird Art. 45c FMG als genügende gesetzliche Grundlage betrachtet, so genügt zumindest nach Schweizer Recht der reichlich versteckte Hinweis auf das Tracking und die allfällige Möglichkeit, dieses auszuschalten, wie sie in vielen kantonalen und Bundeswebsites praktiziert wird.[465] Wird die Eignung als gesetzliche Grundlage allerdings verneint, so kann dies allein nicht genügen, um eine Bearbeitung von Personendaten zu rechtfertigen.

186 Zu beachten ist, dass neben der schweizerischen Datenschutzgesetzgebung allenfalls auch die DSGVO zur Anwendung kommt. Wie weiter oben beschrieben, ist die DSGVO gemäss deren Artikel 3 Abs. 2 lit. b extraterritorial anwendbar, wenn eine Datenbearbeitung dazu dient, das Verhalten betroffener Personen zu beobachten, soweit dieses auf dem Gebiet der Europäischen Union stattfindet. Es ist davon auszugehen, dass es hierfür nicht darauf ankommt, ob sich die Website gezielt an Personen in der EU richtet. Dadurch wäre jede Website, auf welcher Cookies auf diese Weise zum Einsatz kommen, von der EU-Datenschutzgesetzgebung erfasst.[466] Dies hat verschiedene Konsequenzen für die Behörde, welche diese Cookies einsetzt. So ist einerseits gemäss Art. 6 DSGVO eine Bearbeitung nur rechtmässig, wenn die Bedingungen dafür erfüllt sind, etwa eine Einwilligung vorliegt (Abs. 1 lit. a), die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt (Abs. 1 lit. e). Die Annahme der letzten Bedingung scheitert wohl daran, dass die Verwendung von Cookies für die Erfüllung einer öffentlichen Aufgabe nicht erforderlich ist, zumal diese Aufgaben in aller Regel auch erfüllt werden können, ohne dass man weiss, wer die Website wie lange besucht hat. Bei Webtracking durch Private wird oft ein überwiegendes, berechtigtes Interesse an der Erhebung der Daten gemäss Art. 6 Abs. 1 lit. f. DSGVO angeführt.[467] Es wird indes davon ausgegangen, dass dieser Rechtfertigungsgrund den Behörden in der Erfüllung ihrer öffentlichen Aufgaben nicht offensteht.[468] Als mögliche Rechtfertigung verbleibt also zumindest für Behörden im Sinne der DSGVO

464 STEIGER, Anwaltsrevue, 2015, S. 18.

465 Viele Websites platzieren diesen etwa auf einer am Ende der Website verlinkten Unterseite «Nutzungsregelungen» oder «Rechtliches», vgl. etwa die Website des Kanton Aargau.

466 DATENSCHUTZBEAUFTRAGTER DES KANTONS BASEL-STADT, Anwendbarkeit der EU-Datenschutzgesetzgebung auf Behörden, Einrichtungen und sonstige Stellen des Kantons Basel-Stadt, S. 5.

467 Vgl. etwa STEIGER, Rechtskonforme Cookies.

468 HEBERLEIN, Ehmann/Selmayr DSGVO, Art. 6, N. 24.

lediglich die Einwilligung. Ob eine konkludente Einwilligung ausreicht oder ob es einer ausdrücklichen Einwilligung bedarf, ist dabei bis anhin noch nicht abschliessend geklärt, wobei auch die oben erwähnte «Cookie-Richtlinie» mangels direkter Anwendbarkeit im nationalen Recht das Problem nicht zu lösen vermag.[469] Dies führt dazu, dass viele Betreiber von Websites eine «aktive» Zustimmung beim ersten Besuch einer Website verlangen, um die Vorgaben der DSGVO sicher zu erfüllen.[470] Zu beachten ist zudem, dass die Anwendung der DSGVO für Schweizer Behörden mit zusätzlichen Rechten für die Privatperson gegenüber den Datenbearbeitenden verbunden ist, welche hier nicht vertieft werden sollen.[471]

187 Weitere Probleme ergeben sich, wenn die Aufbereitung der entsprechenden Daten durch Dritte (i.d.R. die Anbieter des jeweiligen Analysetools) erfolgt. Der EDÖB erachtete dies als Bekanntgabe an Dritte, so dass zusätzlich die Voraussetzungen der Bekanntgabe an Dritte gemäss Art. 19 DSG zu beachten sind.[472] Fraglich ist jedoch, ob es sich dabei nicht vielmehr, wie im deutschen Schrifttum angenommen, um eine Datenbearbeitung im Auftrag handelt.[473] In diesem Fall hätte der Auftraggeber gemäss Art. 10a DSG sicherzustellen, dass der Beauftragte die Daten nur so bearbeitet, wie er dies selber dürfte, und sich an die Grundsätze der Datenbearbeitung (insb. Datensicherheit) hält.[474] Letztlich gilt es zu beachten, dass die Server der wichtigsten Anbieter derartiger Analysedienste, wie etwa «Google Analytics», oftmals im Ausland stationiert sind. Ist dies der Fall, so sind weitere gesetzliche Voraussetzungen zu beachten. Datenbekanntgaben ins Ausland dürfen gemäss Art. 6 DSG nur erfolgen, wenn dort ein angemessener Schutz für diese Daten (etwa vor Zugriffen durch ausländische Behörden) durch eine entsprechende Gesetzgebung oder entsprechende vertragliche Garantien oder eine Einwilligung im Einzelfall gewährleistet ist.[475]

469 RAUER/ETTIG, ZD, 2018, S. 255.

470 RAUER/ETTIG, ZD, 2018, S. 255.

471 So stehen den Betroffenen etwa ein explizites Recht auf Löschung gemäss Art. 17 DSGVO oder das Recht auf Datenportabilität nach Art. 20 DSGVO zu; vgl. DATENSCHUTZBEAUFTRAGTER DES KANTONS BASEL-STADT, Anwendbarkeit der EU-Datenschutzgesetzgebung auf Behörden, Einrichtungen und sonstige Stellen des Kantons Basel-Stadt, S. 7.

472 Vgl. zum Ganzen: Erläuterungen des EDÖB zum Einsatz von Webanalysetools für Bundesorgane.

473 Vgl. SCHRÖDER, S. 165.

474 Vergleichbar für die EU: Art. 28 DSGVO.

475 Gerade in den USA wird der Schutz von Gesetzes wegen als nicht gleichwertig erachtet. Daher müssen sich Unternehmen im Rahmen des «Swiss-US Privacy Shield» zu gewissen Schutzmassnahmen verpflichten, damit eine Datenbekanntgabe möglich ist; vgl. Eidgenössischer Datenschutz-und Öffentlichkeitsbeauftragter, Privacy Shield – das Wichtigste in Kürze.

cc) Fazit

188 Es bleibt festzuhalten, dass der Einsatz von Webtracking vor allem für Behörden aktuell mit erheblicher Rechtsunsicherheit verbunden ist. Umstritten ist bereits, ob es sich bei den erhobenen Daten um Personendaten handelt. Zumindest bei vollständig erhobenen IP-Adressen bestehen grundsätzlich technische Möglichkeiten, die Person dahinter zu identifizieren. Wird das Vorliegen von Personendaten bejaht, so sind nach der hier vertretenen Auffassung sowohl die Vorgaben der schweizerischen Datenschutzgesetzgebung als auch der DSGVO zu beachten. Als gesetzliche Grundlage der Datenbearbeitung kommt im Schweizer Recht Art. 45c FMG in Frage, welcher die Benutzung von «Cookies» von der Einwilligung der Person abhängig macht. Auch das europäische Datenschutzrecht lässt Webtracking nur bei gültiger Einwilligung zu. Ungeklärt ist jedoch bisher, ob diese auch konkludent erfolgen kann oder bei der ersten Abfrage der Website explizit erteilt werden muss. Weitere Voraussetzungen sind zu beachten, wenn die Auswertung durch einen Dritten erfolgt und dieser seinen Sitz im Ausland hat.

189 Will die Behörde aus datenschutzrechtlicher Perspektive auf der sicheren Seite handeln, so ist das Tracking bis zur Klärung der Rechtslage zu unterlassen, auch zumal es für die Erfüllung der öffentlichen Aufgaben nicht zwingend erforderlich ist. Wird es trotzdem durchgeführt, so sollten immerhin zwingend die erhobenen IP-Adressen um den letzten Teil gekürzt werden, da eine Identifizierbarkeit damit kaum mehr mit vertretbarem Aufwand möglich sein dürfte. Wird von einer Unterlassung des Trackings abgesehen, so ist es so datenschutzfreundlich wie möglich auszugestalten. In diesem Falle wäre eine Einwilligung möglichst beim ersten Besuch der Website durch den Nutzenden einzuholen, damit die mutmasslichen Vorgaben des europäischen Rechts erfüllt sind. Im Weiteren sind so wenig Daten wie notwendig zu erheben. Wird zur Analyse ein Programm einer Drittfirma verwendet, so ist dies klar zu kennzeichnen, und es ist sicherzustellen, dass die bearbeitende Stelle sich ebenfalls an die datenschutzrechtlichen Vorgaben hält.

ii) Social Media

190 Nutzt der Staat Social-Media-Plattformen zur Information der Bevölkerung, so stellen sich hinsichtlich der Erhebung von Daten der Benutzer weitere Probleme. Die Behörde tritt – wie bereits angemerkt – als Nutzerin des jeweiligen Netzwerks auf und muss sich dessen Nutzungsbedingungen unterwerfen. Bei der Nutzung dieser Netzwerke überträgt der Benutzer den Betreibern die Nutzungsrechte an einer Vielzahl eigener Daten. Neben offensichtlichen Daten wie Name, Geburtsdatum und E-Mail-Adresse speichern diese Plattformen

etwa, welche Seiten betrachtet oder mit «Gefällt mir» markiert wurden. Dabei hat die Behörde kein Mitbestimmungsrecht darüber, wie die Nutzung der vom jeweiligen Betreiber erhobenen Personendaten datenschutzrechtlich ausgestaltet wird. Die entsprechenden Daten können im Rahmen der Nutzungsbedingungen genutzt werden, um personalisierte Werbeangebote anzuzeigen, und dürfen gegebenenfalls auch an Drittparteien weitergegeben werden.[476] Auch behält es sich Facebook im Rahmen seiner Nutzungsbedingungen vor, Daten an Aufsichts-, Strafverfolgungs- und Vollstreckungsbehörden auf Anfrage bekanntzugeben.[477]

aa) Grundrechtsbindung der Plattformbetreiber

Weiter oben wurde ausgeführt, dass sich auch die Plattformbetreiber grund- 191
sätzlich an die schweizerische Rechtsordnung zu halten haben.[478] Einen wesentlichen Teil dieses Rechts stellen verfassungsmässig gewährten Grundrechte dar. Es ist daher die Frage zu stellen, inwiefern die Plattformbetreiber an diese gebunden sind. Gemäss Art. 35 Abs. 1 BV müssen die Grundrechte in der gesamten Rechtsordnung zur Geltung kommen, was indes nicht bedeutet, dass sie zwingend eine umfassende Rechtswirkung im Sinne eines justiziablen Anspruchs nach sich ziehen.[479] Gemäss Art. 35 Abs. 2 BV binden die Grundrechte in erster Linie den, der staatliche Aufgaben wahrnimmt. Die Plattformbetreiber stellen eine Plattform zur Verfügung, welche der Staat zur Information der Bevölkerung oder zur Kommunikation mit Privaten – und somit in Erfüllung einer staatlichen Aufgabe – benutzen kann. Dadurch erfüllen die Plattformen jedoch nicht bereits eine staatliche Aufgabe, zumal das Bereitstellen dieser Möglichkeit für den Staat auch nicht der Hauptzweck dieser Plattformen darstellt. Als Private sind sie in ihrem Handeln somit grundsätzlich nicht direkt an die Grundrechte gebunden.

Gemäss Art. 35 Abs. 3 BV können die Behörden aber dafür sorgen, dass die 192
Grundrechte im Sinne einer indirekten Horizontalwirkung dort unter Privaten zu beachten sind, wo sie sich dafür eignen. Dies kann insbesondere der Fall sein, wenn zwischen Privaten ein erhebliches Machtgefälle besteht, welches dazu führt, dass Grundrechte beeinträchtigt sein könnten, oder wenn von Privaten besondere Gefährdungen für andere ausgehen.[480] Art. 35 Abs. 3 BV verpflichtet in erster Linie die Behörden. So hat einerseits der Gesetzgeber

476 Vgl. SÖBBING, InTeR, 2018.

477 Vgl. die Datenschutzrichtlinie von Facebook.

478 Siehe oben Rz. 117 ff.

479 WALDMANN, BSK BV, Art. 35, N. 14.

480 SCHWEIZER, SG Komm. BV, Art. 35, N. 48.

dafür zu sorgen, dass private Rechtsbeziehungen grundrechtskonform ausgestaltet sind, und die rechtsanwendenden Behörden haben unbestimmte Rechtsbegriffe grundrechtskonform auszulegen.[481]

193 Für die Betreiber von Social-Media-Plattformen ist daher in erster Linie das Gesetzesrecht verbindlich. Zu denken ist hier etwa an die Datenschutzgesetzgebung, welche auch für Datenbearbeitungen durch Private gilt.[482] Im dritten Abschnitt (Art. 12 ff. DSG) statuiert das Gesetz Regelungen, welche sich an private Datenbearbeiter richten. Eine Datenbearbeitung durch Private kann die Persönlichkeit der betroffenen Person verletzen, wenn die Bearbeitenden die Grundsätze des Datenschutzgesetzes nicht einhalten (vgl. Art. 4, Art. 5 Abs. 1 und Art. 7 Abs. 1 DSG). Eine Persönlichkeitsverletzung kann jedoch gemäss Art. 13 DSG durch die Einwilligung des Verletzten, ein überwiegendes öffentliches Interesse oder das Gesetz gerechtfertigt werden. Von entscheidender Bedeutung ist im vorliegenden Verhältnis die Möglichkeit der Einwilligung: Um soziale Netzwerke benutzen zu können, müssen die Nutzer deren Allgemeine Geschäftsbedingungen akzeptieren, welche in der Regel eine weitgehende Erlaubnis zur Benutzung der eigenen Personendaten enthalten.[483]

194 Wiederholt wurde die Frage aufgeworfen, ob die Einwilligung, welche die Benutzenden durch Akzeptieren der Nutzungsbedingungen erteilen, überhaupt in vollem Masse gültig ist.[484] Problematisch sind dabei vor allem die weitreichenden Befugnisse, welche den Betreibern erteilt werden und deren Umfang für den Benutzer oft kaum ersichtlich ist. Es muss etwa die Frage aufgeworfen werden, ob noch von einer freiwilligen Einwilligung gesprochen werden kann, wenn bei einer Nicht-Einwilligung die Nutzung des Dienstes nicht möglich ist.[485] In diversen Gerichtsurteilen wurden zumindest Teile der Datenverwendung jeweils eingeschränkt. So hat das Landgericht Berlin etwa entschieden, dass die von Facebook vorgesehene, weit formulierte Einwilligungserklärung, gemäss welcher Namen und Profilbild der Nutzer für kommerzielle Inhalte eingesetzt und in die USA weitergeleitet werden dürfen, nicht genügend bestimmt ist. Deshalb könne in diesem Zusammenhang keine freiwillige und in informierter Weise abgegebene Einwilligung angenommen

481 Vgl. WALDMANN, BSK BV, Art. 35, N. 67 f.

482 Vgl. bereits explizit Art. 2 Abs. 1 lit. a DSG.

483 Bericht Social Media 2017, S. 22, wobei aufgrund der weitreichenden Natur hier in verschiedenen Punkten Zweifel an der Gültigkeit dieser Einwilligung bestehen müssen. Vgl. SÖBBING, InTeR, 2018, S. 184. Für die EU ist die Einwilligung etwa in Art. 6 Abs. 1 lit. a DSGVO, für die Schweiz in Art. 13 Abs. 1 i.V.m. Art. 12 Abs. 1 lit. a DSG geregelt.

484 Vgl. Bericht Social Media 2017, S. 24.

485 Indes verhindert nicht jede Einschränkung der Entscheidungsfreiheit eine freiwillige Einwilligung, vgl. BAERISWYL, SHK-DSG, Art. 4, N. 66.

werden.[486] Das deutsche Bundeskartellamt hat Facebook zudem die Zusammenführung von Nutzerdaten aus verschiedenen Quellen untersagt.[487] Auch in Irland, wo der Facebook-Konzern seinen europäischen Hauptsitz hat, sind verschiedene Klagen hängig[488], und im Nachgang des bereits erwähnten «Cambridge Analytica»-Skandals muss Facebook mit einer hohen Bussgeldzahlung rechnen, da es die Daten seiner Benutzenden nicht genügend geschützt haben soll.[489] In der Schweiz fand bisher noch keine gerichtliche Auseinandersetzung darüber statt, ob die Nutzungsbestimmungen von sozialen Medien wie Facebook mit dem geltenden Recht vereinbar sind. Der Social-Media-Bericht des Bundesrats von 2011 erachtete jedoch die Übertragung umfassender Nutzungsrechte an den Plattformbetreiber und die oftmals unklare Verwendung der verwendeten Daten ebenfalls als zumindest problematisch.[490]

bb) Mitverantwortung des Staates

Es soll aufgrund des Fokus der Arbeit eine substanzielle Auseinandersetzung 195
mit der Frage unterlassen werden, ob die Nutzungsbedingungen von Facebook das Schweizer Datenschutzrecht verletzen. Stattdessen soll vielmehr die Frage beantwortet werden, welche Konsequenzen eine Verletzung der Datenschutzbestimmungen durch die Plattformen für den Staat und dessen Nutzung der Plattform hätte. Insbesondere soll die Frage thematisiert werden, ob sich der Staat allenfalls für durch diese Anbieter begangene Persönlichkeitsverletzungen mitverantworten müsste. Aufgrund der Tatsache, dass er die entsprechenden Dienstleistungen zur Erfüllung einer staatlichen Aufgabe nutzt, kann zumindest die Annahme geäussert werden, dass die Verwaltung die Personendaten jener Privaten, die mit ihr über soziale Medien in Kontakt treten wollen, einer erhöhten Missbrauchsgefahr aussetzt.

Aus zivilrechtlicher Sicht ist diese Frage vergleichsweise einfach zu be- 196
antworten, da grundsätzlich jeder, der an einer Persönlichkeitsverletzung mitwirkt, für seinen Beitrag daran zur Verantwortung gezogen werden kann.[491] Der Begriff der Mitwirkung ist dabei weit zu verstehen.[492] Das Datenschutzgesetz konkretisiert in Art. 12 – wie weiter oben bereits erwähnt –, dass eine

486 Urteil des Landgerichts Berlin Az. 16 O 341/15 vom 16. Januar 2018.

487 Vgl. BUNDESKARTELLAMT.

488 DPA, Irische Datenschützer: Sieben Verfahren gegen Facebook, heise Online, 2. Februar 2019.

489 KANG, F.T.C. Approves Facebook Fine of About $5 Billion, The New York Times, 12. Juli 2019.

490 Vgl. Bericht Social Media 2017, S. 15 ff.

491 ROSENTHAL, Jusletter, 17. Juni 2019, N. 13.

492 MEILI, BSK ZGB I, Art. 28, N. 37.

Datenbearbeitung die Persönlichkeit des Betroffenen verletzen kann, wenn Personendaten ohne Rechtfertigungsgrund oder entgegen der Datenbearbeitungsgrundsätze bearbeitet oder bekanntgegeben werden. Die Rechtfertigungsgründe sind dabei in Art. 13 DSG zu finden, wobei für die Datenbearbeitung durch die Plattformbetreiber die Einwilligung durch Akzeptieren der Nutzungsbedingung einschlägig, aber gerade auch (wie soeben dargestellt) umstritten sein kann.

197 Das schweizerische Datenschutzrecht schliesst die Rechte und Pflichten bei der Datenbearbeitung und Datenbekanntgabe daran an, wer der «Inhaber einer Datensammlung» ist (vgl. etwa Art. 8 Abs. 1 DSG). Der Begriff ist in Art. 3 Bst. i DSG definiert und umfasst diejenigen Privatpersonen oder Bundesorgane, die über den Zweck und den Inhalt der Datensammlung entscheiden. Dadurch soll sichergestellt werden, dass Betroffene bei der Durchsetzung ihrer Rechte denjenigen zur Ansprechperson haben, welcher die zur Einhaltung des Datenschutzes nötigen Parameter einer Datenbearbeitung festlegen kann.[493] Über den Zweck entscheidet derjenige, welcher die Datenbearbeitung veranlasst hat und deren Ziel bestimmt.[494] Im Unterschied dazu ist der Auftragsbearbeiter zu sehen, welcher eine Datenbearbeitung, über die von seinem Auftraggeber entschieden wurde, nur noch ausführt.[495] Hinsichtlich der eingesetzten Mittel wird derjenige als verantwortlich angesehen, der darüber entscheidet, in welcher Art und Weise ein Ergebnis oder Ziel erreicht werden soll.[496] Dabei geht es insbesondere darum, wie die datenschutzrechtlich relevanten Faktoren einer Datenbearbeitung ausgestaltet sein sollten.[497]

198 Eine generelle Mitverantwortlichkeit des Staates ist nach dem Geschriebenen aus verschiedenen Gründen abzulehnen. Der Staat entscheidet bei den Datenbearbeitungen durch die Plattformen in der Regel weder über deren Zweck noch deren Inhalt. Diese Entscheidungen treffen die Plattformbetreiber allein. Ebenfalls zu beachten bleibt, dass der Zugriff auf die jeweiligen Fanseiten auch ohne Registrierung möglich ist. Es ist also niemand gezwungen, sich den Nutzungsbedingungen der Betreiber zu unterwerfen, um Zugriff auf die durch staatliche Stellen verbreiteten Informationen auf der Plattform zu erhalten. Aus diesem Grund ginge es zu weit, die Behörden in genereller Weise für das Datenschutzregime einer Plattform und daraus resultierende Persönlichkeitsverletzungen (mit)verantwortlich zu machen. Problematisch wäre

493 ROSENTHAL, Jusletter, 17. Juni 2019, N. 14.

494 ARTIKEL-29-DATENSCHUTZGRUPPE, Opinion 1/2010, S. 11.

495 ROSENTHAL, Jusletter, 17. Juni 2019, N. 16.

496 ARTIKEL-29-DATENSCHUTZGRUPPE, Opinion 1/2010, S. 17.

497 Etwa Speicherungsdauer, vgl. ROSENTHAL, Jusletter, 17. Juni 2019, N. 33.

es lediglich, wenn der Staat auf eine Plattform zurückgriffe, welche in offensichtlicher und grober Weise gegen das schweizerische Datenschutzrecht verstossen würde.[498] Auch wenn – wie soeben ausgeführt – gewisse Zweifel an der Datenschutzkonformität etwa von Facebook bestehen, liegt hinsichtlich der bekanntesten Plattformen wohl jedenfalls keine offensichtliche Datenschutzverletzung vor.

cc) Datenbearbeitung für den Staat

Während eine generelle Verantwortlichkeit des Staates für Datenbearbeitungen durch die Anbieter von sozialen Medien nach dem soeben Geschriebenen generell abgelehnt werden kann, gibt es Fälle, in denen der Staat ursächlich für eine bestimmte Datenbearbeitung oder -bekanntgabe durch die Plattformbetreiber ist, diese also ohne staatliches Zutun nicht oder nicht im selben Masse erfolgen würde. So kann die öffentliche Verwaltung unter Umständen auf Daten von Facebook und anderen Betreibern zurückgreifen. Es stellt sich die Frage, ob der Staat zumindest in diesen Fällen für allfällige Persönlichkeitsverletzungen durch Datenbearbeitungen im Sinne des Datenschutzgesetzes mitverantwortlich ist. 199

Denkbar ist etwa, dass Behörden Plattformbetreiber von Gesetzes wegen verpflichten können, gewisse Daten zu speichern, um diese den Behörden im Bedarfsfalle (etwa im Rahmen der Strafverfolgung) zukommen zu lassen. Anderseits stellt Facebook den Inhabern von Fanseiten unabdingbar und kostenlos das Tool «Facebook Insights» zur Verfügung, welches statistische Informationen zu den Besuchenden ihrer Seite auswertet und dadurch ermöglicht, das Nutzerverhalten zu analysieren.[499] Die «Fanseite» ist in der Regel sowohl für Facebook-Nutzer abrufbar als auch für Besucher, die keinen Facebook-Account haben. Beim Besuch der entsprechenden Seite werden durch das soziale Netzwerk verschiedene Nutzerdaten in einem «Cookie» gespeichert.[500] Die Betreiber von Fanseiten haben dabei ein gewisses Mitbestimmungsrecht, welche Daten für sie wichtig sind und erhoben oder ausgewertet werden sollen.[501] 200

• *Datensammlung für Behörden*

In den letzten Jahren wurden in gewissen Gesetzen entsprechende Pflichten geschaffen, welche auch die Anbieter von sozialen Medien betreffen und diese 201

498 LANGER, AJP, 2014, S. 954.

499 HOFFMANN/SCHULZ/BRACKMANN, ZD, 2013, S. 123.

500 HÄRTING/GÖSSLING, NJW, 2018, S. 2523 f.

501 Vgl. Urteil des EuGH C-210/16 vom 5. Juni 2018, E. 36.

verpflichten können, gewisse Daten an staatliche Stellen weiterzugeben. So hat z.B. Facebook als abgeleiteter Kommunikationsdienst i.S. von Art. 2 lit. c. BÜPF zu gelten, was zur Folge hat, dass der Betreiber Überwachungen durch den Dienst Überwachung Post- und Fernmeldeverkehr dulden und den Behörden Randdaten liefern muss.[502] Unter Umständen kann diese Verpflichtung sogar weiter gehen.[503] Plattformbetreiber wie z.B. Facebook sehen bereits in ihren Nutzungsbedingungen vor, dass Social-Media-Plattformen auf Anfrage hin Daten über Nutzende an Strafverfolgungs- oder Vollstreckungsbehörden weitergeben können.[504]

202 Es ist indes fraglich, ob eine derartige Datenbearbeitung überhaupt eine Persönlichkeitsverletzung darstellt. Selbst wenn die Einwilligung in die entsprechende Datenbearbeitung und -bekanntgabe als nicht zulässig erachtet werden sollte, ist es wahrscheinlich, dass einer der weiteren Rechtfertigungsgründe greift. So ist gemäss Art. 13 DSG eine Rechtfertigung möglich, wenn ein Gesetz die Bearbeitung von Personendaten vorsieht. In diesem Falle hat der Gesetzgeber die Abwägung zwischen den öffentlichen und den privaten Interessen an der Datenbearbeitung vorgenommen.[505] Auch falls eine Datenbekanntgabe im Ausnahmefall nicht gesetzlich verankert sein sollte, kann sie zumindest in Einzelfällen gestützt auf ein überwiegendes öffentliches Interesse gerechtfertigt sein.[506]

203 Staaten fragen dabei internationale Anbieter in vermehrtem Masse direkt nach Daten zur Verwendung in Verwaltungs- oder Strafverfahren an.[507] Zu beachten ist an dieser Stelle, dass Facebook in der Praxis gegenüber den Anfragen von Behörden eine restriktive Haltung einnimmt und Anfragen oftmals auch ablehnt.[508] Sofern sich der Plattformanbieter auf den Standpunkt stellt, die entsprechenden Daten nicht herausgeben zu müssen, kann er unter Umständen rechtlich zur Herausgabe verpflichtet werden.[509] Dies

502 Vgl. dazu explizit Botschaft BÜPF, S. 2708.

503 Vgl. etwa HANSJAKOB, N. 1381.

504 Vgl. etwa die Nutzungsbedingungen von Facebook.

505 RAMPINI, BSK DSG/BGÖ, Art. 13, N. 15.

506 Dies ist indes hinsichtlich privater Bearbeiter nur mit Zurückhaltung anzunehmen, vgl. RAMPINI, BSK DSG/BGÖ, Art. 13, N. 47.

507 ALTWICKER, in: Migration, Datenübermittlung und Cybersicherheit, S. 124. Daraus ergeben sich spannende völkerrechtliche Fragen, welche an dieser Stelle nicht im Fokus stehen sollen; für eine eingehendere Behandlung siehe ALTWICKER, in: Migration, Datenübermittlung und Cybersicherheit.

508 GYR, Für die Staatsanwaltschaften liefert Facebook wenig Daten, Neue Zürcher Zeitung, 15. April 2018, mit Verweis auf den Facebook Transparency-Report.

509 Als Rechtsgrundlage dient dabei z.B. das Übereinkommen über Cyberkriminalität des Europarats (CCC); vgl. BGE 141 IV 108, E. 4.3 ff.; ALTWICKER, in: Migration, Datenübermittlung und Cybersicherheit, S. 107 ff.

ist jedoch aufgrund des Territorialitätsprinzips ebenfalls mit Schwierigkeiten verbunden.[510] So ist etwa ein direktes Editionsbegehren an eine im Ausland domizilierte Anbieterin über die Herausgabe der Randdaten nicht zulässig.[511] Ebenso wenig können Daten bei der Schweizer Vertretung von Facebook herausverlangt werden, wenn die Datenhoheit beim europäischen Sitz der Firma liegt.[512] In diesen Fällen ist der langwierigere Weg über die internationale Rechtshilfe zu beschreiten.[513]

• *Facebook Insights*

Im Rahmen der Facebook Insights stellt Facebook den Anbietern von Fanseiten, wie sie auch staatliche Stellen grundsätzlich betreiben, unentgeltlich und unabdingbar gewisse statistische Auswertungen zur Verfügung. Diese Daten werden dem Betreiber der Fanseite anonymisiert und aufgearbeitet zur Verfügung gestellt. Auch wenn der Betreiber der Fanseite somit keine Rückschlüsse auf die jeweiligen Besuchenden ziehen kann, ist es zumindest für Facebook möglich, die Betroffenen zu identifizieren. Dies reicht aus, um das Vorliegen personenbezogener Daten anzunehmen.[514] 204

Auch hier stellt sich die Frage, ob überhaupt eine Persönlichkeitsverletzung vorliegt. Im Gegensatz zur Datenbekanntgabe an Behörden im Rahmen von Verfahren ist hier keine gesetzliche Pflicht ersichtlich. Facebook sieht in seinen Nutzungsbedingungen vor, dass die Daten der Benutzenden zu zusammengefassten Statistiken und Einblicken aufbereitet werden dürfen, um Personen und Unternehmen Aufschluss über die Nutzung ihres Angebots zu ermöglichen.[515] Nach dem bereits Ausgeführten ist fraglich, ob diese weitreichende Einwilligung den Anforderungen von Art. 4 Abs. 5 DSG genügt, um eine Persönlichkeitsverletzung zu rechtfertigen.[516] Allenfalls könnte mit dem öffentlichen Interesse argumentiert werden, dass der Staat durch die Auswertungen seine Dienstleistung verbessern könne. Selbst wenn dies angenommen wird, ist indes kaum davon auszugehen, dass dies die privaten Interessen der Betroffenen überwiegen kann. 205

510 GRAF, Jusletter IT, 21. September 2017, N. 26; ALTWICKER, in: Migration, Datenübermittlung und Cybersicherheit, S. 120 f.

511 BGE 141 IV 108, 5.2. ff.

512 Vgl. BGE 143 IV 21.

513 Zusammenfassung von BGE 141 IV 108 ff. E. 5.3 und 5.5 in Urteil des Bundesgerichts 1B_29/2017 vom 24. Mai 2017 E. 4.7; ferner ROTH, Jusletter 17. August 2015, N. 30.

514 Urteil des EUGH C-210/16 vom 5. Juni 2018, E. 38.

515 Vgl. etwa die Datenrichtlinie von Facebook.

516 Siehe oben Rz. 194.

206 Dadurch, dass der Staat eine Fanseite betreibt, profitiert er davon, dass die Plattform gewisse Daten auch für ihn erhebt und aufbereitet. Die entsprechende Datenaufbereitung durch Facebook ist dabei nicht optional. Facebook würde die Daten entsprechend nicht im selben Masse bearbeiten und bekanntgeben, wenn der Staat keine Fanseite anbieten würde. Schliesslich hat der Staat zumindest ein Mitbestimmungsrecht, welche Daten für ihn in diesem Rahmen erhoben werden sollen. Unter diesen Voraussetzungen kann dem Staat eine Mitverantwortung für allfällige Verletzungen durch missbräuchliche Datennutzungen der Anbieter zumindest nicht von vorneherein abgesprochen werden.

207 Wie bereits ausgeführt, wird die datenschutzrechtliche Verantwortlichkeit dadurch bestimmt, wer über den Zweck und den Inhalt der Datensammlung bestimmen kann. Dies ist indes nicht immer einfach zu bestimmen, gerade in Konstellationen wie der vorliegenden. Das staatliche Organ kann, wenn es eine Fanseite auf Facebook eröffnet, gewisse Parameter festlegen, nach welchen es die Auswertung der Daten erhalten möchte. Die Datenbearbeitung verbleibt hingegen in erheblichem Masse bei Facebook, welches weitgehende Autonomie geniesst und nicht durch die Weisungen des Betreibers der Fanseite gebunden ist. In derartigen Fällen muss auch derjenige, welcher die Daten für jemand anderen bearbeitet, nicht bloss als Auftragsbearbeiter, sondern ebenfalls als Verantwortlicher angesehen werden.[517]

208 Es ist möglich, dass mehrere Einrichtungen gemeinsam für eine Datenbearbeitung verantwortlich sind, wenn die oben genannten Anforderungen für sie jeweils separat erfüllt sind.[518] Während in der Schweiz bisher – soweit ersichtlich – keine Rechtsprechung zur gemeinsamen Verantwortlichkeit ergangen ist, hatte der EuGH sich damit zu befassen, ob das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) den privaten Betreiber einer Fanseite wegen der mutmasslich widerrechtlichen Erhebung der Daten anweisen durfte, die Facebook-Seite einzustellen. Dabei befand das Gericht, dass Seitenbetreiber auf Facebook gemeinsam mit der Anbieterin für die entsprechende Bearbeitung von Daten verantwortlich sind.[519] Der Gerichtshof begründete dies damit, dass der Betreiber durch die von ihm vorgenommene Definition der Zielgruppe und der zu erhebenden Statistiken zur Datenbearbeitung beiträgt. Keine Rolle spiele demgemäss, dass der Betreiber der Fanseite die Daten nur in anonymisierter Form erhalte, da er bereits

517 ROSENTHAL, Jusletter, 17. Juni 2019, N. 34.

518 ROSENTHAL, Jusletter, 17. Juni 2019, N. 77.

519 Vgl. Urteil des EuGH C-210/16 vom 5. Juni 2016.

durch den Betrieb der Seite am Entscheid über Zwecke und Mittel der Verarbeitung der personenbezogenen Daten beteiligt ist.[520]

Dies hat nach dem Geschriebenen auch für die Schweiz zu gelten. Dadurch, dass die Betreiber einer Facebook-Fanseite über die wesentlichen Parameter bestimmen können, kontrollieren sie einerseits den damit verfolgten Zweck und anderseits auch die verwendeten Mittel (also welche Daten durch Facebook ausgewertet werden) und sind damit mindestens als mitverantwortlich zu betrachten.[521] Anders wäre dies allenfalls zu beurteilen, wenn Facebook für alle Fanpages dieselben Statistiken führen würde und die Behörde nur bestimmen könnte, welche davon ihr angezeigt werden, da sie auf diese Weise keinen wesentlichen Einfluss mehr auf die Datenbearbeitung hätte.[522] 209

Auch wenn das Urteil des EuGH in erster Linie private Anbieter behandelt, sprechen gute Gründe dafür, dass die daraus abgeleiteten Folgen auch für staatliche Auftritte zu gelten haben. Der Staat bleibt auch bei seinem Auftritt in den sozialen Medien an die Grundrechte gebunden.[523] Da sich die jeweilige Behörde bewusst zur Aufgabenerfüllung der Dienste der Social-Media-Plattformen bedient, ist ihr auch der durch den Betrieb ihres Auftritts vermittelte Eingriff in die informationelle Selbstbestimmung mit zuzurechnen.[524] Aktuell herrscht indes noch Uneinigkeit darüber, was das Urteil des EuGH für die Betreibenden bestehender Fanseiten zu bedeuten hat. Einige Autoren gehen davon aus, dass der Betrieb von Facebook-Fanseiten ohne eine den Anforderungen von Art. 26 DSGVO genügende Vereinbarung rechtswidrig ist[525], während andere zuerst das Urteil des deutschen Bundesverfassungsgerichts in der Sache abwarten, da sich der Europäische Gerichtshof in seinem Urteil lediglich zur Frage der Mitverantwortung, jedoch nicht zur Rechtmässigkeit der Datenbearbeitungen durch Facebook an sich geäussert hat.[526] 210

Wird eine Mitverantwortung des Verwaltungsorgans, welches eine entsprechende Seite betreibt, bejaht, so ist die eidgenössische oder kantonale Datenschutzgesetzgebung zu beachten. Diese fordert für jede Datenbearbeitung durch Bundesorgane gemäss Art. 17 DSG eine gesetzliche Grundlage. 211

520 Vgl. Urteil des EuGH C-210/16 vom 5. Juni 2018, E. 36 ff.

521 ROSENTHAL, Jusletter, 17. Juni 2019, N. 73.

522 Vgl. zum Ganzen: ROSENTHAL, Jusletter, 17. Juni 2019, N. 74.

523 Siehe oben Rz. 122.

524 Vgl. zum Ganzen: ENGELER, MMR, 2017, S. 655.

525 Vgl. STEIGER, Online-Beitrag vom 10. September 2018, mit Einschränkungen auch HEMMERT-HALSWICK, MMR-Aktuell, 2018. Inzwischen ist eine solche verfügbar; vgl. etwa FACEBOOK, Informationen zu Seiten-Insights. Für eine detailliertere Auseinandersetzung mit Art. 26 DSGVO siehe sogleich Rz. 213.

526 Vgl. etwa HÄRTING/GÖSSLING, NJW, 2018, S. 2526; SCHWENKE, Keep calm and carry on, heise Online, 25. November 2018.

Für eine derart weitgehende Datenbearbeitung, wie diese bei der Aufbereitung der Daten durch den Plattformbetreiber geschieht, wird sich im geltenden Recht kaum eine Grundlage finden lassen. Eine gesetzliche Grundlage, welche die entsprechende Datenbearbeitung rechtfertigen könnte, wäre zumindest anzudenken.[527] Es ist allerdings aufgrund des grossen Umfangs der durch diese Regelung zu erfassenden Daten m.E. fraglich, ob dies wirklich zielführend und realisierbar ist. Ob die Betroffenen wirksam in die Datenbearbeitung einwilligen können, ist nach dem eingangs in diesem Kapitel Geschriebenen zumindest zweifelhaft. Zudem ist zu beachten, dass eine Einwilligung nach der in dieser Arbeit vertretenen Auffassung die gesetzliche Grundlage nicht zu ersetzen vermag.[528]

212 Sollte eine entsprechende weite gesetzliche Grundlage jemals verabschiedet werden, ist darin im Hinblick auf die gemeinsame Verantwortlichkeit insbesondere zu klären, wer für die Wahrnehmung der gesetzlichen Pflichten (Auskunftsrecht, Berichtigungsrecht) verantwortlich ist. Da der Staat die entsprechenden Daten nicht selbst bearbeitet, kann er die Erfüllung dieser Ansprüche nicht eigenständig gewähren, sondern ist auf die Kooperation des Plattformbetreibers angewiesen, da dieser die Datenhoheit innehat. Das Datenschutzgesetz regelt die Möglichkeit mehrerer Verantwortlicher und deren Konsequenzen nur rudimentär in Artikel 16. Demgemäss ist dasjenige Bundesorgan verantwortlich, welches die Personendaten in Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt. Absatz 2 dieser Bestimmung sieht vor, dass bei einer gemeinsamen Bearbeitung durch Bundesorgane und Private der Bundesrat die Kontrolle und Verantwortung regeln kann.[529] In der EU schreibt Art. 26 Abs. 2 DSGVO vor, dass die gemeinsam Verantwortlichen in solchen Konstellationen in einer Vereinbarung in transparenter Form festlegen, wer die sich aus der DSGVO ergebenden Pflichten erfüllt (etwa Informationspflichten oder Auskunftspflichten). Das Schweizer Recht sieht de lege lata keine vergleichbare Regelung vor, gemäss welcher vertraglich ausgemacht werden kann, welcher der gemeinsam Verantwortlichen die Erfüllung dieser gesetzlichen Pflichten übernimmt. Auch der Entwurf zur Totalrevision des Datenschutzgesetzes sieht in dieser Hinsicht keine Neuerung vor, wird doch Art. 16 DSG mit lediglich redaktionellen Änderungen in Art. 29 E-DSG überführt.[530]

527 Vgl. ENGELER, MMR, 2017, S. 655.

528 Für eine ausführlichere Diskussion, ob das öffentliche Zugänglichmachen von Daten auf Social Media eine wirksame Einwilligung in die Datenbearbeitung darstellt, siehe weiter unten Rz. 386.

529 Auch viele Kantone sehen analoge Regelungen vor, vgl. etwa Art. 7 IDG BL, Art. 5 Abs. IDG ZH.

530 Botschaft Rev. DSG 2017, S. 7078.

dd) Fazit

Die meisten Social-Media-Plattformen erheben im Rahmen ihrer Nutzungsbedingungen eine grosse Menge an Daten über ihre Nutzer. Der Staat kann, auch wenn er eine eigene Präsenz auf diesen Plattformen unterhält, nicht grundsätzlich für deren Datenbearbeitungen verantwortlich gemacht werden, da er weder über den Zweck noch den Inhalt dieser Datenbearbeitungen eine direkte oder indirekte Gestaltungsmacht hat. Indes werden gewisse Daten durch die Plattformbetreiber für den Staat erhoben. Handelt es sich dabei um Daten, welche die Betreiber aufgrund von Gesetzespflichten erheben müssen, so ist diese Bearbeitung gerechtfertigt im Sinne des Datenschutzgesetzes. Problematisch ist jedoch die von Facebook zur Verfügung gestellte, nicht deaktivierbare Möglichkeit, im Rahmen des Betriebs einer Fanseite gewisse Nutzerdaten zu erheben und auszuwerten. Zwar erfolgt die Sammlung und Aufbereitung der Daten durch den Plattformbetreiber, doch kann der Betreiber einer Fanseite bestimmen, nach welchen Parametern diese geschehen soll. Der Staat muss im Rahmen dieser Bearbeitung als zumindest mitverantwortlich erachtet werden. Dies führt dazu, dass unter anderem eine gesetzliche Grundlage gemäss Art. 17 DSG für diese Bearbeitung bestehen müsste. 213

Da aktuell keine derartige Grundlage ersichtlich ist, müssten staatliche Stellen vom Betrieb einer Facebook-Fanpage absehen. Es fragt sich allerdings, ob dies praktikabel ist. Die andere Möglichkeit wäre es, auf Facebook als Anbieter dergestalt einzuwirken, dass zumindest für gewisse Seiten auf die Erhebung der «Facebook Insights» verzichtet oder diese Option deaktivierbar gemacht wird.[531] Aus der gemeinsamen Verantwortlichkeit ergeben sich weitere Pflichten, etwa betreffend die Rechte der Betroffenen gemäss der Datenschutzgesetzgebung, deren Gewährung – im Rahmen einer entsprechenden Gesetzesgrundlage oder einer vertraglichen Vereinbarung – zu klären wäre. Sollten die Behörden dennoch ein entsprechendes Profil betreiben wollen, müssen sie sich der fehlenden gesetzlichen Grundlage und Regelung der Verantwortlichkeit zumindest bewusst sein und die Benutzer des Angebots soweit möglich darauf hinweisen. Auch unter diesem Gesichtspunkt muss der Staat sicherstellen, dass seine Informationstätigkeit weiterhin zusätzlich über andere Kanäle erbracht wird und kein Zwang zur Nutzung einer bestimmten Plattform besteht.[532] 214

531 Vgl. SCHWENKE, Keep calm and carry on, heise online, 25. November 2018.

532 HOFFMANN/SCHULZ/BRACKMANN, ZD, 2013, S. 126.

3. Weitere betroffene Grundrechtspositionen

215 Der Staat hat in seiner Informationstätigkeit – wie bereits aufgezeigt wurde – einen weiten Ermessensspielraum. Durch die relativ grosse Freiheit läuft die behördliche Informationstätigkeit auch Gefahr, in Grundrechtspositionen einzugreifen. Denkbar sind etwa Einschränkungen der Wirtschaftsfreiheit (Art. 27 BV) durch Warnungen der Behörden, welche Auswirkungen auf den Wettbewerb haben, oder Einschränkungen der Wahl- und Abstimmungsfreiheit (Art. 34 BV) durch behördliche Information in Wahlen und Abstimmungen. Bei diesen Grundrechtspositionen ist die Gefahrenlage jedoch vergleichbar, wenn die Information im Internet oder offline erfolgt, so dass im Rahmen dieser Arbeit nicht weiter darauf eingegangen werden soll. Konkrete Fragen ergeben sich auch hinsichtlich des aus Art. 9 BV abgeleiteten Anspruchs, von staatlichen Organen nach Treu und Glauben behandelt zu werden. Hier lässt sich insbesondere fragen, inwiefern der Staat durch im Internet getätigte Aussagen gebunden ist und für diese haften muss. Dies soll jedoch im späteren Verlauf der Arbeit behandelt werden.[533]

4. Information ausschliesslich über das Internet

216 Nach dem soeben Ausgeführten ist es grundsätzlich zulässig, dass Behörden auch online die Bevölkerung informieren. Zum Zeitpunkt dieser Arbeit informieren viele Behörden in der Regel mehr oder minder zeitgleich online und analog (etwa über Medienmitteilungen und -konferenzen). Durch diese Doppelspurigkeit entstehen dem Staat in der Regel Zusatzkosten, etwa weil Medienkonferenzen abgehalten oder Druckerzeugnisse für die amtliche Publikation hergestellt werden müssen.[534] Entsprechende Kosten könnten eingespart werden, indem die jeweilige Information nur noch über das Internet als mittlerweile wohl verbreitetster und weitreichendster Informationskanal zur Verfügung gestellt wird. Soweit ersichtlich verzichtet kein Kanton im Rahmen seiner allgemeinen Informationstätigkeit gänzlich auf die herkömmlichen Kommunikationswege. Vielmehr handelt es sich bei Websites und sozialen Medien aktuell um freiwillige Zusatzangebote.[535] Die wichtigen Informationen stehen den Betroffenen in der Regel auch offline, etwa über die Zeitung oder das Fernsehen, zur Verfügung. Es wird davon ausgegangen, dass höchstens weniger wichtige Informationen (etwa das Teilen von Land-

533 Siehe dazu unten Rz. 278 ff. und 287 ff.

534 Vgl. zu den Kosten des Bundesblatts etwa: Botschaft Rev. PublG, S. 7069.

535 Vgl. aber die Bestimmung von Art. 6 Abs. 3 BGÖ, gemäss der im Internet zugängliche Daten als veröffentlicht im Sinne des BGÖ gelten. Für eine vertiefte Auseinandersetzung mit dieser Bestimmung unter dem Aspekt von Art. 8 Abs. 2 BV siehe sogleich Rz. 241 ff.

schaftsbildern aus dem jeweiligen Kanton als Werbung) ausschliesslich über Internet-Kanäle erfolgen können, wobei hier in Frage gestellt werden darf, ob dies noch Teil des staatlichen Informationsauftrags darstellt.[536]

Indes verzichten einige Kantone bereits in gewissen Rechtsbereichen zu- 217
gunsten der Online-Publikation auf anderweitige Kanäle und publizieren etwa ihr Amtsblatt nur noch im Internet.[537] Argumentiert wird dabei mit den veränderten Nutzungsgewohnheiten, welchen zufolge das bereits online angebotene Amtsblatt in den jeweiligen Kantonen von der grossen Mehrheit auch auf diesem Weg konsultiert wird und nur noch wenige Personen das Amtsblatt in Papierform abonnieren. So hatte etwa das Amtsblatt des Kantons Zürich zuletzt bei 700'000 Haushalten auf dem Kantonsgebiet eine Abonnentenzahl von lediglich ca. 1'600, wovon die Mehrzahl zudem Behörden von Kantonen und Gemeinden waren.[538] Aus diesem Grund sieht der Kanton Zürich seit dem 1. Januar 2018 vor, dass das Amtsblatt auf der Internetsite des Kantons erscheinen soll, während die Papierversion lediglich noch fakultativ ist (§ 15 Abs. 1 und Abs. 3 PublG ZH). In der dazugehörenden Publikationsverordnung werden weitere Punkte zur Erscheinungsweise, insbesondere zu den Publikationsdaten, zum Datenschutz und zur Integrität geregelt. Im Folgenden soll untersucht werden, inwiefern die ausschliessliche Online-Publikation des Amtsblatts rechtlich zulässig ist. Ob eine alle Bereiche umfassende, ausschliessliche Online-Informationstätigkeit rechtlich zulässig ist, soll dagegen an späterer Stelle vertieft betrachtet werden.[539]

a) Diskriminierungsverbot

Gemäss Art. 8 Abs. 2 BV darf niemand diskriminiert werden, namentlich nicht 218
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. Diese Aufzählung sensibler Merkmale nach Art. 8 Abs. 2 BV wird als nicht abschliessend betrachtet, jedoch hat eine verbotene Diskriminierung an persönliche Eigenschaften anzuknüpfen, die nicht oder nur schwer abänderbar sind.[540] In der Schweiz ist das Internet zwar augenscheinlich weit verbreitet, aber es steht aus verschiedenen Gründen noch

536 Vgl. Zum Ganzen: LANGER, AJP, 2014, S. 952.

537 Etwa die Kantone ZH und AG; dazu sogleich ausführlicher Rz. 220 ff.

538 Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 4.4.1, ähnliche Verhältnisse bestehen auch bei den amtlichen Publikationen des Bundes; vgl. Botschaft Rev. PublG, S. 7061.

539 Siehe dazu unten Rz. 485 ff.

540 SCHWEIZER/BIGLER-EGGENBERGER/KÄGI-DIENER, SG Komm. BV, Art. 8, N. 62.

nicht der gesamten Bevölkerung offen.[541] Personen ohne Internetzugang können durchaus benachteiligt sein, wenn eine staatliche Dienstleistung im Internet angeboten wird, sie können allerdings nach dem soeben Geschriebenen richtigerweise nicht als im Rahmen von Art. 8 Abs. 2 BV besonders geschützte Gruppe betrachtet werden.[542] Es bleibt zu beachten, dass etwa bei Personen in älteren Bevölkerungsschichten die Internetnutzung und das entsprechende Know-how noch wenig verbreitet sind und mit zunehmendem Alter rapide abnehmen.[543] Entsprechendes hat umso mehr für Smartphones oder die Social-Media-Nutzung zu gelten. Je nach Ausgestaltung der entsprechenden Webangebote ist auch denkbar, dass diese Personen aufgrund von Behinderungen[544] oder der Sprache weniger gut offenstehen.[545]

219 Mit der Frage, ob eine Umstellung auf eine reine Online-Publikation rechtlich unter dem Aspekt des Diskriminierungsverbots zulässig ist, hatte sich anhand dieser und anderer Regelungen auch das Bundesgericht zu befassen. Es erachtete es als zutreffend, dass ältere Personen bei der Verwendung von elektronischen Geräten mehr Mühe haben und daher durch die entsprechende Regelung stärker als andere Bevölkerungsgruppen betroffen sein können. Indes führte es aus, dass wohl bereits vor dem Erlass der Regelung in Anbetracht der geringen Abonnentenzahlen der kleinste Teil der älteren Bevölkerung die gedruckte Form des Amtsblatts abonniert und zuhause konsultiert hatte. Zudem merkte es an, dass mit zunehmender Etablierung des Internets und fortschreitender Zeitdauer die erforderlichen Kompetenzen auch im älteren Bevölkerungsteil wachsen würden. Damit die Beschränkung des Zugangs zu staatlichen Aktivitäten oder Informationen indes nicht zu einem möglichen Verlust der Teilnahmemöglichkeiten der Betroffenen an staatlichen Entscheiden führt, müssten für diese Ausweichmöglichkeiten vorgesehen werden.[546]

220 Die Regelung im Kanton Zürich, welche das Bundesgericht zu beurteilen hatte, statuiert in Art. 15 Abs. 3 PublG ZH, dass das Amtsblatt nach wie vor

541 Siehe dazu bereits oben Rz. 146.

542 Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 5.4.

543 Vgl. BFS, S. 1.

544 Der Begriff soll hier und im weiteren Verlauf der Arbeit im Sinne des Behindertengleichstellungsgesetzes verwendet werden und bedeutet «eine Person, der es eine voraussichtlich dauernde körperliche, geistige oder psychische Beeinträchtigung erschwert oder verunmöglicht, alltägliche Verrichtungen vorzunehmen, soziale Kontakte zu pflegen, sich fortzubewegen, sich aus- und weiterzubilden oder eine Erwerbstätigkeit auszuüben» (vgl. Art. 2 Abs. 1 BehiG).

545 LANGER, AJP, 2014, S. 952, für eine vertiefte Auseinandersetzung vgl. weiter unten Rz. 487 ff.

546 Vgl. zum Ganzen: Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 5.4.

gedruckt veröffentlicht werden kann, wenn eine Nachfrage dazu besteht.[547] Zudem sieht der Regierungsrat eine Übergangsfrist vor, in welcher die beiden Versionen parallel erscheinen sowie Hilfeleistungen für die Benachteiligten angeboten werden. Darunter zu verstehen ist etwa die Möglichkeit, auf Anfrage weiterhin eine gedruckte Version oder Einsicht in die relevanten Geschäfte bei der jeweiligen Verwaltungsbehörde zu erhalten. Unter diesen Umständen wurde eine Ablösung des Internet-Amtsblatts als zulässig und eine damit allenfalls einhergehende geringfügige Diskriminierung älterer Personen als sachlich gerechtfertigt erachtet.[548]

b) Informationsfreiheit

Das Bundesgericht hatte sich zudem damit zu befassen, ob eine Online-Publikation amtlicher Publikationsorgane einen Eingriff in die Informationsfreiheit gemäss Art. 16 Abs. 3 BV darstellt. Diese beinhaltet unter anderem den Anspruch darauf, Informationen aus allgemein zugänglichen Quellen zu beschaffen, wobei der Gesetzgeber entscheiden kann, welche Informationen als öffentlich zugänglich im Sinne dieser Bestimmung gelten.[549] Neben den im Rahmen des Öffentlichkeitsprinzips oder gesetzlicher Bestimmungen als öffentlich zugänglich geltenden Quellen werden auch Tatsachen, über welche die Behörden von sich aus informieren, als öffentlich zugänglich betrachtet.[550] Im Rahmen der weiter oben bereits erwähnten Vorgaben von Art. 180 Abs. 2 BV können die Behörden dabei frei entscheiden, wie und worüber sie aktiv informieren. Es ergibt sich aus der Verfassungsbestimmung kein einklagbarer Individualanspruch zur Information über ein bestimmtes Thema.[551] 221

Sofern die Behörde jedoch aktiv informiert, ergibt sich aus der Informationsfreiheit ein Anspruch auf rechtsgleiche und willkürfreie Information.[552] Eine Informationspflicht der Behörden ergibt sich grundsätzlich aus dem bereits erwähnten Art. 180 Abs. 2 BV, wobei diese – wie bereits ausgeführt wurde – den Behörden ebenfalls einen weiten Gestaltungsspielraum lässt. Daher wird sie in verschiedenen Bereichen durch die einschlägige Sachgesetzgebung konkretisiert, in der etwa ausgeführt wird, worüber die Behörde im konkreten Bereich zu informieren hat.[553] Durch eine entsprechende Nennung 222

547 Vgl. den Antrag des Regierungsrates des Kantons Zürich, S. 23.

548 Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 5.4.

549 Kley/Tophinke, SG Komm. BV, Art. 16, N. 36.

550 Vgl. Müller/Schefer, S. 523.

551 Vgl. Hertig, BSK BV, Art. 16, N. 28, wobei sich je nachdem ein Anspruch auf passive Information aus dem jeweiligen Öffentlichkeitsgesetz ergeben kann.

552 Hertig, BSK BV, Art. 16, N. 28, m.w.H.

553 Brunner, ZBl, 2010, S. 598 f.

wird der grundrechtlich geschützte Zugang zu den entsprechenden Informationen gesetzlich betont.[554]

223 Daher untersteht gemäss der bundesgerichtlichen Rechtsprechung auch die Veröffentlichung des Amtsblatts der Informationsfreiheit. Durch die gesetzliche Verpflichtung zur Publikation wird dieser grundrechtliche Anspruch zusätzlich unterlegt. Erfolgt die Information ausschliesslich online, ist in erster Linie fraglich, ob überhaupt ein Eingriff in die Informationsfreiheit vorliegt. Zu beachten ist, dass der Staat bis anhin auf vielen verschiedenen Kanälen informiert, von denen einige für die Bürger gratis (z.B. Abstimmungsinformationen), andere jedoch mit Zusatzkosten verbunden sind (Amtsblatt, Zeitungsabonnemente). Dadurch, dass eine Verwaltung nur noch online über ihre Website oder gar ihren Social-Media-Kanal informiert, kann der Zugang insbesondere zu den ehemals kostenpflichtigen Informationen für viele Personen gar erleichtert werden. Lediglich für einen kleinen Teil der Bevölkerung, welcher nicht oder nicht täglich über einen Computer oder einen Internetzugang verfügt, wird die Erreichbarkeit bzw. der Empfang dieser Informationen erschwert. Zumindest hinsichtlich dieser Personen liegt daher ein Eingriff in den Schutzbereich der Informationsfreiheit vor.[555]

i) Gesetzliche Grundlage

224 Nach den oben ausgeführten Grundsätzen ist eine Behörde gestützt auf den allgemeinen Informationsauftrag frei im Entscheid, über welches Medium sie informiert, sofern dieser Auftrag nicht durch eine spezifische gesetzliche Grundlage präzisiert wird. Entscheidet sich eine Behörde indes, nur noch über einen bestimmten Kanal zu informieren, so ist dazu aus verschiedenen Gründen eine gesetzliche Grundlage zu fordern. Eine entsprechende Einschränkung kann, wie soeben ausgeführt wurde, in gewisse Grundrechtspositionen eingreifen, oder die Personen können in der Ausübung bestimmter Rechte eingeschränkt werden. Auch die allenfalls mit einer entsprechenden Umstellung verbundenen technischen und organisatorischen Schwierigkeiten können eine gesetzliche Grundlage notwendig machen.[556] Die Bestimmtheit der gesetzlichen Grundlage richtet sich dabei nach der Schwere des Eingriffs, welche jeweils im Einzelfall unter Einbezug aller Umstände zu beurteilen ist.[557]

225 Würde die öffentliche Verwaltung des Bundes oder eines Kantons die gesamte Informationstätigkeit ausschliesslich über das Internet erbringen, so

554 Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 4.2.

555 Vgl. zum Ganzen: Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 4.2.

556 Vgl. oben Rz. 137.

557 EPINEY, BSK BV, Art. 36, N. 33 f.

wären – wie soeben ausgeführt – potenziell verschiedene Grundrechtspositionen in unterschiedlicher Schwere betroffen. Daher wäre für eine entsprechende gesetzliche Grundlage ein hohes Mass an Bestimmtheit zu verlangen.[558] Soll indes die Informationstätigkeit lediglich in einem bestimmten Rechtsbereich exklusiv online vorgenommen werden, so sind auch die Anforderungen an die gesetzliche Grundlage für einen Eingriff in die Informationsfreiheit geringer. Das Bundesgericht hatte sich auch unter diesem Gesichtspunkt bereits damit auseinandergesetzt, ob ein Kanton das Amtsblatt ausschliesslich elektronisch publizieren darf.[559] Dabei hat es eine entsprechende Regelung in § 15 Abs. 1 PublG ZH, welche vorsieht, dass die amtlichen Publikationsorgane auf einer Internetsite des Kantons veröffentlicht werden, und dies im Verordnungsrecht konkretisiert, als ausreichende gesetzliche Grundlage beurteilt.[560]

ii) Öffentliches Interesse

Das öffentliche Interesse an einer rein elektronischen Publikation kann etwa darin liegen, dass auf diese Weise mehr Personen einfacher und ohne die Medien als Intermediäre Zugriff zu staatlichen Informationen erhalten. Ersetzt die Internetpublikation zudem ein Druckerzeugnis wie das Amtsblatt, so kann der Aufwand für die Erstellung und den Versand der Papierversion durch den Herausgeber eingespart werden. Dieses öffentliche Interesse wurde vom Bundesgericht ohne Weiteres als genügend erachtet.[561] 226

iii) Verhältnismässigkeit

Schliesslich hat die entsprechende Umstellung auf eine reine Online-Publikation auch verhältnismässig ausgestaltet zu sein. Das Bundesgericht erachtete etwa die Publikation des Amtsblatts über das Internet als geeignet, um einen grösseren Adressatenkreis zu erreichen und Ressourcen zu sparen. Zur Erreichung dieses Zwecks erblickte es kein milderes Mittel.[562] Dies, zumal es zu beachten gilt, dass das Internet als Informationsplattform in vielen Bereichen 227

558 Eine entsprechende Regelung wäre indes auch aus Verhältnismässigkeitsüberlegungen problematisch; siehe dazu sogleich Rz. 227.

559 Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 4.2.

560 Vgl. Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 4.3.2; ebenso für eine ähnlich ausgestaltete Regelung in Art. 13 Abs. 1 des aargauischen Publikationsgesetzes, vgl. Urteil des BGer 1C_577/2013 vom 2. Oktober 2013, E. 3.3.1, wobei das Bundesgericht in diesem Fall eine Dreitagesfrist für Stimmrechtsbeschwerden, welche sich aus dem Zusammenspiel dieser Bestimmung mit der einschlägigen Gemeindeordnung ergab, als nicht haltbar erachtete (siehe dazu weiter unten Rz. 232).

561 BGer 1C_137/2018 vom 27. November 2018, E. 4.4.

562 BGer 1C_137/2018 vom 27. November 2018, E. 4.4.

gegenüber Druckerzeugnissen oder der Konsultation der Medien an Bedeutung gewonnen hat.[563] Augenscheinlich ist dies vor allem bei amtlichen Publikationen wie dem Amtsblatt oder den amtlichen Sammlungen. Hier gibt es oftmals lediglich noch eine kleine Zahl an Abonnenten, wobei aufgrund der Tatsache, dass einige Exemplare an andere öffentliche Stellen ausgeliefert werden, kaum damit gerechnet werden kann, dass viele der Abonnenten des Amtsblatts die gedruckte Version benutzen, gerade weil sie keinen Internetzugang haben.[564] Somit kann von einer bescheidenen Zahl an effektiv durch die Umstellung Betroffenen ausgegangen werden. Dieser Einschätzung soll hier gefolgt werden. Auch in anderen Bereichen sind Einsparungen oder eine grössere potenzielle Reichweite durch eine ausschliessliche Online-Publikation durchaus denkbar.

228 Kritischer zu beurteilen ist, ob die mit dem Eingriff einhergehende Einschränkung der privaten Interessen im Hinblick auf das oben genannte öffentliche Interesse zumutbar ist. Eine Vielzahl von Informationshandlungen der Gemeinwesen sind für die meisten Adressaten nicht direkt mit der Ausübung von Rechten und Pflichten verbunden, etwa wenn darüber berichtet wird, dass der Bundesrat sich mit Staatschefs anderer Länder getroffen hat oder wenn ein neuer Amtsstellenleiter online vorgestellt wird. Entsprechende Informationen dienen in erster Linie der proaktiven oder begleitenden Information, und es besteht nach dem bisher Ausgeführten kein Rechtsanspruch darauf, diese zu erhalten und wahrnehmen zu können. Es ist daher m.E. zumutbar, dass diese Informationen lediglich online erfolgen.

229 Schwerer können die privaten Interessen dann wiegen, wenn die jeweilige Information in weitere Grundrechtspositionen eingreift. Aus der staatlichen Schutzpflicht vor Gefährdungen des Lebens kann sich – wie weiter oben ausgeführt – eine Informationspflicht z.B. hinsichtlich von Naturkatastrophen ergeben.[565] Um dieser Pflicht nachzukommen, muss im Fall einer Naturkatastrophe die gesamte Bevölkerung erreicht werden können, was über das Internet aktuell noch nicht gewährleistet werden kann. Auch wenn dereinst die gesamte Bevölkerung über das Internet erreicht werden und dieses Mittel auch bedienen kann, ist zu bedenken, dass die IT-Infrastruktur immer auch ein gewisses Restrisiko beinhaltet, in kritischen Situationen nicht vollständig funktionsfähig zu sein, etwa durch einen Ausfall der Stromversorgung oder eine Überlastung des Internetaufkommens.[566] Daher führt auch

563 Vgl. etwa die Zahlen der Werbewoche, wonach 2017 90 % der Befragten angaben, das Internet zu nutzen, während unter 50 % Tageszeitungen konsultierten.

564 Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 4.4.

565 Vgl TSCHENTSCHER, BSK BV, Art. 10, N. 18.

566 Vgl. dazu vertiefend: Strategie SKI.

bis auf Weiteres kaum ein Weg am Aufrechterhalten herkömmlicher Informationswege vorbei. Auch aus diesem Grund geschieht die Alarmierung in der Schweiz mithilfe von Sirenenalarmen und Durchsagen über Radio und Fernsehen.[567] Informationen via Internet oder Apps wie «Alertswiss» können hier höchstens komplementär, aber nicht ersetzend wirken.

230 Aus Art. 34 Abs. 2 BV, welcher die freie Willensbildung vor Volksabstimmungen garantiert, ergibt sich auch, dass diese Informationen rechtsgleich und willkürfrei vermittelt werden und alle Stimmberechtigten darauf Zugriff haben müssen. Bei einer Verbreitung lediglich über das Internet wäre dies nicht gegeben. Auch aus diesem Grund kann das «Abstimmungsbüchlein» zwar elektronisch bereitgestellt werden, es ist jedoch weiterhin an alle Stimmberechtigten postalisch zu übermitteln.[568] Eine Information lediglich über das Internet kann daher aus Gründen der Verhältnismässigkeit aktuell nicht als zulässig erachtet werden, ohne dass Massnahmen für diejenigen Personen getroffen werden, welchen die entsprechenden Kanäle nicht offenstehen.

231 Differenzierter kann dies beurteilt werden, wenn lediglich über gewisse Rechtsbereiche nur noch online informiert wird. So hatte sich das Bundesgericht auch unter dem Aspekt der Informationsfreiheit mit der Vermittlung amtlicher Publikationen ausschliesslich über den Online-Kanal befasst.[569] Die auf diese Weise publizierten Informationen können ebenso mit der Wahrnehmung von Rechten verbunden sein, etwa im Bereich der politischen Rechte oder von Einsprachen (z.B. im Baubewilligungsverfahren). Informationen etwa über Baugesuche sind in einer amtlichen Publikation zu publizieren. Findet diese Publikation nur noch im Internet statt, hat dies insbesondere auch Auswirkungen auf den Beginn des jeweiligen Fristenlaufs. Die gedruckte Version des Amtsblatts erscheint in der Regel an ein oder zwei bestimmten, gesetzlich festgeschriebenen Wochentagen, womit den Betroffenen klar ist, wann sie allenfalls mit der Auslösung einer für sie wichtigen Frist rechnen müssen. Mit der Möglichkeit der Internetpublikation können solche Informationen nun ohne Bindung an einen Wochentag publiziert werden. Es kann den Bürgern jedoch nicht zugemutet werden, ständig das Internet zu konsultieren, weil sie ansonsten befürchten müssen, dass sie den Beginn einer für sie relevanten Frist verpassen.[570]

232 Hinsichtlich dreissigtägiger (Einsprache-)Fristen, welche in der schweizerischen Rechtsordnung etwa für Einsprachen die Regel bilden, hat das

567 Vgl. etwa BUNDESAMT FÜR BEVÖLKERUNGSSCHUTZ, Die Alarmierung der Bevölkerung.

568 Vgl. zum Ganzen: LANGER, AJP, 2014, S. 951.

569 Urteil des BGer 1C_577/2013 vom 2. Oktober 2013, Urteil des BGer 1C_137/2018 vom 27. November 2018.

570 Vgl. zum Ganzen: Urteil des BGer 1C_577/2013 vom 2. Oktober 2013, E.3.3.2.

Bundesgericht eine Publikation im Internetamtsblatt als zulässig beurteilt, da auch bei einer nicht täglichen Konsultation des Internets regelmässig 25 Tage zur Wahrung der Frist verbleiben, wenn das Amtsblatt (wie die auch nach dem bisherigen Publikationsrhythmus möglich war) einmal pro Woche konsultiert wird.[571]. Auch die Publikation referendumsfähiger Beschlüsse auf Kantonsebene, welche im zu beurteilenden Fall eine dreissigtägige Sammelfrist vorsehen, im Internetamtsblatt wird als zulässig erachtet, da in diesem Fall eine gewisse Organisation bei den Referendumsergreifenden vorausgesetzt werden kann und auch bei nicht sofortiger Kenntnisnahme noch eine zumutbare Frist zur Sammlung der Unterschriften verbleibt.[572]

233 Je kürzer die jeweiligen Fristen sind, umso problematischer ist die geschilderte Thematik. Da Fragen der politischen Rechte oft zeitkritisch sind, etwa weil eine Abstimmung vorbereitet oder ein Ergebnis zeitnah erwahrt werden muss, sehen viele Kantone und der Bund für Stimmrechtsbeschwerden eine kürzere Beschwerdefrist vor.[573] Das Bundesgericht erachtet dabei auch eine dreitägige Frist zur Ergreifung einer Stimmrechtsbeschwerde nicht per se als verfassungswidrig.[574] Begründet wird dies damit, dass im Regelfall bei kantonalen und eidgenössischen Angelegenheiten die Abstimmungsdaten bekannt sind und allfällige Anfechtungsakte oder Vorbereitungshandlungen zeitlich bestimmbar sind und entsprechend schnell zur Kenntnis genommen werden können.[575] Als problematisch hat das Bundesgericht die Frist indes bei Gemeindebeschlüssen beurteilt, welche verbindlich online publiziert werden sollen. Bei diesen ist in der Regel kein vorgängiger Einblick in die Tagesordnung der Gemeindebehörden und die behandelten Geschäfte möglich. Wird die Online-Publikation zur Erhebung der Stimmrechtsbeschwerde als verbindlich betrachtet, würde eine dreitägige Frist den Bürger quasi dazu zwingen, ständig das Internet zu konsultieren, um keinen Fristenlauf zu verpassen. Das Bundesgericht hat sich mit einer entsprechenden Regelung in erster Linie unter dem Aspekt der politischen Rechte gemäss Art. 34 BV befasst, da sich die zu beurteilende Informationshandlung auf die Ausübung dieses Rechts auswirkte. Dabei hat es diese Fristenregelung als Verletzung von Art. 34 BV betrachtet.[576]

234 Noch nicht befasst hat sich das Bundesgericht damit, wie eine entsprechende Regelung im Hinblick auf ebenfalls denkbare fünf- oder zehntägige Fris-

571 Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 4.4.2.

572 Vgl. BGE 140 I 58, E. 4.2.2.

573 Vgl. STEINMANN/MATTLE, BSK BGG, Art. 100, N. 17.

574 Vgl. etwa BGE 121 I 1, E. 3b.

575 Urteil des BGer 1C_577/2013 vom 2. Oktober 2013, E. 3.3.1.

576 Vgl. zum Ganzen: Urteil des BGer 1C_577/2013 vom 2. Oktober 2013, E.3.3.

ten zu bewerten wäre. Soll das Amtsblatt nur noch online publiziert werden, ist vor allem für kurze Fristen eine Lösung zu finden, welche die Ausübung der jeweiligen (z.B. politischen) Rechte nicht erschwert oder gar verunmöglicht. Wie eine entsprechende Regelung ausgestaltet sein könnte, zeigt etwa die Publikationsverordnung des Kantons Zürich. Art. 12 Abs. 6 PublV ZH sieht vor, dass amtliche Texte in der Rubrik «Rechtsetzung und politische Rechte» in der Regel am Freitag veröffentlicht werden. Da auf diese Weise die bisherigen Gewohnheiten der Leser beibehalten werden können und keine Schlechterstellung gegenüber dem bisherigen Herausgaberhythmus erfolgt, kann eine solche Regelung – ihre korrekte Umsetzung vorbehalten – als zulässig erachtet werden.[577]

5. Fazit

Die weit gefassten Vorgaben an die Informationstätigkeit aufgrund der Verfassung und der jeweiligen Gesetzesgrundlagen lassen grundsätzlich eine Information über jedes verfügbare Medium zu, solange dieses für die jeweilige Botschaft geeignet ist. Grundsätzlich können Behörden also auch via Internet oder soziale Medien informieren. Nur wo die gesetzlichen Vorgaben explizit ein gewisses Medium vorsehen, ist dieses zwingend zur Information zu verwenden. Gibt der Staat im Rahmen seiner Informationstätigkeit über das Internet Personendaten bekannt, so hat er sich an die einschlägigen Bestimmungen der Datenschutzgesetzgebung zu halten. Hierbei ist in der Regel eine Abwägung zwischen öffentlichen und privaten Interessen durchzuführen, wobei auch zu beachten ist, dass das öffentliche Interesse an einer Information in der Regel mit dem Lauf der Zeit abnimmt und schliesslich erlischt. 235

Viele Behörden erheben (allein oder durch Drittanbieter) auf ihrer Website Daten über ihre Benutzer. Dabei besteht für den Staat unter Umständen die Möglichkeit, die Benutzenden über die IP-Adresse zu identifizieren. Daher wird für die Bearbeitung eine genügende gesetzliche Grundlage benötigt, welche allenfalls in Art. 45c FMG vorliegen könnte. Diese setzt allerdings die Einwilligung der Betroffenen voraus, wobei hier Fragen nach deren Modalitäten und deren Wirksamkeit offenbleiben. Eine entsprechende Bearbeitung ist daher zu unterlassen oder zumindest so datenschonend wie möglich auszugestalten (etwa durch Unkenntlichmachung der IP-Adresse vor der Bearbeitung und Verzicht auf Beizug externer Dritter). Auch viele Social-Media-Plattformen erheben Daten für die Behörden als Betreiber von Fanseiten und werten diese aus. Aufgrund der Rechtsprechung muss die Behörde für diese Datenbearbeitungen (und allfällige resultierende Persönlichkeitsverletzungen) als mitverantwortlich betrachtet werden. Für eine entsprechende 236

577 Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 4.4.2.

Bearbeitung besteht keine gesetzliche Grundlage. Da sich weitere Unsicherheiten etwa hinsichtlich der Gewährung der Betroffenenrechte ergeben, sind staatliche Behörden dazu angehalten, von diesen Möglichkeiten aktuell keinen Gebrauch zu machen oder deren Nutzung wenigstens so datenschutzfreundlich wie möglich auszugestalten.

237 Sofern sich ein Gemeinwesen entscheidet, einen gewissen Teil seiner Informationstätigkeit, wie dies in verschiedenen Kantonen bei der amtlichen Publikation geschehen ist, nur noch online zu erbringen, kann dies unter dem Gesichtspunkt des Diskriminierungsverbots und insbesondere der Meinungsfreiheit problematisch sein. Dies ist vor allem dort der Fall, wo durch die amtliche Publikation weitere Grundrechtspositionen – etwa politische Rechte – berührt sind. Insbesondere in diesen Fällen ist für eine verhältnismässige Ausgestaltung entsprechender Regelungen zu achten, welche eine Konsultation vor Ort oder Übergangsregelungen vorsieht und es ermöglicht, dass Fristen auch gewahrt werden können, ohne dass täglich das Internet bzw. das entsprechende Web-Angebot konsultiert werden muss.

C. Passive Informationstätigkeit der Verwaltung und Digitalisierung

1. Generelle Zulässigkeit

238 Die Informationstätigkeit auf Gesuch hin ist im Öffentlichkeitsgesetz des Bundes und in denjenigen Kantonen, welche das Öffentlichkeitsprinzip kennen, in kantonalen Öffentlichkeitsgesetzen geregelt. In der Regel ist die Stellung eines Einsichtsgesuchs an keine bestimmten Voraussetzungen oder Formvorgaben gebunden und kann etwa mündlich vor Ort oder per E-Mail gestellt werden.[578] Auch das Stellen eines Gesuchs über ein auf einer Website integriertes Formular ist zulässig.[579] In den Kantonen ist ein Einsichtsgesuch in öffentliche Dokumente oft ebenfalls nicht an eine bestimmte Form gebunden.[580]

239 Die Gewährung des Zugangs erfolgt von Gesetzes wegen vor Ort oder durch die Anforderung von Kopien, wie dies Art. 6 Abs. 2 BGÖ explizit vorsieht. Auch auf kantonaler Ebene besteht in der Regel sowohl die Möglichkeit der Einsichtsgewährung vor Ort als auch der Aushändigung, z.B. auf einem Informationsträger.[581] Bereits in der Botschaft zum BGÖ wird auf die Möglichkeit einer Bereitstellung von Informationen per E-Mail hingewiesen und diese generell als begrüssenswert erachtet.[582] Einer derartigen Übermittlung auf

578 Vgl. etwa Art. 7 Abs. 1 VBGÖ; s. Botschaft BGÖ, S. 2019.

579 Vgl. etwa die entsprechende Möglichkeit auf der Webseite des BAFU.

580 Vgl. etwa Art. 31 IDG BS; WALDMEIER, PK IDG BS, Art. 31, N. 2.

581 Darunter zu verstehen sind etwa Kopien oder elektronische Datenträger; vgl. Art. 34 Abs. 1 lit. a IDG BS; RUDIN, PK IDG BS, Art. 34, N. 9.

582 Vgl. Botschaft BGÖ, S. 2004.

elektronischem Weg steht hierbei nichts im Weg, allerdings ist dem Schutzbedarf der übermittelten Informationen angemessen Rechnung zu tragen, wobei insbesondere ausreichend garantiert werden muss, dass die Übermittlung nicht an unberechtigte Dritte erfolgt.[583] Die passive Behördeninformation ist indes ebenfalls als Teil des gesamten Systems der Aktenführung zu verstehen. Nur dort, wo Akten bereits elektronisch geführt werden, macht auch eine Bekanntgabe auf elektronischem Wege Sinn.[584]

Bisher ist ein Anspruch auf einen Online-Zugriff oder ein Abrufverfahren, 240
also auf einen dynamischen Zugang, im Öffentlichkeitsgesetz des Bundes nicht vorgesehen.[585] Zu beachten ist indes, dass in diesem Bereich die Grenzen zwischen passiver und aktiver Informationstätigkeit verschwimmen.[586] Die Behörden können Informationen, welche bei ihnen häufig nachgefragt werden, auf ihrer Website den Privaten zur Verfügung stellen. In diesem Zusammenhang ist insbesondere Art. 6 Abs. 3 BGÖ zu thematisieren. Gemäss dieser Bestimmung führt die Veröffentlichung eines amtlichen Dokuments in einem Publikationsorgan oder auf einer Internetsite des Bundes dazu, dass der Anspruch auf Zugang zu diesem Dokument als erfüllt gilt. Die angefragte Behörde kann sich in diesem Fall darauf beschränken, der gesuchstellenden Person die entsprechende Internetadresse anzugeben, wie Art. 3 Abs. 2 VBGÖ ausführt. Das BGÖ regelt eigentlich ausdrücklich nur die passive Informationstätigkeit der Behörden und nicht die aktive.[587] Art. 6 Abs. 3 BGÖ stellt jedoch eine wichtige Scharniernorm zwischen diesen beiden Formen dar. Die Bestimmung soll einen Anreiz für die Behörden schaffen, vermehrt Informationen aktiv zu publizieren, da auf diese Weise der Aufwand für die Prüfung und Gewährung des Zugangs hinsichtlich dieser Daten im Einzelfall unterbleiben kann.[588] Dieser Artikel zeigt auf, dass der aktiven Information wohl inskünftig eine grössere Bedeutung zukommen soll als der passiven.[589] Entsprechende Hinweise ergeben sich auch aus Art. 19 VBGÖ, gemäss welchem wichtige Dokumente so schnell wie möglich im Internet zu publizieren sind, sofern dies keinen unangemessenen Aufwand verursacht und der Veröffentlichung keine gesetzlichen Bestimmungen entgegenstehen.[590]

583 ROSENTHAL, Handkommentar DSG, Art. 8, N. 24; RUDIN, PK IDG BS, Art. 34, N. 10.
584 Siehe dazu weiter unten Rz. 352 f.
585 HÄNER, SHK BGÖ, Art. 10, N. 30.
586 MAHON/GONIN, SHK BGÖ, Art. 6, N. 30.
587 Botschaft BGÖ, S. 1997.
588 MAHON/GONIN, SHK BGÖ, Art. 6, N. 66.
589 NUSPLIGER, SHK BGÖ, Das Öffentlichkeitsprinzip in den Kantonen, N. 12.
590 MAHON/GONIN, SHK BGÖ, Art. 6, N. 67.

2. Diskriminierungsverbot

241 Die Regelung von Art. 6 Abs. 3 BGÖ wird teils als nicht ganz unproblematisch erachtet in Anbetracht der Tatsache, dass nicht alle Personen über einen Internetzugang verfügen bzw. die Anwendung dieser Technologie beherrschen.[591] Allenfalls könnte dadurch für gewisse Gruppen (etwa Menschen ab einem gewissen Alter) gar eine durch Art. 8 Abs. 2 BV verbotene Diskriminierung vorliegen. Hierbei kann nicht nur eine Regelung, welche eine Person unmittelbar aufgrund ihrer Zugehörigkeit zu einer bestimmten Gruppe ungleich behandelt, diskriminierend sein, sondern auch eine Regelung, welche in ihren tatsächlichen Auswirkungen übermässig Angehörige einer solchen Gruppe betrifft.[592] Ob eine Gruppe überdurchschnittlich häufig von einer Regelung betroffen ist, lässt sich oft nur durch statistische Auswertungen nachweisen.[593]

242 Die Regelung von Art. 6 Abs. 3 BGÖ nimmt nicht explizit auf eine bestimmte «sensible Gruppe» Bezug. Jedoch sind Personen ohne Computer- bzw. Internetzugang von der staatlichen Informationstätigkeit ausgeschlossen, wenn diese nur noch online erfolgen sollte. In einem anderen Zusammenhang hat das Bundesgericht entschieden, dass Personen ohne Internetzugang durchaus benachteiligt sein können, wenn eine staatliche Dienstleistung nur noch im Internet angeboten wird, es sich dabei aber nicht um eine im Rahmen von Art. 8 Abs. 2 BV besonders geschützte Gruppe handelt. Eine entsprechende Regelung beträfe indes überdurchschnittlich häufig ältere Personen, da diese in der Regel mehr Mühe mit der Nutzung neuer Technologien haben bzw. diese gar nicht bedienen können.[594] Das Alter wird in Art. 8 Abs. 2 BV explizit als sensibles Merkmal genannt. Das Bundesgericht merkt entsprechend an, dass eine Regelung, durch welche eine staatliche Information nur noch über das Internet verfügbar ist, so umgesetzt werden müsse, dass für die betroffenen Personen entsprechende Ausweichmöglichkeiten bestehen.[595] In der Botschaft zum BGÖ wird statuiert, dass der Verweis auf ein im Internet publiziertes amtliches Dokument mit dem Hinweis zu verbinden sei, dass auf entsprechendes Gesuch hin eine Kopie ausgestellt werden kann.[596] Wenn dies in der Praxis zeitnah und zweckdienlich umgesetzt wird, so ist davon

591 HÄNER, SHK BGÖ, Art. 10, N. 23.

592 Sog. mittelbare Diskriminierung; vgl. etwa BGE 139 I 169, E. 7.2.1.

593 Vgl. etwa WALDMANN, BSK BV, Art. 8, N. 118.

594 Siehe dazu oben Rz. 218.

595 Vgl. zum Ganzen: BGer 1C_137/2018 vom 27. November 2018, E. 5.4.

596 Botschaft BGÖ, S. 2004.

auszugehen, dass durch Art. 6 Abs. 3 BGÖ keine rechtlich relevante Ungleichbehandlung begründet wird.

3. Informationelle Selbstbestimmung

Wenn in einem im Rahmen der passiven Informationstätigkeit herausverlangten Dokument Daten von Drittpersonen enthalten sind, können diese allenfalls in ihrem Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) betroffen sein. Die einschlägigen Datenschutz- und Öffentlichkeitsgesetze konkretisieren daher, unter welchen Voraussetzungen die Bekanntgabe von Personendaten im Rahmen der passiven Informationstätigkeit zulässig ist. Im Bund sind gemäss Art. 9 BGÖ amtliche Dokumente, welche Personendaten von Drittpersonen enthalten, nach Möglichkeit zu anonymisieren. Falls dies nicht möglich oder nicht sinnvoll ist, z.B. da die Drittperson der gesuchstellenden Person bekannt ist oder trotz der Anonymisierung aus dem Kontext bestimmt werden kann, verweist Art. 9 Abs. 2 BGÖ darauf, dass die Zugangsgesuche nach Art. 19 DSG zu beurteilen sind. Die Bekanntgabe von Personendaten ist demnach etwa zulässig, wenn eine gesetzliche Grundlage dies vorsieht. Dies dürfte indes selten der Fall sein. Relevant ist daher im Kontext der passiven Informationstätigkeit vor allem Art. 19 Abs. 1bis DSG, welcher eine Bekanntgabe gestützt auf das Öffentlichkeitsgesetz auch erlaubt, wenn ein überwiegendes öffentliches Interesse besteht oder die betreffenden Personendaten im Zusammenhang mit der Erfüllung öffentlicher Aufgaben stehen.[597] Zu beachten ist hier des Weiteren Art. 11 BGÖ, gemäss dem die Behörde, welche Zugang zu einem Dokument zu gewähren gedenkt, das Personendaten enthält, den betroffenen Personen Gelegenheit zur Stellungnahme einräumen muss. 243

Die soeben beschriebenen Artikel legen fest, unter welchen Umständen eine Bekanntgabe von Personendaten Dritter im Rahmen der passiven Informationstätigkeit zulässig ist. Die jeweilige Abwägung zwischen öffentlichem Interesse und privaten Interessen der betroffenen Partei ist jedoch im Einzelfall vorzunehmen. 244

4. Fazit

Das Öffentlichkeitsprinzip fand ab dem Ende der 90er-Jahre verstärkt Eingang in die hiesige Rechtsordnung. Es erstaunt daher wenig, dass die technologischen Möglichkeiten, welche etwa das Internet mit sich bringt, darin zumindest teilweise bereits Beachtung finden. So sind Gesuche in der Regel formlos möglich, also auch per E-Mail oder Online-Formular. Auch können 245

597 Vgl. PARTSCH/BOURESH/HÄNER, BSK DSG/BGÖ, Art. 9 BGÖ, N. 13.

die entsprechenden Dokumente z.B. per E-Mail zugesandt werden. Es zeigt sich, nicht zuletzt auch durch Art. 6 Abs. 3 BGÖ, dass den Behörden ein Anreiz gegeben werden soll, vermehrt aktiv über das Internet anstatt reaktiv zu kommunizieren. Weitergehende Entwicklungen, etwa im Sinne eines Abrufverfahrens, sind bis zum jetzigen Zeitpunkt noch nicht vorgesehen. Indes ist auch die passive Behördeninformation als Teil eines Gesamtsystems der Aktenführung zu verstehen und nur in dem Masse zweckmässig, in welchem Akten bereits elektronisch geführt werden.[598]

246 Zu beachten ist, dass dort, wo die Informationstätigkeit im Sinne von Art. 6 Abs. 3 BGÖ verstärkt durch Publikation im Internet betrieben wird, auch Personen ohne Internetzugang oder genügendes technologisches Wissen weiterhin die Möglichkeit haben sollen, die entsprechenden Informationen zu erhalten. Weiter ist es wichtig, dass die Behörden bei der passiven Informationstätigkeit das Risiko der Publikation fremder Personendaten beachten. Dabei ist das Interesse der Person, deren Daten bekanntgegeben werden, mit dem Interesse an der Bekanntgabe abzuwägen und den betroffenen Personen – sofern möglich – Gelegenheit zur Stellungnahme zu geben.

II. Behördenkommunikation

247 Neben der behördlichen Informationstätigkeit hat sich durch das Internet auch die informelle Kommunikation zwischen den Behörden und der Bevölkerung ausserhalb von Verfahren verändert. Während man früher noch persönlich in der Gemeindeverwaltung vorsprach oder allenfalls per Brief oder Telefon um Rat suchte, findet diese Kommunikation heute zu einem grossen Teil per E-Mail statt.[599] Viele Kantone bzw. deren Dienststellen sind – wie bereits ausgeführt – auch in den sozialen Medien anzutreffen. Ein grosser Vorteil des Behördenauftritts in Social-Media-Angeboten ist, dass die Personen auf die Beiträge der Verwaltung reagieren (etwa mit «Likes» oder Kommentaren) und mit dieser auch direkt in einem Chat in Kontakt treten können. Dies führt zu einer Egalisierung von privater und öffentlicher Kommunikation.[600] In gewissen Bereichen werden sogar auf «künstlicher Intelligenz» basierende Chatbots eingesetzt, welche ohne menschlichen Einfluss mit den Ratsuchenden interagieren. Da dies bisher meist im Rahmen von Pilotversuchen geschieht, soll eine detaillierte Auseinandersetzung damit im letzten

598 Siehe weiter unten Rz. 352.

599 KRCMAR/MÜLLER/SCHEIBER/EXEL/MOTZET/BASTIN, S. 14.

600 Bericht Social Media 2017, S. 8.

Teil dieser Arbeit vorgenommen werden.[601] Vorliegend soll untersucht werden, welche Probleme mit der Behördenkommunikation über bereits verbreitete Mittel wie Social Media aus rechtlicher Hinsicht verbunden sind.

A. Zulässigkeit der Behördenkommunikation via neue Technologien

1. Grundsätzliches

248 Wie weiter oben dargelegt wurde, ist die Behördeninformation grundsätzlich nicht an eine bestimmte Form gebunden. Dies hat auch für die informelle Kommunikation zu gelten. Erst im Rahmen eines hängigen Verfahrens besteht unter anderem aus Beweiszwecken ein Bedarf an Formalisierung der Kommunikation. Es steht den Behörden daher frei zu wählen, welche Kommunikationskanäle sie der Bevölkerung öffnen. Es spricht also grundsätzlich nichts dagegen, dass die Verwaltung über soziale Medien mit sich in Verbindung treten lässt. Das Aufkommen des Internets und anderer neuer Technologien hat dabei viele Fragen gegenüber der «herkömmlichen» persönlichen Kommunikation nicht grundlegend verändert und diese sollen daher nicht vertieft bearbeitet werden. Wo allerdings im Rahmen der Behördenkommunikation Personendaten bearbeitet werden, gibt es einige Einschränkungen zu beachten.

2. Informationelle Selbstbestimmung

249 Überall dort, wo durch die Behörde im Rahmen der Kommunikation Personendaten bearbeitet werden, sind – wie bereits ausgeführt – die Vorgaben der Datenschutzgesetzgebung zu betrachten. Viele der damit verbundenen Fragestellungen – etwa, ob die Behörden die Daten und Informationen, welche sie vom Privaten im Rahmen des Kommunikationsakts erhalten, aufbewahren und bearbeiten dürfen – stellten sich unter dem Gesichtspunkt der informationellen Selbstbestimmung schon, als die Behörde nur per Brief oder später per Telefon erreicht werden konnte. Die Vorgaben der Datenschutzgesetzgebung an die Bearbeitung von Personendaten wurden im Rahmen dieser Arbeit bereits behandelt, so dass auf die dazu getätigten Ausführungen verwiesen werden kann.[602]

250 Zu beachten sind unter dem Vorbehalt abweichender spezialgesetzlicher Regelungen auch an dieser Stelle die Grundsätze der Datenbearbeitung, welche in Art. 4, Art. 5 Abs. 1 und Art. 7 Ab. 1 DSG verankert sind. Im vorliegenden Zusammenhang ist insbesondere der Grundsatz der Datensicherheit gemäss Art. 7 DSG zu beachten, gemäss welchem Personendaten durch angemessene

601 Siehe unten Rz. 512 ff.

602 Siehe dazu oben Rz. 74 ff.

technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden müssen. Hierzu muss erneut betont werden, dass E-Mail grundsätzlich nicht als sicherer Kommunikationskanal gewertet werden kann. Aus diesem Grund sollten Personendaten – insbesondere besonders schützenswerte oder vertrauliche Informationen – grundsätzlich nicht über diesen Kanal kommuniziert werden.[603]

251 Es muss indes m.E. zumindest die Möglichkeit bestehen, dass die Verwaltung durch die Bürger per E-Mail verschlüsselt erreicht werden kann. In Deutschland ist z.B. jede Behörde aufgrund von § 2 Abs. 1 des E-Government-Gesetzes verpflichtet, einen Weg zur sicheren Übermittlung elektronischer Dokumente einzurichten, und jede Bundesbehörde muss über einen sogenannten «De Mail»-Zugang verfügen. Bei «De Mail» handelt es sich um eine staatlich anerkannte Infrastruktur für verschlüsselte E-Mail-Kommunikation. In gewissen Bereichen können über diese Plattform rechtsverbindliche Verfahrenshandlungen vorgenommen werden.[604] Auch in der Schweiz bestehen Dienste, welche eine sichere elektronische Übermittlung gewährleisten können.[605] Im Rahmen der Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV) hat der Bund die Grundlage geschaffen, dass elektronische Eingaben bei Bundesbehörden in Verwaltungsverfahren möglich sind. Gemäss Art. 4 Abs. 1 VeÜ-VwV führt er dabei eine Liste, welche Behörde Eingaben über welchen Kanal entgegennimmt. Seit 1. Januar 2017 sind elektronische Eingaben bei jeder Bundesbehörde zugelassen.[606] Auf Kantonsstufe ist die Verwendung der entsprechenden Lösungen indes nicht vorgeschrieben, so dass diese auch nicht flächendeckend Einzug gehalten hat. Zumindest in Teilen bedingt durch diesen Fakt sind die Nutzung entsprechender E-Mail-Lösungen und generell die Verschlüsselung von E-Mails aufseiten der privaten Nutzer noch nicht wirklich verbreitet. Es wäre daher angebracht, aufseiten der Behörden weitere Anstrengungen zur Verbreitung dieser Dienste zu unternehmen.

B. Kommunikation via Social Media

252 Neben der Möglichkeit der einseitigen Information durch die Behörden zeichnen sich soziale Netzwerke dadurch aus, dass die Verwaltung mit den Nutzenden in ein wechselseitiges Kommunikationsverhältnis treten kann. In der Regel können auf der jeweiligen Social-Media-Präsenz auch durch Dritte Beiträge

603 ROSSNAGEL, NJW, 2011, S. 1473; siehe detailliert weiter unten Rz. 329.

604 ROSSNAGEL, NJW, 2011, S. 1473 f.

605 Vgl. etwa die Liste der anerkannten Plattformen des Bundesamts für Justiz.

606 GLASER, ZSR, 2015, S. 303.

erstellt oder Kommentare zu Beiträgen angebracht werden. Dabei kann der Inhaber der Social-Media-Präsenz selbst bestimmen, welche Beiträge auf seiner Seite angezeigt werden sollen und welche nicht. Teilweise fordern Betreibende von Fanseiten die Benutzer im Rahmen einer sogenannten «Netiquette» zur Beachtung gewisser Verhaltensweisen auf (etwa das Unterlassen von rassistischen, sexistischen oder sonst wie herabwürdigenden Beiträgen).[607] Halten sich die Benutzer nicht an diese Regeln, so behalten sich die Betreibenden einer Seite beispielsweise vor, den jeweiligen Beitrag von ihrer Seite zu entfernen. Dies hindert eine Person allerdings nicht daran, denselben Beitrag erneut oder andere Beiträge zu verfassen, welche ebenfalls nicht der «Netiquette» entsprechen. Daher besteht auch die Möglichkeit, einen Benutzer zu sperren (oder zu blockieren), so dass dieser auf der jeweiligen Seite keine Interaktionen mehr tätigen kann, solange er mit seinem Konto beim jeweiligen Dienst eingeloggt ist. Loggt er sich nicht ein, bleibt es ihm in der Regel möglich, die Beiträge auf der jeweiligen Seite zu lesen, aber nicht mehr, mit dieser (etwa durch Kommentare) zu interagieren.

Die Löschung von Äusserungen kann entweder durch die Plattformbe- 253
treiber selbst oder durch den Staat als Betreiber der jeweiligen Facebook-Fanseite vorgenommen werden. Dass staatliche Betreiber von dieser Möglichkeit Gebrauch machen, wurde etwa ersichtlich, als die Hamburger Polizei anlässlich des G20-Gipfels im Juli 2017 verschiedene Accounts für ihre Seite blockierte.[608] Auch ein ehemaliger US-Präsident war dafür bekannt, dass er unliebsame Benutzer von seinem Twitter-Profil verbannen lässt.[609]

1. Meinungsfreiheit

Durch das Löschen von Beiträgen und das Sperren von Konten ist es dem staat- 254
lichen Betreiber möglich, missliebige Personen – zumindest im betreffenden Social-Media-Kanal – aus dem öffentlichen Diskurs auszuschliessen. Diese Massnahmen können daher allenfalls einen Eingriff in die Meinungsfreiheit darstellen. Art. 16 Abs. 2 BV und Art. 10 EMRK schützen die Freiheit jeder Person, eine Meinung zu haben, zu bilden und sie ungehindert zu äussern und zu verbreiten. Der Begriff der Meinung ist dabei weit zu verstehen und umfasst «die Ergebnisse von Denkvorgängen sowie rational fassbar und mitteilbar

607 Kofferwort aus dem englischen Net und dem französischen «Etiquette» für Verhaltensweisen; vgl. Definition des Worts Netiquette in der Online-Version des Duden. Vgl. auch die Facebook-Netiquette der Präsenz des Kantons Aargau.

608 Vgl. KALSCHEUER/JACOBSEN, NJW, 2018, S. 2358.

609 Vgl. etwa die Rechtssache Appeal from the United States District Court for the Southern District of New York 18-1691, Knight First Amendment Institute et al v. Donald J. Trump et al. vom 23. Mai 2018.

gemachte Überzeugungen in der Art von Stellungnahmen, Wertungen, Anschauungen, Auffassungen und dergleichen».[610] Die Kommunikationsform und das Kommunikationsmittel, über welches man seine Meinung kundtun möchte, können grundsätzlich frei gewählt werden.[611] Es versteht sich daher, dass auch Äusserungen in sozialen Medien durch die Meinungsfreiheit geschützt sind. Dadurch, dass gewisse Beiträge von der Behörde gelöscht werden können oder eine Person gar daran gehindert werden kann, auf eine gewisse Website zuzugreifen, ist es ihr nicht mehr möglich, ihre Meinung frei zu äussern, so dass ein Eingriff in die Meinungsfreiheit stattfindet.

255 Äussert sich eine Person in den sozialen Medien, so kann dies verschiedene Formen annehmen. Positive Rückmeldungen (z.B. Likes) sind in der Regel im interessierenden Zusammenhang von den Behörden gewünscht und werden daher von diesen kaum gelöscht. Jedoch lässt die Plattform auch Raum für negative Wortmeldungen, etwa in der Form von Kritik an der Amtsführung der Behörde oder Beleidigungen. Für den Schutz der Meinungsfreiheit kommt es indes nicht auf den Inhalt oder den Wert einer Meinung an. Insbesondere soll es möglich sein, Kritik ohne Angst vor Sanktionen äussern zu können, selbst wenn diese unberechtigt sein mag.[612] Ein neues Phänomen ist die Verbreitung von «Fake News», welche insbesondere über Social Media geschieht. Dabei handelt es sich etwa um «wider besseren Wissens geäusserte, unwahre Tatsachenbehauptungen, die zum Zweck der politischen Manipulation, aus finanziellen Interessen oder anderen eigennützigen Motiven verbreitet werden (…)».[613] In Deutschland sind derartige bewusst unwahre Tatsachenbehauptungen vom Schutzbereich der Meinungsfreiheit ausgenommen.[614] In der Schweiz sollen jedoch gerade auch mithin unhaltbare, falsche oder provozierende Meinungen geäussert werden dürfen.[615] Das Verbreiten von «Fake News» fällt in der Schweiz somit grundsätzlich unter den Schutzbereich der Meinungsfreiheit.

a) Löschungen durch Plattformbetreiber

256 Bevor auf die Möglichkeit der staatlichen Löschung und Sperrung eingegangen wird, soll kurz thematisiert werden, unter welchen Umständen die Plattformbetreiber selbst entsprechend tätig werden und welche Probleme dies

610 BGE 117 Ia 472, E. 3.c).

611 HERTIG, BSK BV, Art. 16, N. 12.

612 Sog. «Chilling effect»; vgl. etwa HERTIG, BSK BV, Art. 16, N. 40.

613 Bericht Social Media 2017, S. 11.

614 HOLZNAGEL, MMR, 2018, S. 20.

615 HERTIG, BSK BV, Art. 16, N. 9.

mit sich bringen kann. Bei den Betreibenden der eingängigen Plattformen handelt es sich um juristische Personen des Privatrechts, welche in der Regel ihren Sitz im Ausland haben. Diese müssen sich, wie oben dargelegt wurde, grundsätzlich an die Schweizer Rechtsordnung halten.[616] Die Plattformbetreiber behalten sich im Rahmen ihrer Nutzungsbedingungen vor, dass sie unter gewissen Umständen Beiträge löschen bzw. Benutzende sperren können, wenn diese den von der Plattform aufgestellten Regeln nicht entsprechen.[617] Jede Person, welche sich auf einem sozialen Medium registriert, muss dessen Nutzungsbedingungen akzeptieren und unterwirft sich somit den von dieser Plattform festgesetzten Regeln auch betreffend die allfällige Löschung von Beiträgen oder des Kontos. Vor allem in Deutschland wird diese Konstellation als «virtuelles Hausrecht» bezeichnet, welches den Betreibern von Websites und Social-Media-Plattformen zusteht.[618] Im Rahmen dieses Hausrechts dürfen sie über die Nutzung ihrer Website verfügen. Die von den jeweiligen Nutzenden bei der Registrierung akzeptierten Nutzungsbedingungen gelten quasi als Hausordnung, bei deren Nichtbefolgung sie die angedrohten Konsequenzen tragen müssen.

257 Die Frage, ob die Berufung auf ein «virtuelles Hausrecht» auch in der Schweiz denkbar ist, wurde bisher kaum diskutiert, geschweige denn rechtlich beurteilt.[619] Die Schweizer Rechtsordnung gewährt Privatpersonen ebenfalls ein Recht darüber zu bestimmen, wer sich in ihrem Haus bzw. ihrer Wohnung aufhält. Dies ergibt sich implizit aus Art. 13 BV, welcher das Recht auf Achtung der Wohnung garantiert und in erster Linie einen Schutz gegen staatliches Eindringen in die Wohnung garantiert.[620] Daraus abgeleitet sehen auch das Strafrecht (Hausfriedensbruch gem. Art. 186 StGB) und das Zivilrecht (vgl. etwa Art. 679 ff. ZGB hinsichtlich des Schutzes von Grundeigentum) gewisse Werkzeuge zum Schutz der Wohnung vor. Diese Bestimmungen gehen indes von einer physischen Räumlichkeit als geschütztem Raum aus.[621] Allenfalls könnte sich ein analoger Schutz im virtuellen Raum höchstens aus

616 Siehe oben Rz. 291 ff.

617 Vgl. etwa die Nutzungsbedingungen von Facebook. Diese verweisen auf die Gemeinschaftsstandards, wo unerwünschtes Verhalten definiert wird: Facebook Gemeinschaftsstandards.

618 Vgl. etwa MAUME, MMR, 2007, S. 620 ff.

619 Vgl. etwa das Votum von RA Martin Steiger anlässlich der Arena vom 31.03.2017: STERN, Hass im Netz: Ein Wutbürger bringt «Arena»-Moderator Projer ins Schwitzen, Aargauer Zeitung, 1. April 2017.

620 DIGGELMANN, BSK BV, Art. 13, N. 26.

621 DIGGELMANN, BSK BV, Art. 13, Art. 13 N. 25; DELNON/RÜDY, BSK Strafrecht, Art. 186, N. 14.

Art. 143bis StGB ergeben, welcher das unbefugte Eindringen in ein Datenverarbeitungssystem unter Strafe stellt und analog dem Hausfrieden den «Computerfrieden» schützt.[622] Indes bleibt es Privaten im Internet im Rahmen der Vertragsfreiheit vorbehalten, die Nutzung einer Website oder eines Diensts an gewisse Nutzungsbedingungen (AGB) zu binden und sich auf diese Weise ein «virtuelles Hausrecht» zu schaffen.

258 Es ist weitergehend die Frage zu stellen, wie frei die Plattformbetreiber bei der Ausgestaltung dieser AGB sind. Das Schweizer Recht kennt einige privatrechtliche Grenzen, welche sich jedoch darin erschöpfen, dass die Vertragsparteien keine unerwarteten oder ungewöhnlichen Klauseln verstecken dürfen. Ansonsten gilt grundsätzlich die Vertragsfreiheit.[623] Wie soeben ausgeführt, können durch eine Löschung von Beiträgen auf Social-Media-Plattformen auch grundrechtliche Positionen – in erster Linie in Form der Meinungsfreiheit – betroffen sein. Die Plattformbetreiber sind, wie weiter oben ausgeführt, nicht unmittelbar an die Grundrechte gebunden. Gemäss Art. 35 Abs. 3 BV haben die Behörden aber dafür zu sorgen, dass die Grundrechte unter Privaten zu beachten sind, wo sie sich dafür eignen. Dies kann auch gerade dort sein, wo unter Privaten ein erhebliches Machtgefälle besteht.[624] Diese indirekte Horizontalwirkung richtet sich in erster Linie an die Behörden, etwa im Rahmen der grundrechtskonformen Auslegung unbestimmter Rechtsbegriffe.

259 In Deutschland haben sich mehrere Gerichte unterer Instanzen mit der Frage befasst, inwiefern die Plattformbetreiber zumindest mittelbar die Meinungsfreiheit zu beachten hätten. Dabei kamen sie zu unterschiedlichen Schlüssen. Generell ging es dabei um eine Interessenabwägung zwischen dem virtuellen Hausrecht der Betreiber und der Meinungsfreiheit der Benutzer. Gewisse Gerichte anerkannten die gelöschten Beiträge als durch die Meinungsfreiheit geschützte Äusserungen, erachteten das Recht von Facebook, für den Betrieb der Plattform zu sorgen und dabei gewisse Regelungen aufzustellen, aber als gewichtiger.[625] Das OLG München hingegen sah ein Überwiegen der Meinungsfreiheit und begründete dies damit, dass Facebook sich durch das Zustandekommen eines Vertrags dazu verpflichtet, im Rahmen von Art. 241 Abs. 2 BGB die Rechte der anderen Vertragspartei zu achten, zu denen auch die Meinungsfreiheit gehöre.[626] In Abwägung der Interessen wurde

622 WEISSENBERGER, BSK Strafrecht, Art. 143bis, N. 5.

623 Vgl. etwa BGE 135 III 225, E. 1.2. f.

624 SCHWEIZER, SG Komm. BV, Art. 35, N. 48; siehe dazu oben Rz. 191 ff.

625 Vgl. etwa LG Frankfurt, Beschluss vom 10. September 2018, Az. 2-03 O 310/18; OLG Karlsruhe, Beschluss vom 25. Juni 2018, Az. 15 W 86/18.

626 Vgl. etwa OLG München, Beschluss vom 24. August 2018 – Az. 18 W 1294/18.

festgestellt, dass Facebook zwar gestützt auf seine Richtlinien Beiträge löschen dürfe, welche gegen die Rechte anderer verstossen, dass im Umkehrschluss aber Beiträge zulässig sein müssen, welche dies eben gerade nicht tun. Gemäss der Rechtsprechung des Bundesverfassungsgerichts verstosse gerade die reine Ausübung der Meinungsfreiheit nicht gegen die Rechte Dritter.[627] Am weitesten ging indes das Landgericht Bamberg, welches aufgrund der Stellung, welche Facebook im öffentlichen Leben und im gesellschaftlichen und politischen Diskurs innehat, die Plattform dazu verpflichtete, einen Beitrag aufgrund der Meinungsfreiheit nicht zu löschen oder den Benutzer nicht zu sperren.[628] Das Gericht erkannte somit bezüglich Facebook aufgrund dessen «Quasi-Monopolstellung» für den öffentlichen Diskurs eine mittelbare Grundrechtswirkung zu, welche einer unmittelbaren Grundrechtswirkung nahekommt.[629]

In der Schweiz gibt es soweit ersichtlich bisher keine Gerichtsurteile, 260
welche sich explizit mit der Löschung von Posts auf Social-Media-Plattformen oder der Blockierung von Benutzern durch die Plattformbetreiber befassen.[630] Thematisiert wurde bis anhin lediglich die straf- oder zivilrechtliche Verantwortlichkeit von Verfassern von Facebook-Posts oder «Tweets» für deren Inhalt, etwa wegen rassistischer oder beleidigender Äusserungen.[631] Zwar wird bei der Auslegung der entsprechenden Straftatbestände jeweils auch die Meinungsäusserungsfreiheit thematisiert[632], jedoch sprechen die Urteile sich nicht dazu aus, ob eine Löschung durch den Plattformbetreiber im jeweiligen Fall zulässig wäre.

Es ist fraglich, inwiefern sich die entsprechende Rechtsprechung auf die 261
Schweiz übertragen lässt. Die unmittelbare Anwendung von Grundrechten ist nach dem bereits Ausgeführten gemäss Art. 35 Abs. 2 BV eng auf das Erfüllen einer staatlichen Aufgabe begrenzt. Auch wenn Facebook eine «Quasi-Monopolstellung» betreffend die gesellschaftliche und politische Meinungsäusserung innehaben sollte, was der Autor aufgrund der vielen anderen, verbleibenden Möglichkeiten zur Meinungsäusserung zumindest als zweifelhaft ansieht, so erfüllt das Netzwerk keine staatliche Aufgabe im Sinne dieser Bestimmung. Das Bundesgericht anerkennt zwar ähnlich dem BVerfG, dass bei

627 LG Berlin Beschluss vom 23. März 2018 Az. 31O21/18; OLG München, Beschluss vom 24. August 2018, Az. 18 W 1294/18.

628 LG Bamberg, Urteil vom 18. Oktober 2018, Az. 2 O 248/18.

629 KNEBEL, MMR, 2019, S. 60.

630 Vgl. jedoch das Urteil des BGer 1C 564/2016 vom 2. März 2017, welches sich mit einer Sperrung durch eine staatliche Stelle befasst; siehe dazu sogleich Rz. 417.

631 Vgl. etwa Urteil des BGer 6B_627/2015 vom 4. November 2015.

632 Urteil des BGer 6B_627/2015 vom 4. November 2015, E. 2.5 f.

der Bewirtschaftung des öffentlichen Grunds (etwa Plakatbewirtschaftung) auch Private an Grundrechte gebunden sein können[633], hat sich aber ausserhalb dieser Thematik noch nicht mit der Drittwirkung der Meinungsfreiheit auf öffentlichem Grund befasst. Aus diesem Grund besteht in der Schweiz aktuell kein Anlass, eine quasiunmittelbare Grundrechtsbindung der Plattformbetreiber anzunehmen.

262 Die hiesige Rechtsordnung kennt das Instrument der indirekte Horizontalwirkung von Grundrechten ebenfalls. Jedoch existiert im Schuldrecht keine mit Art. 241 Abs. 2 BGB (auf welchen sich das OLG München beruft) vergleichbare Regelung. Allenfalls liesse sich der für die gesamte Rechtsordnung geltende Begriff des Handelns nach Treu und Glauben, welcher in Art. 2 Abs. 1 ZGB statuiert ist, heranziehen. Indes wird argumentiert, dass diese Norm in der Schweiz aus Gründen der Kompetenzordnung nicht zu weit ausgelegt werden soll.[634] Es ist daher fraglich, ob die Schweizer Gerichte den Plattformbetreibern ähnliche Fesseln anlegen würden.

b) Löschungen durch den Staat

263 Wie weiter oben bereits erläutert, ist der Staat durch seinen Auftritt auf einer Plattform der sozialen Medien ebenfalls ein Nutzer dieser Plattform und muss sich an deren Regelungen halten. Zusätzlich ist staatliches Handeln aber stets auch durch die Grundrechte begrenzt. In diesem Rahmen hat der Staat auch die Meinungsfreiheit zu beachten. Gerade wenn er selber entscheiden kann, welche Meinungen er auf seinem Auftritt in den sozialen Medien zeigen will, so bringt dies eine grosse Gefahr mit sich, dass unbeliebte Meinungen und Kritik unterdrückt werden und rückt unter Umständen gar in die Nähe der Zensur, welche als Kerngehalt der Kommunikationsgrundrechte ausdrücklich verboten ist.[635] Das Bundesgericht hatte sich bisher in einem einzigen Fall mit der staatlichen Sperrung eines Facebook-Nutzers zu befassen. Da der betroffene Nutzer von der Facebook-Seite der Polizei Waadt zum Zeitpunkt der gerichtlichen Auseinandersetzung allerdings bereits wieder entsperrt worden war, traten weder das kantonale Gericht noch das Bundesgericht mangels eines aktuellen schutzwürdigen Interesses auf die entsprechende Beschwerde ein.[636] Das Bundesgericht vertröstete den Beschwerdeführer darauf, bei einer weiteren (allenfalls permanenten) Sperrung über ein aktuelles Interesse zu verfügen, und gab ihm dabei quasi als Tipp mit, dass es ihm

633 BGE 127 I 84, E. 3b.

634 Vgl. etwa HONSELL, BSK ZGB I, Art. 2, N 5.

635 ZELLER/KIENER, BSK BV, Art. 17, N. 35.

636 Vgl. Urteil des BGer 1C 564/2016 vom 2. März 2017, E. 2 ff.

unbenommen sei, dann einen Eingriff in die Meinungsfreiheit und die Rechtsgleichheit sowie einen Verstoss gegen das Informationsgesetz des Kantons zu rügen.[637]

Vorliegend soll unabhängig von diesem konkreten Fall in erster Linie die Meinungsfreiheit thematisiert werden. Diese gilt – wie alle Freiheitsrechte – nicht absolut und kann nach den Grundsätzen von Art. 36 BV eingeschränkt werden. 264

i) Gesetzliche Grundlage

Nach den allgemeinen Regeln von Art. 36 BV ist zum Eingriff in ein Grundrecht eine gesetzliche Grundlage erforderlich. Gründe, die Meinungsfreiheit einer Person zu beschränken, lassen sich insbesondere dort finden, wo durch die Äusserungen andere Personen in Grundrechten oder geschützten Rechtsgütern eingeschränkt werden. Zu denken ist etwa an das soziale Ansehen von Personen. Diesem Zweck dienen etwa der privatrechtliche (Art. 28 ZGB) und der strafrechtliche Ehrenschutz (Art. 173 ff. StGB).[638] Auch Meinungsäusserungen, welche z.B. öffentlich zu Gewalt aufrufen (Art. 259 StGB) oder jemanden aufgrund seiner Rasse, Ethnie oder Religion diskriminieren (Art. 261bis StGB), sind unter Strafe gestellt. Die entsprechenden Bestimmungen stellen die gesetzliche Grundlage für den jeweiligen Eingriff in die Meinungsfreiheit dar.[639] Sie sind dabei grundrechtskonform auszulegen.[640] Es wird davon ausgegangen, dass durch die entsprechende rechtliche Grundlage auch der Staat ermächtigt wird, allfällige Äusserungen von seinem Social-Media-Auftritt zu entfernen.[641] Gerade im Bereich von politischen oder gesellschaftlich relevanten Äusserungen, wie sie wohl in den sozialen Medien oft vorliegen, ist dabei zu beachten, dass die jeweilige Äusserung nicht nur im privaten Interesse des Grundrechtsträger liegen, sondern in einer Demokratie daran auch ein öffentliches Interesse bestehen kann. Dies ist in der Interessenabwägung im Rahmen der Verhältnismässigkeitsprüfung zu berücksichtigen.[642] 265

Neben den genannten Beispielen gibt es Äusserungen, welche nicht gegen eine konkrete Rechtsnorm verstossen, aber trotzdem von den Behörden nicht erwünscht sind. Wie weiter oben ausgeführt, fällt etwa das Verbreiten von falschen Tatsachenbehauptungen in der Schweiz ebenfalls unter den 266

637 Vgl. Urteil des BGer 1C 564/2016 vom 2. März 2017, E. 3.

638 KLEY/TOPHINKE, SG Komm. BV, Art. 16, N. 14.

639 Vgl. etwa BGE 132 III 641, E. 5.2.

640 RIKLIN, BSK Strafrecht, Art. 173, N. 35.

641 Bericht Social Media 2017, S. 17.

642 KLEY/TOPHINKE, SG Komm. BV, Art. 16, N. 16.

Schutzbereich der Meinungsäusserungsfreiheit.[643] Gerade hier sind Szenarien denkbar, in denen kein straf- oder zivilrechtlich relevantes Handeln vorliegt. Auch Kritik an der Amtsführung kann geäussert werden, ohne dass z.B. eine Ehrverletzung begangen wird. Es ist daher zu prüfen, ob eine Grundlage besteht, um derartige Äusserungen zu entfernen und/oder den verantwortlichen Benutzer gar zu sperren.

267 Die Aktivität der Behörden auf Social-Media-Plattformen ist – wie bereits angedeutet – nur sehr oberflächlich geregelt. Allfällige Regeln auf Gesetzes- oder Verordnungsstufe bestimmen, wenn überhaupt, die internen Zuständigkeiten zur Information und Kommunikation. In gewissen Kantonen regeln eine «Social-Media-Strategie» oder «Social Media Guidelines» den Umgang mit sozialen Medien und sehen dabei in erster Linie Verhaltensanweisungen an die Mitarbeitenden im beruflichen Umgang mit sozialen Medien vor.[644] Dabei handelt es sich um interne Dienstanweisungen einer vorgeordneten an eine nachgeordnete Behörde. Als sogenannte Verwaltungsverordnungen sind diese zwar für die Verwaltungsmitarbeitenden rechtlich verbindlich, sie können aber für aussenstehende Dritte keine Rechte und Pflichten begründen.[645] Auch wenn sie sich also über die Sperrung von Personen oder die Löschung von Beiträgen äussern würden, könnten diese Weisungen aufgrund ihrer Rechtsnatur gegenüber Dritten keine genügende gesetzliche Grundlage darstellen. Die teilweise angeführten «Netiquetten» der jeweiligen Site-Betreibenden können mangels Normativität ebenfalls nicht als gesetzliche Grundlage dienen, um eine Löschung von Beiträgen oder Sperrung zu rechtfertigen.[646]

ii) Konzept eines virtuellen Hausrechts

268 Als gesetzliche Grundlage bringen diverse deutsche Autoren ins Spiel, dass auch der Staat analog zu privaten Betreibenden in sozialen Medien im Rahmen der Ausübung seines «virtuellen Hausrechts» Benutzenden den Zugang zu den von ihm betreuten Seiten verwehren und deren Beiträge löschen darf.[647] Es ist unbestritten, dass dem Staat hinsichtlich seiner Verwaltungsgebäude ein öffentlich-rechtliches Hausrecht zusteht und er gewisse Massnahmen ergreifen kann, um den Dienstbetrieb aufrechtzuerhalten. Dazu zählt

643 Siehe oben Rz. 255.

644 So ist darin etwa zu lesen, dass Zuständigkeiten oder Geheimnispflichten zu respektieren seien, vgl. die Social-Media-Guidelines des Kantons Zürich.

645 Vgl. zum Ganzen HÄFELIN/MÜLLER/UHLMANN, N. 81 ff.; TSCHANNEN/ZIMMERLI/MÜLLER, § 41 N. 11 ff.

646 Vgl. etwa LANGER, AJP, 2014, S. 953.

647 Vgl. etwa KALSCHEUER/JACOBSEN, NJW, 2018; MILKER, NVwZ, 2018; MAUME, MMR, 2007.

unter anderem, dass er Personen den Zutritt zu seinen Gebäuden untersagen kann.[648] Ein entsprechendes virtuelles Hausrecht müsste jedoch hohe Anforderungen erfüllen. So muss etwa eine nachhaltige Störung des Dienstbetriebs vorliegen oder unmittelbar und ernsthaft drohen und müssen die entsprechenden Verhaltensregeln im Vorneherein bekannt sein. Zudem reicht nicht jede geringfügige missliebige Äusserung oder Störung aus, da eine öffentliche Diskussion auch zugespitzte Äusserungen aushalten muss.[649] Des Weiteren wäre bei der Ausübung des virtuellen Hausrechts durch Sperrungen oder Löschungen von Beiträgen auch die Verhältnismässigkeit zu beachten. Unter diesem Aspekt lässt sich fragen, ob die Blockierung überhaupt geeignet ist, da sie durch das Erschaffen eines neuen Accounts umgangen werden kann. Hinsichtlich der Erforderlichkeit wäre zu prüfen, ob im konkreten Fall die Löschung eines einzelnen Beitrags oder eine temporäre Sperrung als milderes Mittel einer unbegrenzten Sperrung vorzugehen haben.[650]

Eine Auseinandersetzung mit der Frage, ob sich der Staat auf ein virtu- 269
elles Hausrecht berufen kann, um im Rahmen seiner virtuellen Auftritte Personen zu sperren oder ihre Einträge zu entfernen, fehlt in der Schweiz vollständig. Im Folgenden soll erläutert werden, ob dieses Instrument im Rahmen der Schweizer Rechtsordnung überhaupt denkbar wäre. Wie bereits abgehandelt, sieht die Schweizer Rechtsordnung ein «virtuelles Hausrecht» nicht grundsätzlich vor, jedoch können private Website-Betreiber dies im Rahmen der Nutzungsbedingungen vereinbaren. Es ist fraglich, ob diese Möglichkeit auch dem Staat offenstehen soll. Zwar hat auch der Staat ein entsprechendes Recht, über die physischen Räume zu bestimmen, an denen er berechtigt ist, insbesondere da er für einen geordneten Betrieb der Verwaltung und den Schutz der Angestellten zu sorgen hat.[651] Im Gegensatz zur privaten Wohnung stellen Verwaltungsgebäude jedoch eine öffentliche Sache dar, d.h., der Staat benutzt diese zur Erfüllung seiner Aufgaben und ist dabei gemäss Art. 35 Abs. 2 BV an die Grundrechte gebunden. Verwehrt er einer Person den Zugang zu einem Gebäude, so kann dadurch eine Vielzahl von Grundrechten betroffen sein.[652] Die Doktrin hat verschiedene Kriterien herausgearbeitet, unter welchen die Nutzung des öffentlichen Grundes zulässig

648 Vgl. KALSCHEUER/JACOBSEN, NJW, 2018, S. 2359.

649 KALSCHEUER/JACOBSEN, NJW, 2018, S. 2361.

650 KALSCHEUER/JACOBSEN, NJW, 2018, S. 2362. Dies dürfte insbesondere bei einmaligen «Vergehen» zu bejahen sein.

651 Vgl. etwa Endentscheid VB.2010.00455 des VRG ZH vom 28. Oktober 2010, E. 3.2.4 und Endentscheid VB.2016.00430 des VRG ZH vom 1. Juni 2017, E. 3.3.1.

652 Vgl. etwa Endentscheid VB.2010.00455 des VRG ZH vom 28. Oktober 2010, E. 3.2.4 und Endentscheid VB.2016.00430 des VRG ZH vom 1. Juni 2017, E. 3.3.1.; Urteil der BVGer C-6123/2009 vom 20. Juni 2011, E. 3 f.

ist, je nachdem, um welche Art von öffentlicher Sache es sich handelt: Unterschieden wird dabei zwischen Finanzvermögen, Verwaltungsvermögen und öffentlichen Sachen im Gemeingebrauch. Beim Verwaltungsvermögen handelt es sich um Werte, welche der Behörde oder einem beschränkten Kreis von Benutzern unmittelbar zur Erfüllung einer öffentlichen Aufgabe dienen (z.B. Schulen oder Spitäler). Das Finanzvermögen dient der Erfüllung der Staatsaufgaben nur mittelbar durch seine Vermögenswerte oder Erträgnisse. Bei der öffentlichen Sache im Gemeingebrauch handelt es sich um Sachen, welche der Allgemeinheit im Gegensatz zum Verwaltungsvermögen zur Benutzung offenstehen (etwa Strassen).[653] Die Kategorien unterscheiden sich dabei etwa in den Voraussetzungen, unter denen sie von Privaten genutzt werden dürfen. Bei Verwaltungsgebäuden handelt es sich nach dieser Unterscheidung unzweifelhaft um Verwaltungsvermögen.[654] Das Gemeinwesen ist nicht ohne Weiteres verpflichtet, Privatpersonen die Nutzung seines Verwaltungsvermögens zu gestatten. In grundrechtsrelevanten Fällen kann sich jedoch für die gesuchstellende Partei ein bedingter Anspruch auf Nutzung der Verwaltungssache aus den betroffenen Grundrechten ergeben. Der Zugang zu einem Gebäude im Verwaltungsvermögen muss rechtsgleich und willkürfrei gestattet werden.[655] Zum Aussprechen von Hausverboten wird als genügende gesetzliche Grundlage erachtet, dass dem jeweiligen Gemeinwesen das Hausrecht über seine Verwaltungsgebäude eingeräumt wird oder es für den Schutz seiner Angestellten zu sorgen hat.[656]

270 Ob sich dieses Konzept indes auf den virtuellen Raum übertragen lässt, ist aus den folgenden Überlegungen fraglich. Man kann den Internetauftritt der öffentlichen Verwaltung und auch deren Social-Media-Auftritt durchaus als öffentliche Sache ansehen, da der Staat sich ihrer zur Erfüllung einer staatlichen Aufgabe bedient. Dass er kein Eigentum an der entsprechenden Social-Media-Plattform hat, spielt für die Kategorisierung als öffentliche Sache keine Rolle.[657] Indes liesse sich eine Charakterisierung als Verwaltungsvermögen kaum rechtfertigen. Zwar dienen Websites und Social-Media-Plattformen dem Staat zur Erfüllung einer staatlichen Aufgabe, jedoch stehen sie grundsätzlich der Allgemeinheit zur Benützung offen, indem jeder sich in diesen Netzwerken «bewegen» darf. Sie wären daher eher noch als öffentliche Sache im Gemeingebrauch zu charakterisieren. Daraus ergibt sich, dass deren

653 Vgl. zum Ganzen: TSCHANNEN/ZIMMERLI/MÜLLER, § 48 N. 11 ff.

654 HÄFELIN/MÜLLER/UHLMANN, N. 2205 ff.

655 TSCHANNEN/ZIMMERLI/MÜLLER, § 50 N. 6.

656 Vgl. etwa Endentscheid VB.2016.00430 des VRG ZH vom 1. Juni 2017, E. 3.3.1; Urteil des BVGer C-6123/2009 vom 20. Juni 2011, E. 3.3.

657 Vgl. BGE 127 I 164, E. 5.b) bb); TSCHANNEN/ZIMMERLI/MÜLLER, § 49 N. 6.

bestimmungsgemässer und gemeinverträglicher Gebrauch grundsätzlich einer unbestimmten Anzahl an Benutzern unentgeltlich und ohne Erteilung einer Erlaubnis offenstehen muss.[658] Lediglich dort, wo der Gebrauch nicht mehr gemeinverträglich ist, wo namentlich andere Benutzer in ihrer eigenen Benutzung beeinträchtigt sind, ist eine Einschränkung denkbar, wobei auch hier die Freiheitsrechte beachtet werden müssen.[659]

271 Bereits die deutschen Vertreter des Konzepts weisen darauf hin, dass das virtuelle Hausrecht gesetzlich nicht verankert ist und die dazu bestehenden richterrechtlichen Grundsätze zu Unsicherheiten in der Anwendung führen.[660] Umstritten ist etwa, ob und wie der Betroffene angehört werden soll und wie ihm die Löschung oder Sperrung mitgeteilt werden muss.[661] Ebenfalls nicht thematisiert wurde bisher, welches Rechtsmittel der betroffenen Person dagegen zur Verfügung steht. Diese Vorbehalte haben aus den soeben genannten Erwägungen auch für die Schweiz zu gelten. Es ist daher für den Moment davon abzusehen, dass staatliche Behörden selbständig gestützt auf ein virtuelles Hausrecht Personen den Zugang zu ihren Social-Media-Auftritten verwehren können.

iii) Zwischenfazit

272 Nach dem soeben Ausgeführten fehlt es staatlichen Behörden aktuell an einer genügenden gesetzlichen Grundlage, um im Rahmen ihres Social-Media-Auftritts Benutzer zu sperren oder deren Beiträge zu löschen, sofern kein straf- oder zivilrechtlich relevantes Verhalten vorliegt. Ein daraus resultierender Eingriff in die Meinungsfreiheit wäre daher nicht zu rechtfertigen. Zu einem ähnlichen Schluss kamen auch die Bundesbehörden, welche im Social-Media-Bericht 2017 davon ausgingen, dass im Bereich der Bekämpfung von «Fake News» Massnahmen der Plattformbetreiber einer Intervention durch die Behörden vorzugehen haben.[662] Andere Länder haben teilweise explizite gesetzliche Grundlagen geschaffen, um gegen entsprechende Einträge vorgehen zu können. Im letzten Teil dieser Arbeit sollen diese genauer betrachtet werden, und es soll geprüft werden, ob ein ähnliches Vorgehen allenfalls auch mit der Schweizer Rechtsordnung vereinbar wäre.[663]

658 HÄFELIN/MÜLLER/UHLMANN, N. 2253 ff.

659 HÄFELIN/MÜLLER/UHLMANN, N. 2274 und 2294 ff.

660 MILKER, NVwZ, 2018, S. 1757.

661 Fraglich ist etwa, ob ein generischer Hinweis durch die Plattformbetreiber über die Sperrung hierzu ausreicht; vgl. etwa MILKER, NVwZ, 2018, S. 1756; a.M. KALSCHEUER/JACOBSEN, NJW, 2018, S. 2361.

662 Bericht Social Media 2017, S. 17.

663 Siehe dazu unten Rz. 507 ff.

C. Fazit

273 Es ist den Behörden grundsätzlich freigestellt, über welche Kanäle sie mit der Bevölkerung informell kommunizieren wollen. Die Kommunikation ist daher auch via E-Mail oder Social Media möglich. Sofern Personendaten kommuniziert werden, haben die Behörden insbesondere die Datensicherheit zu beachten. Daher sollten entsprechende Angaben nicht über unverschlüsselte Kanäle versendet werden. Bei der Kommunikation über Social Media ist es dem Staat möglich, im Rahmen seines Auftritts Kommentare von Benutzern, welche z.B. die Diskussion stören, zu löschen oder diesen den Zugriff zur jeweiligen Seite zu blockieren, was einen Eingriff in die Meinungsfreiheit darstellt. Stellt die zugrundeliegende Meinungsäusserung straf- oder zivilrechtlich relevantes Handeln (z.B. «Hate Speech») dar, ist eine Löschung in der Regel unproblematisch. Jedoch sind Fälle denkbar, welche diese Schwelle nicht überschreiten, aber dennoch nicht gewünscht sind (etwa das Verbreiten von Fake News). Derartiges Verhalten darf mangels gesetzlicher Grundlage von den Behörden nicht durch Löschung oder Blockierung sanktioniert werden. Auch der Rückgriff auf das Konzept eines virtuellen Hausrechts überzeugt in rechtlicher Hinsicht bisher nicht.

III. Rechtsfolgen behördlicher Informations- und Kommunikationstätigkeit

274 Zwar ist die behördliche Informationstätigkeit, wie weiter oben dargelegt wurde, nicht in erster Linie auf Rechtswirkungen bei den betroffenen Privaten ausgelegt. Dennoch kann sie mittelbare Rechtswirkungen hervorrufen, etwa indem sie in die Grundrechte der betroffenen Person eingreift oder indem eine Person durch eine über das Internet verbreitete Information einen Vermögensschaden oder einen anderweitigen rechtlich relevanten Nachteil erleidet. Im folgenden Kapitel soll daher geklärt werden, wie eine Person dagegen vorgehen kann, wenn durch eine entsprechende Information z.B. in ihre Grundrechte eingegriffen wurde (Rechtsschutz) oder wenn sie aufgrund der behördlichen Information zu Schaden kam (Verantwortlichkeit). Diesbezüglich ergeben sich bei der behördlichen Information über das Internet gewisse rechtliche Probleme spezifischer Art, welche in diesem Kapitel beleuchtet werden.

A. Rechtsschutz

275 Die behördliche Informationstätigkeit kann, wie weiter oben ausgeführt wurde, auf verschiedene Arten gegen durch die Verfassung garantierte Rechte verstossen. Zu denken ist einerseits daran, dass die generelle Ausgestaltung

der Informationstätigkeit gegen ein Grundrecht – wie bereits dargestellt etwa die informationelle Selbstbestimmung oder die Meinungsfreiheit – verstösst. Der Ermessensspielraum der Behörden in der Ausgestaltung der Informationstätigkeit ist relativ weit, so dass bisher kaum jemals eine entsprechende Verletzung gerichtlich festgestellt werden musste. Entsprechende rechtsverletzende kantonale Erlasse können gemäss Art. 82 lit. b. BGG beim Bundesgericht im Rahmen der sogenannten «abstrakten Normenkontrolle» auf ihre Vereinbarkeit mit dem übergeordneten Recht überprüft werden.[664] Die abstrakte Normenkontrolle gilt, wie dem Wortlaut von Art. 82 BGG zu entnehmen ist, nur für kantonale Erlasse.[665] Wird im Rahmen der abstrakten Normenkontrolle festgestellt, dass eine mit dem übergeordneten Recht konforme Auslegung nicht möglich ist, kann die entsprechende kantonale Norm durch den Entscheid des Bundesgerichts aufgehoben werden.[666] Die Anwendung von Bundesgesetzen kann das Bundesgericht zwar prüfen, es darf diesen jedoch – selbst wenn sie gegen die Verfassung verstossen – nicht die Anwendung untersagen, was sich aus Art. 190 BV ergibt.[667]

Ebenfalls denkbar ist, dass der einzelne Informationsakt gegen ein Grundrecht verstösst. Zu denken ist hier etwa an die Publikation von Personendaten durch die Behörde. Bei der passiven Informationstätigkeit ist eine Konsultation von betroffenen Personen vor der Bekanntgabe ausdrücklich vorgesehen.[668] Im Rahmen der aktiven Informationstätigkeit besteht hingegen in der Regel kein Verfahrensmechanismus, welcher der betroffenen Person einen Anspruch auf eine Konsultation vor der Veröffentlichung ihrer Personendaten gibt, so dass die Anhörung der Betroffenen dem Ermessen der informierenden Behörde obliegt.[669] Es bleibt den Betroffenen daher nur die Möglichkeit des nachträglichen Rechtsschutzes, indem sie gestützt auf Art. 25a VwVG den Erlass einer anfechtbaren Verfügung über die Informationstätigkeit als Realakt verlangen und Unterlassungs-, Beseitigungs- oder Feststellungsansprüche geltend machen können.[670] 276

664 Vgl. etwa WALDMANN/AEMISEGGER/SCHERRER REBER/STEINMANN/MATTLE, BSK BGG, Art. 82, N. 24. Die Kantone können auch ein eigenes Verfahren zur abstrakten Normkontrolle vorsehen, welches zuvor durchlaufen werden muss, sie sind aber nicht dazu verpflichtet; vgl. BGE 141 I 36, E. 1.2.2.

665 WALDMANN/AEMISEGGER/SCHERRER REBER/STEINMANN/MATTLE, BSK BGG, Art. 82, N. 29.

666 WALDMANN/AEMISEGGER/SCHERRER REBER/STEINMANN/MATTLE, BSK BGG, Art. 82, N. 68.

667 EPINEY, BSK BV, Art. 190, N. 2 f.

668 Vgl. etwa Art. 11 BGÖ, siehe oben Rz. 168.

669 Siehe oben Rz. 168 und BRUNNER, ZBl, 2010, S. 609 und 634.

670 BRUNNER, ZBl, 2010, S. 634.

277 Wurden in widerrechtlicher Weise Daten über eine Person bekanntgegeben, so gibt die Datenschutzgesetzgebung des Bundes ihr weitere Instrumente an die Hand. Die Widerrechtlichkeit einer Bearbeitung ergibt sich dabei aus Art. 12 und Art. 13 DSG und ist etwa gegeben, wenn für die Bekanntgabe der entsprechenden Daten keine genügende gesetzliche Grundlage bestand. Gemäss Art. 25 DSG kann, wer ein schutzwürdiges Interesse hat, vom verantwortlichen Bundesorgan verlangen, dass es (a.) das widerrechtliche Bearbeiten von Personendaten unterlässt; (b.) die Folgen eines widerrechtlichen Bearbeitens beseitigt oder (c.) die Widerrechtlichkeit des Bearbeitens feststellt. Hinsichtlich der Bekanntgabe von Daten über das Internet kann hier insbesondere der Anspruch auf Beseitigung der Folgen des widerrechtlichen Bearbeitens von Interesse sein. Die Geltendmachung der Ansprüche aus Art. 25 Abs. 1 DSG setzt indes voraus, dass das Bearbeiten der Personendaten widerrechtlich erfolgt. Der Anspruch aus Art. 25 DSG geht dabei dem weiter oben vorgestellten Anspruch aus Art. 25a VwVG als *lex specialis* vor.[671] Ein weiteres Instrument, welches die Datenschutzgesetzgebungen des Bundes und vieler Kantone kennt, ist die Sperrung der Bekanntgabe. Gemäss Art. 20 DSG kann jede betroffene Person, die ein schutzwürdiges Interesse glaubhaft macht, vom verantwortlichen Bundesorgan verlangen, dass es die Bekanntgabe von bestimmten Personendaten sperrt. Eine entsprechende Sperre kann indes verweigert werden, wenn eine Rechtspflicht zur Bekanntgabe besteht oder die Erfüllung der Aufgabe des Bundesorgans durch die Bekanntgabe gefährdet wäre.[672]

B. Haftung des Staates für Information und Kommunikation im Internet

278 Neben der Verletzung von Grundrechtspositionen kann eine staatliche Information für Private auch weitere negative Konsequenzen haben. Dies einerseits dadurch, dass einer Person durch eine (mitunter falsche oder fälschlicherweise bekanntgegebene) behördliche Information ein finanzieller Schaden entsteht, etwa indem Lebensmittelwarnungen herausgegeben werden, welche zu einem Gewinneinbruch bei einem bestimmten Produkt führen.[673] Anderseits ist eine Schädigung dadurch denkbar, dass eine Behörde über ihre Internetsite eine falsche Auskunft gibt, die eine Person zu einer für sie nachteiligen Vermögensdisposition bewegt. Entsprechende Konstellationen existierten bereits vor den Zeiten des Internets, weswegen Bund und Kantone

671 BANGERT, BSK DSG/BGÖ, Art. 25 DSG, N. 18.

672 Es kann daher beispielsweise nicht verlangt werden, dass die eigenen Personendaten bei der Polizei gesperrt werden, um der polizeilichen Verfolgung zu entgehen; vgl. zum Ganzen EHRENSPERGER, BSK DSG/BGÖ, Art. 20 DSG, N. 8.

673 Vgl. etwa BGE 118 Ib 473.

öffentlich-rechtliche Staatshaftungsordnungen erlassen haben. Diese gehen davon aus, dass der Staat unter gewissen Voraussetzungen kausal für Schäden haftet, welche durch Handlungen seiner Angestellten verursacht werden.[674] Diese Haftungsnormen sollen hier kurz vorgestellt werden, wobei der Schwerpunkt auf diejenigen Punkte gelegt werden soll, welche sich durch die Kommunikation über das Internet verändert haben. Zu beachten ist dabei insbesondere, dass eine einmal veröffentlichte Information im Internet bestehen bleibt und die Behörde nach der Veröffentlichung keine Kontrolle mehr darüber hat, wer die Information sieht und gestützt darauf handelt.

1. Generelle Voraussetzungen der Staatshaftung

Gemäss Art. 146 BV haftet der Bund für Schäden, die seine Organe in Ausübung amtlicher Tätigkeiten widerrechtlich verursachen. Konkretisiert wird diese Haftung durch das Verantwortlichkeitsgesetz.[675] Auch die Kantone sehen für die Handlungen ihrer Organe grundsätzlich eine ausschliessliche Haftung des Gemeinwesens vor, deren Voraussetzungen sich eng an diejenigen des Bundes anlehnen und die ebenfalls in Haftungs- oder Verantwortlichkeitsgesetzen (teilweise auch im kantonalen Beamtenrecht) geregelt sind.[676] Zusätzlich gibt es indes eine grosse Menge an spezialgesetzlichen Regelungen, welche die Haftungsvoraussetzungen in gewissen Bereichen verschärfen oder mindern und in diesen Bereichen den allgemeinen Staatshaftungsgesetzen vorgehen.[677] In der vorliegenden Arbeit soll in erster Linie die allgemeine Staatshaftung thematisiert werden. Gemäss Art. 3 VG haftet der Bund für den Schaden, den ein Beamter in Ausübung seiner amtlichen Tätigkeit einem Dritten widerrechtlich zufügt, ohne Rücksicht auf das Verschulden des Beamten. Anhand dieser Regelung soll betrachtet werden, inwiefern die bestehenden Rechtsgrundlagen Lösungen auch für die Informations- und Kommunikationstätigkeit des Bundes im Internet bieten oder ob hier allenfalls rechtliche Lücken bestehen. Nach dieser generellen Betrachtung werden einige spezifische Konstellationen detailliert untersucht. 279

- *Schaden*

Damit eine Haftung des Staates überhaupt in Frage kommt, muss in erster Linie ein Schaden bei der betroffenen Person vorliegen. Zur Definition des 280

674 Vgl. etwa auf Bundesebene Art. 3 VG.

675 SCHAUB, BSK BV, Art. 146, N. 24.

676 UHLMANN, Staatshaftungsrecht, N. 28.

677 Zu denken ist etwa an die Haftung des Bundes für durch Armeeangehörige verursachte Schäden gemäss Art. 135 ff. MG; für weitere Beispiele, vgl. UHLMANN, Staatshaftungsrecht, N. 34 ff.

Schadens wird dabei oft auf die privatrechtliche Praxis verwiesen, wonach ein Schaden dann gegeben ist, wenn eine ungewollte Vermögensverminderung des Geschädigten vorliegt.[678] Zu unterscheiden ist dabei in erster Linie zwischen Personen-, Sach- und Vermögensschäden.[679] Kommt eine Person durch die Informationstätigkeit des Staates zu Schaden, so ist in erster Linie eine Schädigung des Vermögens die Folge.[680] Es kann jedoch unter Umständen auch Fälle geben, in denen eine Person körperlich zu Schaden kommt, etwa wenn sie infolge fehlerhafter Kartendaten des Bundes bei einer Wanderung in den Bergen verunfallt.[681]

• *Zurechnung zum Staat*

281 Das schädigende Verhalten muss zudem dem Staat zugerechnet werden können. Wessen Verhalten dem Staat zugerechnet werden kann, ist in den jeweiligen Haftungsgesetzen geregelt. Für den Bund zählt etwa Art. 1 Abs. 1 VG die dem Gesetz unterstellten Personen auf. Auch die Kantone regeln die Normadressaten ähnlich und gehen von einem weiten Anwendungsbereich aus.[682] Die staatliche Informationstätigkeit im Internet wird in der Regel durch eine oder mehrere kantonale oder Bundesbehörden wahrgenommen, so dass das Erfüllen dieser Voraussetzung in der Regel keine Probleme mit sich bringt.

• *Amtliche Tätigkeit*

282 Weiter wird vorausgesetzt, dass die schädigende Handlung in Ausübung einer amtlichen Tätigkeit erfolgt ist. Damit soll verhindert werden, dass der Staat das «Betriebsrisiko» für sämtliche Handlungen seiner Beamten übernehmen muss, auch wenn diese nichts mit deren Tätigkeit zu tun haben, etwa wenn ein Beamter während seiner Arbeit einen Diebstahl begeht. Die Beamten müssen gerade aufgrund ihrer amtlichen Stellung in der Lage gewesen sein, die schädigende Handlung vorzunehmen, und die Geschädigten müssen diese als Amtshandlung betrachten dürfen.[683] Auch diese Voraussetzung bereitet im Hinblick auf die Verbreitung von Informationen in der Regel keine spezifischen Probleme im Vergleich zur selben Handlung, welche offline erfolgt. So stellt ein Beitrag auf einer Social-Media-Plattform eines Kantons ebenso eine Amtshandlung dar wie eine telefonische oder mündliche Auskunft durch die jeweilige Person.

678 KESSLER, BSK OR I, Art. 41 OR, N. 3.
679 UHLMANN, Staatshaftungsrecht, N. 85.
680 Vgl. für OGD: WEBER/LAUX/OERTLY, S. 185 f.
681 KETTIGER, in: Jahrbuch 2016/2017, S. 113.
682 UHLMANN, Staatshaftungsrecht, N. 98.
683 HÄFELIN/MÜLLER/UHLMANN, N. 2109.

• *Widerrechtlichkeit*

Schliesslich muss die schädigende Handlung widerrechtlich sein. Widerrechtlichkeit ist dabei einerseits gemäss herrschender Lehre und Rechtsprechung dann gegeben, wenn das Gemeinwesen in absolut geschützte Rechtsgüter (wie Leib und Leben, Freiheit oder Persönlichkeit) eingreift, was als sogenanntes Erfolgsunrecht bezeichnet wird.[684] Da das Vermögen kein absolut geschütztes Rechtsgut ist, sind reine Vermögensschädigungen nur dann widerrechtlich, wenn sie eine Norm der Rechtsordnung verletzen, welche explizit zum Schutz des Vermögens gedacht ist. Die Bezeichnung hierfür ist Verhaltensunrecht.[685] 283

Wie soeben dargestellt, ist ein haftungsgesetzlich relevanter Schaden, welcher nicht das Vermögen betrifft, bei der behördlichen Informationstätigkeit eher unwahrscheinlich. Daher müsste eine entsprechende Rechtsnorm im vorliegenden Kontext explizit das Vermögen der Betroffenen schützen. Zur Beurteilung der Widerrechtlichkeit sind daher die Sachgesetze zu konsultieren, welche die Informationstätigkeit der Behörden im konkreten Bereich regeln. Bei diesen Bestimmungen stehen indes meist andere Interessen als der Schutz wirtschaftlicher Interessen der Betroffenen im Vordergrund, etwa der Schutz der Gesundheit der Bevölkerung.[686] Aus Gründen der Verhältnismässigkeit wird aber dennoch eine gewisse Rücksichtnahme auf private Interessen verlangt.[687] Die Rechtsprechung nimmt daher eine haftungsbegründende Widerrechtlichkeit in der Informationstätigkeit nur an, wenn bei der Informationshandlung unverantwortbare Fehler gemacht wurden.[688] 284

Problematisch ist hierbei, dass die Informationsqualität oft von verschiedenen Faktoren abhängig ist. Der Wert einer Information ist daher immer auch im Rahmen des jeweiligen Kontextes zu bewerten.[689] Oft lässt sich erst im Nachhinein feststellen, dass eine Information, etwa aufgrund von neuen wissenschaftlichen Erkenntnissen, mangelhaft oder gar falsch war.[690] In gewissen Fällen muss eine Information unter Zeitdruck erfolgen, bevor vollständige, wissenschaftliche Gewissheit über den Informationsgegenstand besteht, da auch ein Zuwarten zu haftungsbegründenden Schäden führen könnte.[691] Gerade in dieser Konstellation wäre es stossend, wenn der Staat 285

684 KESSLER, BSK OR I, Art. 41 OR, N. 33.

685 UHLMANN, Staatshaftungsrecht, N. 118.

686 BGE 118 1b 473, E. 5.c.

687 Vgl. für das neue EpG, Botschaft Rev. EpG, S. 367.

688 BGE 118 1b 473, E. 5.b.

689 GASSER, FS Druey, Variationen über Informationsqualität, S. 745.

690 DRUEY, S. 243.

691 BGE 118 1b 473, E. 18.a.; Bericht Informationstätigkeit. S. 1569.

dafür geradestehen müsste, dass sich eine Information nachträglich als unzutreffend herausstellte, welche er im damaligen Zeitpunkt unter Umständen gar unter Zeitdruck nach bestem Wissen und Gewissen abgegeben hat. Daher erachtet es die bundesgerichtliche Praxis als ausreichend, wenn die Information korrekt und sachgemäss erfolgt ist. Die Richtigkeit sei dabei nicht nach dem heutigen Wissensstand, sondern nach demjenigen zum Zeitpunkt der Information zu bewerten.[692] Generell lässt sich feststellen, dass die Hürden für eine Staatshaftung wegen Fehlinformation dadurch relativ hoch angesetzt sind. Eine Staatshaftung wurde in relevanten Fällen bisher nur aufgrund spezialgesetzlicher Haftungsgrundlagen[693] oder bei groben Fehlern[694] bejaht.

286 Das soeben Ausgeführte hat auch zu gelten, wenn die Information über das Internet erfolgt. Zu beachten ist indes, dass Informationen über das Internet um ein Vielfaches schneller verbreitet werden können. Ist eine Fehlinformation einmal publiziert worden, so ist deren weitere Verbreitung nicht mehr in der Kontrolle der Behörde. Sie kann allenfalls von Drittpersonen auf deren eigenen Websites oder Social-Media-Auftritten wiedergegeben werden. Dies führt dazu, dass eine entsprechende Information auch sehr viel schwerer wieder komplett aus dem Internet entfernt werden kann. Die Behörden haben dieser Gefahr in ihrer Informationstätigkeit Rechnung zu tragen. Dies kann meines Erachtens etwa bedeuten, dass den Eigenheiten der Informationstätigkeiten über das Internet (insbesondere hinsichtlich Ausbreitungsgeschwindigkeit, Reichweite und Irreversibilität) inskünftig im Rahmen des erforderlichen Sorgfaltsmassstabs Rechnung zu tragen ist.

2. Vertrauensschutz bei fehlerhafter Information im Internet

287 Es kann vorkommen, dass eine Behörde gegenüber einer Privatperson eine falsche Aussage trifft und diese Person dadurch zu einer Disposition veranlasst wird, welche sie ansonsten nicht getätigt hätte. Ein Beispiel dafür ist etwa, wenn die Behörde falsche Angaben zur Bebaubarkeit eines Grundstücks publiziert und eine Person darauf basierend ein Baugesuch einreicht, welches abgelehnt wird und auf Kosten der Partei erneut gestellt werden muss. Einige Kantone sehen für derartige Fälle im jeweiligen Haftungs- oder Verantwortlichkeitsgesetz Normen vor, nach denen der Staat bei vorsätzlich

692 BGE 118 Ib 473, E. 7. Dabei sind in erster Linie die jeweils vorherrschenden Meinungen zu berücksichtigen, bei umstrittenen Themen ist jedoch auch auf andere vertretbare Meinungen zu verweisen; vgl. TSCHANNEN, ZSR, 1999, S. 436.

693 Vgl. etwa BGE 116 II 480, E. 3 ff.

694 Etwa weil eine Behörde Resultate einer Studie, welche sich auf die Umweltverträglichkeit von Mehrwegbechern bezog, so veröffentlicht, dass sich diese auf sämtliches Mehrweggeschirr beziehen; vgl. Urteil des Appellationsgerichts des Kantons Basel-Stadt AS.2009.302 vom 18. Dezember 2009, abgedruckt in URP 2012, S. 55–63.

oder grobfahrlässig erfolgten Falschauskünften für daraus entstehende Schäden haftet. Auch wenn keine entsprechende Haftungsnorm besteht oder kein Vorsatz vorliegt, ergibt sich aus dem Grundsatz von Treu und Glauben, dass die Person unter gewissen Umständen in ihrem Vertrauen geschützt werden muss.[695] Das Bundesgericht hat einen Katalog an Voraussetzungen entwickelt, bei deren Erfüllung das Vertrauen des Betroffenen in eine falsche Aussage geschützt werden kann, was etwa zur rechtlichen Bindung der Behörde an die getätigte Aussage, aber auch zum Ersatz des daraus für den Betroffenen resultierenden Schadens führen kann.[696] Die Voraussetzungen für den Vertrauensschutz sind danach erfüllt, wenn: a) es sich um eine vorbehaltlose Auskunft der Behörden handelt; b) die Auskunft sich auf eine konkrete, den Bürger berührende Angelegenheit bezieht; c) die Amtsstelle, welche die Auskunft gegeben hat, hierfür zuständig war oder der Bürger sie aus zureichenden Gründen als zuständig betrachten durfte; d) der Bürger die Unrichtigkeit der Auskunft nicht ohne Weiteres hat erkennen können; e) der Bürger im Vertrauen hierauf nicht ohne Nachteil rückgängig zu machende Dispositionen getroffen hat; f) die Rechtslage zur Zeit der Verwirklichung noch die gleiche ist wie im Zeitpunkt der Auskunftserteilung; g) das Interesse an der richtigen Durchsetzung des objektiven Rechts dasjenige des Vertrauensschutzes nicht überwiegt.[697]

288 Diese Voraussetzungen stammen aus einer Zeit, in welcher Private die Behörden noch mit konkreten Fragen anhand eines Amtsbesuchs oder per Telefon oder E-Mail konsultierten. Mit der Verbreitung des Internets erkannten jedoch die Verwaltungen dessen Potenzial und begannen (auch im Geiste von Gesetzesbestimmungen wie dem bereits thematisierten Art. 6 Abs. 3 BGÖ)[698] damit, wichtige Informationen in der Form von Merkblättern oder «FAQ»[699] auf ihren Websites zu publizieren. Dadurch steht der behördlichen Auskunft nun nicht mehr ein konkreter Fall gegenüber, sondern eine Vielzahl möglicher Fälle. Es ist daher fraglich, ob die vom Bundesgericht entwickelten Regelungen auf diese Konstellation angewendet werden können und ob die Amtsstellen sich somit auf die dort veröffentlichten Informationen behaften lassen müssen. Diese Frage ist von Lehre und Rechtsprechung bis heute noch nicht abschliessend geklärt worden.[700]

695 Vgl. HÄFELIN/MÜLLER/UHLMANN, N. 624 ff.

696 Vgl. etwa ROHNER, SG Komm. BV, Art. 9, N. 52.

697 BGE 137 II 182, E 3.6.

698 Siehe oben Rz. 239 ff.

699 «Frequently Asked Questions», eine Zusammenstellung häufig gestellter Fragen.

700 Vgl. HÄFELIN/MÜLLER/UHLMANN, N. 670.

289 Problematisch ist dies einerseits hinsichtlich der Voraussetzung, dass die Auskunft sich auf eine konkrete, den Privaten berührende Angelegenheit beziehen muss. Unbestritten ist, dass die erteilte Auskunft eine gewisse inhaltliche Bestimmtheit aufzuweisen hat.[701] Stellt eine Behörde über ihre Website Informationen zur Verfügung, so ist es ihr kaum möglich, jeden denkbaren Sachverhalt konkret abzudecken, zu welchem der Rechtssuchende im Internet eine Antwort sucht. Auch kann eine entsprechende Anfrage sehr unspezifisch sein oder ein gefundenes Ergebnis aus dem Zusammenhang gerissen oder falsch interpretiert werden.[702] Lange Zeit war daher die Auffassung vorherrschend, dass eine derartige allgemeine Auskunft nicht bindend sein kann, sondern dass für die Verbindlichkeit eine Auseinandersetzung mit dem konkreten Sachverhalt gegeben sein muss.[703] Allerdings wird mittlerweile zumindest in gewissen Teilen der Lehre und Rechtsprechung davon ausgegangen, dass eine Auskunft auf einem vorgedruckten Formular durchaus eine Vertrauensbasis darstellen kann, auch wenn sie nicht konkret an einen individuellen Adressaten gerichtet ist, zumal derartige Merkblätter eine einheitliche und rechtsgleiche Praxis gewährleisten können.[704] Letztendlich ist wohl nach den Umständen des Einzelfalls zu beurteilen, ob die entsprechende Auskunft als Vertrauensgrundlage in Betracht gezogen werden kann. Zumindest in den Fällen, in welchen die Auskunft gezielt der Information der betreffenden Personen dient, kann eine Eignung kaum von vorneherein verneint werden.[705]

290 Ebenfalls Schwierigkeiten bringt im Zusammenhang mit der Online-Information mit sich, dass die Auskunft, um vertrauensbildend zu wirken, vorbehaltslos erfolgen muss. Eine behördliche Auskunft wird als nicht schützenswert erachtet, wenn die Behörde zum Ausdruck bringt, dass sie sich in dieser Frage nicht festlegen möchte.[706] Viele Gemeinwesen bedienen sich daher einer Praxis aus der Privatwirtschaft und bringen auf ihrer Internetsite einen Vorbehalt (sog. «Disclaimer») an, dass sie keine Gewährleistung für die Richtigkeit der Inhalte übernehmen und insbesondere Haftungsansprüche, welche sich aus deren Inhalt ergeben, ablehnen.[707] Auf kantonaler Ebene wird für gewisse Bereiche (z.B. Geodaten) ein entsprechender Haftungsausschluss teilweise gar als generell-konkrete Regelung im jeweiligen Verordnungsrecht

701 Vgl. HÄFELIN/MÜLLER/UHLMANN, N. 668.

702 Vgl. KETTIGER, in: Jahrbuch 2016/2017, S. 116.

703 Vgl. IMBODEN/RHINOW, Bd. 1, S. 469.

704 Vgl. etwa BGE 129 II 125, E. 5.6; vgl. auch Vgl. HÄFELIN/MÜLLER/UHLMANN, N. 670; UHLMANN/STOJANOVIC, SZW, 2017, S. 736.

705 Vgl. HÄFELIN/MÜLLER/UHLMANN, N. 670.

706 HÄFELIN/MÜLLER/UHLMANN, N. 682.

707 Vgl. etwa den Disclaimer auf der Website des Kantons Basel-Landschaft.

statuiert.[708] Es ist aus mehreren Gründen zu bezweifeln, ob eine solche Beschränkung rechtswirksam vorgenommen werden kann.

In der Lehre wird ein entsprechender «Disclaimer» regelmässig als wenig zweckmässig angesehen.[709] Gegen die Wirksamkeit solcher Klauseln spricht einerseits der zwingende Charakter des Staatshaftungsrechts, welcher einer Wegbedingung der Haftung des Staates entgegensteht.[710] Wo durch das Gesetz eine rechtliche Pflicht zur Publikation von Daten in einer gewissen Qualität besteht, ist ein Haftungsausschluss durch einen Hinweis auf der Website oder auf Verordnungsstufe nicht zweckmässig, da auf diese Weise bundesrechtliche Vorgaben auf tieferer Hierarchiestufe ausgehebelt werden könnten.[711] Allerdings wird die Möglichkeit einer Einwilligung im Staatshaftungsrecht nicht grundsätzlich abgelehnt.[712] In jedem Fall müsste die Kenntnis des Haftungsausschlusses sichergestellt und ein derartiges Einverständnis mit dem «Disclaimer», auch um die Beweisbarkeit sicherzustellen, durch eine klare Zustimmung – etwa des Betätigens eines Buttons bei Betreten der Website – eingeholt werden.[713] In der Praxis befindet sich ein entsprechender «Disclaimer» indes meist reichlich versteckt auf der Website und wird daher von kaum einem Benutzer je gelesen.[714] Dies ist umso problematischer, als die entsprechenden Haftungsausschlüsse auch für die ganze Site Geltung beanspruchen, was somit dazu führen würde, dass keine einzige auf der Website getätigte Aussage Vertrauensfolgen auslösen kann.[715] 291

Zusammenfassend ist es m.E. nicht zuletzt aufgrund dieser vorherrschenden technischen Umsetzung fraglich, ob die Haftung auf diese Weise wegbedingt werden kann. Es dürfte hier den Behörden obliegen, für Rechtssicherheit zu sorgen. Denkbar wäre allenfalls eine technische Lösung, wie diese bereits von vielen Websites auch im privaten Bereich im Hinblick auf die Erhebung von Randdaten (Cookies etc.) verfolgt wird. Der Benutzende müsste dann beim Betreten der Website vom Haftungsausschluss Kenntnis nehmen und diesen durch Anklicken eines Buttons bejahen. Ob diese Zustimmung auch bewusst erfolgt oder das Fenster einfach weggeklickt wird, ist erfahrungsgemäss zu 292

708 KETTIGER, in: Jahrbuch 2016/2017, S. 118 f.

709 HÄFELIN/MÜLLER/UHLMANN, N. 670. KETTIGER, in: Jahrbuch 2016/2017.

710 Vgl. UHLMANN, Staatshaftungsrecht, N. 149 oder WEBER/LAUX/OERTLY, S. 190.

711 KETTIGER, in: Jahrbuch 2016/2017, S. 118 f.

712 Teilweise sogar explzit vorgesehen, vgl. UHLMANN, Staatshaftungsrecht, N. 149.

713 KETTIGER, in: Jahrbuch 2016/2017, 118 f.

714 Vgl. etwa den Disclaimer auf der Website des Kantons Basel-Landschaft.

715 Dies ist insbesondere problematisch, wenn die entsprechende Behörde kein weiteres Publikationsorgan hat, womit jeglicher Kommunikation die Verbindlichkeit abgehen würde, vgl. UHLMANN/STOJANOVIC, SZW, 2017 S. 736 f.

bezweifeln. Eine weitere Möglichkeit wäre eine gesetzliche Regelung, in welcher ein entsprechender Vorbehalt angebracht wird. Dies ist indes nur dort zulässig, wo keine höherrangige Verpflichtung besteht, Daten in einer gewissen Qualität zu publizieren.

293 Trotz der inzwischen beachtlichen Masse an auf Behörden-Websites publizierten Informationen fand eine gerichtliche Auseinandersetzung mit diesem Thema bisher noch nicht statt. Dies lässt darauf schliessen, dass nur in seltenen Fällen ausschliesslich gestützt auf Internetinformation hin nicht wiedergutzumachende Dispositionen ergriffen wurden oder dass im Zweifelsfall vor entsprechenden Ausgaben noch einmal auf anderem Wege bei der Behörde nachgefragt wird.

3. Haftung für den Social-Media-Auftritt

294 Im Grundsatz unterscheiden sich die Information und Kommunikation über Social-Media-Plattformen nicht von der herkömmlichen Internetkommunikation, was ihre Rechtsfolgen angeht. Für Aussagen auf diesen Angeboten wird daher ebenfalls nur gehaftet, wenn die entsprechenden Voraussetzungen gemäss dem einschlägigen Staatshaftungsrecht gegeben sind. Auch der Vertrauensschutz für Aussagen durch Behörden auf Social-Media-Plattformen ist grundsätzlich nach den soeben dargestellten Vorgaben zu bewerten. Wohl ist bei der Kommunikation über Facebook eine bessere Orientierung an der konkreten Anfrage des Gesprächspartners möglich, da etwa Nachfragen (z.B. via Kommentarfunktion) möglich sind. Jedoch ist auch zu beachten, dass wichtige Fragen durch den auskunftssuchenden Bürger kaum in erster Linie über Social Media gestellt und beantwortet werden.[716]

295 Zu beachten bleibt, dass der Staat mit seiner Social-Media-Präsenz auch eine Plattform für den Austausch unter Personen bietet, auf welcher diese untereinander kommunizieren können, etwa indem sie ihre jeweiligen Beiträge kommentieren. Dabei kann es auch zu strafrechtlich (etwa Beschimpfungen) und/oder zivilrechtlich (Persönlichkeitsverletzungen) relevanten Handlungen unter den Teilnehmenden kommen.[717] Es ist daher zu prüfen, ob der Staat, welcher die Plattform für die entsprechenden Aussagen bietet, hier eine Mitverantwortung trägt und allenfalls auch ins Recht gefasst werden kann. Immerhin ist bei einer Persönlichkeitsverletzung gemäss Art. 28 ZGB jeder passivlegitimiert, welcher an dieser mitwirkt, wobei diese Voraussetzung weit zu verstehen ist.[718] Das Bundesgericht hat hinsichtlich eines privaten

716 Vgl. LANGER, AJP, 2014, S. 954 ff.

717 Bericht Social Media 2017, S. 62.

718 MEILI, BSK ZGB I, Art. 28, N. 37.

Betreibers eines Forums (einer Zeitung) festgelegt, dass die Schweiz im Gegensatz zu anderen Ländern keine Haftungsprivilegierung für Anbietende von Internetdienstleistungen kennt und somit die allgemeinen Regeln von Art. 28 ZGB zum Einsatz gelangen. Demgemäss erachtete es eine Haftung als denkbar, wenn die Beiträge Dritter nicht regelmässig kontrolliert oder auf Aufforderung hin nicht gelöscht werden.[719]

296 Es ist aufgrund dieser Rechtsprechung nicht abzusehen, dass der Staat umfassender haften sollte.[720] Das Bundesgericht regt im entsprechenden Entscheid an, dass die bisherige Regelung allenfalls zu unerwünschten Konsequenzen führen kann, es jedoch nicht Sache der Justiz, sondern des Gesetzgebers sei, diese zu korrigieren.[721] Der Bundesrat befasste sich daraufhin mit der Frage, ob eine entsprechende Anpassung der gesetzlichen Regelungen notwendig sei. Er kam dabei zum Schluss, dass auch das geltende Recht genügend Instrumente biete, um den Kreis der Passivlegitimierten einzuschränken. So müsse der Beitrag an der Verletzung als adäquat kausal angesehen werden können und insbesondere aus Verhältnismässigkeitsgründen dort von einer Haftung abgesehen werden, wo der Bezug zur Rechtsverletzung verschwindend klein ist.[722] Auch aufgrund der ständigen technischen Entwicklung erachtete der Gesetzgeber eine umfassende Regelung zur Beschränkung der Passivlegitimation als kaum umsetzbar.[723] Daraus folgend ist es durchaus möglich, dass der Staat für Äusserungen Dritter auf seiner Facebook-Seite haftbar gemacht werden kann, wenn sein Beitrag adäquat kausal zur Verletzung beigetragen hat. Dies kann, wie im zitierten Bundesgerichtsentscheid ausgeführt, der Fall sein, wenn etwa ein verletzender Kommentar trotz Aufforderung nicht gelöscht wurde. Wie weiter oben ausgeführt, kann die Löschung von Kommentaren ihrerseits Auswirkungen auf die Grundrechte (insbesondere die Meinungsfreiheit) des Verletzenden haben. Liegt jedoch eine relevante Persönlichkeitsverletzung vor, so sollte die Löschung zum Beispiel durch Art. 28 ZGB als gesetzliche Grundlage gedeckt sein.[724]

4. Haftung für Verlinkung anderer Angebote

297 Auf staatlichen Websites oder Social-Media-Plattformen können auch sogenannte «Hyperlinks» angebracht werden, also Querverweise zu anderen

719 Urteil des BGer 5A_792/2011 vom 14. Januar 2013; vgl. zur privatrechtlichen Verantwortlichkeit CIOLA-DUTOIT/COTTIER, medialex, 2008, S. 72.

720 Vgl. LANGER, AJP, 2014, S. 945 f.

721 Urteil 5A_792/2011 vom 14. Januar 2013, E. 6.3.

722 Bericht Provider, S. 97; konkretisierend etwa BGE 141 III 513.

723 Vgl. etwa Bericht Provider, S. 98.

724 Siehe dazu oben Rz. 265.

Angeboten oder Websites, welche nicht von der jeweiligen Behörde betrieben werden. Nun ist es möglich, dass eine entsprechend verlinkte Seite rechtswidrige Inhalte enthält oder aufgrund einer dortigen Auskunft die Privatperson zu Schaden kommt. Es ist in diesem Zusammenhang fraglich, ob die Behörde eine Verantwortlichkeit übernehmen muss für den Inhalt der verlinkten Homepage, da sie immerhin auf die jeweilige Seite hinweist. Auch diese Frage wurde bisher erst im privatrechtlichen Bereich diskutiert, wobei für die Verantwortlichkeit in erster Linie darauf abgestützt wird, ob durch die Verlinkung eine Sorgfaltspflicht verletzt wurde.[725] Indes erscheint eine Verlinkung auf private Angebote für eine Behörden-Website grundsätzlich nicht zweckdienlich. Sinnvoll erscheinen Links in erster Linie, wenn auf andere öffentlich-rechtliche Körperschaften oder auf Private, welche öffentlich-rechtliche Aufgaben erfüllen, verwiesen wird.[726] Viele Websiten der öffentlichen Verwaltung behelfen sich indes auch hier damit, im Rahmen eines «Disclaimers» darauf hinzuweisen, dass der Besuch verlinkter Angebote auf eigene Gefahr des Nutzers geschieht und keinerlei Verantwortung durch den Betreiber übernommen wird.[727] Wie weiter oben bereits beschrieben wurde, ist umstritten, ob bzw. unter welchen Umständen ein solcher Haftungsausschluss mittels «Disclaimer» für öffentliche Organe gültig vorgenommen werden kann.[728]

5. Haftung für Open Government Data

298 Publiziert eine Behörde Daten als Open Government Data (OGD) zur expliziten Weiterverwendung, so stellt sich ebenfalls die Frage, inwiefern sie zur Verantwortung gezogen werden kann, wenn diese Daten fehlerhaft sind und sich daraus für jemanden ein Schaden ergibt. Auch hier sind grundsätzlich die bereits erläuterten Prinzipien des Staatshaftungsrechts anzuwenden. Aus verschiedenen Gründen kann davon ausgegangen werden, dass die Publikation von Daten als Open Government Data für den Staat grundsätzlich lediglich ein geringes Haftungsrisiko mit sich bringt.[729] Einerseits ist auch bei der Publikation von Datensätzen im Rahmen von Open Government Data wohl mehrheitlich erst im Nachhinein festzustellen, ob die Daten auf inhaltlicher Ebene fehlerhaft waren. Daraus ergibt sich, dass, ausser bei krassen Fällen

725 Vgl. FRECH, S. 32.

726 Vgl. etwa die Website des Kantons Aargau, welche dies explizit festhält.

727 Vgl. hierzu ebenfalls den Webauftritt des Kantons Aargau.

728 Siehe oben Rz. 290 ff.

729 Vgl. LAUX, S. 18; FRAEFEL/KUHN/NEURONI/RIEDL/SCHMID, S. 69; WEBER/LAUX/OERTLY, S. 179 ff.

von Pflichtverletzungen durch den zuständigen Beamten, kaum je eine Verhaltensunrecht begründende Widerrechtlichkeit vorliegen kann.[730]

Anderseits stellt sich bei der Vertrauenshaftung ebenfalls das Problem, 299
dass eine Behörde bei der Publikation eines Datensatzes nicht voraussehen kann, von wem und zu welchem Zweck dieser benutzt wird. Zwar besteht diese Unsicherheit auch bei online publizierten Merkblättern, welche gemäss der hier vertretenen Ansicht durchaus eine Vertrauensgrundlage darstellen können.[731] Jedoch wird mit den online als OGD publizierten Daten in noch kleinerem Masse eine Aussage getroffen, sondern diese werden lediglich der Öffentlichkeit zur Verfügung gestellt. Eine Haftung ist allenfalls dann möglich, wenn eine Behörde konkrete Kenntnis hatte, wozu ein möglicher Empfänger die Daten einsetzen will.[732] Zu denken ist dabei etwa daran, dass ein publizierter Datensatz aufgrund der darin erhaltenen Daten nur einen bestimmten Zweck erfüllen kann (z.B. Flugpläne, gewisse Landkarten) oder die Behörde konkret aussagt, dass ein Datensatz für den Einsatz in einem gewissen Gebiet geeignet ist.[733]

6. Fazit

Auch im Bereich der behördlichen Tätigkeit im Internet haftet der Staat für 300
Schäden, welche Privaten durch falsche Auskünfte oder widerrechtliches Handeln des Staates zugefügt wurden. Die entsprechenden Rechtsgrundlagen stehen einer Haftung für die Internettätigkeit grundsätzlich nicht entgegen. Problematisch kann indes bei der Informationstätigkeit des Staats einerseits sein, dass sich Fehler oftmals erst im Nachhinein als solche herausstellen und daher selten die notwendige Schwelle für widerrechtliches Handeln erreicht wird. Bei auf der Website oder als Open Government Data publizierten Informationen oder Datensätzen ist zudem fraglich, ob diese als vorbehaltslose und an den Einzelnen gerichtete Vertrauensgrundlage überhaupt geeignet sind. Dies kann zumindest für Websites unter Umständen angenommen werden. Es ist festzustellen, dass sich Bund und Kantone bisher kaum damit befasst haben, welche Auswirkungen die Anerkennung von Internetinformation als Vertrauensgrundlage für sie haben kann. Oftmals begnügen sie sich damit, auf ihrer Website darauf aufmerksam zu machen, dass sie keine Haftung für die Richtigkeit der Inhalte übernehmen. Es ist allerdings fraglich, ob durch solche «Disclaimer» die Haftung rechtsgültig

730 Vgl. WEBER/LAUX/OERTLY, S. 179.

731 Siehe weiter oben Rz. 289.

732 WEBER/LAUX/OERTLY, S. 179 ff.

733 Vgl. LAUX, S. 12 f.

ausgeschlossen werden kann. Daher ist es wichtig, dass der Staat bei seiner Informationstätigkeit im Internet grösstmögliche Sorgfalt walten lässt, um keine fehlerhaften Informationen zu publizieren. Dies gilt auch, wenn er Angebote auf seiner Webseite verlinkt oder auf einem Social-Media-Kanal eine Plattform für Diskussionen bietet. Hier muss das öffentliche Organ im Rahmen seiner Sorgfaltspflicht etwa darauf achten, dass persönlichkeitsverletzende Beiträge auf Aufforderung hin gelöscht werden. Aus der Tatsache, dass sich bisher kaum gerichtliche Entscheidungen in diesen Angelegenheiten finden lassen, ist entweder zu schliessen, dass die Behörden ihrer Sorgfaltspflicht gut nachkommen oder dass es schlicht kaum zu entsprechenden Schäden kommt bzw. dass diese nicht die Intensität erreichen, welche eine gerichtliche Intervention der Betroffenen bewirken.

IV. Zusammenfassung

301 Das informelle Verwaltungshandeln hat sich durch die Informations- und Kommunikationstechnologie verändert. Dies zeigt sich daran, dass es eine grosse Vielfalt an Angeboten gibt, die Verwaltungsinformationen online zugänglich machen, sei dies über Websites, Social-Media-Plattformen oder Apps. Diese Angebote tragen dazu bei, dass die Verwaltung heutzutage effizienter und transparenter informieren kann als in der Zeit vor dem Internet. Die Transparenz des Verwaltungshandelns stellt ein Ziel des E-Government dar, welches auf diese Weise gefördert werden konnte.

302 Die Informationstätigkeit der Verwaltung über Internet lässt sich weitestgehend in den bestehenden Rechtsrahmen einfügen. Einen Grund dafür stellt dar, dass Verfassung und einschlägige Gesetze kaum Vorgaben hinsichtlich der Ausgestaltung der Kommunikationstätigkeit machen. In einigen Bereichen waren indes Gesetzesanpassungen notwendig, um die rechtskonforme Abwicklung garantieren zu können. So musste etwa im Rahmen von Anpassungen des BGÖ und des DSG klargestellt werden, dass Personendaten im Rahmen der Behördeninformation nur publiziert werden dürfen, sofern und solange das öffentliche Interesse daran überwiegt. Die entsprechenden Informations- und Kommunikationsmöglichkeiten treten bisher ergänzend zu den bestehenden Kommunikationsmitteln hinzu, so dass auch Personen, welche z.B. aufgrund ihres Alters nicht über Internetzugang oder die entsprechenden Fertigkeiten verfügen, dadurch nicht diskriminiert werden. Betreffend die Online-Publikation der amtlichen Publikation hatte sich die Rechtsprechung auch damit zu befassen, ob es in gewissen (vorderhand eng begrenzten) Rechtsbereichen zulässig ist, ausschliesslich online zu informieren. Dies wurde dann bejaht, wenn für nicht digitalaffine Bevölkerungsteile Vorkehrungen im Sinne

von Übergangsregelungen oder Konsultationsmöglichkeiten vor Ort getroffen wurden und die Regelungen so ausgestattet sind, dass die Ausübung anderer Grundrechte nicht vereitelt wird.

Sofern eine konkrete Informationshandlung im Internet grundrechtliche Rechtspositionen verletzt, stehen den Betroffenen gewisse Rechtsschutzmöglichkeiten offen. Sie können etwa gemäss Art. 25a VwVG eine Verfügung über den jeweiligen Realakt erlangen oder datenschutzrechtliche Behelfe ergreifen. Sofern ihnen durch eine Informationshandlung ein Schaden entsteht, ist auch im Internet die Staatshaftungsgesetzgebung zu beachten. 303

In einigen Teilbereichen sind die Behörden online tätig, ohne dass eine vertiefte Auseinandersetzung mit den damit für die Privaten bestehenden Rechtsfolgen stattgefunden hat. Zu gelten hat dies insbesondere für die Tätigkeit auf Social-Media-Plattformen. Hier kennen viele öffentliche Organe im Rahmen ihres Auftrittes zwar Regeln für die eigenen Mitarbeitenden und für die Personen, welche diese Plattform besuchen. Ungeregelt ist jedoch, wie mit Personen zu verfahren ist, welche den Betrieb stören oder ungewünschte Meinungen kundtun. Sofern keine straf- oder zivilrechtlich relevanten Äusserungen vorliegen, kann es mangels entsprechender gesetzlicher Grundlagen als Verletzung der Meinungsfreiheit angesehen werden, wenn Personen vom jeweiligen Auftritt ausgesperrt werden. Es ist daher in der aktuellen Situation anzuraten, die Sperrung von Personen oder die Löschung von Kommentaren Privaten zu überlassen. Ebenfalls keine detaillierte Regelung findet aktuell die Erhebung von Randdaten auf der Website oder Social-Media-Angeboten zu Analysezwecken. Hier besteht eine beachtliche Rechtsunsicherheit einerseits hinsichtlich der Frage, ob es sich bei den entsprechenden Daten um Personendaten handelt, anderseits hinsichtlich der gesetzlichen Grundlage. Aus diesem Grund sollten Behörden aktuell im Bereich der Analyse von Nutzerdaten zurückhaltend agieren oder bestenfalls ganz darauf verzichten. 304

Fragezeichen ergeben sich letztlich bei der Haftung von Behörden für Inhalte ihrer Internetauftritte. Problematisch ist hier insbesondere die Offenheit des Adressatenkreises. Dadurch ist den Behörden oftmals nicht bewusst, wer die entsprechende Information in welchem Sinne nutzt. Es muss davon ausgegangen werden, dass gewisse Informationen durchaus als haftungsbegründende Vertrauensgrundlage für Private dienen können. Es ist meines Erachtens naheliegend zu verneinen, dass die auf den Websites angebrachten Haftungsausschlüsse im Falle einer gerichtlichen Auseinandersetzung eine Verantwortlichkeit wirksam wegbedingen können. 305

§ 4 Elektronischer Rechtsverkehr

306 Ein grosser Teil des Verwaltungshandeln ist auf den Erlass einer Verfügung ausgerichtet und lässt sich daher dem rechtlichen Verwaltungshandeln zuordnen. Durch das Aufkommen von E-Mail und Internet haben sich in erster Linie neue Möglichkeiten ergeben, mit der Verwaltung innerhalb von Verfahren zu kommunizieren.[734] Auf diese Weise soll es eines Tages möglich sein, Rechtsfälle komplett elektronisch abzuwickeln, was als elektronischer Rechtsverkehr umschrieben wird.[735] Im Bund und vielen Kantonen wurden daher bereits Möglichkeiten geschaffen, um mit der Verwaltung im Rahmen von Verfahren elektronisch zu kommunizieren. Im Folgenden soll betrachtet werden, welche Auswirkungen diese Veränderungen auf die Rechte der Betroffenen haben können. Das erstinstanzliche Verwaltungsverfahren, welches in der Regel im Erlass einer Verfügung endet, ist dabei in den Verwaltungsverfahrensgesetzen des Bundes und der Kantone geregelt.[736] Diese Verwaltungsverfahrensgesetze können vorsehen, dass gewisse Verfahren von deren Geltungsbereich ausgenommen werden (im Bund Art. 2 und 3 VwVG) oder in Spezialgesetzen eingehender geregelt werden (im Bund Art. 4 VwVG). Es sprengt den Rahmen dieser Arbeit, sämtliche möglichen Konstellationen abzudecken, so dass sich der Betrachtungsgegenstand grundsätzlich auf das Verwaltungsverfahren, wie es in der Verwaltungsverfahrensgesetzgebung des Bundes geregelt ist, begrenzen wird. Kantonale oder spezialgesetzliche Regelungen sollen dort erwähnt werden, wo sie zusätzliche Aspekte einbringen.

307 Unter dem Titel des elektronischen Rechtsverkehrs soll es Verfahrensparteien in erster Linie ermöglicht werden, auf elektronischem Weg anstatt auf Papier mit den Verwaltungsbehörden zu kommunizieren. Verbunden damit sind jedoch auch Anpassungen in der Aktenführung, der Archivierung oder der Akteneinsicht.[737] Damit der elektronische Verkehr im Rahmen von Verwaltungs- und Gerichtsverfahren zulässig ist, wird eine entsprechende gesetzliche Grundlage benötigt.[738]

308 Auf Bundesebene wurden im Rahmen der Totalrevision der Bundesrechtspflege zu Beginn der 2000er-Jahre die entsprechenden Grundlagen geschaffen. Das Gesetz sieht in Art. 11b VwVG vor, dass Parteien eine elektro-

734 Für die Kommunikation ausserhalb des Verfahrens siehe weiter oben Rz. 247 ff.

735 Bericht Bischof, S. 5.

736 Vgl. etwa Art. 5 VwVG.

737 Bericht Bischof, S. 6. Auf diese Aspekte soll im Rahmen dieser Arbeit, abgesehen vom Akteneinsichtsrecht, nicht detailliert eingegangen werden.

738 BGE 142 V 152, E. 2.4, m.w.H.

nische Zustellungsadresse wählen und Zustellungen an sie rechtsverbindlich elektronisch erfolgen können. Art. 21a VwVG statuiert die Möglichkeit und die Umstände der elektronischen Eingabe an Behörden. Art. 21a Abs. 2 VwVG sieht daher vor, dass elektronische Eingaben mit einer qualifizierten elektronischen Signatur gemäss dem Bundesgesetz vom 18. März 2016 über die elektronische Signatur versehen sein müssen. Zudem können weitere Vorgaben gemacht werden, etwa zu den zugelassenen Dateiformaten sowie dazu, ob eine bestimmte anerkannte Zustellplattform verwendet werden muss oder die Eingabe auch ungesichert per E-Mail erfolgen kann. Konkretisiert wird diese Gesetzesbestimmung durch die Verordnung über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens vom 18. Juni 2010 (VeÜ-VwV, SR 172.021.2).[739] In Art. 26 VwVG wird die elektronische Akteneinsicht geregelt. In Art. 34 VwVG ist schliesslich die elektronische Eröffnung von Verfügungen mit dem Einverständnis der Partei geregelt. Die entsprechenden Änderungen traten per 1. Januar 2007 in Kraft. Auch viele – indes noch nicht alle – Kantone sehen inzwischen in ihren entsprechenden Verfahrensordnungen Regelungen zum elektronischen Rechtsverkehr vor.[740]

309 Aus rechtlicher Sicht können sich in verschiedenen Phasen eines Verfahrens im Zusammenhang mit dem elektronischen Rechtsverkehr und mit den soeben genannten Bestimmungen rechtliche Probleme (insbesondere hinsichtlich des Rechts auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV und hinsichtlich des rechtlichen Gehörs nach Art. 29 Abs. 2 BV) für die Betroffenen ergeben, welche im Folgenden betrachtet werden. Das Verwaltungsverfahren ist grundsätzlich wenig formalisiert und lässt sich, etwa im Gegensatz zu Gerichtsverfahren, oft nicht trennscharf in verschiedene Verfahrensschritte aufteilen.[741] In einem ersten Schritt hat eine Eröffnung des Verfahrens stattzufinden. Es ist anerkannt, dass es zwei mögliche Arten gibt, wie ein Verfahren eröffnet werden kann: Entweder leitet die Behörde von sich aus – also von Amtes wegen – ein Verfahren ein, oder eine Privatperson stellt ein Gesuch auf Erteilung eines Rechts oder Feststellung eines Rechtszustands, woraufhin die Behörde dieses zu beurteilen hat.[742] Im Laufe des Verfahrens dürfen oder müssen die Parteien im Rahmen ihrer Mitwirkungspflicht[743] unter Umständen weitere Eingaben an die Behörde tätigen, und es ist ihnen

739 Vgl. EGLI, PK VwVG, Art. 21a, N. 21.

740 Für eine Übersicht aus dem Jahr 2016 vgl. Fischer, Elektronischer Behördenverkehr im Kanton Bern.

741 HÄNER, in: Jahrbuch 2017/2018, S. 26.

742 Vgl. etwa KIENER/RÜTSCHE/KUHN, S. 116–118.

743 Vgl. dazu etwa Art. 13 VwVG, siehe dazu unten Rz. 400 ff.

nach Art. 29 BV das rechtliche Gehör zu gewähren. Seinen Abschluss findet das erstinstanzliche Verfahren nach dem VwVG in der Regel durch den Erlass einer Verfügung. Aufgrund der soeben ausgeführten Bestimmungen des VwVG erachtet der Autor es hinsichtlich des elektronischen Rechtsverkehrs als opportun, das Verfahren für die vorliegende Betrachtung in die Verfahrenseröffnung, elektronische Eingaben im Verfahrensverlauf und das Verfahrensende aufzuteilen.

I. Verfahrenseröffnung

310 Nach dem soeben Ausgeführten wird das Verfahren entweder durch die Behörde von Amtes wegen eingeleitet oder eine Privatperson stellt ein Gesuch auf Erteilung eines Rechts oder Feststellung eines Rechtszustands, woraufhin die Behörde dieses zu beurteilen hat.[744] Die beiden Arten der Verfahrenseröffnung sind in unterschiedlichem Masse von der Digitalisierung betroffen. Eröffnet die Behörde das Verwaltungsverfahren von sich aus, so kann dieser Schritt durchaus mithilfe von digitaler Technologie erfolgen, etwa indem in der betreffenden Geschäftsführungssoftware ein neuer Fall eröffnet wird. Obliegt es der betroffenen Partei, ein Verwaltungsverfahren durch die Stellung eines Gesuchs in Gang zu bringen, sind ebenfalls Szenarien denkbar, in denen dies mithilfe von Internet- oder Kommunikationstechnologien geschehen kann. Für Privatpersonen kann es etwa eine Erleichterung darstellen, wenn sie ein Verfahren per E-Mail oder über ein Formular auf der Website in Gang bringen können, anstatt persönlich bei der Behörde vorsprechen zu müssen.

311 Vor allem für die Benutzenden ist es sinnvoll, dass die entsprechenden Formulare an einem bestimmten Ort der Website gebündelt zur Verfügung stehen. Auf dieser oft als «Online-Schalter» bezeichneten Website können Formulare zum Download bezogen oder direkt online ausgefüllt werden.[745] Einen Zusatznutzen kann es für den Benutzenden auch bieten, wenn gewisse Daten, welche sich in der Regel nicht ändern (z.B. Name oder Geburtsdatum), nicht für jedes Gesuch erneut eingegeben werden müssen oder eine Übersicht über die hängigen Verwaltungsverfahren und deren Verfahrensstand angeboten wird. Damit die Daten den jeweiligen Benutzenden zugeordnet werden können und nur diese darauf Zugriff haben, muss für solche Applikationen die Möglichkeit der Registrierung und der Authentifizierung etwa mit einem Passwort im Rahmen eines sogenannten Behörden- oder Onlineportals vorgesehen

744 Vgl. etwa KIENER/RÜTSCHE/KUHN, S. 116–118.

745 Vgl. etwa den Online-Schalter des Kantons Basel-Landschaft.

werden.[746] Im Rahmen dieser Portale kann zwischen Fachanwendungen, welche jeweils nur einen bestimmten Rechtsbereich abdecken, und umfassenden Behördenportalen, deren Ziel es ist, alle verfügbaren elektronischen Dienstleistungen unter einem einzigen Dach zusammenzufassen, unterschieden werden. Übergreifende Portale werden dabei für mehrere Behörden betrieben, welche alle in gewissem Masse auf die darauf gespeicherten Daten Zugriff haben.[747] Verschiedene Kantone betreiben bereits ein entsprechendes Portal[748] oder haben zumindest die entsprechenden Rechtsgrundlagen geschaffen.[749] Im folgenden Kapitel soll betrachtet werden, ob diese verschiedenen Möglichkeiten der Verfahrenseröffnung auf elektronischem Weg mit der geltenden Rechtsordnung vereinbar sind.

A. Generelle Zulässigkeit

Im Gegensatz zum Strafprozess oder zum privatrechtlichen Gerichtsverfahren gibt es im erstinstanzlichen Verwaltungsverfahren grundsätzlich keinen formellen Akt der Verfahrenseröffnung.[750] Auch aus diesem Grund gibt es in der Verwaltungsverfahrensordnung des Bundes und der Kantone in der Regel keine gesetzliche Grundlage, welche sich explizit mit der Einleitung des Verfahrens befasst. Dementsprechend macht das Verwaltungsverfahren des Bundes die Eröffnung des Verfahrens nicht von expliziten einschränkenden Formvorschriften abhängig.[751] 312

1. Eröffnung durch die Behörde

Eröffnet eine Behörde das Verfahren von sich aus, so ist es zulässig, dass sie der Partei erst im Zeitpunkt der Gewährung des rechtlichen Gehörs die Verfahrenseröffnung mitteilt.[752] An die Eröffnung des Verfahrens sind daher grundsätzlich keine formellen Anforderungen gestellt. In der Regel wird dies wohl dadurch geschehen, dass die Behörde eine Akte zum jeweiligen Verfahren auf Papier oder – heutzutage wohl üblicher – in einem elektronischen Geschäftsführungssystem anlegt. Für die betroffene Person hat es dabei keine 313

746 Merkblatt Online-Portale, S. 2. Unter dem Begriff Portal wird ein im Internet verfügbarer Eintrittspunkt für Benutzerinnen und Benutzer zu den digitalen Dienstleistungen und Geschäftsabwicklungen mit öffentlichen Organen (kommunalen, kantonalen und Bundesbehörden) verstanden.

747 Vgl. zum Ganzen: Merkblatt Online-Portale.

748 Vgl. etwa den Guichet virtuel des Kanton Jura.

749 Vgl. REGIERUNGSRAT DES KANTONS BASEL-STADT, S. 6.

750 UHLMANN, in: Das erstinstanzliche Verwaltungsverfahren, S. 2 m.w.H.

751 UHLMANN, in: Das erstinstanzliche Verwaltungsverfahren, S. 3.

752 KÖLZ/HÄNER/BERTSCHI, N 388.

unterschiedlichen Rechtswirkungen, ob eine Fallakte aus Papier über sie angelegt wird oder ob die entsprechenden Daten in ein Computersystem eingegeben werden.[753] Die geltende Rechtsordnung steht grundsätzlich einer formlosen Eröffnung des Verfahrens nicht entgegen, so dass die Digitalisierung in diesem Bereich keine rechtlichen Auswirkungen für die Privaten nach sich zieht. Es ist jedoch zu beachten, dass gewisse Spezialgesetze formelle Voraussetzungen an die Eröffnung durch die Behörden stellen können und so die Formlosigkeit der Verfahrenseröffnung begrenzen.[754]

2. Eröffnung durch Gesuchstellung

314 Die Verwaltungsverfahrensgesetze machen – wie bereits ausgeführt – in der Regel auch keine Vorgaben darüber, in welcher Form ein Gesuch auf Eröffnung eines Verfahrens zu stellen ist. Inhaltliche Anforderungen finden sich allenfalls in spezialgesetzlichen Regelungen.[755]. Hierbei ist zu beachten, dass bei der Online-Einreichung über Gesuchsformulare oder per E-Mail einfacher über die Identität des Gesuchstellers getäuscht werden kann, als wenn ein Gesuch mündlich oder schriftlich (z.B. in Form eines unterschriebenen Briefs) gestellt wird. Es kann daher unter Umständen nicht nachgewiesen werden, ob die Person, welche das entsprechende Gesuch stellt, auch diejenige ist, für die sie sich ausgibt. Somit ist es theoretisch möglich, im Namen einer anderen Person – unter Umständen sogar gegen deren Willen – ein Gesuch zu stellen und somit ein Verwaltungsverfahren anzustossen. Im analogen Verkehr mit Behörden dient in der Regel die handschriftliche Unterschrift dazu, die Authentizität und Integrität der elektronischen Nachricht sicherzustellen.[756]

315 Wenn eine Eingabe per E-Mail oder über ein Online-Formular eingereicht wird, ist eine handschriftliche Unterzeichnung nicht mehr möglich. Mit dieser Problematik hatte sich auch der Gesetzgeber bei der Einführung des elektronischen Rechtsverkehrs mit Bundesbehörden zu befassen. Der Bundesgesetzgeber kam dabei zum Schluss, dass es den Betroffenen auch im elektronischen Rechtsverkehr möglich sein muss, ihr Einverständnis mit dem Inhalt kundzutun und zu erklären, dass sie die entsprechenden Rechtsfolgen auf

753 Zu beachten gilt es allenfalls, zu welchem Zeitpunkt ein Verfahren als eröffnet gilt, da die Festlegung dieses Zeitpunkts durchaus rechtliche Konsequenzen für die Parteien haben kann; vgl. dazu unten Rz. 331.

754 Vgl. etwa Art. 28 Abs. 1 KG, Eröffnung einer Untersuchung durch amtliche Publikation, UHLMANN, in: Das erstinstanzliche Verwaltungsverfahren, S. 4.

755 Vgl. HÄNER, in: Jahrbuch 2017/2018, S. 27 f; diese können dabei zusätzliche Erfordernisse an das Gesuch, etwa gewisse Formvorschriften, aber auch Erleichterungen vorsehen. Vgl. etwa Art. 18 AsylG, wonach jede Äusserung einer Person, mit der sie zu erkennen gibt, dass sie Schutz sucht, als Asylgesuch zu gelten hat.

756 Vgl. Botschaft ZertES, S. 5684 f.

sich nehmen, wie dies im analogen Rechtsverkehr durch die handschriftliche Signatur der Fall ist. Aus diesem Grund sieht Art. 21a Abs. 2 VwVG vor, dass elektronische Eingaben mit einer qualifizierten elektronischen Signatur versehen sein müssen. Zudem können weitere Vorgaben gemacht werden, etwa zu den zugelassenen Dateiformaten sowie dazu, ob eine bestimmte anerkannte Zustellplattform verwendet werden muss oder die Eingabe per E-Mail erfolgen kann.[757]

316 Der Begriff der Eingabe gemäss Art. 21a VwVG ist dabei nach der herrschenden Lehre grundsätzlich weit zu verstehen und umfasst alle schriftlichen Rechtsvorkehren im Rahmen eines Verfahrens, also sämtliche Rechtsschriften inklusive der Beilagen. Nicht erfasst werden schriftliche Mitteilungen ausserhalb des Verfahrens (z.B. Informationsanfragen) oder mündlicher Verkehr.[758] Zwar kann ein Gesuch auf Einleitung eines Verfahrens sich in gewissen Fällen aus einem formlosen schriftlichen Verkehr per E-Mail ergeben. Gerade dort, wo ein Gesuch unter der Verwendung eines von der Behörde zur Verfügung gestellten Online-Formulars eingereicht wird, kann ihm aber auch ein gewisser formeller Charakter, welcher einer Rechtsschrift ähnlich ist, nicht abgesprochen werden. Daher ist wohl aufgrund des weiten Begriffsverständnisses auch ein Gesuch auf Eröffnung eines Verfahrens als Eingabe im Sinne dieser Bestimmung zu verstehen und es sind somit die entsprechenden Vorgaben zu beachten.

317 Eine qualifizierte elektronische Signatur hat gemäss Art. 21a Abs. 2 VwVG nach den Vorgaben des ZertES zu erfolgen.[759] Hierbei sieht die vom Bundesgesetzgeber gewählte Regulierung vor, dass es keine vom Bund entwickelte Signaturlösungen gibt, sondern entsprechende Dienste durch Private entwickelt werden sollen, welche allerdings vom Bund anerkannt werden und zu diesem Zweck umfassende Voraussetzungen erfüllen müssen.[760] Dies führt dazu, dass es in der Schweiz verschiedenen Anbieter elektronischer Signaturen gibt.[761] Da die meisten Personen in einem Jahr nur wenige Male mit der Verwaltung Kontakt haben und diese Dienste teilweise mit Zusatzkosten oder weiterem Aufwand verbunden sind, werden sie aktuell in der Schweiz noch

757 Botschaft Rev. Bundesrechtspflege, S. 4260; zur Unsicherheit von E-Mail als Zustellungsart, siehe unten Rz. 329.

758 EGLI, PK VwVG, Art. 21, N. 3.

759 Siehe dazu oben Rz. 308.

760 Botschaft ZertES, S. 5693.

761 Für eine Übersicht vgl. die Liste der gemäss ZertES anerkannten Anbieterinnen von Zertifizierungsdiensten des Bundes: ADMIN, Liste der gemäss Bundesgesetz über die elektronische Signatur (ZertES) anerkannten Anbieterinnen von Zertifizierungsdiensten.

kaum genutzt.[762] Nach dem soeben Ausgeführten wäre es daher einem grossen Teil der Bevölkerung verwehrt, Verfahren per E-Mail oder über ein Gesuchformular online zu eröffnen. Dies scheint nicht praktikabel.

318 Abgeschwächt wird dieses Problem allerdings durch verschiedene gesetzliche Erleichterungen. So sieht einerseits Art. 6 VeÜ-VwV vor, dass auf eine elektronische Signatur verzichtet werden kann, wenn die Identifizierung der Absenderin oder des Absenders und die Integrität der Übermittlung in anderer geeigneter Weise sichergestellt sind.[763] Denkbar ist etwa, dass die betroffene Person im Rahmen eines Gesuches weitere Dokumente einreichen muss, über welche in der Regel nur sie selber verfügt. Betreibt die Behörde oder der Kanton ein Online-Portal, in welchem die entsprechenden Gesuche gestellt werden können, so kann die Identifizierung auch durch ein entsprechendes zuordenbares Benutzerkonto sichergestellt werden.[764] Zudem sieht die VeÜ-VwV in Art. 5 Abs. 2 und Art. 6 Abs. 2 vor, dass der Partei eine Nachfrist gesetzt werden soll oder kann, innert der die Eingabe per Post vorgenommen werden kann, wenn ihre Eingabe nicht gelesen werden kann oder eine elektronische Signatur fehlt.

319 Gerade dort, wo die Behörde ein Formular online bereitstellt, weckt sie dadurch auch berechtigte Erwartungen, dass aufgrund der Einreichung des ausgefüllten Formulars ein Verfahren eröffnet wird. Würde die Behörde daraufhin von der Eröffnung eines Verfahrens Abstand nehmen, so würde sie sich widersprüchlich verhalten. Es ergibt sich aus dem Rechtsgrundsatz der Wahrung von Treu und Glauben, welcher in Art. 9 BV als grundrechtlicher Anspruch verankert ist, dass sich solches Verhalten nicht zum Nachteil des Betroffenen auswirken darf.[765]

3. Fazit

320 Der informelle Charakter der Verfahrenseröffnung im Verwaltungsverfahren steht einer Verfahrenseröffnung auf elektronischem Wege grundsätzlich nicht entgegen bzw. begünstigt diese gar grundsätzlich. Bei der Verfahrenseröffnung von Amtes wegen ergeben sich für die Parteien keine Unterschiede dadurch, ob diese elektronisch erfolgt oder nicht. Wird das Verfahren durch ein Gesuch der Person per E-Mail oder Formular eröffnet, so stellt sich indes mangels Unterschrift die Frage, auf welche Weise die Identität und Integrität gewährleistet werden kann. Art. 21a VwVG verlangt für elektronische Eingaben

762 KRCMAR/MÜLLER/SCHEIBER/EXEL/MOTZET/BASTIN,. S. 29.

763 Vgl. EGLI, PK VwVG, Art. 21a, N. 21.

764 Gewisse Plattformen sehen gar ein Login mit SwissID vor; vgl. den Guichet virtuel des Kanton Jura.

765 TSCHENTSCHER, BSK BV, Art. 9, N. 23.

grundsätzlich eine elektronische Signatur. Diese Anforderung wird jedoch in verschiedener Weise abgeschwächt, etwa dadurch, dass der Identitätsnachweis auch auf andere Weise erbracht werden kann. Viele Behörden lassen daher in der Praxis die Eröffnung zumindest einfacher Gesuche oft auch per E-Mail oder Online-Formular zu.[766] Lediglich wo ein Sachgesetz weitere Voraussetzungen vorsieht, indem ein Gesuch etwa eine handschriftliche Unterschrift benötigt, ist auf diese strikteren Voraussetzungen zu bestehen.

B. Rechtliche Probleme

1. Informationelle Selbstbestimmung

Füllt eine Person ein Formular online aus und kann sie dieses direkt über das Internet oder gar über ein Online-Portal bei der jeweiligen Amtsstelle einreichen, so gibt sie Daten über sich bekannt, mit welchen sie bestimmt oder bestimmbar ist. Es handelt sich hierbei also um Personendaten im Sinne von Art. 3 DSG (bzw. der jeweiligen kantonalen Datenschutzgesetzgebungen). Je nach Aufgabe des spezifischen Formulars oder Portals kann es sich dabei gar um besonders schützenswerte Personendaten handeln.[767] Wenn durch die Zusammenstellung der erhobenen Daten wesentliche Aspekte der Persönlichkeit beurteilt werden können, so handelt es sich gar um ein Persönlichkeitsprofil im Sinne von Art. 3 lit. d. DSG. Wie sich bereits aus dem Gesetzeswortlaut von Art. 3 lit. e DSG ergibt, umfasst das Bearbeiten von Personendaten grundsätzlich jeden Umgang mit Personendaten und insbesondere auch das Beschaffen derselben. Die jeweilige Datenschutzgesetzgebung ist daher bei der Erhebung von Personendaten auch im Rahmen eines Online-Formulars oder Behördenportals zu respektieren. 321

Werden durch Organe des Bundes Personendaten bearbeitet, so bedürfen diese dazu gemäss Art. 17 DSG einer gesetzlichen Grundlage. Für besonders schützenswerte Personendaten oder Persönlichkeitsprofile wird gar ein Gesetz im formellen Sinne benötigt, welches die Bearbeitung ausdrücklich vorsieht (Art. 17 Abs. 2 DSG). Ob für ein bestimmtes Online-Formular oder ein Behördenportal eine gesetzliche Regelung notwendig ist und auf welcher Stufe diese zu erfolgen hat, ist hauptsächlich von der Ausgestaltung des Formulars abhängig. Relevant sein kann dabei neben der Menge und Art der betroffenen Daten oder deren Speicherung etwa auch, wie viele Amtsstellen und zu welchem Zweck Zugriff auf die jeweiligen Daten haben.[768] Angesichts 322

766 HÄNER, in: Jahrbuch 2017/2018, S. 28

767 Etwa wenn Daten über die Konfession zur Ermittlung der Kirchensteuerpflicht erhoben werden, da es sich dabei um Daten über religiöse Anschauungen handelt (vgl. Art. 3 lit. c Ziff. 1 DSG).

768 Vgl. zum Ganzen Merkblatt Online-Portale, S. 6.

der enormen Vielfalt an möglichen Datenbearbeitungen können an die gesetzliche Grundlage indes keine hohen Anforderungen gestellt werden, sondern es muss in der Regel ausreichen, dass die Informationsbearbeitung in einem klar ersichtlichen sachlichen Zusammenhang mit der Aufgabe des betreffenden Organs steht.[769]

323 Ebenfalls zu beachten sein dürfte in diesem Fall die Möglichkeit, dass beim Vorliegen einer Einwilligung im Einzelfall auf das Vorliegen einer gesetzlichen Grundlage im formellen Sinn verzichtet werden kann (vgl. Art. 17 Abs. 2 lit. c. DSG). Somit könnten die Benutzenden unter Umständen auch Daten bekanntgeben, zu deren Bekanntgabe sie nicht gesetzlich verpflichtet sind. Die Botschaft zum Datenschutzgesetz statuiert klar, dass auch bei einer Einwilligung gemäss lit. c. zumindest eine gesetzliche Grundlage im Sinne von Art. 17 Abs. 1 DSG vorliegen müsse.[770] Während die herrschende Lehre dieser Ansicht folgt[771], wird sie teilweise zunehmend kritisch betrachtet.[772] Im neuen Datenschutzgesetz soll daher in Art. 30 Abs. 4 E-DSG vorgesehen werden, dass von den Anforderungen an eine gesetzliche Grundlage nach Art. 30 Abs. 1 DSG (also einer gesetzlichen Grundlage im materiellen Sinn) auch abgewichen werden kann, wenn dessen Voraussetzungen (etwa das Vorliegen einer Einwilligung) erfüllt sind.[773] Nach der aktuellen Rechtslage dürfte – nach dem oben Ausgeführten – allerdings auch bei einer Einwilligung eine gesetzliche Grundlage zu fordern sein, auch wenn diese im jeweiligen Einzelfall durchaus weit gefasst sein kann. Damit eine Einwilligung als genügend betrachtet werden kann, hat diese in jedem Falle den Vorgaben von Art. 4 Abs. 5 DSG gemäss freiwillig und nach angemessener Information zu erfolgen. Da die Bekanntgabe oft auch im Sinne der Betroffenen ist, welche das Verfahren durch die Gesuchstellung überhaupt erst angestossen haben, dürfte es indes aus praktischer Sicht selten vorkommen, dass diese gegen eine entsprechende Bearbeitung rechtlich vorgehen.

324 Das soeben Geschriebene gilt ebenfalls, wenn die entsprechenden Formulare über ein Behördenportal mit einer Authentifizierung («Login») zugänglich gemacht werden. Ein zentrales Behördenportal bringt dem Privaten die Möglichkeit, eine Vielzahl von verschiedenen Daten zu speichern. Zudem

769 Botschaft DSG, S. 467. BALLENEGGER, BSK DSG/BGÖ, Art. 17 DSG, N. 18. Viele kantonale Regelungen sehen vor, dass eine Datenbearbeitung sich entweder auf eine gesetzliche Grundlage stützen oder zumindest zur Erfüllung einer gesetzlichen Aufgabe erforderlich sein muss, vgl. anstatt vieler Art. 9 IDG BL.

770 Botschaft DSG, S. 468.

771 Vgl. MUND, SHK-DSG, Art. 17, N. 14; BALLENEGGER, BSK DSG/BGÖ, Art. 17 DSG N. 25.

772 Bericht Normkonzept, S. 37 f.; JÖHRI, Handkommentar DSG, Art. 17, N. 75; PÄRLI, digma, 2014, S. 23; vgl. auch VASELLA, Kommentierung zum Urteil des BVGer A-3548/2018.

773 Botschaft Rev. DSG 2017, S. 7081.

ist es auch möglich, dass verschiedene Behörden Zugriff auf dieses Portal und die für sie relevanten Daten haben. Durch diese grössere Ansammlung von Personendaten und potenziellen Empfängern mehren sich auch die technischen Risiken sowie die Gefahr von Datenverlust oder -diebstahl. Aus diesen Gründen ist eine Regelung entsprechender Portale auf Gesetzesebene zu fordern. Diese sollte den Aufbau, die Rechte und Pflichten von Nutzern und Behörden und die Verantwortlichkeit explizit regeln.[774] Zudem spricht auch die durch ein Durchlaufen des Gesetzgebungsprozesses höhere demokratische Legitimierung für eine Regelung auf Gesetzesebene.[775]

a) Grundsätze der Datenbearbeitung

Neben den Vorgaben an die gesetzlichen Grundlagen sind im vorliegenden Kontext, sofern keine spezialgesetzlichen Grundlagen davon Abweichendes festlegen, auch die Datenbearbeitungsgrundsätze zu beachten.[776] Die Nichtbeachtung dieser Grundsätze durch Bundesorgane stellte eine Verletzung des Persönlichkeitsrechts dar.[777] In diesem ist einerseits das in Art. 4 Abs. 2 DSG geregelte Verhältnismässigkeitsprinzip zu erwähnen, gemäss dem nur diejenigen Daten beschafft werden sollen, welche für den jeweiligen Zweck explizit benötigt werden.[778] Weiter hat die Beschaffung von Personendaten und deren Zweck für die betroffenen Personen erkennbar zu sein. Ebenfalls zu beachten ist der Aspekt der Datensicherheit nach Art. 7 DSG.[779] 325

i) Verhältnismässigkeit

Aus dem Grundsatz der Verhältnismässigkeit ergibt sich, dass nur diejenigen Daten erhoben werden, welche von der Behörde zur Erfüllung der Aufgabe auch benötigt werden. Es ist offensichtlich, dass ein sozialhilferechtlicher Anspruch nur dann durch eine Behörde beurteilt werden kann, wenn sie gewisse Daten zur Vermögenssituation der betroffenen Partei kennt. Jedoch ist die Abgrenzung, ob ein Datum benötigt wird, nicht immer einfach. Es besteht daher die Gefahr, dass Behörden die entsprechenden Gesetzesbestimmungen weit formulieren, um auf diese Weise auch Daten zu erheben, welche unter Umständen im konkreten Fall keinen Einfluss auf den entsprechenden Anspruch haben.[780] Formularlösungen können zudem im Vergleich zu einem 326

774 Vgl. zum Ganzen Merkblatt Online-Portale, S. 7.

775 REGIERUNGSRAT DES KANTONS BASEL-STADT, S. 6. Vgl. etwa Art. 1b IDV BS.

776 MAURER-LAMBROU/STEINER, BSK DSG/BGÖ, Art. 4 DSG, N. 3; siehe dazu oben Rz. 78.

777 MAURER-LAMBROU/STEINER, BSK DSG/BGÖ, Art. 4 DSG, N. 4.

778 MAURER-LAMBROU/STEINER, BSK DSG/BGÖ, Art. 4 DSG, N. 11.

779 Vgl. Merkblatt Online-Portale, S. 7.

780 Vgl. BGE 136 I 87, E. 8.3.

Gesuch auf Papier an gewisse Grenzen stossen, indem teilweise nur Auswahlmöglichkeiten gegeben werden, um der Behörde die Verarbeitung der Daten zu erleichtern (z.B. Ja/Nein-Antworten). Entsprechende Lösungen sollten daher grundsätzlich auf die notwendigen Angaben beschränkt werden und dafür vermehrt «Kommentarfelder» oder «Freifelder» beinhalten, in welchen die Gesuchstellenden weitere, aus ihrer Sicht allenfalls relevante Angaben zum Gesuch mitteilen können.

ii) Erkennbarkeit

327 Es ergibt sich bereits aus den Grundsätzen des Datenschutzrechts, dass Daten grundsätzlich bei den betroffenen Personen zu beschaffen sind.[781] In diesem Sinne ist eine Beschaffung von Personendaten über Formulare oder Behördenportale aus Transparenzüberlegungen grundsätzlich durchaus im Sinne des Datenschutzes. Damit die Betroffenen die ihnen zustehenden Rechte auch geltend machen können, muss erkennbar sein, welche Daten zu welchem Zweck und auf welcher Grundlage erhoben werden. Dies vor allem dann, wenn eine gesetzliche Grundlage nach Art. 17 DSG fehlt und daher eine Einwilligung der betroffenen Person als notwendig erachtet wird.[782] Eine besondere Gefahr für die Betroffenen besteht dabei, wenn Daten durch Bundesbehörden in grossem Umfang oder systematisch erhoben werden. Auch deswegen sieht der Bundesgesetzgeber in Art. 18 und Art. 18a DSG gewisse Informationspflichten vor, wenn Daten systematisch, namentlich mit Fragebogen, erhoben werden.[783]

328 So hat das Bundesorgan gemäss Art. 18 DSG den Zweck und die Rechtsgrundlage des Bearbeitens, die Kategorien der an der Datensammlung Beteiligten und der Datenempfänger bekannt zu geben. Um ihre Rechte geltend zu machen, sind der betroffenen Person zudem gemäss Art. 18a DSG bei allen Datenerfassungen ihre Rechte gemäss dem Datenschutzgesetz bekannt zu geben.[784] Um diesen Anforderungen zu genügen, müssen die jeweiligen Formulare oder Portallösungen grundsätzlich die jeweiligen Informationen beinhalten. Es ist indes zu bezweifeln, dass diese Vorgaben in der Praxis überall vollständig beachtet werden. Nach dem soeben Ausgeführten könnte dies im schlimmsten Falle zu einer Rechtswidrigkeit der Bearbeitung führen und

781 Botschaft DSG, S. 468.

782 MUND, SHK-DSG, Art. 18, N. 6.

783 In vielen kantonalen Datenschutzgesetzen bestehen ähnliche Regelungen; vgl. etwa Art. 15 IDG BS. Es ist davon auszugehen, dass diese Pflicht nicht nur bei Fragebogen aus Papier, sondern auch bei entsprechenden digitalen Angeboten zu gelten hat; vgl. explizit. HUSI, PK IDG BS, Art. 15, N. 9.

784 MUND, SHK-DSG, Art. 18a, N. 8.

somit dazu, dass den Betroffenen die Rechte nach Art. 25 DSG offenstehen, d.h., dass sie vom verantwortlichen Organ verlangen können, die Bearbeitung zu unterlassen oder deren Folgen zu beseitigen. Da indes eine Datenbekanntgabe über ein Formular gerade im vorliegenden Zusammenhang oftmals im Interesse der Betroffenen selbst liegt, ist dies bisher noch nicht problematisch in Erscheinung getreten.

iii) Datensicherheit

Aus dem Grundsatz der Datensicherheit gemäss Art. 7 DSG ergibt sich, dass das 329
bearbeitende Organ durch angemessene Massnahmen für die Sicherheit der bearbeiteten Personendaten zu sorgen hat. Wichtig ist in diesem Sinne insbesondere, dass die Daten während der Übermittlung an die Behörde genügend geschützt sind. Um dies sicherzustellen, sind Personendaten lediglich verschlüsselt zu übermitteln.[785] Dies hat insbesondere auch für den Verkehr per E-Mail zu gelten, zumal dieser grundsätzlich nicht als sicherer Kommunikationskanal bewertet werden kann. Einerseits ist es vergleichsweise einfach möglich, über diesen Kanal eine falsche Identität vorzutäuschen.[786] Anderseits senden E-Mail-Programme der herkömmlichen privaten Anbieter die jeweiligen Mailings teilweise nicht verschlüsselt, wodurch diese abgefangen werden können. Aus diesem Grund dürfte es nicht zulässig sein, Personendaten – insbesondere besonders schützenswerte oder vertrauliche Informationen – über diese Kanäle zu kommunizieren.[787] Indes bieten auch private E-Mail-Anbieter inzwischen Möglichkeiten zur Verschlüsselung der Daten.[788]

Auch bei Behördenportalen mit Login-Funktion verdient der Grundsatz 330
der Datensicherheit verstärkte Beachtung. Dies insbesondere dann, wenn es den Benutzenden möglich sein soll, später erneut auf eingegebene Daten zuzugreifen, und somit eine grosse Menge an Daten über die jeweiligen Personen gespeichert wird. Aus diesem Grund sind bei diesen Portalen weitere technische und organisatorische Massnahmen zu treffen, um die Datensicherheit zu gewährleisten, etwa hinsichtlich der Wahl des Authentifizierungsverfahrens. Je nach Art der gespeicherten Personendaten kann es ausreichend sein, ein Login mit Benutzername und Passwort vorzusehen. Werden dagegen besondere Personendaten (z.B. Gesundheitsdaten der Person) gespeichert, sollte das entsprechende Login mit einer Mehrfaktor-Authentifizierung versehen

785 STAMM-PFISTER, BSK DSG/BGÖ, Art. 7, N. 27; die entsprechenden Vorgaben in Art. 9 VDSG sind gemäss Art. 20 VDSG auch für Bundesorgane zu beachten; vgl. STAMM-PFISTER, BSK DSG/BGÖ, Art. 7, N. 43.

786 ROSSNAGEL, NJW, 2011, S. 1473.

787 ROSSNAGEL, NJW, 2011, S. 1473.

788 Vgl. die Erläuterungen des EDÖB zur Verschlüsselung von E-Mails im privaten Bereich.

werden. Dabei erhält der Benutzer etwa nach der Eingabe der Benutzerdaten eine SMS-Nachricht auf eine zuvor hinterlegte Telefonnummer, um zu verifizieren, dass es sich um die richtige Person handelt.[789] Auch für die Übermittlung der Daten an die Behörde und deren Speicherung bei der Behörde sind geeignete Schutzmassnahmen zu treffen. Insbesondere ist zu klären, dass in der Verwaltung nur diejenigen Personen Zugriff haben, welche die Daten auch zur Erfüllung ihrer gesetzlichen Aufgaben benötigen, also etwa die zuständigen Sachbearbeitenden. In diesem Sinne ist es gerade bei behördenübergreifenden Portalen wichtig, dass die jeweiligen Amtsstellen nur auf diejenigen Daten Zugriff haben, welche in ihrem Fachbereich liegen.[790]

2. Zeitpunkt der Verfahrenseröffnung

331 Die Bundesverfassung gewährt durch Art. 29 BV jeder Person, welche sich in einem Rechtsanwendungsverfahren befindet, gewisse Rechte, welche für eine gleiche und gerechte Behandlung sorgen sollen.[791] Dazu zählen etwa der Anspruch auf rechtliches Gehör, welcher das Akteneinsichtsrecht und die Teilnahme an weiteren Beweiserhebungen umfasst, oder die Möglichkeit, eine vorsorgliche Massnahme zu beantragen. Die entsprechenden Rechte werden durch das einschlägige Verfahrensrecht konkretisiert.[792] Diese Garantien gelten indes nur, wenn ein Verfahren bereits eingeleitet wurde, d.h., wenn es rechtshängig ist.[793] Die informelle Natur der Verfahrenseröffnung kann bei der Zuhilfenahme elektronischer Technologien zu gewissen Problemen führen.

332 Sieht eine spezialgesetzliche Regelung vor, dass das Verfahren mit dem Zeitpunkt der Mitteilung an den Betroffenen hängig wird, so stellt der Zeitpunkt dieser Bekanntgabe den Beginn des Verfahrens dar, ab welchem der Partei die damit verbundenen Rechte zuerkannt werden. Reicht eine Person ein Gesuch ein, so ist ebenso unstrittig der Zeitpunkt der Einreichung des Gesuches als Verfahrensbeginn zu werten.[794] Schwierigkeiten bei der Feststellung des relevanten Zeitpunkts können sich jedoch ergeben, wenn das Verfahren aus einer zunächst informellen Kommunikation zwischen der

789 Vgl. Merkblatt Online-Portale, S. 4.

790 Vgl. etwa § 11 des Gesetzes über ein zentrales elektronisches Behördenportal des Kantons Basel-Stadt (Behördenportalgesetz, 153.300) vom 11. Januar 2017, welcher vorsieht, dass die Zugriffsrechte geregelt und Zugriffe protokolliert werden müssen; vgl. Merkblatt Online-Portale, S. 7.

791 WALDMANN, BSK BV, Art. 29, N. 7 und 12.

792 WALDMANN, BSK BV, Art. 29, N. 6.

793 Vgl. zum Ganzen: UHLMANN, in: Das erstinstanzliche Verwaltungsverfahren, S. 7; vgl. etwa Art. 1 VwVG.

794 Vgl. zum Ganzen: HÄNER, Anwaltsrevue, 2009, S. 175; UHLMANN, in: Das erstinstanzliche Verwaltungsverfahren, S. 4.

Behörde und der Privatperson heraus entsteht. Gerade wenn keine Rechtsvertretungen involviert sind, spielt sich die Kommunikation teilweise unkompliziert per E-Mail zwischen den Verfahrensbeteiligten ab. Dabei werden unter Umständen bereits Sachverhaltsabklärungen vorgenommen sowie durch die Behörden Fristen zur Akteneinreichung oder für Stellungnahmen gesetzt, während den Beteiligten nicht vollständig bewusst ist, dass sie sich bereits in einem Verwaltungsverfahren befinden.[795]

333 Die Behörden verfügen aufgrund der Formlosigkeit der Verfahrenseröffnung oft über einen weiten Ermessensspielraum. Dies kann dazu verleiten, den Verfahrensbeginn über Gebühr hinauszuzögern und den informellen Kontakt länger aufrechtzuerhalten.[796] In der Lehre wird davon ausgegangen, dass die Behörde den Zeitpunkt des Verfahrensbeginns im Interesse der Partei so zeitnah wie möglich wählen und die damit einhergehenden Rechte bereits ab einem frühen Zeitpunkt gewähren soll. Ausgehend vom Verfügungsbegriff gemäss Art. 5 VwVG soll der Verfahrensbeginn spätestens dann angenommen werden, wenn die Behörde Vorkehrungen trifft, welche den Erlass einer Verfügung erwarten lassen.[797]

334 Daraus ergibt sich, dass eine Behörde nicht beliebig lange in einem informellen Austausch mit dem Privaten bleiben kann, ohne dass ein Verfahren als eröffnet betrachtet werden muss.[798] Zeigt der oder die Betroffene zumindest implizit den Willen, dass ein Verfahren eröffnet bzw. der informelle Kontakt in ein formelles Verfahren übergeleitet werden soll, und kommt die Behörde diesem Wunsch nicht nach, so kann sie allenfalls gegen das Verbot der Rechtsverweigerung oder Rechtsverzögerung im Sinne von Art. 29 BV verstossen.[799] Indes haben die Rechtssuchenden in diesem Fall verschiedene Möglichkeiten, um die Eröffnung eines Verfahrens zu erzwingen. Zu denken ist einerseits an die Rechtsverzögerungs- oder Rechtsverweigerungsbeschwerde (nach Art. 46a VwVG), anderseits an den Erlass einer Feststellungsverfügung nach Art. 25 VwVG oder Art. 25a VwVG (bei Realakten).[800] Falls eine Behörde die Eröffnung eines Verfahrens gar absichtlich hinauszögert, um den Verfahrensparteien gewisse Rechte nicht gewähren zu müssen, kann dies auch rechtsmissbräuchliches Verhalten und somit einen Verstoss gegen das Gebot

795 HÄNER, in: Jahrbuch 2017/2018, S. 27.

796 UHLMANN, in: Das erstinstanzliche Verwaltungsverfahren, S. 15.

797 Vgl. etwa HÄNER, Anwaltsrevue, 2009, S. 175; UHLMANN, in: Das erstinstanzliche Verwaltungsverfahren, S. 4; vgl. auch Gutachten des Bundesamts für Justiz vom 31.1.2005, in: VPB 70 (2006), Nr. 46, E. 1 und 3.2.

798 HÄNER, in: Jahrbuch 2017/2018, S. 27.

799 Vgl. als Beispiel: Urteil des BVGer B-8099/2009 vom 11.3.2010.

800 UHLMANN, in: Das erstinstanzliche Verwaltungsverfahren, S. 7.

von Treu und Glauben (Art. 9 BV) darstellen. Durch diese Möglichkeiten wird der Zeitpunkt des Verfahrensbeginns justiziabel.[801]

335 Es besteht für die Behörden daher die Pflicht, von einer möglichst frühen Einleitung des Verfahrens auszugehen und den Betroffenen bereits zu diesem Zeitpunkt die zustehenden Verfahrensrechte zu gewähren. Es ist davon auszugehen, dass ein Verfahren dann als eröffnet zu gelten hat, wenn mit gewisser Sicherheit gesagt werden kann, dass die Behörde eine Verfügung erlassen wird.

C. Fazit

336 Die schweizerische Rechtsordnung steht der elektronischen Verfahrenseröffnung aufgrund der informellen Natur des Verfahrensbeginns grundsätzlich nicht entgegen. Indes muss die Identität der Gesuchstellenden auf irgendeine Weise verifiziert werden können, wobei dies neben der elektronischen Signatur auch auf andere Weise geschehen kann, etwa durch die Einforderung einer eingescannten Unterschrift oder dadurch, dass sich die betroffene Person auf einem Portal einloggen muss (z.B. mit Angabe eines Passworts). Daher ist inzwischen oftmals auch eine Verfahrenseröffnung via E-Mail, im Internet aufgeschaltete Gesuchsformulare oder Online-Portale mit Login-Funktion möglich. Die Nutzungserhebungen der Nationalen E-Government-Studie 2019 zeigen, dass der Kontakt über E-Mail oder Behördenportale zwar noch seltener ist als der persönliche oder telefonische Kontakt, dass jedoch gewisse, v.a. einfache Gesuche (etwa Fristerstreckung der Steuererklärung) inzwischen von einem nicht geringen Teil der Befragten online vorgenommen werden.[802]

337 Da auf diese Weise auch Daten über eine Person bearbeitet werden, müssen die Vorgaben und die Grundsätze des Datenschutzrechts beachtet werden. Relevant ist in diesem Zusammenhang, dass sich die Datenbeschaffung auf eine gesetzliche Grundlage stützt, dass nur diejenigen Daten erhoben werden, welche benötigt werden und dass die Datenbeschaffung sowie deren Rechtsgrundlagen erkennbar sind. Zudem muss die Datensicherheit jederzeit gewährleistet sein. Werden die Daten im Rahmen eines Behördenportals über längere Zeit gespeichert, sind aufgrund des zusätzlichen Gefahrenpotenzials striktere Vorgaben zu erfüllen. Zu beachten gilt auch, dass die Verfahrensrechte den Betroffenen erst ab dem Beginn des Verfahrens zustehen. Gerade wenn sich das Verfahren aus einem informellen Kontakt ergibt – was bei E-Mail-Kontakt durchaus vorkommen kann –, ist der Verfahrensbeginn nur schwer feststellbar. In diesen Fällen besteht die Gefahr, dass eine Behörde den Beginn

801 UHLMANN, in: Das erstinstanzliche Verwaltungsverfahren, S. 13.

802 BUESS/RAMSDEN/BIERI, S. 25 ff.

hinauszögert. Die Rechtsordnung gibt den Betroffenen indes Instrumente an die Hand, dies zu verhindern bzw. sich dagegen zur Wehr zu setzen.

II. Verfahrenslauf

A. Elektronische Eingaben

1. Generelle Vorgaben

338 Auch nach der Verfahrenseröffnung kann es im Verwaltungsverfahren immer wieder vorkommen, dass die Parteien – etwa im Rahmen ihrer Mitwirkungspflicht nach Art. 13 VwVG[803] – dazu aufgefordert werden, zusätzliche Unterlagen einzureichen oder dies aus eigenem Antrieb tun. Entsprechende Ersuchen durch die Verwaltungsbehörde ergehen dabei in der Regel schriftlich und unter Ansetzung einer Frist. Eine elektronische Abwicklung entsprechender Eingaben (z.B. per E-Mail) ist technisch durchaus möglich, indes hat das soeben zur Möglichkeit der elektronischen Einreichung gemäss Art. 21a VwVG Ausgeführte aufgrund des weiten Verständnisses des Begriffs der Eingabe auch im Rahmen des laufenden Verfahrens zu gelten. Dementsprechend ist auch hier grundsätzlich eine elektronische Signatur zu fordern, wenn die Identifizierung nicht bereits auf andere Weise festgestellt werden kann.[804] Auch hier kann in spezialgesetzlichen Grundlagen von den allgemeinen Vorgaben abgewichen werden und es können zusätzliche Vorgaben an die Einreichung von Eingaben gemacht werden. Die Grenze stellt hierbei der überspitzte Formalismus dar. Gemäss Art. 29 Abs. 1 BV ist es unter diesem Titel als Ausfluss des Verbots der Rechtsverweigerung untersagt, rigorose Formvorschriften aufzustellen, deren Strenge sachlich nicht gerechtfertigt werden kann.[805]

339 Während sich nach dem oben Ausgeführten im Bereich der Verfahrenseröffnung aus entsprechenden Zusatzerfordernissen noch selten gerichtliche Auseinandersetzungen ergeben haben, hat die Frage, in welcher Form im Laufe des Verfahrens Eingaben eingereicht oder Einsprachen getätigt werden, die Gerichte schon mehrere Male beschäftigt.[806] Problematisch ist dabei, dass einige verwaltungsrechtliche Spezialgesetze explizit die Schriftlichkeit von Eingaben oder Einsprachen verlangen, wie dies etwa im Steuerrecht der Fall ist.[807]

803 Dazu weiter unten Rz. 338 ff.

804 Siehe zu Beispielen soeben im letzten Kapitel. Denkbar ist etwa, dass die jeweiligen Personen die entsprechenden Dokumente im Rahmen einer Portallösung speichern können, zu dem nur sie die Zugangsdaten haben, oder sich auf andere Weise mit einem persönlichen Zugangscode identifizieren können.

805 BSK BV, 29, N. 30.

806 Vgl. anstatt vieler: BGE 143 I 187, BGE 142 V 152.

807 Vgl. etwa Art. 132 DBG oder Art. Art. 48 Abs. 1 StHG.

Im Sozialversicherungsrecht darf der Bundesrat zwar gemäss Art. 55 Abs. 1bis ATSG vorsehen, dass die Bestimmungen des VwVG im Anwendungsbereich dieses Gesetzes gelten sollen, indes hat er von dieser Möglichkeit bis anhin keinen Gebrauch gemacht.[808] Aus diesem Grund hat eine schriftlich erhobene Einsprache nach Art. 52 ATSG aufgrund von Art. 10 Abs. 4 ATSV explizit eine Unterschrift der einspracheführenden Person oder ihrer Rechtsvertretung zu enthalten.[809]

340 Gemäss der Rechtsprechung verlangt die Schriftlichkeit im Sinne dieser Bestimmungen, sofern nichts anderes vermerkt ist, in Anlehnung an Art. 14 Abs. 1 OR eine handschriftliche Unterschrift, wobei Art. 14 Abs. 2bis OR die qualifizierte elektronische Unterschrift der eigenhändigen Unterschrift gleichstellt. E-Mails oder andere Messaging-Dienste ohne anerkannte elektronische Unterschrift können somit die Anforderungen der Schriftform nicht erfüllen.[810] Das Unterschriftserfordernis dient insbesondere im Hinblick auf die mit der elektronischen Übermittlung verbundenen Risiken dazu, die Authentizität und Integrität der elektronischen Nachricht sicherzustellen.[811] Die Vorgabe, dass Eingaben von der betroffenen Person oder ihrer Rechtsvertretung eigenhändig zu unterzeichnen sind, stellt daher nach der Rechtsprechung auch keinen überspitzten Formalismus dar.[812]

341 Als Anschauungsbeispiel soll hier das Steuerrecht dienen. In vielen Kantonen und auch für gewisse Bundessteuern stehen inzwischen Computerprogramme zur Verfügung, mittels welcher man die Steuererklärung am Computer ausfüllen und übermitteln kann. Da aber die Steuergesetze oft vorsehen, dass die Steuererklärung schriftlich (bzw. mit Unterschrift versehen) einzureichen ist, muss teilweise zusätzlich eine Quittung ausgedruckt und unterzeichnet an die Steuerverwaltung gesendet werden. Auch wenn die Möglichkeit, die Steuererklärung online auszufüllen, rege genutzt wird, ist sie somit oftmals nicht vollständig medienbruchfrei ausgestaltet.[813] Einzelne Kantone sind daher dazu übergegangen, bei der Einreichung der Steuererklärung auf das Erfordernis der Unterschrift zu verzichten und die Steuerpflichtigen sich z.B. mit einem persönlichen Zugangscode identifizieren zu lassen.[814] Auch

808 BGE 143 I 187, E. 2.3.

809 Vgl. BGE 142 V 152, E. 2.4.

810 Vgl. BGE 142 V 152, E. 2.4.

811 Vgl. etwa Botschaft ZertES, S. 5684 f.

812 BGE 142 V 182, E. 4.2; allenfalls kann sich indes ein Anspruch auf Ansetzung einer Nachfrist ergeben, vgl. dazu sogleich, s. auch GLASER, ZSR, 2015, S. 302.

813 Vgl. BUESS/RAMSDEN/BIERI, S. 29.

814 Vgl. etwa die entsprechende Regelung im Kanton Obwalden: Medienmitteilung vom 7. Juli 2017.

der Bundesrat will in gewissen Bereichen des Steuerrechts auf das Unterschriftserfordernis verzichten. Stattdessen möchte er eine elektronische Bestätigung der Angaben durch die abgabepflichtige Person vorsehen bzw. diese gar zur elektronischen Abgabe verpflichten.[815]

2. Fristenwahrung

342 Wo die elektronische Eingabe mit der Ansetzung einer Frist verbunden ist, müssen zudem die Vorgaben von Art. 21a Abs. 3 VwVG beachtet werden. Daher wird an dieser Stelle kurz auf diese Bestimmung eingegangen. Gemäss diesem Artikel gilt die Frist bei elektronischer Eingabe als gewahrt, wenn das Informatiksystem, welchem die elektronische Zustelladresse der Behörde angehört, vor dem Ablauf der Frist den Empfang bestätigt. Dies heisst, dass eine fristwahrende Eingabe solange möglich ist, wie das System bis 24:00:00 Uhr des letzten Tages der Frist eine Empfangsbestätigung versenden kann.[816] Auf den ersten Blick sind die Parteien im Vergleich zur herkömmlichen Eingabe per Post also zumindest gleichgestellt.[817] Zumal das Internet im Gegensatz zu Postfilialen auch keine Öffnungszeiten kennt, könnte man allenfalls gar eine Besserstellung vermuten. Indes liegt das mit der Übertragung verbundene Risiko bis zum Zeitpunkt der Empfangsbestätigung, insbesondere auch für Probleme im eigenen Informatiksystem, auf der Seite der Partei. Während bei der postalischen Eingabe der Anwalt sich (unter Umständen mit Zeugen) zum Briefkasten begeben kann, ist er bei IT-Problemen in der Regel auf fremde Hilfe angewiesen. Dies dürfte in der Praxis dazu führen, dass für die elektronische Eingabe noch ein Puffer eingerechnet werden müsste, damit bei Systemproblemen immer noch eine fristwahrende Eingabe auf der Post möglich ist. Somit würde die Frist faktisch verkürzt.[818] Wichtig ist daher, dass auf beiden Seiten zuverlässige, performante Systeme vorhanden sind. Zu beachten bleibt in diesem Zusammenhang im erstinstanzlichen Verfahren immerhin, dass eine Behörde gemäss Art. 32 VwVG auch verspätet eingebrachte Parteivorbringen beachten kann, sofern diese ausschlaggebend sind.[819]

815 Vgl. Bericht Rev. Steuerbereich, S. 1 ff.

816 EGLI, PK VwVG, Art. 21a, N. 25.

817 Dies immer vorausgesetzt, das Informatiksystem aufseiten der Behörde ist automatisiert und ununterbrochen in Betrieb; vgl. Botschaft Rev. Bundesrechtspflege, S. 4267 und 4298.

818 HÄNER, in: Jahrbuch 2017/2018, S. 36.

819 HÄNER, in: Jahrbuch 2017/2018, S. 37.

3. Konsequenzen formell fehlerhafter Eingaben

343 In der Regel ist es für den Betroffenen aufgrund der Aufforderung einer Behörde ersichtlich, in welcher Form eine Eingabe eingereicht werden kann oder muss. Zudem sorgen wohl auch die alternativen Möglichkeiten der Identifizierung dafür, dass wohl selten eine elektronische Eingabe aus formellen Gründen nicht angenommen wird. Dabei ist es auch denkbar, dass die Behörden in der Praxis etwa darauf verzichten, eine nicht verschlüsselte E-Mail zurückzuweisen, obwohl sie dies unter Umständen tun müssten.[820] Dennoch hatten sich Lehre und Rechtsprechung damit zu befassen, welche Konsequenzen das Fehlen einer elektronischen Signatur oder auch eine elektronische Einreichung, welche im jeweiligen Verfahren nicht vorgesehen ist, haben können.

344 Im Anwendungsbereich des VwVG wird davon ausgegangen, dass das Fehlen einer elektronischen Signatur nicht dazu führen muss, dass eine entsprechende Eingabe ungültig ist oder auf eine Einsprache nicht eingetreten werden kann. Vielmehr sieht bereits Art. 6 Abs. 2 VeÜ-VwV die Ansetzung einer kurzen Nachfrist zur Verbesserung vor. Der Partei steht es offen, die Eingabe mit einer qualifizierten elektronischen Signatur zu wiederholen oder sie gemäss den Voraussetzungen von Art. 21 VwVG handschriftlich unterschrieben einzureichen.[821]

345 Ausserhalb des Anwendungsbereichs des VwVG wird – wie bereits ausgeführt – eine explizite gesetzliche Grundlage für den elektronischen Rechtsverkehr gefordert. Auch hier ist inzwischen in vielen Bereichen die qualifizierte elektronische Signatur der eigenhändigen Unterschrift gleichgestellt, womit E-Mails ohne Signierung den Vorgaben nicht entsprechen und als ungültig betrachtet werden können.[822] Indes kann sich unter Umständen aus dem jeweils einschlägigen Verfahrensrecht ein Anspruch auf Ansetzung einer Nachfrist ergeben.[823] Ausgenommen von diesem Anspruch sind Fälle des offensichtlichen Rechtsmissbrauchs, welche etwa dann angenommen werden, wenn die Unterlassung nicht unfreiwillig erfolgt.[824] Im Rahmen seiner Rechtsprechung dazu hat das Bundesgericht konkretisiert, dass bei der Übermittlung per gewöhnlichem E-Mail oder Fax die Unterschrift gemäss der Natur der Sache von vorneherein fehle, was zumindest für professionelle Anwender ersichtlich sein muss, womit in diesen Fällen naheliege, dass nur

820 HÄNER, in: Jahrbuch 2017/2018, S. 28.

821 EGLI, PK VwVG, Art. 21a, N. 24; CAVELTI, VwVG-Kommentar, Art. 21a, N. 18.

822 Vgl. Urteil des BGer 1P.254/2005 vom 30. August 2005, E. 2.3, BGE 142 V 152, E. 2.4

823 Vgl. Urteil des BGer 1P.254/2005 vom 30. August 2005, E. 2.5.

824 BGE 121 II 252, E. 4b.

entsprechend gehandelt wurde, um eine entsprechende Nachfrist zu erlangen und dadurch Zeit zu gewinnen.[825] Bei Eingaben durch juristische Laien ist indes auch bei einer Einreichung per E-Mail nicht leichthin von offensichtlichem Rechtsmissbrauch auszugehen. Hier kann unter Umständen sogar eine Nachfristsetzung zur Nachbesserung angebracht sein, wenn die Behörde in der Rechtsmittelbelehrung darauf hinweist, dass eine Einreichung per E-Mail unwirksam ist.[826]

346 Schliesslich kann es vorkommen, dass die kantonalen Verfahrensordnungen – wie in einem Fall betreffend den Kanton Wallis – noch keine Regelungen zum elektronischen Rechtsverkehr vorsehen und für diese im betreffenden Bereich auch keinen Raum lassen. In einem entsprechenden Fall ist auch die qualifizierte elektronische Signatur einer eigenhändigen Unterschrift nicht gleichgestellt. Dies kann zur Folge haben, dass selbst auf eine elektronisch eingereichte Eingabe, welche über eine qualifizierte elektronische Signatur verfügt und somit den Vorgaben des Bundesrechts genügen würde, nicht eingetreten werden kann, ohne dass dadurch Bundesrecht verletzt wird. Daran ändert auch nichts, dass der Bundesgesetzgeber und eine Vielzahl der Kantone dem elektronischen Rechtsverkehr inzwischen mit Nachdruck zum Durchbruch verhelfen wollen.[827]

4. Fazit

347 Elektronische Eingaben im Verfahrenslauf sind grundsätzlich zulässig, wobei auch hier eine Identifizierung der betreffenden Partei notwendig ist. Dies kann grundsätzlich durch eine elektronische Signatur oder auf andere Weise geschehen, etwa mittels eines Logins auf einem Behördenportal. Sofern eine gesetzliche Grundlage Schriftlichkeit verlangt, ist davon auszugehen, dass darunter eine handschriftliche Unterschrift oder eine qualifizierte elektronische Signatur zu verstehen ist. Eine Einreichung per E-Mail kann diese Vorgabe daher nicht erfüllen.

348 Aus Sicht der Zielsetzungen des E-Government ist es durchaus zu begrüssen, dass in gewissen Bereichen und Kantonen vermehrt Wege gesucht werden, um elektronische Eingaben zu ermöglichen oder zu vereinfachen und dennoch den Zweck der Formvorschriften zu wahren. Diese abweichenden Regelungen stellen allerdings auch ein Problem dar, da damit in zweierlei Hinsicht eine Rechtszersplitterung verbunden ist. Einerseits sehen in

825 Im Bereich des Sozialversicherungsrechts explizit so angenommen unter anderem in BGE 142 V 152, E. 4.5.

826 Urteil des BGer 1P.254/2005 vom 30. August 2005, E. 2.5.

827 Vgl. zum Ganzen: BGE 143 I 187, E. 3.1.

«horizontaler» Ebene aktuell noch nicht alle Kantone Regelungen zum elektronischen Rechtsverkehr vor. Anderseits können bereichsspezifische Regelungen einer entsprechenden Regelung im Einzelfall entgegenstehen.[828] Daraus ergibt sich, dass für die Möglichkeit der Einreichung einer elektronischen Eingabe erstens der betreffende Kanton diesen Kanal offenhalten muss, aber zweitens auch die Notwendigkeit, dass das einschlägige materielle Recht diese Möglichkeit nicht ausschliesst. Diese Rechtszersplitterung stellt durchaus ein Hindernis für die Digitalisierung des Verwaltungshandelns dar[829] und kann gerade auch für Laien problematisch sein.[830] Sie kann jedoch auch als Chance genommen werden, um die allgemeinen Verfahrensrechtserlasse einer umfassenden Überprüfung zu unterziehen und diese gegebenenfalls zu reformieren.[831]

B. Rechtliches Gehör

349 Neben den bereits beschriebenen Mitwirkungspflichten stehen den Parteien in einem Verfahren auch gewisse Rechte zu. Aus Art. 29 BV und Art. 6 EMRK ergibt sich, dass der Einzelne in einem Rechtsanwendungsverfahren einen Anspruch auf faire Behandlung hat.[832] Konkretisiert wird dies insbesondere durch den in Art. 29 Abs. 2 BV verankerten Anspruch auf rechtliches Gehör. Dieser räumt der Verfahrenspartei verschiedene Befugnisse ein, damit sie ihren Standpunkt im Verfahren wirksam zur Geltung bringen kann.[833] Der Anspruch auf rechtliches Gehör umfasst verschiedene Teilgehalte: So muss der Verfahrensteilnehmende etwa darüber orientiert werden, dass er sich in einem Verfahren befindet, er muss zum Verfahrensgegenstand angehört werden und an allfälligen Beweiserhebungen teilnehmen können. Zudem muss ein Entscheid der Behörde ihm gegenüber begründet werden. Damit er seine Mitwirkungsrechte wahrnehmen kann, muss es ihm möglich sein, Einsicht in die Verfahrensakten der Behörde zu erlangen.[834] Die meisten dieser Rechte

828 Vgl. GLASER, SJZ, 2018, S. 186.

829 GLASER, SJZ, 2018, S. 186.

830 So kann eine über eine anerkannte Zustellungsplattform eingereichte, digital signierte Beschwerde (welche vor Bundesgericht angenommen werden müsste) von kantonalen Gerichten und Verwaltungsinstanzen in einem Kanton, welcher keine Regelungen zum elektronischen Rechtsverkehr kennt, nicht angenommen werden; vgl. BGE 143 I 187, E. 3.4.

831 GLASER/EHRAT, LeGes, 2019, N. 49 ff., mit Verweis auf entsprechende Anstrengungen im Kanton Freiburg und KAHL, JuS, 2018, S. 1029; vgl. auch GLASER, SJZ, 2018.

832 WALDMANN, BSK BV, Art. 29, N. 8 ff.

833 BGE 136 I 184, E. 2.2.1.

834 Weitere Ausführungen zu den Teilgehalten, vgl. STEINMANN, SG Komm. BV, Art. 29, N. 44 ff.

haben dabei in ihrem Wesen durch die Digitalisierung keine Veränderung erfahren oder diese Veränderungen sind an anderer Stelle zu betrachten. So stellt etwa die Begründung des Entscheids einen Teil der Eröffnung einer Verfügung dar. Eine Verfügung kann – wie weiter unten ausgeführt wird – durchaus elektronisch eröffnet werden. Da sich für den Begründungsanspruch daraus keine Veränderungen ergeben, soll an dieser Stelle nicht vertieft darauf eingegangen werden.

1. Anhörung vor Erlass einer Verfügung

Für erstinstanzliche Verfahren auf Bundesebene regelt Art. 30 VwVG explizit, 350
dass die Behörde die Parteien grundsätzlich anzuhören hat, bevor sie verfügt. Das Recht auf vorgängige Anhörung umfasst dabei den Anspruch, sich vor dem Erlass einer Verfügung zu tatsächlichen und rechtlichen Entscheidungsgrundlagen, aber auch zu allfälligen neu erhobenen Beweismitteln, behördlichen Sachverhaltselementen oder zu Eingaben einer Gegenpartei äussern zu können.[835] Art. 30 VwVG macht dabei keine Vorgaben zur Form der Anhörung, so dass die Behörden einen gewissen Ermessensspielraum haben, wie sie die Betroffenen anhören wollen. Die Behörden müssen lediglich eine angemessene Form der Kommunikation gewähren, wobei deren Ausgestaltung von den konkreten Umständen abhängt.[836] Die Anhörung geschieht im Verwaltungsverfahren in der Regel schriftlich.[837] Unabhängig von der gewählten Form hat die Gehörsgewährung im Rahmen einer formellen Verfahrenshandlung zu erfolgen. Der Betroffene muss erkennen können, dass die Behörde die betreffende Handlung im Hinblick auf die Gewährung des rechtlichen Gehörs in einem konkreten Verfahren vornimmt. Ist dies gegeben, so werden aber beispielsweise auch Telefongespräche oder Videokonferenzen als zulässige Form der Anhörung betrachtet.[838]

Sollte eine Gehörsgewährung via E-Mail in Betracht gezogen werden, so 351
sind wiederum Vorbehalte hinsichtlich der Identifizierbarkeit anzubringen. Nach dem weiter oben Ausgeführten muss auch in diesen Fällen nach den Grundsätzen von Art. 21a VwVG und der VeÜ-VwV eine Identifizierung durch eine qualifizierte elektronische Signatur oder auf andere Weise möglich sein. Gerade wo bereits ein vorbestehender Kontakt zwischen Behörden und Parteien stattgefunden hat, wäre durchaus denkbar, dass die Identifizierung auch auf diese Weise als genügend betrachtet werden kann. Eine Behörde, welche

835 WALDMANN/BICKEL, PK VwVG, Art. 30, N. 4.
836 SUTTER, VwVG-Kommentar, Art. 30, N. 2.
837 WALDMANN/BICKEL, PK VwVG, Art. 30, N. 39.
838 WALDMANN/BICKEL, PK VwVG, Art. 30, N. 46.

die Anhörung per E-Mail durchführt, aber die Person nicht darauf hinweist, dass die Eingabe elektronisch zu unterzeichnen ist, würde zudem wohl entgegen dem Grundsatz von Treu und Glauben handeln. Es ist derzeit jedoch davon auszugehen, dass aus Gründen der Rechtssicherheit die Anhörung regelmässig noch auf dem althergebrachten, schriftlichen Weg gewährt und wahrgenommen wird.

2. Elektronische Akteneinsicht

352 Aus dem rechtlichen Gehör ergibt sich im Weiteren ein Anspruch auf Einsicht in Akten, welche geeignet sind, als Grundlage eines eine Person oder Sache betreffenden Entscheids zu dienen. Das Akteneinsichtsrecht stellt eine wichtige Bedingung dar, um die anderen Rechte, welche sich aus dem rechtlichen Gehör ergeben, wahrnehmen zu können.[839] Auf Bundesebene regeln Art. 26 ff. VwVG die Akteneinsicht. Die Bestimmung geht davon aus, dass diese grundsätzlich am Ort der Behörde zu erfolgen hat, was allerdings anhand der heutigen Realitäten kaum mehr zeitgemäss scheint.[840] Zumindest im Bundesrecht ist indes das Gesuch auf Akteneinsicht nicht an eine bestimmte Form gebunden, könnte also z.B. auch per E-Mail erfolgen.[841]. Seit Januar 2007 sieht Art. 26 Abs. 1bis VwVG zudem vor, dass die Aktenstücke auf elektronischem Weg zur Einsichtnahme zugestellt werden können, wenn die Partei oder ihr Vertreter damit einverstanden ist. Von dieser Rechtsänderung versprach sich der Gesetzgeber eine Reduktion der Verfahrenskosten und ein Instrument zur Vermeidung von Verfahrensverzögerungen. Die elektronische Akteneinsicht wurde indes nur dort als zulässig erachtet, wo auch der elektronische Verkehr zwischen Behörde und Parteien zugelassen ist.[842] Im Gegensatz zur elektronischen Eingabe sind bei der elektronischen Akteneinsicht keine weiteren Voraussetzungen (etwa eine elektronische Signatur oder eine bestimmte Zustellplattform) zu erfüllen.[843] Ob eine Behörde die elektronische Akteneinsicht gewähren will, liegt allerdings in ihrem Ermessen. Es besteht somit kein einklagbarer Anspruch darauf, die Akten auf diesem Weg zu erhalten.[844] Da die elektronische Gewährung eine wesentliche Besserstellung für die Partei im Sinne der Verfahrensökonomie und der Kostentragung darstellt, geht die Lehre indes davon aus, dass sich ein solcher Anspruch indes aus dem Rechtsgleichheitsgebot ergeben könnte. In diesem Sinne könnte sich der bisher

839 WALDMANN, BSK BV, Art. 29, N. 54.

840 JÖRGER, Anwaltsrevue, 2019, S. 482, vgl. bereits ALBERTINI, S. 249 ff.

841 WALDMANN/OESCHGER, PK VwVG, Art. 26, N. 71.

842 Vgl. zum Ganzen: Botschaft Rev. Bundesrechtspflege, S. 4271 f.

843 Vgl. BRUNNER, VwVG-Kommentar, Art. 26, N. 49.

844 Vgl. Botschaft Rev. Bundesrechtspflege, S. 4406; JÖRGER, Anwaltsrevue, 2019, S. 485.

beschränkte Anspruch auf Erstellung von Kopien im Zuge der technologischen Entwicklung auf die Erstellung und das Zusenden von Scans ausweiten.[845]

353 Die Rechtsgrundlagen für die elektronische Akteneinsicht sind somit auf Bundesebene grundsätzlich vorhanden. Da immer noch die meisten Anwälte ihre Eingaben auf Papier einreichen, besteht indes vonseiten der Verwaltung und der Gerichte oftmals kein Bestreben, die elektronische Aktenführung mit letzter Konsequenz zu verfolgen.[846] Daher ist die elektronische Akteneinsicht in der Regel noch in einem Bestell-/Liefermodus ausgestaltet, d.h., die Partei muss die Dateien bestellen und diese werden ihr dann (oftmals ausgedruckt) zugeliefert. Denkbar wäre allerdings auch ein System, in welchem die Partei bzw. ihre Rechtsvertretung innerhalb der ihr zugänglichen Dateien die relevanten Dateien selbständig suchen und herunterladen kann. Dies würde zwar einen zusätzlichen Komfort für die Partei bedeuten, ist aber aus technologischer Sicht schwieriger realisierbar.[847] Einige Kantone sehen hier weitergehende Regelungen vor, wonach auch die Freigabe von Dokumenten zulässig ist. Darunter zu verstehen ist, dass den Einsichtssuchenden ein Link zugesendet wird, mit dem sie die bereitgestellten Daten von einem Server herunterladen können.[848] Je mehr die digitale Aktenführung zum Standard wird, desto mehr werden sich auch entsprechende Lösungen aufdrängen.[849]

354 Der Bericht des Bundesrats, welcher sich in Beantwortung einer Motion mit dem Stand der Umsetzung des elektronischen Akteneinsichtsrechts befasste, kam bezogen auf den Stand im Jahr 2012 zum Schluss, dass eine harmonisierte Lösung aller Gerichte, welche eine Akteneinsicht im Sinne eines Online-Portals mit Suchmodus für die elektronische Akteneinsicht – und somit auch die gesamte elektronische Aktenführung – ermöglicht, am sinnvollsten wäre.[850] Eine entsprechende Lösung wurde allerdings aus finanziellen Gründen vonseiten des Bundes zum damaligen Zeitpunkt als nicht opportun erachtet.[851] Inzwischen wurde von dieser Ansicht zumindest teilweise abgewichen, und es soll im Rahmen des Projekts «Justitia 4.0», welches weiter unten genau betrachtet wird, zumindest die Aktenführung der höchsten kantonalen und der Bundesgerichte auf einer übergreifenden Plattform harmonisiert werden.[852]

845 Vgl. WALDMANN/OESCHGER, PK VwVG, Art. 26, N. 87.
846 Bericht Bischof, S. 8.
847 Bericht Bischof, S. 10.
848 Vgl. etwa § 48 Abs. 1 bis VRG/LU, s. dazu auch JÖRGER, Anwaltsrevue, 2019, S. 485.
849 JÖRGER, Anwaltsrevue, 2019, S. 485.
850 Bericht Bischof, S. 14 f.
851 TSCHÜMPERLIN, SJZ, 2018, S. 318.
852 Siehe weiter unten Rz. 569 ff.

C. Fazit

355 Handlungen der Parteien während des laufenden Verwaltungsverfahrens können grundsätzlich elektronisch vorgenommen werden. Dabei hat jedoch die Identifikation der Parteien jederzeit sichergestellt zu sein. Dies kann entweder durch eine qualifizierte elektronische Signatur oder auf andere Weise (etwa durch ein Login auf einem Behördenportal) geschehen. Spezialgesetzliche Bestimmungen können abweichende Regelungen vorsehen, wobei oft die Schriftlichkeit von Eingaben verlangt wird. Ohne weitere Präzisierungen ist diese so zu verstehen, dass eine handschriftliche oder eine qualifizierte elektronische Signatur vorliegen muss und eine Einreichung per E-Mail somit nicht ausreicht. Werden die entsprechenden Formvorschriften nicht erfüllt, so wird den Betroffenen oftmals eine Nachfrist zur Verbesserung oder zur manuellen Einreichung gewährt. Davon abgesehen werden kann indes bei rechtsmissbräuchlichem Verhalten. Der Umstand, dass je nach Gemeinwesen oder Rechtsbereich unterschiedliche Regelungen hinsichtlich der Zulässigkeit elektronischer Eingaben vorliegen können, kann gerade für Rechtsunkundige verwirrend wirken. Nebenbei stellt diese Rechtszersplitterung auch einen gewichtigen Hemmschuh der Digitalisierung dar. Um hier Abhilfe zu schaffen, sollten Schritte zur schweizweiten oder rechtsbereichsübergreifenden Vereinheitlichung ergriffen werden, worauf weiter unten eingegangen wird. Auch die Gewährung des rechtlichen Gehörs ist grundsätzlich auf verschiedene Weisen möglich, wobei hier ebenfalls die Identifizierung gewährleistet sein muss. Zu guter Letzt kann die Akteneinsicht mittlerweile auf elektronischem Weg erfolgen. Die grundsätzlich nach wie vor bestehende Papierlastigkeit des Verfahrens führt allerdings dazu, dass von dieser Möglichkeit wohl noch selten Gebrauch gemacht wird und entsprechende Umstellungen auf digitale Lösungen nur zögerlich vollzogen werden.

III. Verfahrensbeendigung

356 Sein Ende findet das erstinstanzliche Verwaltungsverfahren in der Regel mit dem Erlass einer Verfügung. Verfügungen sind im Bund gemäss Art. 34 Abs. 1 VwVG schriftlich zu eröffnen. Sofern dies Schriftlichkeit eine eigenhändige Unterschrift verlangt, wird eine Eröffnung per E-Mail grundsätzlich als nicht zulässig betrachtet.[853] Art. 34 Abs. 1bis VwVG, welcher mit der Revision der Bundesrechtspflege per 1. Januar 2007 eingefügt wurde, erlaubt jedoch unter gewissen Voraussetzungen die elektronische Eröffnung von Verfügungen.

853 GLASER, ZSR, 2015, S. 306; UHLMANN/SCHILLING-SCHWANK, PK VwVG, Art. 34, N. 7.

Einerseits muss die Partei, welche eine elektronische Eröffnung möchte, über eine elektronische Zustelladresse gemäss Art. 11b VwVG verfügen.[854] Im Weiteren wird das Einverständnis der Partei benötigt. Die Anforderungen an diese Zustimmung sind in Art. 8 VeÜ-VwV geregelt. Gemäss diesem Artikel hat die Zustimmung schriftlich und ausdrücklich zu erfolgen, braucht jedoch nicht unterschrieben zu sein. Daraus ergibt sich, dass die Zustimmung auch per E-Mail rechtsgültig erklärt werden kann. Mangels Ausdrücklichkeit nicht als diesen Vorgaben genügend angesehen wird, wenn eine Partei an einer Stelle im Schreiben ihre E-Mail-Adresse (etwa im Briefkopf) angibt.[855] Die Zustimmung kann grundsätzlich nur für ein bestimmtes Verfahren erteilt werden. Wer regelmässig mit derselben Behörde verkehrt, kann dieser allerdings auch mitteilen, dass ihm alle Verfügungen elektronisch eröffnet werden sollen.[856] Des Weiteren sehen Art. 34 Abs. 1bis VwVG und die VeÜ-VwV auch gewisse technische Voraussetzungen vor, welche erfüllt sein müssen, damit eine Verfügung elektronisch eröffnet werden kann. So sind in Art. 9 ff. VeÜ-VwV gewisse Anforderungen an die Modalitäten der Verfügungseröffnung geregelt (etwa hinsichtlich des Dateiformats oder der elektronischen Signatur).

Auch weitere Fragen in diesem Zusammenhang werden durch die ge- 357
setzliche Regelung geklärt. So gilt gemäss Art. 10 VeÜ-VwV erst der Zeitpunkt des Herunterladens durch die Adressatin oder den Adressaten als Zeitpunkt der Zustellung und löst somit den Fristenlauf aus. Wird eine richtig adressierte elektronische Verfügung nicht abgerufen, so gilt die Zustellung dennoch als Erstzustellungsversuch im Sinne von Art. 20 Abs. 2bis VwVG und löst somit die Zustellungsfiktion aus, gemäss der die Zustellung am siebten Tage nach dem Eingang als erfolgt gilt, auch wenn sie nicht heruntergeladen wurde.[857] Weiter gilt es zu beachten, dass Art. 34 Abs. 1bis VwVG eine «Kann»-Bestimmung ist. Entsprechend steht es der Behörde frei, ob sie dem Wunsch der Partei Folge leistet, die Verfügung elektronisch zu eröffnen. Diese Regelung wird, gerade falls mehrere Personen in ein Verfahren involviert sind, aus Gründen der Verfahrensökonomie und zur Gewährleistung eines einheitlichen Zustellungszeitpunkts bis zur Durchsetzung der elektronischen Eröffnung als Standard als vertretbar erachtet. Ansonsten sind jedoch kaum Gründe ersichtlich, aus welchen eine Behörde dem Wunsch der Partei auf elektronische Zustellung nicht entsprechen sollte. Schliesslich ist für die Beteiligten kein

854 PEDUZZI, Anwaltsrevue, 2009, S. 188.

855 PEDUZZI, Anwaltsrevue, 2009, S. 188.

856 MARANTELLI/HUBER, PK VwVG, Art. 11b, N. 30.

857 MARANTELLI/HUBER, PK VwVG, Art. 11b N. 34; PEDUZZI, Anwaltsrevue, 2009, S. 190.

freiwilliger Verzicht auf die Einhaltung der Eröffnungsvoraussetzungen möglich, da auf diese Weise ihre Verfahrensrechte ausgehöhlt werden könnten.[858]

358 Wird eine Verfügung per E-Mail eröffnet, ohne dass die Voraussetzungen von Art. 34 Abs. 1bis erfüllt sind, so wurde diese Verfügung nicht ordnungsgemäss eröffnet. Art. 38 VwVG legt fest, dass den Parteien aus einer mangelhaften Eröffnung kein Nachteil erwachsen darf. Dies bedeutet, dass es der Partei weder erschwert noch verunmöglicht werden darf, ein Rechtsmittel zu ergreifen.[859] Die Behörde dürfte sich also in einem solchen Fall also beispielsweise nicht darauf berufen, dass eine Rechtsmittelfrist mit der Mitteilung des Entscheids per E-Mail zu laufen begann, und auf eine Einsprache dagegen aus Fristgründen nicht eintreten. In der Praxis könnte der Mangel indes in vielen Fällen durch eine Nachreichung der Eröffnung per Brief geheilt werden, falls diese von der Partei verlangt wird. Eine Eröffnung über den unsicheren E-Mail-Kanal ist im Weiteren auch aus Datenschutzgründen kritisch zu betrachten.[860]

359 Der Bund kann den Kantonen nicht vorschreiben, dass diese ebenfalls eine elektronische Eröffnung von Verfügungen vorsehen müssen.[861] Dennoch haben bereits einige Kantone diese Eröffnungsform ebenfalls in ihre Rechtsordnung integriert. In Kantonen, die eine entsprechende Möglichkeit nicht gesetzlich vorsehen, ist die elektronische Eröffnung nicht zulässig.[862] Weder auf der Ebene der Kantone noch auf der Ebene des Bundes sind Zahlen darüber ersichtlich, zu welchem Anteil Verfügungen bereits online eröffnet werden. Quantitative Beobachtungen können immerhin betreffend die Rechnungsstellung durch Behörden gemacht werden, wobei zu beachten ist, dass Rechnungsstellungen und Zahlungsaufforderungen durch Behörden nur unter gewissen Umständen Verfügungscharakter zukommt.[863] Viele Gemeinwesen bieten inzwischen die E-Rechnungsstellung an.[864] Immerhin 33 % der Befragten der Nationalen E-Government Studie 2019 geben an, diese Dienstleistung auch bereits genutzt zu haben.[865] In jedem Fall ist die elektronische Eröffnung von Verfügungen wohl noch nicht zum Standard für den

858 Vgl. zum Ganzen: PEDUZZI, Anwaltsrevue, 2009, S. 190.

859 Art. 38 VwVG, N. 5 ff.

860 Vgl. zum Ganzen oben: Rz. 329.

861 MARANTELLI/HUBER, PK VwVG, Art. 11b, N. 19.

862 GLASER, ZSR, 2015, S. 307.

863 Vgl. etwa das Urteil des BGer 2C_444/2015 vom 4. November 2015, E. 3.2.3, m.w.H.

864 So ist es etwa in der Bundesverwaltung möglich, mit E-Rechnungen zu bezahlen, und für Lieferanten gar verpflichtend, diese Möglichkeit zu nutzen, vgl. etwa die Website der Eidgenössischen Finanzverwaltung.

865 BUESS/RAMSDEN/BIERI, S. 28.

praktizierenden Anwalt geworden, wie dies vor zehn Jahren prophezeit wurde.[866] Die Gründe hierfür sind wohl darin zu suchen, dass auch die Eröffnung an gewisse Voraussetzungen gebunden ist. Dabei sind diese Vorgaben zwar in erster Linie durch die Behörde zu beachten, bedeuten für diese aber wohl einen gewissen Zusatzaufwand. Daher ist auch die elektronische Eröffnung einer Verfügung als Teil eines Systems zu sehen, welches zwar mit seinen Rechtsgrundlagen den elektronischen Rechtsverkehr ermöglicht, aber aufgrund praktischer Hindernisse und der mangelnden Durchsetzung trotzdem noch weitgehend auf Papierbasis funktioniert.

IV. Zusammenfassung

Durch die Revision der Gesetzgebung zum Verwaltungsverfahren auf Bun- 360
desebene wurden Rechtsgrundlagen geschaffen, welche den elektronischen Rechtsverkehr weitgehend ermöglichen und etwa elektronische Eingaben, die Akteneinsicht oder die elektronische Eröffnung von Verfügungen begünstigen sollen. Auch viele Kantone haben entsprechende Grundlagen geschaffen. Aus Gründen der Identifizierbarkeit und der Integrität des Rechtsverkehrs sind diese Formen an gewisse Voraussetzungen gebunden, indem etwa Eingaben elektronisch unterzeichnet werden. Meist kann darauf aber verzichtet werden, wenn die Identifizierbarkeit auf andere Weise gewährleistet ist. Dass je nach Rechtsbereich und Gemeinwesen andere Regeln vorgesehen werden können, kann die Verbreitung des elektronischen Rechtsverkehrs durchaus hemmen und die Nutzung für Private unattraktiv machen.

§ 5 Erkenntnisquellen der Verwaltung

Sowohl im rechtlichen, auf den Erlass einer Verfügung ausgerichteten als 361
auch im tatsächlichen Verwaltungshandeln haben die Behörden den rechtserheblichen Sachverhalt festzustellen, auf dessen Basis sie eine Verfügung erlassen oder tatsächlich handeln können. Sofern die Behörde in einem Verfahrensrahmen handelt, gibt ihr das einschlägige Verwaltungsverfahrensrecht dabei gewisse Vorgaben. Dass die Behörden sich aber auch im Rahmen des tatsächlichen Verwaltungshandelns an gewisse Vorgaben hinsichtlich der Sachverhaltsfeststellung zu halten haben, ergibt sich bereits aus dem Legalitätsprinzip gemäss Art. 5 BV. Überall dort, wo tatsächliches Verwaltungshandeln Rechte und Pflichten betrifft, kann die betroffene Person, ein

866 PEDUZZI, Anwaltsrevue, 2009, S. 190.

schutzwürdiges Interesse vorausgesetzt, gestützt auf Art. 25a VwVG zudem den Erlass einer Verfügung verlangen.[867] Da spätestens im Verfahren auf den Erlass dieser Verfügung die Vorgaben des VwVG ebenfalls zu beachten sind, ist davon auszugehen, dass auch im Hinblick auf das tatsächliche Verwaltungshandeln dieselben Anforderungen an die Sachverhaltsfeststellung zu fordern sind. Entsprechend rechtfertigt sich im Folgenden die generelle Orientierung an diesen Vorgaben.

362 Gemäss Art. 12 VwVG stellen die Behörden den Sachverhalt von Amtes wegen fest. Aus dem sogenannten Untersuchungsgrundsatz ergibt sich, dass die Behörde für die Ermittlung des rechtserheblichen Sachverhalts zuständig ist und somit auch die Beweisführungslast trägt.[868] Sie kann dabei auf ihr eigenes Fachwissen und allgemein bekanntes Wissen zurückgreifen. Sie darf sich jedoch auch anderer Quellen bedienen, wenn sie über die daraus gewonnenen Tatsacheninformationen Beweis führt. In diesem Rahmen muss sie der betroffenen Person die Möglichkeit geben, sich dazu zu äussern.[869] Der Pflicht der Behörden sind verschiedene Grenzen gesetzt. So muss der Aufwand der Sachverhaltsermittlung immer verhältnismässig sein.[870] Hierbei muss das Interesse an der Wahrheitsfindung mit dem Interesse an einem schnellen Entscheid abgewogen werden.[871] Ebenfalls eine Grenze stellen die Persönlichkeitsrechte der betroffenen Personen dar, welche etwa Nachforschungen im Bereich der Privat- und Intimsphäre verwehren sollen.[872] Eingeschränkt werden kann der Untersuchungsgrundsatz auch durch die Mitwirkungspflicht der Betroffenen, welche in Art. 13 VwVG statuiert wird.

363 Art. 12 VwVG sieht vor, dass sich die Behörde verschiedener Beweismittel bedienen kann. Nach dem Wortlaut der Bestimmung können dies Urkunden, Auskünfte der Parteien, Auskünfte oder Zeugnis von Drittpersonen, Augenscheine oder Gutachten von Sachverständigen sein. In der herrschenden Rechtsauffassung wird die Aufzählung möglicher Beweismittel als nicht abschliessend verstanden, und es sollen auch Beweismittel zulässig sein, welche das Gesetz nicht ausdrücklich nennt.[873] Insbesondere der Urkundenbegriff

867 Siehe dazu oben, Rz. 275.

868 AUER/BINDER, VwVG-Kommentar, Art. 12 N. 16.

869 KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 12, N. 69.; zum Aspekt des rechtlichen Gehörs sogleich Rz. 366.

870 Vgl. etwa BGE 100 Ib 358, E. 1.

871 KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 12, N. 33.

872 Vgl. etwa BGE 115 Ia 234, E. 5.

873 Vgl. etwa HÄNER, in: Das erstinstanzliche Verwaltungsverfahren, S. 48; KÖLZ/HÄNER/BERTSCHI, N 468.

ist dabei technologieneutral gewählt.[874] So können als Urkunde unter Rückgriff auf den strafrechtlichen Urkundenbegriff (Art. 110 Ziff. 4 StGB) auch alle Aufzeichnungen auf Bild und Datenträgern verstanden werden, sofern sie bestimmt oder geeignet sind, eine Tatsachen von rechtlicher Bedeutung zu beweisen. Auf diese Weise zählen beispielsweise auch Modelle, Fotografien oder Ton- und Videoaufnahmen als Urkunden.[875] Der Augenschein als weitere Kategorie des Beweises lebt hingegen davon, dass die Gegebenheiten durch Sinneswahrnehmung bewertet werden sollen. Dies bedingt, dass die entsprechenden Beweismittel durch Personen mit ihren Sinnen wahrgenommen werden müssen (z.B. Sehen, Hören, Riechen).[876] Immerhin wird es als zulässig erachtet, dass Behörden sich hierbei durch den Einsatz technischer Hilfsmittel und Messgeräte unterstützen lassen können.[877] Art. 12 VwVG steht somit technologischen Neuerungen und den sich daraus ergebenden Beweismitteln nicht entgegen. Die Grenze ist dort zu ziehen, wo durch Auslegung Beweismittel geschaffen werden sollen, die im Verwaltungsverfahren gerade ausgeschlossen sein sollen, wie etwa das Parteiverhör.[878]

I. Recherchen

Im Rahmen von Art. 12 VwVG können Behörden – wie soeben ausgeführt – 364
eigene Recherchen führen, sofern sich die Betroffenen zu deren Ergebnissen äussern können. Das Internet und die zunehmende Vernetzung haben dazu geführt, dass sich den Behörden neue Erkenntnisquellen eröffnet haben, welche die amtsinterne Recherche erleichtern. Das Internet bietet eine grosse Fülle an Informationen, welche jederzeit und in der Regel auch kostenfrei abgerufen werden können. Diese Quellen können etwa genutzt werden, um den Inhalt oder Gehalt der Aussagen von Parteien zu verifizieren.[879] So kann nachgeprüft werden, ob ein Asylbewerber hinsichtlich seiner Herkunft die Wahrheit sagt, indem die Karte der Umgebung seines Dorfes mit seinen Erzählungen abgeglichen wird. Auch durch ihr eigenes Handeln und Auftreten im Internet und insbesondere den sozialen Medien können Personen Informationen über sich bekanntgeben, welche sie einer Behörde in einem Verfahren

874 AUER/BINDER, VwVG-Kommentar, Art. 12, N. 20.

875 Vgl. zum Ganzen: KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 12, N 87 f.; auch Urteil des BVGer A-6640/2010 vom 19. Mai 2011, E. 5.5.2.

876 KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 12, N. 132 ff.

877 Vgl. etwa BGE 104 Ia 69 E. 3b, jedoch kann z.B. die Konsultation eines Geoinformationssystems einen Augenschein nicht vollständig ersetzen; vgl. dazu weiter unten Rz. 377.

878 Vgl. zum Ganzen etwa: AUER/BINDER, VwVG-Kommentar, Art. 12, N. 20.

879 Vgl. KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 12, N. 176.

unter Umständen nicht preisgeben würden.[880] Relevant ist dies etwa im Sozialversicherungsrecht, wo etwa die Beurteilung einer anspruchsbegründenden Invalidität grundsätzlich auf Momentaufnahmen und Begutachtungen der betroffenen Person beruht. Wie die Diskussion über die Observation von Bezügern von Sozialversicherungsleistungen im Vorfeld der Abstimmung vom 25. November 2018 zeigte, beschäftigte das Thema, dass gewisse Personen dieses System ausnutzten und trotz einer Rente Tätigkeiten nachgingen, welche ihnen nicht möglich hätten sein sollen, die Schweizer Bevölkerung nicht unwesentlich.[881] Es stellt sich die Frage, ob es für die Behörden zulässig ist, von diesen umfassenden Möglichkeiten, welche ihnen durch das Internet eröffnet werden, Gebrauch zu machen, und inwiefern die betroffenen Personen vor einem Missbrauch dieser Daten im Verfahren durch die Behörden geschützt sind.

A. Das Internet als Erkenntnisquelle

365 Im Internet sind heutzutage Informationen in enormer und stetig wachsender Zahl auf Knopfdruck verfügbar. So bieten Rechercheplattformen wie «Wikipedia» zu jedem erdenklichen Thema eine Fülle an Informationen und können z.B. für die Definition eines im Verfahren umstrittenen Begriffs benutzt werden.[882] Juristische Fachartikel sowie Rechtsnormen oder Entscheide von anderen Gerichten können ebenfalls ohne grosse Umstände im Internet abgerufen werden, während diese früher ohne entsprechende Hilfsmittel und mit entsprechendem Aufwand etwa in einer Bibliothek oder der systematischen Gesetzessammlung konsultiert werden mussten.[883] Auch verschiedene öffentliche Register wie das Grundbuch oder das Handelsregister sind inzwischen online einsehbar. Diese Möglichkeiten stehen oft sowohl für die Behörden als auch für die Verfahrensparteien offen. Für die Behörden ist es daher naheliegend, dass die entsprechenden Erkenntnisse mit Verweis auf die Offenkundigkeit des Wissens einem Entscheid zugrunde gelegt werden, ohne dass die Person sich dazu äussern kann. Wie nachfolgend betrachtet werden soll, beinhaltet die Schweizer Rechtsordnung gewisse Vorkehrungen, aufgrund welcher dies nicht ohne Weiteres zulässig ist.

880 Dies teils sogar unbewusst; vgl. die Frau aus dem Kanton Aargau, welcher die Rente gekürzt wurde, weil sie zu viel twitterte: SERAFINI, Aargauerin wird IV-Rente halbiert – weil sie zu viel auf Facebook und Twitter ist, watson.ch, 4. November 2017.

881 Dies zeigt etwa die Stimmbeteiligung von immerhin 47,5% gemäss der Website des Bundes.

882 Vgl. etwa BGE 141 V 37, in dem sich das Bundesgericht bei der Qualifikation der Sportart «Dirt Bike», als absolutes Wagnis im Sinne des UVG auf einen «Wikipedia»-Artikel stützte.

883 Vgl. INFANGER, Justice – Justiz – Giustizia, 2017, S. 4; vgl. weiterführend zur Datifizierung des Rechts: ALTWICKER, Chinese Journal of International Law, 2019, S. 220.

1. Rechtliches Gehör

Aus Art. 29 Abs. 2 BV ergibt sich, dass der Anspruch der Verfahrensparteien 366
auf rechtliches Gehör gewahrt werden muss. Der Anspruch soll den Parteien die effektive Mitwirkung in Verfahren ermöglichen, mittels welcher in ihre Rechtsstellung eingegriffen werden kann.[884] Um den Anspruch auf rechtliches Gehör gewährleisten zu können, muss es den Betroffenen in erster Linie möglich sein, sich zum Verfahrensgegenstand zu äussern. Das rechtliche Gehör umfasst dabei ein Recht, an der Beweiserhebung teilzunehmen.[885] Es muss den Parteien in diesem Rahmen zumindest möglich sein, sich zu Beweisen zu äussern, welche geeignet sind, den Entscheid zu beeinflussen.[886] Es ist zu beachten, dass das rechtliche Gehör formeller Natur ist, sprich einer Partei unabhängig von ihrer Berechtigung an der Sache zusteht.[887] Das Bundesgericht schliesst daraus, dass eine Verletzung des Anspruchs grundsätzlich zur Aufhebung des Entscheids führt. Es schränkt dabei jedoch ein, dass eine nicht besonders schwerwiegende Verletzung des rechtlichen Gehörs geheilt werden kann, wenn die entsprechende Rechtshandlung (z.B. die Anhörung zum Beweismittel) vor der nächsthöheren Instanz mit derselben Kognition nachgeholt und die Verletzung somit geheilt wird.[888]

Der Untersuchungsgrundsatz umfasst dabei nur Tatsachen- und nicht 367
Rechtsfragen. Daher wird aufseiten der Behörde die Kenntnis des einschlägigen Rechts vorausgesetzt.[889] Insofern sich die Recherche daher auf die rechtliche Sachverhaltsanalyse und das Studium von Normen und Rechtsprechung beschränkt – auch wenn dies mithilfe von Internetdatenbanken geschieht –, ist darüber kein Beweis zu führen.[890] Kein Beweis geführt werden muss auch über Tatsachen, die offenkundig sind. Darunter werden Tatsachen subsumiert, welche zum Allgemeinwissen bzw. zum Erfahrungsschatz gehören oder zumindest einer grossen Zahl an Personen bekannt sind.[891] Es würde z.B. niemand daran zweifeln, dass die Tatsache «Der Zweite Weltkrieg dauerte von 1939 bis 1945» allgemein bekannt ist und Privaten nicht erneut unterbreitet

884 STEINMANN, SG Komm. BV, Art. 29, N. 42.

885 Vgl. zum Ganzen, WALDMANN, BSK BV, Art. 29, N. 50.

886 Vgl. Etwa BGE 137 II 266, E. 3.2; BGE 135 V 465, E. 4.3.2.

887 WALDMANN, BSK BV, Art. 29, N. 76.

888 STEINMANN, SG Komm. BV, Art. 29 N. 59, mit Verweis auf die Rechtsprechung.

889 KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 12, N. 17.

890 INFANGER, Justice – Justiz – Giustizia, 2017 S. 4. Jedoch muss sich die betroffene Partei auch zu den rechtlichen Überlegungen der Behörde äussern können, dies ergibt sich indes bereits aus Art. 30 VwVG; siehe dazu jedoch weiter oben Rz. 350.

891 Vgl. etwa VETTER/PEYER, in: Recht im digitalen Zeitalter, S. 763 m.w.H.

werden müsste, sollte sie einem Entscheid zugrunde gelegt werden. Daher müssen notorische Tatsachen nicht im Beweisverfahren erhoben werden, und es müssen sich die Verfahrensparteien auch nicht dazu äussern können.[892]

368 Damit eine Information als notorisch erachtet werden kann, muss sie nach konstanter Rechtsprechung nicht die ganze Zeit im Bewusstsein des Entscheiders präsent sein. Es reicht aus, dass sie aus öffentlich zugänglichen Quellen überprüft werden kann.[893] Das Internet hat es enorm vereinfacht, sich zu einem bestimmten Thema kundig zu machen, und eine Vielzahl der Informationen stehen grundsätzlich überall auf der Welt und jederzeit allen Menschen kostenlos offen. Daher könnte durchaus argumentiert werden, dass diese nach dem Ausgeführten als gerichtsnotorisch zu gelten haben. Würden nun Tatsachen, welche eine Behörde oder ein Gericht aus dem Internet erlangt hat, als gerichtsnotorisch angesehen werden, so können sie von der Behörde dem jeweiligen Entscheid zugrunde gelegt werden, ohne dass die Privaten zur jeweiligen Tatsache angehört werden müssen. Werden die entsprechenden Tatsachen indes nicht als notorisch erachtet, so muss den Privaten die Gelegenheit gegeben werden, sich dazu zu äussern, andernfalls eine Verletzung des rechtlichen Gehörs vorliegt.

369 Problematisch ist dabei jedoch, dass durch das Aufkommen des Internets unzählige Informationen auf einfache Weise öffentlich zugänglich gemacht wurden, welche dies in der analogen Welt nicht im selben Umfang waren, etwa mittels Vergleichsportalen zu Krankenkassenprämien, Miet- oder Kaufpreisen von Immobilien. Nicht alle diese Informationen sind dabei gleich verlässlich.[894] Die Wahl der konsultierten Sites und der Zeitpunkt der Konsultation sind daher geeignet, den Ausgang eines Verfahrens wesentlich mitzubestimmen, womit es umso schwerwiegender ist, falls sich das Gericht auf nicht verlässliche Informationen stützt.

370 Das Bundesgericht musste sich daher in den letzten Jahren mehrere Male mit der Frage der Gerichtsnotorietät von Internetquellen befassen. Eine entsprechende Auseinandersetzung fand jedoch nur selten im Bereich des Verwaltungsrechts statt.[895] Vorliegend ist vor allem die Rechtsprechung in strafrechtlichen Belangen analogieweise beizuziehen, da in diesem Bereich ebenfalls die Untersuchungsmaxime gilt (vgl. Art. 6 Abs. 1 StPO). Das Privatrecht, in dem grundsätzlich die Parteien mit ihren Vorbringen für die Erstellung des Sachverhalts verantwortlich sind, eignet sich dagegen nur beschränkt

892 Vgl. etwa KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 12, N. 69 und 178.

893 Vgl. BGE 143 IV 380, BGE 135 III 88, E. 4.1.

894 Vgl. dazu insbesondere auch die Diskussion über «Fake News» weiter oben Rz. 254 ff.

895 Vgl. aber immerhin BGE 141 V 37 im Bereich des Sozialversicherungsrechts.

als Analogieobjekt.[896] Die Rechtsprechung geht davon aus, dass Internetquellen als gerichtsnotorisch gelten können. Dabei sind jedoch aufgrund der ungewissen Verlässlichkeit lediglich Informationen als allgemein bekannt einzuordnen, welche aus einem Angebot stammen, das einen «offiziellen Anstrich» hat. Das Bundesgericht nennt als Beispiel etwa Internetquellen des Bundesamts für Statistik, den Internetfahrplan der SBB oder Handelsregistereinträge aus dem Internet.[897] Indes bleibt das Bundesgericht seiner Doktrin nicht immer in stringenter Weise treu. Im Folgenden soll die Rechtsprechung daher anhand verschiedener neuer Erkenntnisquellen, welche sich durch das Internet ergeben haben, genauer betrachtet werden.

a) Online-Nachschlagewerke

Durch Online-Nachschlagewerke wie «Wikipedia» kann zum Beispiel überprüft werden, ob ein Wort in einem bestimmten Sinn verstanden werden kann. Daraus können Schlüsse gezogen werden, etwa ob durch dessen Verwendung in einem bestimmten Kontext ein (Straf-)Tatbestand erfüllt wird.[898] In der analogen Welt erfüllen Lexika oder Wörterbücher wie der Duden eine ähnliche Funktion, und es wurde in der Regel nicht bestritten, dass entsprechend definierte Begriffe einem Entscheid als allgemein bekannt zugrunde gelegt werden konnten.[899] 371

Entsprechende Online-Angebote sind dabei in der Regel kostenlos für alle zugänglich und somit unter Umständen besser erreich- und nutzbar als kostenpflichtige Lexika. Der Unterschied zu analogen Nachschlagewerken besteht darin, dass Einträge in Online-Nachschlagewerken wie «Wikipedia» grundsätzlich von jedem Benutzenden jederzeit geändert werden können, was dazu führt, dass auch (absichtlich oder unabsichtlich verbreitete) Falschinformationen ihren Eingang auf eine entsprechende Seite finden können. Die Qualitätskontrolle ist dabei im Wesentlichen den Benutzenden selbst überlassen. Dies scheint zumindest für «Wikipedia» in der Regel zu funktionieren, da Fehler schnell entdeckt werden und eine Studie festgestellt hat, dass entsprechende Einträge in der Regel kaum ungenauer sind als diejenigen in entgeltlichen Nachschlagewerken.[900] Dennoch fehlt es den entsprechenden Angeboten wie «Wikipedia» am vom Bundesgericht in seiner Praxis verlangten «offiziellen Charakter», ist es doch nicht mit den dort als Beispiel 372

896 Vgl. zu dieser Thematik VETTER/PEYER, in: Recht im digitalen Zeitalter, S. 759 ff.

897 Vgl. zum Ganzen BGE 143 IV 380, E. 1.2.

898 Vgl. BGE 143 IV 380, siehe dazu sogleich unten Rz. 373.

899 INFANGER, Justice – Justiz – Giustizia, 2017, S. 6.

900 Vgl. etwa GILES, Nature, 2005, S. 900 ff.

zitierten Angeboten wie Zugfahrplänen der SBB oder Handelsregistereinträgen vergleichbar, welche von staatlichen oder zumindest vom Staat kontrollierten Stellen erstellt und gepflegt werden. Daraus lässt sich schliessen, dass Wissen aus Online-Nachschlagewerken grundsätzlich Entscheiden nicht als notorisches Wissen zugrunde gelegt werden darf. Wenn eine Behörde somit den Betroffenen zu den entsprechenden Tatsachen kein rechtliches Gehör gewährt, verstösst sie gegen die bundesgerichtliche Praxis.

373 Diese Feststellung hat insbesondere auch für andere, weniger bekannte Nachschlagewerke zu gelten. So hat das Bundesgericht etwa als unzulässig betrachtet, dass eine Vorinstanz den Begriff «muzz» aufgrund eines Eintrags auf der Seite «Wiktionary» als Synonym für alle Muslims als notorisch bezeichnet und in der Folge den Beschwerdeführer wegen Rassendiskriminierung im Sinne von Art. 261 StGB verurteilt hat, ohne dass sich dieser zur besagten Quelle äussern konnte.[901] Das Bundesgericht führte dazu aus, dass es sich bei «Wiktionary» um keine offizielle Quelle handle und diese aufgrund der einfachen Veränderbarkeit nicht als genügend zuverlässig gelten könne.[902] Wohl unproblematisch ist die Verwendung von Online-Nachschlagewerken dort, wo sie nur der Verifikation einer juristischen Subsumtion dienen.[903] Es erscheint jedoch als fraglich, ob ein Gericht bei der Subsumtion in weitem Masse auf eine «Wikipedia»-Definition abstellen darf, ohne dass die Parteien sich zu dieser äussern können, wie dies beim «Dirt Bike»-Entscheid (BGE 141 V 37) der Fall war.[904] Als problematisch wird auch erachtet, wenn ein Gericht eine Kurzsuche im Internet als notorisch bezeichnet, sofern die Parteien nicht von sich aus entgegenstehende glaubhafte Darstellungen vorlegen.[905]

374 Zusammenfassend lässt sich feststellen, dass Online-Nachschlagewerke durchaus von den Behörden als Erkenntnisquelle verwertet werden dürfen. Zwar können grössere Datenbanken wie «Wikipedia» grundsätzlich von jeder Person bearbeitet werden, jedoch ist aufgrund der schieren Anzahl an Bearbeitenden davon auszugehen, dass sich die «richtige» Ansicht mit grosser Wahrscheinlichkeit durchsetzt und diese daher als verlässliche Quelle gelten können. Dennoch verfügen sie nicht über den vom Bundesgericht geforderten «offiziellen Anstrich». Wenn eine entsprechende Definition einen

901 BGE 143 IV 380, E. 1.3.

902 BGE 143 IV 380, E. 1.3.1.

903 BGE 139 III 165 E. 4.3.2.; vgl. VETTER/PEYER, in: Recht im digitalen Zeitalter, S. 773; Urteil des Obergerichts des Kantons Zürich vom 17. Juli 2012, LF 120036, E. 3.3.3, in welchem zur Verifizierung der offenkundigen Tatsache, dass ein Supermarkt auch Frischprodukte führt, auf dessen Homepage verwiesen wurde.

904 INFANGER, Justice – Justiz – Giustizia, 2017, S. 6.

905 Vgl. etwa das Urteil des Zürcher Handelsgerichts ZR 111 (2012), Nr. 118, S. 313 ff., E. 6., INFANGER, Justice – Justiz – Giustizia, 2017, S. 5.

wesentlichen Bestandteil des Verfahrens ausmacht, etwa für die Einordnung unter einen Tatbestand, darf diese nicht ohne Weiteres als notorisch betrachtet werden. Gerade bei Unsicherheiten hinsichtlich der Notorietät eines Begriffs ist die Behörde gut beraten, wenn sie die Parteien einlädt, sich zu den vermeintlich notorischen Begriffen zu äussern, da ansonsten eine Verletzung des rechtlichen Gehörs vorliegen könnte.

b) Weitere Internetquellen

Nach den Ausführungen des Bundesgerichts sind Informationen aus weiteren Internetquellen nur dann als notorische Tatsachen zu werten, wenn sie einen offiziellen Charakter haben. Somit dürften die Behörden grundsätzlich nur Websites anderer Behörden und deren Informationen einem Entscheid zugrunde legen, ohne den Betroffenen das rechtliche Gehör zu gewähren. So hat das Bundesgericht etwa die Notorietät des LIBOR-Zinssatzes verneint, da dieser nicht auf einer Rechtsregel basierte.[906] Nicht als zulässig erachtet wurde in der Rechtsprechung auch, dass der Richter bei der Festsetzung des Anwaltshonorars seine Berechnung auf einen im Internet verfügbaren Rechner basierte und diese Information den Parteien nicht mitteilte.[907] Auch wo sich die Vorinstanz auf mehrere unabhängige Internetquellen oder im Internet verfügbare Artikel stützte, erachtete das Bundesgericht diese Informationen nicht als notorisch und verlangte entsprechend, dass sich die Betroffenen dazu äussern können.[908] Wenn also durch den Richter noch Zusatzschritte im Sinne einer Auswahl oder einer komplexen Berechnung vollbracht werden müssen, schadet dies der Notorietät. Das Bundesgericht ist indes von dieser Praxis abgewichen, indem es Währungsumrechnungskurse ebenfalls als notorisch bezeichnete, da diese mit wenig Aufwand im Internet kontrolliert werden können. Die Literatur geht in Anbetracht dieser nicht immer konsistenten Rechtsprechung davon aus, dass die Information im Internet leicht zugänglich und verlässlich sein muss, um als notorisch gelten zu können.[909] 375

c) Register

Diverse Register, wie das Grundbuch oder das Handelsregister, sind inzwischen ebenfalls im Internet abrufbar. So müssen etwa Handelsregistereinträge 376

906 BGE 134 III 224 E. 5.2 in Pra 2008 Nr. 143; kritisch hierzu etwa VETTER/PEYER, in: Recht im digitalen Zeitalter. S. 777.

907 Urteil des BGer 6B_102/2016 vom 9. Februar 2017, E. 3.

908 Urteil des BGer 6B_103/2015 vom 21. April 2015, E. 2; Urteil des BGer 6B_734/2016 vom 18. Juli 2017, E. 1.

909 Vgl. INFANGER, Justice – Justiz – Giustizia, 2017, S. 6; VETTER/PEYER, in: Recht im digitalen Zeitalter, S. 769 f.

gemäss Art. 12 Abs. 1 der Handelsregisterverordnung (HRegV; SR 221.411) für Einzelabfragen im Internet unentgeltlich zur Verfügung stehen.[910] Auch das Grundbuch ist öffentlich zugänglich. In der Grundbuchverordnung wird vorgesehen, dass eine Konsultation ohne Interessensnachweis möglich sein muss, jedoch ist die öffentliche Zugänglichmachung im Internet bisher lediglich zulässig und noch nicht verpflichtend. Die Grundbuchdaten gelten daher nur in dem Umfang, in dem sie kostenlos elektronisch verfügbar sind, als offenkundige Tatsachen.[911] Das Bundesgericht hat sie daher in Einklang mit der oben genannten Rechtsprechung als notorisch bezeichnet, da sie öffentlich jedermann zugänglich sind.[912] Diese Offenkundigkeit ergibt sich indes nicht aus der Abrufbarkeit im Internet, sondern aus der Öffentlichkeit der jeweiligen Register.[913]

d) Geoinformationssysteme

377 Die öffentliche Verwaltung sammelt in ihrer Tätigkeit auch eine Vielzahl an raumbezogenen Daten (z.B. Pläne von Orten, Gefahrenkarten etc.). Viele dieser Daten werden entweder von staatlicher Seite oder von Privaten in sogenannten Geoinformationssystemen digital aufbereitet und der Öffentlichkeit zur Verfügung gestellt.[914] Gerade in verwaltungsrechtlichen Verfahren – etwa im Bereich der Raumplanung – macht es für die Behörden Sinn, diese Daten beizuziehen. Durch die Konsultation dieser Geoinformationssysteme können sich die Behörden Aufwand ersparen und diese zum Beispiel für einen «informellen Augenschein» nutzen.[915] Diese Systeme sind für die Benutzenden grundsätzlich offen zugänglich, und gerade kantonale und eidgenössische Geoinformationssysteme müssen aufgrund ihres offiziellen Charakters auch als verlässlich bezeichnet werden. Dies spricht dafür, dass sie als gerichtsbekannt angesehen werden können. Problematisch ist, dass diese Systeme in der Regel nicht ständig aktualisiert werden und somit fraglich sein kann, ob sie zum Zeitpunkt der Konsultation die Wirklichkeit noch verlässlich abbilden. Wo die Systeme zudem anstelle eines formellen Augenscheins durch die Behörde benutzt werden, ist zu beachten, dass den Personen auf diese Weise die Möglichkeit genommen wird, sich dazu so zu äussern, wie sie dies

910 INFANGER, Justice – Justiz – Giustizia, 2017, S. 8.

911 Vgl. zum Ganzen: VETTER/PEYER, in: Recht im digitalen Zeitalter, S. 776 f.

912 Urteil des BGer 4A_195/2014, 4A_197/2014 vom 27. November 2014 E. 7.3.1; Urteil des BGer 4A_100/2016 vom 13. Juli 2016.

913 INFANGER, Justice – Justiz – Giustizia, 2017, S. 9.

914 Vgl. dazu etwa Botschaft GeoIG, S. 7843. vgl. etwa das Geoportal des Bundes, aber auch private Anbieter wie Googles Kartendienst «Google Earth».

915 INFANGER, Justice – Justiz – Giustizia, 2017, S. 9.

im Rahmen des Augenscheins hätten tun können. Gerade in Fällen, in welchen sich Personen aufgrund der unmittelbaren Kenntnis vor Ort dazu besser äussern könnten, sollte ihnen diese Möglichkeit auch eingeräumt werden, wenn sich die Behörden auf Geoinformationssysteme stützen.[916]

2. Fazit

Das Internet räumt den Behörden neue Möglichkeiten der amtsinternen Recherche ein. Werden die sich daraus ergebenden Erkenntnisse indes durch die Behörde bei der Ermittlung des Sachverhalts zugrunde gelegt, so müssen die betroffenen Personen die Gelegenheit haben, sich dazu zu äussern. Wird ihnen diese nicht eingeräumt, so kann dies eine Verletzung des Anspruchs auf rechtliches Gehör darstellen. Davon ausgenommen werden können die Daten, welche als allgemein bekannt (oder notorisch) gelten. Für die Notorietät von Informationen spricht, wenn diese öffentlich zugänglich sind und einfach überprüft werden können. Gerade deshalb, weil durch das Internet eine grosse Fülle an Informationen öffentlich zugänglich geworden ist, muss dem Aspekt der Verlässlichkeit dieser Daten ein höheres Gewicht beigemessen werden. Als verlässlich erachtet werden in der Rechtsprechung insbesondere Angebote mit einem offiziellen Anstrich. Aber auch Angebote, welche nicht von offizieller Seite stammen, wurden vom Bundesgericht bereits als notorisch bezeichnet. Sieht man sich die Fälle näher an, in welchen das Bundesgericht eine Notorietät trotz fehlendem offiziellem Anstrich bejahte, fallen immerhin einige Gemeinsamkeiten auf. Als bekannt wird eine Information aus dem Internet insbesondere dann angesehen, wenn es ein entsprechendes Angebot bereits in der Zeit vor dem Internet gab und dieses lediglich die Zugänglichkeit erleichtert hat. So waren z.B. die Währungskurse in Banken und Wechselstuben ausgehängt oder konnten dort erfragt werden, während heute verschiedene Websites ähnliche Dienste «auf Knopfdruck» anbieten. «Wikipedia» wiederum wird beispielsweise in der Tradition von Nachschlagewerken wie Lexika gesehen. Gegen eine Notorietät spricht, wenn die im Internet verfügbaren Inhalte durch weitere Schritte zur Verwendung aufgearbeitet werden, etwa indem ein Algorithmus die Durchschnittsmiete berechnet oder der Richter eine Auswahl unter verschiedenen Zeitungsartikeln trifft. Im Zweifelsfall tut die betroffene Behörde gut daran, den Betroffenen das rechtliche Gehör über im Rahmen ihrer amtsinternen Recherche gefundene Erkenntnisse zu gewähren, da eine andernfalls resultierende Gehörsverletzung aufgrund der formellen Natur des rechtlichen Gehörs zur Aufhebung des Entscheids führen kann. 378

916 INFANGER, Justice – Justiz – Giustizia, 2017, S. 8.

B. Recherche in sozialen Medien

379 Wie bereits weiter oben ausgeführt wurde, besitzt heutzutage ein grosser Teil der Einwohner der Schweiz ein Konto auf mindestens einer Social-Media-Plattform. Viele Personen stellen auf diesen Plattformen Fotos online, schreiben Kommentare oder teilen andere Inhalte. Diese Informationen können dabei je nach den vorgenommenen Privatsphäre-Einstellungen in verschiedenem Masse von anderen Benutzenden der Plattform eingesehen werden, unter Umständen sogar durch jede Person oder Behörde, welche die betreffende Person auf dieser Plattform mit ihrem Namen sucht. In gewissen verwaltungsrechtlichen Verfahren können Informationen, welche die Personen auf diesem Weg über sich preisgeben, eine wichtige Rolle spielen. Zu denken ist dabei in erster Linie an das Sozialversicherungsrecht. Die Sozialversicherungsträger sind bei der Prüfung von Begehren in diesem Bereich (etwa betreffend eine Invalidenrente) regelmässig auf Arztzeugnisse und Gutachten angewiesen.[917] Während diese nur Momentaufnahmen vermitteln können, sind Daten, welche eine Person im Internet preisgibt, unter Umständen geeignet, ein anderes Bild zu zeichnen. Wenn etwa eine Person, welche wegen eines Rückenleidens eine Invalidenrente bezieht, auf Facebook Fotos von sich beim Sport oder beim Heben schwerer Gegenstände veröffentlicht, können Zweifel an der rentenbegründenden Invalidität aufkommen.

380 Tatsächlich haben Sozialversicherungsträger bereits in verschiedenen Fällen Leistungsbegehren auch gestützt auf Einträge insbesondere auf Facebook abgelehnt oder widerrufen, wodurch sich auch Gerichte mit diesem Phänomen zu befassen hatten.[918] Im Bereich des Sozialversicherungsrechts dürfen die Versicherungsträger gemäss Art. 43 ATSG Abklärungen zur Beurteilung der Begehren treffen. Dabei steht ihnen in Anlehnung an Art. 12 VwVG ein weites Feld an möglichen Beweismitteln offen[919], so dass Recherchen im Internet nicht von vorneherein ausser Betracht fallen. Daher erachtet das Bundesgericht in seiner Rechtsprechung eine Verwendung von Facebook-Recherchen nicht als rechtswidrige Sachverhaltsabklärung.[920] Indes bestehen durchaus grundrechtliche Überlegungen, sich mit dieser Frage vertieft auseinanderzusetzen.

917 Vgl. etwa Art. 43 und Art. 44 ATSG.

918 Vgl. etwa Urteil des BGer 8C_192/2017 vom 25. August 2017, E. 5.4.3.2; anstatt vieler aus der kantonalen Rechtsprechung: Urteil des Versicherungsgerichts des Kantons St. Gallen IV 2016/145 vom 6. Dezember 2016, E. 3.2.6; Urteil des Sozialversicherungsgerichts des Kantons Zürich IV.2015.00744 vom 28. September 2015 E. 2.2.

919 KIESER, SK ATSG, Art. 43, N. 30.

920 Urteil des BGer 8C_909/2017 vom 26. Juni 2018, E. 6.2. m.w.H.

1. Eingriff in die Privatsphäre

Die Recherche in Social-Media-Profilen (insb. Facebook) als Grundlage für einen Rentenentscheid wird mit Blick auf ihre Zulässigkeit in der Literatur mit der Observation von Sozialversicherungsbezügern verglichen.[921] Zwar ist offensichtlich, dass ein Medium wie Facebook nicht eins zu eins mit dem öffentlichen Raum, in welchem entsprechende Observationen durchgeführt werden, gleichgestellt werden kann. Dennoch sind gewisse Gemeinsamkeiten nicht von der Hand zu weisen, besteht doch auch bei Facebook – sofern eine Person die entsprechenden Privatsphäre-Einstellungen nicht anpasst – die Möglichkeit, dass das Profil einer Person inklusive ihrer Einträge oder Fotos von einer unbegrenzten Menge an Personen eingesehen werden kann.[922] Hinsichtlich von Observationen werden dabei in erster Linie das Recht auf persönliche Freiheit (nach Art. 10 Abs. 2 BV), das Recht auf Privatsphäre (nach Art. 13 Abs. 1 BV) und das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) thematisiert.[923] Daher soll im Folgenden überprüft werden, ob bzw. in welchem Masse entsprechende Überlegungen auch hinsichtlich der Internetrecherche in sozialen Medien zu gelten haben. 381

i) Achtung des Privat- und Familienlebens

Art. 13 BV Abs. 1 BV garantiert unter anderem die Achtung des Privat- und Familienlebens. Dieser Anspruch auf Privatsphäre ist im Sinne eines Rechts, alleingelassen zu werden, auszulegen und schützt davor, dass der Staat in die private Sphäre, also in Räume und Bereiche privater Lebensgestaltung, eingreift.[924] Es wird weitgehend davon ausgegangen, dass auch Handlungen, welche in der Öffentlichkeit vorgenommen werden, unter den Schutzbereich des Grundrechts fallen, sofern ein Interesse des Betroffenen an Geheimhaltung oder Vertraulichkeit existiert.[925] Weniger klar ist indes, was dies für die Kommunikation im Internet bedeutet. Es kann wohl richtigerweise davon ausgegangen werden, dass Websites und Blogs nicht unter die Privatsphäre fallen, da sie gerade den Zweck haben, eine Information der Öffentlichkeit zugänglich zu machen.[926] Beiträge auf sozialen Medien wie Facebook werden 382

921 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 277.

922 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 277.

923 Statt vieler: BGE 137 I 327 E. 4.4; EICHENBERGER/PRIBNOW, HAVE, 2017, S. 276.

924 MÜLLER/SCHEFER, S. 139 f.

925 BREITENMOSER/SCHWEIZER, SG Komm. BV, Art. 13, N. 13; vgl. etwa auch: Urteil des EGMR P.G. und J.H. gegen Vereinigtes Königreich 44787/98 vom 25. September 2001, Ziff. 56; vgl. etwa hinsichtlich der Observation auch BGE 137 I 327, E. 4.4 m.w.H.

926 MÜLLER/SCHEFER, S. 205; EICHENBERGER/PRIBNOW, HAVE, 2017, S. 278.

dagegen normalerweise in erster Linie an einen bestimmten Adressatenkreis, etwa die jeweiligen «Freunde», gerichtet. Je nach Privatsphäre-Einstellungen sind diese Beiträge jedoch für alle Benutzenden öffentlich einsehbar, was den Betroffenen unter Umständen nicht bewusst ist.[927]

383 Das Bundesgericht hat in ständiger Rechtsprechung anerkannt, dass die Verwendung öffentlich zugänglicher Beiträge auf Social Media zur Recherche in Rentenverfahren keinen Eingriff in die Privatsphäre darstellt, ohne diese Einschätzung indes weiter zu begründen.[928] Nach dem soeben Geschriebenen lässt sich durchaus auch ein anderer Schluss vertreten, insbesondere wenn den Betroffenen unter Umständen die Öffentlichkeit ihrer Aussagen nicht bewusst ist und sie nicht damit rechnen, dass eine staatliche Stelle auf diese Daten zugreifen könnte, um etwa einen Rentenanspruch zu beurteilen.[929] Anzumerken ist hierzu m.E. immerhin, dass aufgrund diverser Skandale und Medienberichte insbesondere um Facebook in den letzten Jahren das generelle Bewusstsein über das Thema «Privatsphäre auf Facebook» wohl eher zugenommen hat. Zudem ist zumindest auf Facebook bei Beiträgen, welche die betroffene Person selber erstellt, mittlerweile standardmässig eingestellt, dass diese nur auf der Plattform befreundeten Personen zugänglich sind.[930]

ii) Informationelle Selbstbestimmung

384 Im Weiteren ist zu prüfen, ob ein Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV vorliegt. Das Recht auf informationelle Selbstbestimmung schützt über den Wortlaut der Regelung hinaus nach herrschender Lehre nicht nur vor dem Missbrauch der persönlichen Daten, sondern gibt den Betroffenen einen – nach den Voraussetzungen von Art. 36 BV einschränkbaren – Anspruch, bei fremder (z.B. staatlicher) Bearbeitung ihrer Daten bestimmen zu können, zu welchem Zweck diese Informationen bearbeitet und gespeichert werden dürfen.[931] Der Anspruch auf informationelle Selbstbestimmung wird durch das Datenschutzrecht konkretisiert.

927 Vgl. EICHENBERGER/PRIBNOW, HAVE, 2017, S. 277 f.; AEBI-MÜLLER/GÄCHTER/ALIOTTA, in: Personen-Schaden-Forum 2011, S. 190. Zu beachten ist zudem die Tatsache, dass auch ein an die eigenen «Freunde» gerichteter Beitrag von diesen weiterverteilt werden kann, vgl. etwa Urteil des Obergerichts des Kantons Zürich SB 130371 vom 25. November 2013, E. 2.2.3.

928 Urteil des BGer 8C_192/2017 vom 25. August 2017, E. 5.4.3.2.

929 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 277.

930 Vgl. etwa: EISHOFER, So stellen sie die Privatsphäre um; vgl. in diesem Zusammenhang auch den in Art. 6 E-DSG und Art. 22 DSGVO erfassten Grundsatz des Datenschutzes durch benutzerfreundliche Voreinstellungen (privacy by design).

931 Vgl. etwa DIGGELMANN, BSK BV, Art. 13 N. 32.

Das Bundesgericht hat sich in seiner bisherigen Rechtsprechung noch nicht damit auseinandergesetzt, ob das Recht auf informationelle Selbstbestimmung durch die Recherche in sozialen Medien betroffen ist.[932] Indes nimmt die Lehre an, dass etwa mit der (unter vielen Faktoren vergleichbaren) Observation durch Sozialversicherungsbehörden stets auch eine Datenverarbeitung verbunden ist.[933] Ein ähnlicher Schluss liegt also auch hinsichtlich der Recherche in sozialen Medien nahe. Verwendet eine Behörde Informationen aus Social Media im Rahmen eines Verfahrens, so handelt es sich dabei zweifelsfrei um Personendaten, da diese von der jeweiligen Facebook-Präsenz der Person stammen und diese somit bestimmt ist (Art. 3 lit. c. DSG). Die Internetrecherche einer IV-Stelle greift somit in das Grundrecht auf informationelle Selbstbestimmung ein, da damit eine Bearbeitung von Personendaten durch die Behörde zusammenhängt.[934] Bei der Recherche in Social-Media-Profilen besteht der Zweck im vorliegenden Zusammenhang gerade darin, Daten über den Gesundheitszustand der Person zu erfahren. Dabei handelt es sich um besonders schützenswerte Personendaten im Sinne von Art. 3 lit. c DSG. Zudem lässt sich je nach Offenherzigkeit der Person in ihrem Facebook-Auftritt gar ein Persönlichkeitsprofil im Sinne der Datenschutzgesetzgebung erstellen.[935] 385

Auch hier stellt sich indes das Problem, wie damit umzugehen ist, dass die Daten durch die jeweilige Person öffentlich zugänglich sind. Das Datenschutzrecht sieht für die Datenbearbeiter gewisse Erleichterungen vor, wenn die Daten durch die Betroffenen selbst öffentlich zugänglich gemacht wurden. So sieht Art. 17 Abs. 2 DSG vor, dass bei einer Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen durch Bundesorgane vom Erfordernis einer gesetzlichen Grundlage im formellen Sinn abgewichen werden kann, wenn die betroffene Person im Einzelfall eingewilligt oder ihre Daten allgemein zugänglich gemacht hat. In der Lehre wird als fraglich erachtet, ob Daten, welche einem eingeschränkten Nutzerkreis – etwa im Rahmen eines sozialen Netzwerks – zugänglich gemacht werden, überhaupt als öffentlich zugänglich gelten sollen.[936] 386

Auch wenn angenommen wird, dass diese Daten als öffentlich zugänglich zu gelten haben, ist es nach der aktuellen Rechtslage fraglich, ob das Vorliegen 387

932 Vgl. Urteil des BGer 8C_909/2017 vom 26. Juni 2018, E. 6.2; 8C_192/2017 vom 25. August 2017, E. 5.4.3.2.

933 Vgl. etwa: HORSCHIK, in: Datenschutz im Arbeits-, Versicherungs- und Sozialbereich: Aktuelle Herausforderungen, S. 91.

934 Vgl. EICHENBERGER/PRIBNOW, HAVE, 2017, S. 278.

935 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 279.

936 Vgl. etwa MUND, SHK-DSG, Art. 17, N. 20, wobei hier davon ausgegangen wird, dass Bundesorgane selten auf öffentlich zugängliche Quellen zugreifen würden.

dieser Ausnahmekonstellation die gesetzliche Grundlage als Ganzes ersetzt oder nur die Notwendigkeit einer formell-gesetzlichen Grundlage entfallen lässt. Zumindest gestützt auf das aktuelle Datenschutzgesetz dürfte dabei noch von Letzterem ausgegangen werden, womit eine gesetzliche Grundlage im materiellen Sinn weiterhin die Bearbeitung dieser Daten vorsehen müsste.[937] Zu beachten ist in diesem Zusammenhang auch, dass die Ausnahmekonstellation nur im Einzelfall gelten soll und nicht für eine regelmässige oder dauerhafte Bearbeitung.[938] Zudem besteht gerade aufgrund der zunehmenden Entwicklung des Internets die Möglichkeit, eine entsprechende Bearbeitung auch öffentlich zugänglicher Daten jederzeit ausdrücklich zu untersagen.[939] Hier stellt sich indes gerade wieder die Problematik, dass oftmals nicht damit gerechnet wird und auch lange nicht ersichtlich ist, dass Organe der öffentlichen Verwaltung die entsprechenden Daten auch bearbeiten.

iii) Persönliche Freiheit

388 Auch Art. 10 Abs. 2 BV garantiert einen Anspruch auf Vertraulichkeit bzw. Diskretion bestimmter personenbezogener Daten, sofern dieser nicht bereits durch andere Grundrechtsbestimmungen gedeckt ist. Diese Garantie spielt insbesondere dann eine Rolle, wenn durch die Daten- oder Informationsbearbeitung dem Betroffenen ein derart gravierender Nachteil entsteht, dass er in seiner freien Persönlichkeitsentfaltung beeinträchtigt wird. Im vorliegenden Fall dürfte dieser Schutzanspruch allerdings regelmässig hinter dem Anspruch auf Schutz der Privatsphäre gemäss Art. 13 Abs. 1 BV zurückstehen.[940]

a) Gesetzliche Grundlage

389 Entgegen der Praxis des Bundesgerichts kann somit m.E. durchaus vertreten werden, dass durch die Recherche in sozialen Medien ein Eingriff in die Privatsphäre oder in die informationelle Selbstbestimmung vorliegt. Ein staatlicher Eingriff in die genannten Grundrechte setzt gemäss Art. 36 BV eine gesetzliche Grundlage voraus. Aus dem Legalitätsprinzip in Art. 5 BV und aus Art. 36 BV ergeben sich gewisse Anforderungen an die gesetzliche Grundlage, welche hier von besonderer Relevanz sind. Bereits aus Art. 36 Abs. 1 Satz 2 BV ergibt sich, dass schwerwiegende Eingriffe grundsätzlich in einem Gesetz vorgesehen sein müssen, wobei darunter ein Gesetz im formellen Sinne zu verstehen ist, welches vom zuständigen Parlament erlassen wurde. Für leichte

937 Siehe zur ausführlichen Diskussion auch oben Rz. 379 ff.

938 MUND, SHK-DSG, Art. 17 N. 18.

939 Botschaft Rev. DSG 2003, S. 2141.

940 Vgl. AEBI-MÜLLER/GÄCHTER/ALIOTTA, in: Personen-Schaden-Forum 2011, S. 192.

Eingriffe reicht dagegen eine Grundlage auf Verordnungsstufe.[941] Im Weiteren muss der Rechtssatz so klar und bestimmt formuliert sein, dass der Bürger sein Verhalten danach richten und die rechtlichen Folgen seines Verhaltens bis zu einem gewissen Grad erkennen kann.[942]

390 Im Bereich des Sozialversicherungsrechts dürfen die Versicherungsträger gemäss Art. 43 ATSG Abklärungen zur Beurteilung der Begehren treffen. In langjähriger Rechtsprechung wurden gestützt auf diese Bestimmung i.V.m Art. 28 ATSG Observationen von Leistungsbezügern als zulässig erachtet.[943] Im Bereich der Invalidenversicherung wurde gestützt auf die Möglichkeit des Beizugs von Spezialisten nach Art. 59 Abs. 5 IVG auch die Observation in öffentlich einsehbaren Räumen der Wohnung als zulässig erachtet.[944]

391 Die auf den genannten Bestimmungen beruhende Zulässigkeit der Observation wurde vom EGMR im Fall Vukota-Bojic als Eingriff in die Privatsphäre gemäss Art. 8 EMRK beurteilt. Der Gerichtshof stellte fest, dass sich die angeführten Gesetzesbestimmungen weder implizit noch explizit zur Observation äussern würden und keine Regelungen etwa hinsichtlich des Bewilligungsprozesses, der Aufsicht, des Rechtswegs oder der Dauer der Überwachung und der Aufbewahrung der Daten vorsehen. Mangels Bestimmtheit könnten sie daher nicht als genügende gesetzliche Grundlagen angesehen werden, welche einen Eingriff zu rechtfertigen vermögen.[945] Das Urteil des EGMR nahm der Gesetzgeber zum Anlass, mit Art. 43a ATSG eine gesetzliche Grundlage für die Observation von versicherten Personen zu schaffen, welche die verdeckte Observation und Aufnahme von Bild- und Tonaufnahmen zulässt, wenn konkrete Anhaltspunkte auf Versicherungsmissbrauch bestehen oder sonstige Abklärungen aussichtslos wären. Die entsprechenden Gesetzesbestimmungen wurden von der Stimmbevölkerung am 25. November 2018 angenommen und traten per 1. Oktober 2019 in Kraft. Indes wurden auch zu dieser gesetzlichen Grundlage bereits grundrechtliche Bedenken laut.[946]

392 Folgt man der Rechtsprechung des EGMR, so bleibt auch für die Internetrecherche fraglich, ob Art. 43 ATSG oder Art. 59 IVG als genügende gesetzliche Grundlage für die damit verbundenen Eingriffe in die Privatsphäre und die informationelle Selbstbestimmung gelten, zumal der Bürger aus einer Rechtsnorm ableiten können muss, welche möglichen Konsequenzen

941 SCHWEIZER, SG Komm. BV, Art. 36, N. 16.

942 SCHINDLER/TSCHUMI, SG Komm. BV, Art. 5, N. 33.

943 BGE 135 I 169, E. 5.4 ff.

944 BGE 137 I 327, E. 5.2 ff.

945 Urteil des EGMR Vukota-Bojic gg. Schweiz Nr. 61838/10 vom 18. Oktober 2016, N. 73 ff.

946 Vgl. etwa. GÄCHTER, HAVE, 2018; HEUSSER, HAVE, 2018.

sich daraus für ihn ergeben, was nach dem soeben Ausgeführten hier kaum gegeben ist.[947]

393 Gerade im Bereich der staatlichen Datenbearbeitungen können aufgrund der schieren Vielzahl an Konstellationen oftmals keine hohen Anforderungen an die Bestimmtheit einer Norm gestellt werden.[948] Zudem ist aufgrund der Tatsache, dass die Daten öffentlich zugänglich sind, die Privilegierung von Art. 17 Abs. 2 DSG zu beachten, durch welche die Anforderungen an die Bestimmtheit ebenfalls heruntergesetzt werden. Dennoch sind Zweifel am Vorliegen einer genügenden gesetzlichen Grundlage angebracht, wobei hinsichtlich Art. 43 ATSG bereits die erwähnte Rechtsprechung des EGMR starke Argumente für eine mangelnde Bestimmtheit zur Datenbearbeitung liefert. Dies hat auch für Art. 59 Abs. 5 IVG zu gelten, zumal die Internetrecherche keineswegs durch Spezialisten durchgeführt werden muss, sondern grundsätzlich jedem Verwaltungsmitarbeiter möglich ist.[949] Der neue Art. 43a ATSG ist bereits aufgrund des Wortlauts auf die Observation und die Herstellung von Bild- und Tonmaterialien zugeschnitten. So ist unter Absatz 4 statuiert, dass die Observation nur an öffentlich zugänglichen oder einsehbaren Orten zulässig ist, wobei damit nur physische Orte gemeint sein können.[950] Somit fällt auch dieser Artikel als gesetzliche Grundlage ausser Betracht. Das Bundesgericht hat durch seine bisherige Rechtsprechung indes entschieden, sich der Frage nach einer gesetzlichen Grundlage gar nicht zu stellen, in dem es bereits a priori davon ausging, dass keine Verletzung vorliegt.

b) Öffentliches Interesse und Verhältnismässigkeit

394 Selbst wenn die Bestimmungen des ATSG als genügende gesetzliche Grundlage für die Social-Media-Recherche angenommen würden, so müsste diese im Weiteren auch im öffentlichen Interesse liegen und verhältnismässig sein. Dies ergibt sich bereits aus Art. 5 Abs. 2 BV, aber auch aus Art. 36 Abs. 2 und Abs. 3 BV. Beim öffentlichen Interesse handelt es sich um einen unbestimmten Rechtsbegriff, welcher durch die Verwaltungsbehörde ausgelegt werden muss. Der Begriff ist dabei grundsätzlich weit zu verstehen.[951] Als öffentliches Interesse kann im vorliegenden Fall daher etwa angeführt werden, dass es im Interesse der Gemeinschaft der Versicherten liegt, den Missbrauch in

947 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 280; AEBI-MÜLLER/GÄCHTER/ALIOTTA, in: Personen-Schaden-Forum 2011, S. 193.

948 MUND, SHK-DSG, Art. 17, N. 8.

949 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 280.

950 Vgl. Bericht PI Überwachung, S. 7425.

951 EPINEY, BSK BV, Art. 5, N. 62 ff.

den Sozialversicherungen zu bekämpfen, und dass nur die Sozialversicherungsleistungen ausbezahlt werden, welche auch geschuldet sind.[952]

In Frage zu stellen ist aber, ob die entsprechende Recherche auch verhält- 395
nismässig ist. Um als verhältnismässig im Sinne der oben genannten Bestimmungen zu gelten, muss die Massnahme geeignet sein, um das entsprechende Ziel zu erreichen (Geeignetheit), es darf kein milderes Mittel geben, um dieses Ziel zu erreichen (Erforderlichkeit), und sie muss für die Betroffenen zumutbar (oder verhältnismässig im engeren Sinne) sein, indem die erwartete Wirkung nicht in einem Missverhältnis zu den betroffenen Interessen steht.[953]

Kritisch hinterfragt werden kann dabei, ob die Recherche auf sozialen 396
Medien überhaupt geeignet ist. Dabei ist in erster Linie zu beachten, dass Beiträge auf sozialen Medien wie Facebook nicht unbedingt die Realität abbilden. Meist wollen sich die Personen auf den Portalen auf eine gewisse Weise darstellen oder inszenieren. Auch fehlt bei den hochgeladenen Bildern oder kurzen Videosequenzen oft der Kontext, in welchem diese aufgenommen wurden. So mag es auch Fälle geben, welche eindeutig erscheinen, dies aber gar nicht sind. Wenn der wegen eines Rückenleidens krankgeschriebene Rentenbezüger auf einem Foto/Video bei Klimmzügen gezeigt wird, kann dies zwar in Widerspruch zu seinem Gutachten stehen, aber ebenso auch physiotherapeutisch verordnet sein. Es ist daher fraglich, ob entsprechende Video- oder Fotobeweise den geforderten Beweisgrad der überwiegenden Wahrscheinlichkeit erreichen können.[954] Indes kann solchen Indizien der Beweiswert im Rahmen des Grundsatzes der freien Beweiswürdigung nicht vollständig abgesprochen werden.[955]

Als problematisch erachtet werden kann dabei zudem, dass gewisse Per- 397
sonen aufgrund ihres Namens etwa auf Facebook viel einfacher aufgefunden werden können als andere, welche aufgrund ihres «gewöhnlichen» Namens viel mehr «Namensvettern» haben und somit in der Masse schwieriger auffindbar sind. Personen mit speziellen Namen müssten also grundsätzlich eher damit rechnen, dass ihre Daten aus Facebook beigezogen werden und sind eher einem Eingriff in ihre Privatsphäre ausgesetzt.[956] Weiter besteht auf Facebook keinerlei rechtliche Pflicht, unter seinem richtigen Namen aufzutreten, sondern es ist problemlos möglich, ein Pseudonym oder einen Spitznamen für

952 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 280.

953 Vgl. EPINEY, BSK BV, Art. 5, N. 70.

954 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 281.

955 MEYER, Mitwirkungsmaxime, S. 397.

956 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 277.

sein Profil auszuwählen.[957] Personen, die von dieser Möglichkeit Gebrauch machen, können von den Behörden noch schlechter oder gar nicht aufgefunden werden. Es ist offensichtlich, dass eine absolute Gleichbehandlung nicht möglich ist, dennoch wird vertreten, dass auch dieser Aspekt zumindest im Rahmen einer Gesamtbetrachtung zu berücksichtigen sei.[958] Indes werden an die Geeignetheit oft niedrige Ansprüche gestellt, so dass es ausreichen kann, wenn die Massnahme zur Erreichung des Zwecks beiträgt.[959] Unter diesen Umständen kann die Facebook-Recherche zumindest aus Sicht der Behörde durchaus geeignet sein. Ob sie auch erforderlich und für den Betroffenen zumutbar ist, kann wohl hauptsächlich anhand des konkreten Einzelfalls betrachtet werden, etwa ob im jeweiligen Fall mildere Mittel zur Verfügung gestanden hätten. Dies ist zumindest nicht von vorneherein auszuschliessen.

398 Zu beachten ist in diesem Zusammenhang auch die einheitliche Praxis von SEM und BVGer hinsichtlich im Asylverfahren eingebrachter Facebook-Posts als Beweismittel (z.B. für exilpolitisches Engagement), welche jeweils als wenig überzeugend beurteilt werden.[960] Es ist nach dem Geschriebenen schwer nachvollziehbar, weswegen eine andere Bewertung der Verlässlichkeit dieser Quelle möglich sein soll, wenn deren Inhalte von den Betroffenen zu ihren Gunsten als Beweismittel eingebracht werden, als wenn dies die Behörden zu deren Ungunsten tun.[961]

c) Fazit

399 Das Bundesgericht erkennt in der Verwendung von öffentlich zugänglichen Daten aus Quellen wie Facebook keinen Eingriff in die Privatsphäre oder die informationelle Selbstbestimmung der Betroffenen. Ein anderer Schluss kann jedoch ebenfalls vertreten werden, insbesondere weil – auch wenn ihre Daten öffentlich zugänglich sind – die Betroffenen sich deren Verwendung in einem Verfahren gegen sie unter Umständen gar nicht bewusst sind. Wird ein Eingriff angenommen, so ist ebenfalls als zweifelhaft zu beurteilen, ob die bestehenden Art. 43 ATSG oder Art. 59 Abs. 5 IVG, welche die Sachverhaltsabklärung durch Sozialhilfebehörden regeln, als genügend bestimmte gesetzliche Grundlagen gelten können. Nicht zuletzt stellen sich auch Fragen

957 Vgl. dazu etwa den Entscheid des LG Berlin Az. 16 O 341/15 vom 16. Januar 2018. Ähnliches dürfte wohl auch für die Schweiz gelten.

958 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 278.

959 WEBER-DÜRLER, FS Moor, Zur neusten Entwicklung des Verhältnismässigkeitsprinzips, S. 594 f.

960 Vgl. statt vieler: Urteil des BVGer E-7836/2015 vom 4. Januar 2016, E. 3.4.

961 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 281, MEYER, Mitwirkungsmaxime, S. 397.

hinsichtlich der Verhältnismässigkeit. Auch wenn das Bundesgericht sich bisher in ständiger Praxis auf den Standpunkt gestellt hat, dass kein Eingriff in die Privatsphäre vorliege, ist es durchaus naheliegend zu erwarten, dass der EGMR hier ähnlich wie hinsichtlich der Observationen zu einem anderen Schluss kommen könnte, sollte er dereinst angerufen werden.

2. Rechtliches Gehör

Nach dem soeben Ausgeführten ist es fraglich, ob sich die Verwendung der entsprechenden Daten auf eine genügende gesetzliche Grundlage stützen kann. Auch wenn man davon ausgehen würde, dass eine solche aufgrund der öffentlichen Zugänglichkeit der Daten nicht benötigt wird, ist den Betroffenen deren mögliche Verwendung im Verfahren wohl oft nicht bewusst. Gerade auch vor diesem Hintergrund ist es daher besonders wichtig, dass der Partei die Möglichkeit gegeben wird, sich zu den Erkenntnissen zu äussern, welche die Behörden aus der Internetrecherche ziehen. Es ist davon auszugehen, dass die Recherchen im Internet durch die Behörden grundsätzlich relativ formlos verlaufen und die aus der Konsultation eines entsprechenden Profils gezogenen Schlüsse in die Auffassung der Behörde Eingang finden können, ohne dass die betroffene Person sich dazu vorzeitig äussern konnte.[962] 400

Wie ebenfalls bereits an anderer Stelle ausgeführt, ergibt sich aus Art. 29 Abs. 2 BV der Anspruch der Verfahrensparteien, am Beweisverfahren mitzuwirken und sich insbesondere zu deren Erkenntnissen äussern zu können. Dies hat auch für das Sozialversicherungsverfahren zu gelten. So akzeptiert das Bundesgericht etwa, dass ein Augenschein unangemeldet durchgeführt werden kann. Dabei muss die Partei aber als Korrektiv die Möglichkeit haben, sich zu deren Verlauf zu äussern.[963] Daraus ergibt sich, dass die Person vor dem Erlass der Verfügung die Gelegenheit erhalten muss, sich zu den daraus gewonnenen Erkenntnissen zu äussern. 401

II. Mitwirkungspflichten

A. Gesetzliche Vorgaben

Die in Art. 12 VwVG statuierte Untersuchungsmaxime wird durch die Mitwirkungspflicht in Art. 13 VwVG ergänzt.[964] Es gibt verschiedene Fälle, in denen es opportun sein kann, dass Parteien zur Mitwirkung verpflichtet werden. Dies hat insbesondere dann zu gelten, wenn sie das Verfahren durch ihr eigenes 402

962 EICHENBERGER/PRIBNOW, HAVE, 2017, S. 282.

963 Vgl. etwa BGE 136 V 113, E. 5.4.

964 AUER/BINDER, VwVG-Kommentar, Art. 13, N. 1.

Begehren eingeleitet haben (Absatz 1) oder in einem Mehrparteienverfahren eigene Begehren stellen (Absatz 2).

403 Worin die konkrete Mitwirkungspflicht in einem Verwaltungsverfahren besteht, ist oft in den jeweiligen Spezialgesetzen umschrieben. So sieht etwa das Asylrecht weitreichende Mitwirkungspflichten für die Asylsuchenden vor. Sie müssen gemäss Art. 8 AsylG etwa ihre Identität offenlegen, Reisepapiere und Identitätsausweise abgeben sowie bei der Erhebung der biometrischen Daten mitwirken oder sich einer vom SEM angeordneten medizinischen Untersuchung unterziehen. Im Steuerrecht besteht eine der wichtigsten Mitwirkungspflichten darin, den Behörden die vollständige und richtige Veranlagung zu ermöglichen, wozu etwa das Einreichen der Steuererklärung gehört.[965] Fehlt eine konkrete Umschreibung im jeweiligen Spezialgesetz, so wird davon ausgegangen, dass die Parteien in erster Linie zur Auskunftserteilung und zur Aktenherausgabe verpflichtet sind.[966] Verweigert die Partei die Mitwirkung, so steht es der Behörde frei, auf das entsprechende Gesuch nicht einzutreten, wie dies etwa Art. 13 Abs. 2 VwVG statuiert. Es können jedoch auch andere Konsequenzen an die fehlende Mitwirkung geknüpft werden, etwa die Berücksichtigung der unterlassenen Mitwirkung zum Nachteil der Partei oder eine Beachtung im Rahmen der Kostenverteilung.[967]

404 Dabei führt Art. 13 VwVG nicht weiter aus, in welcher Form die Mitwirkung zu erfolgen hat, so dass davon ausgegangen werden kann, dass sie sich ebenfalls auf alle Arten der Sachverhaltserhebung und die in Art. 12 VwVG erwähnten Beweismittel erstreckt.[968] Durch die technologieneutrale Formulierung von Art. 12 VwVG stehen diese Beweismittel – wie weiter oben dargelegt wurde – der Ausnutzung technologischer Neuerungen grundsätzlich nicht entgegen.[969]

405 Als konkretes Beispiel angeführt werden kann hier eine aktuell hängige parlamentarische Initiative, gemäss welcher die Mitwirkungspflichten im Asylrecht (Art. 8 ff. AsylG) inskünftig auch das Recht der zuständigen Behörde umfassen soll, Mobiltelefone und Computer zu überprüfen, bzw. die Pflicht der Asylbewerbenden, die entsprechenden Geräte herauszugeben, wenn ihre Identität nicht auf anderem Wege festgestellt werden kann. Begründet wird dies damit, dass viele Flüchtlinge ohne Ausweispapiere in die Schweiz kommen, was die Identitätsfeststellung erschwert, aber oft Mobiltelefone besitzen,

965 Vgl. etwa Art. 126 DBG.

966 KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 13, N. 42.

967 KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 13, N. 80 ff.

968 AUER/BINDER, VwVG-Kommentar, Art. 13, N. 3.

969 Siehe oben Rz. 363.

über welche sich allenfalls Hinweise auf die Identität der Person oder ihre Fluchtroute gewinnen lassen.[970] Während sich die Initiative aktuell noch in parlamentarischer Beratung befindet, wurde diese Form der Mitwirkung im Rahmen von Pilotversuchen in Empfangs- und Verfahrenszentren bereits angewendet.[971] Da Art. 12 VwVG – wie weiter oben beschrieben – keine abschliessende Regelung über zulässige Beweismittel darstellt, würde diese Bestimmung der Verwendung von solcherart gewonnenen Erkenntnissen grundsätzlich nicht entgegenstehen.

406 Ihre Grenzen findet die Mitwirkungspflicht in erster Linie in Geheimhaltungspflichten (etwa durch das Anwaltsgeheimnis) und im Verhältnismässigkeitsprinzip. Eine dem Verfahrensbeteiligten auferlegte Mitwirkungspflicht muss daher einerseits zur Feststellung des Sachverhalts relevant, darf aber anderseits nicht mit unverhältnismässigem Aufwand verbunden sein. Weiter muss sie anhand der konkreten Umstände auch zumutbar sein. Zu denken ist dabei etwa daran, dass die betroffenen Personen in unverhältnismässiger Weise in ihren Grundrechten eingeschränkt werden. Keine Rolle betreffend die Zumutbarkeit spielt indes, ob sich die Ausübung der Mitwirkungspflicht für den Betroffenen positiv oder negativ auswirkt.[972] So ist es etwa als zulässig zu erachten, dass von einem Asylbewerbenden ein Nachweis über seine Identität (z.B. in der Form von Reisepapieren) erbracht werden muss, auch wenn dadurch ersichtlich werden könnte, dass er nicht aus dem Land stammt, aus welchem er behauptet zu kommen, oder dass er unter falschem Namen eingereist ist. Diese Pflicht findet aufgrund des strafrechtlichen Selbstbelastungsverbots dort ihre Grenze, wo die Person sich einer strafrechtlichen Verfolgung aussetzen könnte.[973]

B. Fazit

407 Die technologieneutrale Formulierung zulässiger Beweismittel spricht für die Zulässigkeit einer Nutzung technologischer Möglichkeiten im Rahmen der Mitwirkung. Grenzen gesetzt sind der Mitwirkungspflicht in erster Linie durch entgegenstehende Geheimhaltungspflichten und durch das Verhältnismässigkeitsprinzip. In diesem Zusammenhang ist zu beachten, dass Grundrechtspositionen der Betroffenen einer entsprechenden Mitwirkungspflicht gegenüberstehen können. Die Durchsuchung von Smartphones oder Computern

970 Vgl. Parlamentarische Initiative 17.423 Rutz.

971 Vgl. etwa SDA, Bund wertet Handy- und Laptopdaten von Flüchtlingen aus, Neue Zürcher Zeitung, 10. August 2019.

972 AUER/BINDER, VwVG-Kommentar, Art. 13, N. 8.

973 Für eine weitere Diskussion dieses Aspekts vgl. KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 13, N. 86 f.

von Flüchtlingen zur Identifizierung kann etwa durchaus die Gefahr schaffen, in deren Recht auf Privatsphäre und das Brief-, Post- und Fernmeldegeheimnis gemäss Art.13 Abs.1 BV und in ihre informationelle Selbstbestimmung nach Art.13 Abs.2 BV einzugreifen, da unter anderem private Daten über die betroffene Person bearbeitet werden. Da die betreffende Gesetzesrevision sich aktuell noch in parlamentarischer Beratung befindet, soll eine vertiefte Auseinandersetzung damit im nächsten Kapitel erfolgen.[974]

III. Amtshilfe

408 Eine Person hat unter Umständen nicht nur einmal mit derselben Behörde zu tun, oder diese muss allenfalls auf einen Entscheid zurückzukommen. Zudem kann es vorkommen, dass verschiedene Behörden dieselben Daten über eine Person benötigen. Eines der Ziele des E-Government ist es, Behördendienstleistungen für alle Beteiligten möglichst effizient gestalten zu können. Diesem Ziel würde es widersprechen, wenn eine Behörde die benötigten Daten bei jedem Verfahren von der betroffenen Person erneut erheben müsste. Aus diesem Grund führen die meisten Verwaltungsstellen Datenbanken oder Register, in denen sie Personendaten speichern. Die entsprechenden Daten wurden durch die Behörden bereits vor dem Zeitalter der Computer – etwa in einem Aktenschrank – abgelegt. Was sich durch den technologischen Fortschritt und die immer grösseren Speicherkapazitäten geändert hat, ist indes die Menge an verfügbaren Daten, welche nun platzsparend und fast unlimitiert abgespeichert werden können, sowie deren Abrufbarkeit und Durchsuchbarkeit.

409 Die gespeicherten Daten können auch für andere Behörden relevant sein. Sie können dabei auf verschiedene Weise von einer Behörde an eine andere weitergegeben werden. Entweder kann eine Behörde von sich aus einer anderen Amtsstelle melden, wenn ihr bei einer Person eine Tatsache auffällt, welche die andere Amtsstelle interessieren könnte (sog. Spontanmeldung). In gewissen Fällen besteht sogar eine entsprechende Meldepflicht. Anderseits kann eine Behörde von sich aus bei einer anderen Amtsstelle Daten abfragen, welche sie bei dieser vermutet. Dabei muss sie in der Regel wissen, dass die gesuchten Daten bei der anderen Behörde vorhanden sind.[975] Zudem muss sie begründen, weshalb sie die entsprechenden Informationen benötigt, da aufgrund der Zuständigkeitsordnung innerhalb der Verwaltung keine Behörde von sich aus ergründen muss, ob die Informationen, die sie besitzt, für

974 Vgl. zum Ganzen unten Rz. 585 ff.

975 Vgl. zum Ganzen mit Beispielen: BUCHLI/FRIEDRICH, S. 35.

andere Behörden relevant sind.[976] Ein entsprechendes Gesuch muss bei jedem Informationsbedürfnis erneut gestellt und begründet werden, was nicht sonderlich effizient ist. Einfacher ist es, wenn andere Behörden von sich aus auf die Daten zugreifen könnten, welche sie aus der jeweiligen Datenbank benötigen, also wenn etwa die Migrationsbehörde sämtliche Sozialhilfebezüger ohne Schweizer Pass abfragen und mit ihrer Datenbank vergleichen könnte, anstatt für jede Person ein entsprechendes Gesuch zu stellen. Das Aufkommen des Internets und die immer raffiniertere Programmierung entsprechender Datenbanken haben es technisch ermöglicht, dass Behörden von sich aus, falls sie dasselbe Programm oder zumindest eine kompatible Schnittstelle benutzen, eine unbestimmte Menge von Daten nach gewissen Parametern abfragen können (z.B. alle Männer zwischen 30 und 40). Solche «Abrufverfahren» ermöglichen die Bekanntgabe der Daten ganz ohne Intervention der bekanntgebenden Behörde.[977]

Die zweifellos effizienteste Möglichkeit der Datenbekanntgabe wäre es, 410
wenn jede Verwaltungsstelle automatisch Zugriff auf die Daten aller anderen Ämter hätte und die für den jeweiligen Fall relevanten Informationen im Sinne eines Abrufverfahrens jederzeit abrufen könnte. Dies wäre jedoch für den betroffenen Bürger mit verschiedenen Einschränkungen verbunden – er würde quasi zum «gläsernen Bürger» werden. Im Folgenden soll daher ausgeführt werden, welche Vorkehrungen die Schweizer Rechtsordnung getroffen hat, um dies zu verhindern. Da es den Behörden bereits vor der Ausstattung der Verwaltung mit Computern möglich war, Daten der betroffenen Personen untereinander preiszugeben, soll dabei ein besonderer Fokus auf diejenigen Arten der Datenbekanntgabe gelegt werden, welche durch die Digitalisierung begünstigt wurden und eine Bekanntgabe in grosser Zahl ermöglichen (z.B. Abrufverfahren).

A. Amtshilfe im Verwaltungsverfahren

Es ergibt Sinn, dass sich Verwaltungsstellen bei der Erfüllung ihrer Aufgaben 411
unterstützen und sich gegenseitig relevante Daten zukommen lassen können. Diese gegenseitige Unterstützung wird Amtshilfe genannt und kann als informationelle Amtshilfe auch die Bekanntgabe von Personen- oder Sachdaten umfassen.[978] Auf Verfassungsebene statuiert Art. 44 Abs. 2 BV, dass sich Bund und Kantone gegenseitig Amtshilfe leisten müssen.[979] Für das

976 BUCHLI/FRIEDRICH, S. 35. Eine Ausnahme davon besteht jedoch dort, wo Meldepflichten bestehen.

977 Vgl. zum Ganzen: WERMELINGER, ZBl, 2004, S. 187.

978 WERMELINGER, ZBl, 2004, S. 175.

979 SCHWEIZER, SG Komm. BV, Art. 44, N. 31.

erstinstanzliche Verfahren erwähnt das Verwaltungsverfahrensgesetz des Bundes die Möglichkeit der Amtshilfe nicht konkret. Es ist in der Lehre jedoch nicht umstritten, dass eine Behörde grundsätzlich die Auskünfte anderer Behörden in der Sachverhaltsermittlung beiziehen kann. Die Konkretisierung dieser Verpflichtung findet dabei in den jeweiligen Spezialgesetzen statt.[980] So befassen sich für das Ausländerrecht etwa Art. 97 und Art. 101 ff. AiG mit der Amtshilfe und Datenbekanntgabe. Die entsprechenden Artikel sehen vor, welche Behörden unter welchen Voraussetzungen Daten an andere Amtsstellen bekanntgeben müssen. In kantonalen Verfahrensgesetzen ist die Amtshilfe teilweise expliziter geregelt. So sieht etwa § 7 Abs. 3 VRG ZH vor, dass Verwaltungsbehörden und Gerichte verpflichtet sind, notwendige Akten herauszugeben, Amtsbericht zu erstatten und Auskünfte zu erteilen. Vorbehalten bleiben dabei indes gemäss dieser Bestimmung besondere Vorschriften über die Geheimhaltung und den Datenschutz.[981] Im Folgenden sollen daher die Grenzen der Amtshilfe genauer betrachtet werden. Da hinsichtlich des Vorliegens von Geheimhaltungsgründen (z.B. Amtsgeheimnis oder Anwaltsgeheimnis) durch die Digitalisierung keine Veränderungen zu erwarten sind, sollen vorliegend lediglich datenschutzrechtliche Aspekte untersucht werden.[982]

B. Datenschutz als Grenze der Amtshilfe

412 Im Rahmen der Amtshilfe werden oft Daten übermittelt, welche eine Person bestimmen oder zumindest bestimmbar machen. Die Bekanntgabe stellt daher immer auch einen Eingriff in das in Art. 13 Abs. 2 BV formulierte Recht auf informationelle Selbstbestimmung dar, gemäss welchem der Bürger Anspruch darauf hat, über die Verwendung seiner Personendaten mitzubestimmen. Daher ist auch bei der Amtshilfe die jeweils einschlägige Datenschutzgesetzgebung zu beachten. Relevant sind in diesem Zusammenhang Art. 17 und Art. 19 DSG, welche für die Bearbeitung und die Bekanntgabe von Personendaten eine gesetzliche Grundlage verlangen. Findet eine Bekanntgabe ins Ausland statt, sind zudem die Vorgaben von Art. 6 DSG zu beachten, welche an dieser Stelle allerdings auch nicht vertieft thematisiert werden sollen.

413 Es gilt zu beachten, dass verschiedene Ausgestaltungen der Amtshilfe (Spontanmeldungen, Meldepflichten und Einzelanfragen) bereits vor der Digitalisierung und dem Aufkommen von Informations- und Kommunikationstechnologien bestanden haben; daher wird auf sie nur kurz eingegangen.

980 KRAUSKOPF/EMMENEGGER/BABEY, PK VwVG, Art. 12, N. 179 ff.

981 PLÜSS, Komm. VRG ZH, Art. 7, N. 182 ff.

982 Indes sieht das Datenschutzrecht durchaus Regelungen zum Umgang mit Geheimhaltungspflichten vor; vgl. Art. 10a DSG oder Art. 19 Abs. 4 lit. b DSG, siehe dazu oben Rz. 77 und 98.

Beim Abrufverfahren handelt es sich dagegen um ein neueres Phänomen. Augenscheinlich ist, dass es zu einer Effizienzsteigerung führen und Redundanzen verringern kann, wenn ein informationssuchendes Organ seine Informationen zielgerichtet aus dem Datenbestand einer anderen staatlichen Stelle beschaffen kann.[983] Aus Sicht der betroffenen Personen besteht mit Blick auf die informationelle Selbstbestimmung ein höheres Risiko dadurch, dass die informationssuchende Behörde auf die Personendaten zugreifen kann, ohne dass die (passiv) bekanntgebende Behörde davon Kenntnis erlangen muss.[984] Insbesondere lässt sich auf diese Weise kaum mehr nachprüfen, ob die erhobenen Personendaten für die Behörde zur Erfüllung ihrer Aufgabe überhaupt erforderlich waren oder ob der zuständige Sachbearbeiter lediglich etwa aus Neugier die Daten seines Nachbars abgerufen hat. Im Vergleich zu den anderen Formen der Datenbekanntgabe handelt es sich beim Abrufverfahren somit zweifelsohne um einen schwereren Eingriff in die informationelle Selbstbestimmung, was insbesondere bei der Ausgestaltung der gesetzlichen Grundlage zu beachten ist.[985]

1. Vorgaben an die gesetzliche Grundlage

Die Datenbearbeitung und Datenbekanntgabe an eine andere Behörde be- 414
nötigen nach dem soeben Ausgeführten in erster Linie eine gesetzliche Grundlage. Diese Grundlage muss aufgrund des Legalitätsprinzips gewisse Voraussetzungen hinsichtlich der Bestimmtheit erfüllen. Damit die gesetzliche Grundlage als genügend erachtet werden kann, muss sie mindestens den Zweck, die beteiligten Bundesorgane sowie das Ausmass der Datenbearbeitung in den Grundzügen festlegen. Allerdings sind an eine solche gesetzliche Grundlage keine allzu hohen Anforderungen zu stellen, da die Datenbearbeitung durch die Bundesverwaltung sehr vielfältig ausfallen kann. Aufgrund der grossen Vielzahl an möglichen Datenbearbeitungen kann es dabei bereits genügen, wenn ein sachlicher Zusammenhang zwischen der Datenbearbeitung und den jeweiligen Aufgaben des Bundesorgans besteht. Der jeweils zu fordernde Grad der Bestimmtheit hängt von den Umständen des Einzelfalls und damit von verschiedenen Kriterien ab, so insbesondere der Schwere des Eingriffs in die Persönlichkeitsrechte, der Art der bearbeiteten Daten, dem Kreis der betroffenen Personen sowie der Komplexität der zu treffenden Entscheidung.[986] Dabei lässt sich aus der allgemeinen Zuständigkeit für die

983 WERMELINGER, ZBl, 2004, S. 187.

984 BOLLIGER/FÉRAUD, S. 100.

985 Vgl. etwa JÖHRI, Handkommentar DSG, Art. 19, N. 74 m.w.H.

986 Vgl. zum Ganzen: Botschaft DSG S. 467.

Bearbeitung von Personendaten im Sinne von Artikel 17 DSG nicht per se auf eine hinreichende gesetzliche Grundlage für die Datenbekanntgabe schliessen.[987] In der gesetzlichen Grundlage müssen daher die Behörde, die für die Bekanntgabe der Personendaten zuständig ist, die Kategorie der weitergegebenen Daten, die datenempfangende Behörde und der Zweck der Bekanntgabe geregelt sein oder sich zumindest daraus erkennen lassen.[988] Problematisch kann dabei sein, dass diese Rechtsgrundlagen in der Rechtsetzung der jeweiligen Bereiche nicht aufeinander abgestimmt sein müssen bzw. sich diesbezüglich Widersprüchlichkeiten ergeben.[989] So kann auf der Seite der um Daten ersuchenden Behörde die Bekanntgabe im Gesetz erlaubt sein, während die bekanntgebende Behörde durch eine Schweigepflicht gebunden ist.[990]

2. Datenschutzrechtliche Grundsätze

415 Bei der Bearbeitung und Bekanntgabe von Personendaten sind stets auch die Grundsätze der Datenbearbeitung zu beachten, wobei der Gesetzgeber bewusste Abweichungen von diesen vorsehen kann und die Grundsätze in diesen Fällen nur noch subsidiär zur Auslegung beigezogen werden müssen.[991] Aus dem Grundsatz der Verhältnismässigkeit und aus dem Grundsatz der Zweckbindung ergibt sich, dass Daten nur in dem Umfang bekanntgegeben werden sollen, in welchem sie auch zur Aufgabenerfüllung notwendig sind. Insbesondere dürfen keine Daten auf Vorrat bekanntgegeben werden.[992] Mit der Bekanntgabe der Daten geht dabei oft eine Änderung des Zwecks einher. Werden Daten plötzlich von einer anderen Behörde in einem anderen Zusammenhang gebraucht, so lässt sich dies schwerlich mit dem Zweckbindungsgebot vereinbaren. Eine absolute Zweckidentität würde dabei aber die Amtshilfe wohl weitgehend verhindern.[993] Die bundesgerichtliche Rechtsprechung betrachtet es daher als genügend, wenn der im Rahmen der Datenbekanntgabe verfolgte Zweck mit dem ursprünglichen Zweck der Datenbeschaffung vereinbar ist.[994] Wird die Weitergabe der Daten durch den ursprünglichen

987 Vgl. etwa JÖHRI, Handkommentar DSG, Art. 19, N. 9; EHRENSPERGER, BSK DSG/BGÖ, Art. 19 DSG, N. 14.

988 Bericht Lustenberger, S. 655.

989 BOLLIGER/FÉRAUD, S. 22.

990 Vgl. hierzu auch Art. 19 Abs. 4 DSG, Bericht Lustenberger, S. 656.

991 Siehe dazu oben Rz. 78.

992 Vgl. WERMELINGER, ZBl, 2004, S. 189.

993 Vgl. WERMELINGER, ZBl, 2004, S. 189, SCHWEGLER, S. 36 und 55.

994 Urteil des BGer 2A.424/2000 vom 13. Februar 2001, wo das Bundesgericht den Zweckbindungsgrundsatz nicht verletzt erachtete dadurch, dass Daten aus dem Asyl- im Ausländerrecht verwendet wurden, da beide die Frage der Anwesenheitsberechtigung von Ausländern in der Schweiz regeln.

Zweck nicht gedeckt, so muss eine neue gesetzliche Grundlage diese Weitergabe separat legitimieren.[995] In Einzelfällen denkbar ist bei einer Zweckänderung allenfalls noch die Anzeige an die betroffene Person, was indes beim heutigen Umfang an Datenbearbeitungen und Bekanntgaben keine praktikable Alternative mehr darstellen dürfte.[996]

Auch dem Aspekt der Datensicherheit gemäss Art. 7 DSG ist Beachtung zu schenken. Dementsprechend müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Abfragen im Einzelfall an eine andere Behörde sind in der Regel nicht an eine gewisse Form gebunden.[997] Den einfachsten Weg zur Übermittlung dieser Personendaten stellt in der Regel der E-Mail-Verkehr dar. Hierbei ist zu beachten, dass das Versenden normaler E-Mails als unsicher gilt, da diese von Unbefugten abgefangen und gelesen werden können.[998] Daher wird eine elektronische Übermittlung – insbesondere bei besonders schützenswerten Personendaten – kritisch betrachtet und nur dann als zulässig beurteilt, wenn die entsprechenden E-Mails zumindest mit einem elektronischen Schlüssel gesichert sind.[999] Inwiefern diese Anforderungen allerdings in der Praxis beachtet werden, sei hier dahingestellt.[1000] 416

3. Zusätzliche Anforderungen an Abrufverfahren

Wie bereits ausgeführt, stellen Abrufverfahren einen schwereren Eingriff in das Recht auf informationelle Selbstbestimmung dar als Datenbekanntgaben, welche einen konkreten Einzelfall betreffen. Auch aus diesem Grund fordern die Datenschutzgesetze hier in der Regel, dass zusätzliche Voraussetzungen erfüllt sind. Auf Stufe des Bundes ist ein Abrufverfahren gemäss Art. 19 Abs. 3 DSG nur dann zulässig, wenn es ausdrücklich vorgesehen ist. Wenn besondere Personendaten oder Persönlichkeitsprofile betroffen sind, dürfen diese nur zugänglich gemacht werden, wenn dies in einem Gesetz im formellen Sinne ausdrücklich erlaubt wird.[1001] Zu fordern ist zusätzlich, dass auch die Kategorien der erhobenen Personendaten und deren Verwendungszweck sowie die Personen, welche darauf Zugriff erhalten, umschrieben sind.[1002] 417

995 BOLLIGER/FÉRAUD, S. 22.

996 WERMELINGER, ZBl, 2004, S. 200.

997 BUCHLI/FRIEDRICH, S. 11.

998 Siehe bereits oben Rz. 329; statt vieler vgl. etwa UNABHÄNGIGES LANDESZENTRUM FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN, S. 37.

999 BUCHLI/FRIEDRICH, S. 12.

1000 Vgl. HÄNER, in: Jahrbuch 2017/2018, S. 28.

1001 Vgl. auf kantonaler Ebene etwa auch § 17 Abs. 1 lit. a IDG ZH, LS 170.4.

1002 Botschaft Rev. DSG 2003, S. 2142.

Gesetzesformulierungen, gemäss denen Personendaten öffentlich zugänglich gemacht oder zur Verfügung gestellt werden sollen, erfüllen die Anforderungen an die genügende Bestimmtheit richtigerweise nicht und können daher keine genügende Grundlage für ein Abrufverfahren darstellen.[1003]

418 Auch bei Abrufverfahren ist der Datensicherheit Rechnung zu tragen. Da hier – wie bereits ausgeführt – grundsätzlich ein Abruf von Daten auch möglich ist, ohne dass die zur Verfügung stellende Behörde dies aktiv erfährt, lässt sich grundsätzlich nicht beurteilen, ob die entsprechenden Daten wirklich benötigt werden oder ob ein Sachbearbeiter die jeweiligen Daten lediglich aus Neugier abruft. Aus diesem Grund ist es wichtig, dass zumindest intern die Zugriffsberechtigungen und die Verwendung der Datenbanken präzise geregelt sind und z.B. über ein Logbuch ersichtlich ist, wann und durch wen welche Zugriffe erfolgen, um der Gefahr von Missbrauch vorzubeugen.[1004] Bei der Schaffung neuer gesetzlicher Grundlagen zur Datenbekanntgabe kommt auch der demokratischen Legitimation eine besondere Bedeutung zu. Gerade in Ämterkonsultationen und Vernehmlassungsverfahren zu entsprechenden gesetzlichen Grundlagen spielt der Umfang der jeweiligen Regelungen eine wichtige Rolle. Es obliegt dem Gesetzgeber, die verschiedenen Interessen abzuwägen und dabei auch den Grundsätzen des Datenschutzes Beachtung zu schenken.

C. Fazit

419 Die zunehmende Datenmenge und die technischen Möglichkeiten sorgen dafür, dass Behörden bei der Erfüllung ihrer Aufgaben auf Datenbanken und Register zurückgreifen und auch Daten benutzen können, welche bei anderen Amtsstellen verfügbar sind. Da auf diese Weise auch Daten über Personen bearbeitet werden, ist deren Recht auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV betroffen. Die Rechtsordnung schränkt auch aus diesem Grund die Möglichkeiten der gegenseitigen Amtshilfe ein. Insbesondere verlangen Art. 17 und Art. 19 DSG das Vorliegen entsprechender Grundlagen zur Datenbekanntgabe, welche gewisse Voraussetzungen hinsichtlich ihrer Bestimmtheit erfüllen müssen. Auch die Grundsätze des Datenschutzgesetzes sind in diesem Zusammenhang zu beachten. Dieses Gesetzeserfordernis führte sowohl auf Bundes- als auch auf kantonaler Ebene zu zahlreichen Gesetzesbestimmungen, welche das Führen zusätzlicher Datenbanken oder neue Möglichkeiten der Bekanntgabe ermöglichen. Besteht eine gesetzliche Grundlage, so ist die Datenbearbeitung oder -bekanntgabe grundsätzlich

1003 MUND, SHK-DSG, Art. 19., N. 25.

1004 BOLLIGER/FÉRAUD, S. 101.

zulässig. Wichtig ist ebenfalls, dass die gesetzlichen Grundlagen durch die ausführenden Ämter konsequent beachtet werden. Die Gefahr besteht weiterhin, dass aufgrund der Vielzahl an sich teilweise überschneidenden Bestimmungen nicht klar ersichtlich ist, ob eine Bekanntgabe zulässig ist. Zudem erfolgt gerade in kleinen Gemeinwesen die Bekanntgabe von Daten inoffiziell auf dem «kleinen Dienstweg». Eine entsprechende Schulung der Behörden auf Aspekte des Datenschutzes ist daher unerlässlich, wenn dieser im Bereich der Datenbekanntgabe nicht ins Leere laufen soll.

Der Datenschutz verunmöglicht durch das Erfordernis einer hinreichenden gesetzlichen Grundlage auf jeden Fall eine Ordnung, in der jede Behörde Zugriff auf alle Informationen über jeden Bürger hat. Dies verhindert den «gläsernen Bürger». Vor allem im Bereich der Strafverfolgung oder der Sozialhilfe beurteilen gewisse Politiker den Datenschutz indes oft als Hinderungsgrund für eine effiziente Aufgabenerledigung und fordern möglichst weite bzw. extensiv zu handhabende gesetzliche Grundlagen.[1005] Es ist zu attestieren, dass der Datenschutz manchmal die effizienteste Lösung nicht zulässt. Jedoch ist mit Blick auf das Legalitätsprinzip und die Grundsätze des Datenschutzes eine gewisse Bestimmtheit der entsprechenden Grundlagen zu fordern. Auch darf der Gehalt von Art. 13 Abs. 2 BV nicht derart ausgehöhlt werden, dass der Kerngehalt der Privatsphäre verletzt wird. Letztlich gilt es an dieser Stelle festzuhalten, dass Effizienzüberlegungen nicht die ausschliessliche Rechtfertigung für ein bestimmtes Verhalten des Staats bilden dürfen.[1006] 420

IV. Zusammenfassung

Durch die technologieneutrale Formulierung der Beweismittel im Verwaltungsverfahren sind auch neue Arten oder Quellen von Beweismitteln zulässig, etwa die Recherche im Internet. Im Zusammenhang mit diesen neuen Möglichkeiten ergeben sich aber einige Fragen, zu welchen das Verwaltungsverfahrensgesetz bisher keine Lösungen vorsieht. Hier können die Grund- oder Verfahrensrechte zugunsten der Betroffenen einschränkend wirken. So ist etwa die Verwendung von Internetquellen in erster Linie durch den Anspruch auf rechtliches Gehör dergestalt eingeschränkt, dass nur gewisse Internetquellen als notorisches Wissen gelten und ohne Anhörung der Parteien einer Entscheidung zugrunde gelegt werden können. Das Bundesgericht erlaubt dagegen Recherchen über Personen auf ihren öffentlich einsehbaren 421

1005 Vgl. etwa die Geschäfte 19.5401 «Übertriebener Datenschutz bei Sozialhilfebezügern» oder 17.5344 «Deckmantel Datenschutz im Staatssekretariat für Migration» im Nationalrat.

1006 Vgl. zum Ganzen: WERMELINGER, ZBl, 2004, S. 205.

Social-Media-Auftritten, da diese keinen Eingriff in die Privatsphäre und das Recht auf informationelle Selbstbestimmung der Betroffenen darstellen. Diese Rechtsprechung ist kritisch zu hinterfragen. In jedem Fall kommt auch hier der Gehörsgewährung eine wichtige Rolle zu.

422 Durch Gesetze können neue Mitwirkungspflichten für die Betroffenen und neue Datenbearbeitungsgrundlagen für die Behörden geschaffen werden. Hierbei können Grundrechtspositionen und das Verhältnismässigkeitsprinzip begrenzend wirken. Hinsichtlich der Datenbekanntgabe von Behörden untereinander (im Sinne der Amtshilfe) steht der Datenschutz einer überbordenden Verknüpfung von Datenbeständen der Behörden entgegen. Neben den Vorgaben an eine genügende gesetzliche Grundlage sind dabei auch die Grundsätze des Datenschutzrechts zu beachten.

§6 Automatisierung in der Verwaltung

423 Wie bereits an verschiedenen Stellen erwähnt, ist die Menge der bei einer Behörde verfügbaren Daten im Laufe der letzten Jahre um ein Vielfaches angestiegen. In vielen Bereichen ist diese sogar so gross geworden, dass der Mensch nicht mehr den Überblick behalten oder allenfalls gar Zusammenhänge erkennen kann. Im selben Zeitraum ist allerdings auch die Computerhardware immer potenter geworden. Mittlerweile können Computer gewisse Berechnungen, für welche ein durchschnittlich begabter Mensch Minuten oder Stunden braucht, innerhalb weniger Sekunden oder Bruchteilen davon erledigen. Möglich gemacht wird diese Effizienz bei der Datenbearbeitung durch Algorithmen. Dabei handelt es sich im Rahmen dieser Arbeit – wie bereits an früherer Stelle definiert – um Regeln zur Lösung eines Problems, welche aus für den Einzelfall relevanten Daten (Input) anhand vordefinierter Regeln einen Output liefern.[1007] Die entsprechenden Regeln können dabei vorgängig in das System einprogrammiert (regelbasierte Systeme / Expertensysteme) oder durch das System aufgrund der Analyse geeigneter Trainingsdaten mithilfe von maschinellem Lernen mitentwickelt werden.[1008]

424 Auch in der öffentlichen Verwaltung ist dieses Potenzial nicht unentdeckt geblieben, so dass in vielen Bereichen in gewissem Ausmass Algorithmen eingesetzt werden. Die Verwendung von Algorithmen hat dabei für die Behörde und die Parteien den Vorteil, dass entsprechende Aufgaben effizienter

1007 Vgl. die ausführliche Definition weiter oben Rz. 38 ff.

1008 Vgl. dazu weiter oben Rz. 41; siehe etwa auch WISCHMEYER, in: Der Terrorist als Feind?, S. 189.

und schneller durchgeführt werden können.[1009] So kann z.B. vorgegeben werden, welche Begriffe ein Computer bei der Untersuchung einer grossen Menge an Dateien spezifisch suchen soll.[1010] Diese Methodik wird etwa im Kanton Zürich im Bereich der Verfolgung von Wirtschaftskriminalität angewendet.[1011] Auch ein Mitarbeiter der Verwaltung könnte diese Aufgabe wahrnehmen, würde aber etwa für die Durchsuchung von zehntausend Seiten wohl mehrere Monate benötigen, während der Computer dies wesentlich schneller erledigen kann. Auch komplexe Berechnungen kann der Computer mit höherer Geschwindigkeit und allenfalls auch präziser durchführen als ein Verwaltungsmitarbeitender. Darüber hinaus können computergestützte Systeme Datensätze nach Korrelationen untersuchen, welche einem Menschen unter Umständen gar nicht auffallen würden.[1012] Zudem wird davon ausgegangen, dass ein Algorithmus grundsätzlich weniger fehleranfällig ist und etwa keine Berechnungsfehler macht. Ein Algorithmus arbeitet zudem fokussiert und birgt nicht die Gefahr der zusätzlichen Aufnahme bzw. Wahrnehmung unnötiger Nebeninformationen.[1013] Einen weiteren Vorteil kann darstellen, dass der Algorithmus im Gegensatz zu einem Menschen anhand der vordefinierten Regeln immer gleich entscheidet und z.B. seine Tagesform oder seine persönlichen Neigungen keinen Einfluss auf den Entscheid haben.[1014]

I. Einsatzbereiche

Wie sich bereits aus den oben genannten Beispielen ergibt, sind vielfältige 425
Einsatzbereiche für Algorithmen in der öffentlichen Verwaltung denkbar. Diese beschränken sich dabei, wie sogleich aufgezeigt werden soll, nicht auf förmliche Verwaltungsverfahren, welche durch eine Verfügung abgeschlossen werden. Vielmehr kann ein Algorithmus auch die Wahrscheinlichkeit für den Eintritt eines Ereignisses berechnen und der zuständige Beamte gestützt darauf weitere Vorkehrungen treffen, welche auch tatsächliches Verwaltungshandeln darstellen können. So können etwa im Rahmen des sogenannten

1009 Vgl. etwa WEBER/HENSELER, EuZ, 2020, S. 29; MARTINI, Blackbox, S. 17.

1010 Dies geschieht vor allem durch sogenanntes «text mining», worunter die Durchsuchung grosser Mengen an unstrukturierten Daten nach gewissen Kriterien mithilfe von Computerunterstützung zu verstehen ist; vgl. ALTWICKER, Chinese Journal of International Law, 2019, S. 227.

1011 Vgl. etwa SRF, News-Beitrag vom 3.8.2019.

1012 WISCHMEYER, in: Der Terrorist als Feind?, S. 192 f.

1013 Vgl. etwa SCHERER, Harvard Journal of Law & Technology, 2016, S. 363; WEBER/HENSELER, EuZ, 2020, S. 29.

1014 MARTINI, Blackbox, S. 47.

«predictive policing» Vorhersagen über die Wahrscheinlichkeit von Delikten getroffen werden und kann die Polizei gestützt auf diese Prognosen ihren Einsatzplan anpassen oder Personen vorladen.[1015] Diese die Handlungsformen übergreifende Stellung rechtfertigt es, das Phänomen der Automatisierung in der Verwaltung als eigenständiges Kapitel zu behandeln.

A. «Predictive policing»

426 Die genannten Vorteile von Algorithmen führen immer öfter auch dazu, dass etwa aufgrund von fortgeschrittenen mathematisch-statistischen Prognosemodellen Vorhersagen für zukünftiges Verhalten oder zukünftige Ereignisse ermittelt werden und aufgrund dieser Erkenntnisse Rückschlüsse getroffen werden können und Einsatzplanungen oder Handlungen erfolgen sollen. Ein wichtiger Bereich, in dem Algorithmen als Entscheidungshilfe oder Prognoseinstrument eingesetzt werden, ist die präventive Polizeiarbeit, das sog. «predictive policing».[1016] Vorteile von «predictive policing» werden insbesondere in seiner Steuerbarkeit gesehen: Durch die vorgängige Definition von relevanten Faktoren soll die Wahrnehmung der Beamten auf diejenigen Dinge beschränkt werden, welche sie wahrnehmen sollten. Aspekte, welche für die Entscheidung keine Rolle spielen sollten, werden dadurch von den Entscheidenden gar nicht wahrgenommen und von der Maschine gelöscht. Auf diese Weise kann «predictive policing» zumindest unter diesem Aspekt für den Betroffenen grundrechtsschonender ausgestaltet sein.[1017]

427 Zu unterscheiden ist hier zwischen raum- und personenbezogenem «predictive policing». Beim raumbezogenen «predictive policing» geht es darum, dass aufgrund bestehender Daten vorausgesagt werden soll, wo es zu weiteren Straftaten kommen kann, und gestützt darauf allenfalls proaktiv zu handeln.[1018] In der Schweiz setzen einige Kantone das System «Precobs» (Pre Crime Observation System) im Kampf gegen Einbruchsdiebstähle ein.[1019] Im System werden entsprechende Delikte an ihrem Tatort eingetragen, da aufgrund der kriminalistischen «Near repeat»-Theorie davon ausgegangen wird, dass Einbrecherbanden innert kurzer Zeit an einem nahen Ort noch einmal

1015 Zum «predictive policing» vgl. sogleich.

1016 Vgl. RADEMACHER, AöR, 2017, S. 368, welcher «predictive policing» als Anwendungsfall von «predictive analytics» einordnet.Für eine Definition von prädiktiver Analytik vgl. DREYER, in: Big Data – Regulative Herausforderungen, S. 135.

1017 RADEMACHER, AöR, 2017, S. 399 ff.

1018 BRAUN BINDER, SJZ, 2019, S. 470.

1019 Für eine aktuelle Übersicht der Kantone, welche die Software einsetzen, vgl. die Website des Instituts für musterbasierte Prognosetechnik.

zuschlagen, wenn sie erfolgreich waren.[1020] Die Polizei kann dann z.B. durch zusätzliche Patrouillen reagieren. Das in der Schweiz eingesetzte System beschränkt sich aktuell auf Einbruchdiebstähle, während es in anderen Ländern weitere Delikte umfassen kann und teilweise auch künstliche Intelligenz zur Mustererkennung eingesetzt wird.[1021]

Die personenbezogene, vorausschauende Polizeiarbeit befasst sich hingegen etwa mit der Frage, ob bei einer bestimmten Person das Risiko besteht, dass sie (wieder) ein Delikt begeht oder gefährdet ist, sich zu radikalisieren. Dazu werden gewisse Daten über diese Person (z.B. anhand eines Fragebogens) erhoben und wird aufgrund von wissenschaftlichen Theorien oder bisher erhobenen Daten ausgewertet, ob von dieser Person ein entsprechendes Risikopotenzial ausgeht. Ein solches System ist etwa die «Strategic Subject List» des Polizeidepartements Chicago, welche aufgrund der sozialen Kontakte das Risiko errechnen soll, dass eine Person in Bandenkriminalität involviert ist, woraufhin die zuständige Behörde diese Person z.B. unter Beobachtung stellen oder zu einem Gespräch einladen kann.[1022] In der Schweiz wird personenbezogenes «predictive policing» bisher erst ansatzweise eingesetzt. So nutzen gewisse Polizeibehörden etwa das System DyRias (Dynamische Risiko Analyse Systeme), um das Risiko zu ermitteln, dass eine Person häusliche Gewalt ausübt oder sich radikalisiert, um daraufhin allenfalls präventive Massnahmen zu ergreifen.[1023] Die Auswertung geschieht dabei soweit ersichtlich ohne maschinelles Lernverfahren, sondern lediglich gestützt auf das Ausfüllen eines Fragebogens, welcher die Antworten anhand bisheriger Erkenntnisse gewichtet und eine Risikoanalyse ausweist.[1024] In eine ähnliche Richtung geht die Möglichkeit, die Rückfallgefahr von verurteilten Straftätern anhand von verschiedenen Merkmalen zu ermitteln und darauf basierend etwa den Vollzug zu lockern. In der Schweiz kommt im Rahmen des «Risikoorientierten Sanktionenvollzugs» (ROS) hierbei ein (eher rudimentäres) Fall-Screening-Tool zum Einsatz, an dem ebenfalls anhand von gewissen gewichteten Merkmalen (Schwere des Delikts, Vorstrafen etc.) der Straftäter in eine der drei Risikokategorien eingeteilt wird, welche als Grundlage für den Entscheid über weitere Massnahmen dienen.[1025] Ein entsprechendes System könnte auch viel umfassender ausgestaltet werden, wie die USA zeigen, wo 428

1020 LEESE, in: Bulletin 2018 zur schweizerischen Sicherheitspolitik, S. 61 m.w.H.

1021 BRAUN BINDER, SJZ, 2019, S. 470.

1022 LEESE, in: Bulletin 2018 zur schweizerischen Sicherheitspolitik, S. 58 f.

1023 Vgl. etwa HARASGAMA, S. 22.

1024 BRAUN BINDER, SJZ, 2019, S. 470; vgl. auch die Internetsite des Anbieters.

1025 TREUTHARDT/LOEWE-BAUR/KRÖGER, SZK, 2018, S. 24 ff.

eine KI-basierte Beurteilungssoftware (COMPAS – Correctional Offender Management Profiling for Alternative Sanctions) aufgrund von 137 Merkmalen die Rückfallwahrscheinlichkeit eines Straftäters errechnet.[1026]

B. Weitere Einsatzbereiche

429 Auch ausserhalb der vorausschauenden Polizeiarbeit sind Bereiche, in denen Algorithmen durch Behörden in ähnlicher Weise eingesetzt werden, durchaus denkbar. Während entsprechende Einsatzmöglichkeiten bisher in der Schweiz aktuell noch selten genutzt werden, sollen im Folgenden vorausschauend dennoch einige (im Rahmen von Pilotprojekten oder im nahen Ausland genutzte) Beispiele vorgestellt werden. So lässt etwa das Staatssekretariat für Migration in einem Pilotprojekt tausend Asylbewerbende von einem Algorithmus auf den Kanton zuteilen, in welchem ihnen die besten Chancen auf eine Arbeitsstelle errechnet wurden.[1027] Dazu haben Forschende der ETH Zürich und der Stanford University durch ein maschinelles Lernverfahren basierend auf Daten der vergangenen Jahre berechnen lassen, welche Kriterien die Arbeitssuche in einem Kanton begünstigen. Gestützt auf diese Schlussfolgerungen werden die Asylbewerbenden auf die Kantone verteilt.[1028] Im Rahmen des Pilotprojekts konnten dabei durchaus relevante Verbesserungen beobachtet werden.[1029]

430 In Österreich wird ein Algorithmus getestet, welcher bei Arbeitslosen aufgrund der Daten vergangener Jahre errechnen soll, welche Chancen sie auf eine Wiedereingliederung in den Arbeitsmarkt haben. Die Personen werden dabei in drei Gruppen eingeteilt, wobei Personen mit hohen oder geringen Integrationschancen weniger Unterstützung bei der Arbeitssuche erhalten sollen als Personen der mittleren Gruppe, bei welchen man sich den grössten Erfolg von Förderungsmassnahmen verspricht.[1030] In den Niederlanden werden Daten über Personen aus verschiedenen Datenbanken im Rahmen der System Risk Indication (SyRI) miteinander verknüpft und automatisch anhand eines Risikomodels untersucht, um damit Personen zu finden, bei denen ein Risiko auf Sozialbetrug besteht. Dieses System wird ausschliesslich in

1026 Vgl. die Projektwebsite von Equivant.

1027 SRF, News-Beitrag vom 10. Mai 2018.

1028 BANSAK/FERWERDA/HAINMUELLER/DILLON/HANGARTNER/LAWRENCE/WEINSTEIN, Science, 2018, S. 328 ff.

1029 BANSAK/FERWERDA/HAINMUELLER/DILLON/HANGARTNER/LAWRENCE/WEINSTEIN, Science, 2018, S. 329 f., wobei die Autoren darauf verweisen, dass der Algorithmus nicht prospektiv im Rahmen eines kontrollierten «trial design» getestet werden konnte.

1030 Vgl. für einen Projektbeschrieb: HOLL/KERNBEISS/WAGNER-PINTER.

ärmeren Gegenden des Landes eingesetzt.[1031] Ebenfalls denkbar ist ein Einsatz von unterstützender «künstlicher Intelligenz» etwa im Bereich der Sprachanalyse bei Flüchtlingen[1032] oder bei der Gesichtserkennung über Video.[1033]

C. Fazit

Wie sich aus dem soeben Geschriebenen erkennen lässt, gibt es durchaus Anwendungsbereiche von Algorithmen in der Verwaltung, von der effizienten Durchsuchung von Dokumenten oder Berechnung von Ansprüchen über komplexe Berechnungen anhand statistischer Verfahren zur Prognostizierung zukünftiger Sachverhalte. Gerade in komplexeren Bereichen, wie etwa im «predictive policing», besteht die Erwartung, dass Algorithmen Zusammenhänge erkennen können, welche sich dem Menschen nicht oder nur mit einem grossen Mehraufwand offenbaren. Die bisher beschriebenen Einsatzbereiche haben gemeinsam, dass die betreffenden Algorithmen von den jeweils für die Entscheidung Verantwortlichen – gegebenenfalls zusammen mit anderen Faktoren – als Grundlage für ihre Entscheidung genommen werden, um allenfalls gestützt darauf weitere Massnahmen zu ergreifen. Die Algorithmen dienen somit lediglich der Entscheidungsunterstützung. Die Entscheidung verbleibt beim Menschen.[1034] Wie einleitend ausgeführt, ist es technisch bereits machbar, dass Algorithmen Entscheidungen auch gänzlich autonom vornehmen können. Verfahren, welche komplett ohne menschlichen Einfluss ablaufen – sogenanntes «Automated Decision Making» –, sind in der Schweiz noch kaum ersichtlich. Eine vorausschauende Auseinandersetzung mit diesem Thema soll daher weiter unten erfolgen.[1035] 431

II. Generelle Zulässigkeit

Den bereits genannten Vorteilen von Algorithmen stehen auch Risiken gegenüber. Es gilt daher im Folgenden zu betrachten, inwiefern der Einsatz von Algorithmen als Entscheidungsunterstützung in der Verwaltung grundsätzlich zulässig ist und inwiefern die schweizerische Rechtsordnung bereits Antworten auf die damit verbundenen Rechtsfragen gefunden hat. Geht es beim 432

1031 Vgl. den Bericht des UN-Sonderberichterstatters für extreme Armut anlässlich eines Gerichtsfalls vor einem niederländischen Gericht, ALSTON, S. 3 ff.

1032 Vgl. BRAUN BINDER, SJZ, 2019, S. 471.

1033 Vgl. etwa MATTER, digma, 2019, S. 14 ff.

1034 Zumindest de iure, de facto kann die Vorgabe des Algorithmus unter Umständen dennoch wesentlichen Einfluss auf den menschlichen Entscheid haben, siehe dazu Rz. 465 ff.

1035 Vgl. weiter unten Rz. 607.

Einsatz von Algorithmen nur darum, eine bestimmte Anzahl von Dokumenten zu durchsuchen oder die Berechnung eines Anspruchs vorzunehmen, so machen diese im Grunde genommen dasselbe wie ein Verwaltungsangestellter, nämlich anhand von gewissen vorgegebenen Daten und Regeln die Inputdaten auszuwerten.[1036] Während die Polizeibeamten ihre Erfahrungen mit den Informationen zum konkreten Sachverhalt abgleichen und gestützt auf die damit erstellte Gefahrenprognose weitere Vorkehrungen treffen, wird beim Einsatz von Algorithmen basierend auf Erfahrungen ebenfalls ein Gefahrenmuster definiert und eine zu untersuchende Datenmenge definiert, woraus ein Wahrscheinlichkeitsurteil (score) über bevorstehende Schadensereignisse errechnet wird. Gestützt auf diese Prognose entscheiden die Beamten über das weitere Vorgehen.[1037] Ihr Einsatz ist damit für die betroffenen Privaten nicht per se mit einer zusätzlichen Gefahr hinsichtlich ihrer rechtlichen Position verbunden, und grundsätzlich profitieren auch sie davon, wenn Entscheide effizienter, schneller und fehlerloser gefällt werden können.

433 Das Verwaltungsverfahrensgesetz sieht keine Regelung darüber vor, auf welche Weise eine Behörde eine gewisse Aufgabe zu erledigen hat und welcher Hilfsmittel sie sich dabei bedienen darf. Nach dem soeben Geschriebenen ist davon auszugehen, dass der Einsatz von Algorithmen grundsätzlich durch die jeweilige gesetzliche Grundlage zur Erfüllung einer Aufgabe ebenfalls gedeckt ist. Besteht eine gesetzliche Grundlage für die jeweilige Tätigkeit der Behörde, so ist grundsätzlich nicht relevant, welche Mittel sie zu diesem Zweck einsetzt. Es würde etwa niemandem in den Sinn kommen, dass die Benutzung eines einfachen Taschenrechners für die Berechnung eines finanziellen Anspruchs gesetzlich geregelt werden muss, wenn die Behörde die Entscheidung über diesen Anspruch rechtmässig treffen kann.

434 Je nach Anwendungsbereich kann indes eine Vielzahl an Grundrechtspositionen betroffen sein. So kann etwa durch eine KI-basierte Gesichtserkennung ein Eingriff in die Versammlungsfreiheit stattfinden, indem Personen sich aufgrund der Identifizierungsgefahr nicht mehr trauen, sich zu versammeln.[1038] Eine erschöpfende Behandlung aller möglichen Konstellationen und betroffenen Grundrechte würde den Rahmen dieser Arbeit sprengen. Stattdessen soll sich diese auf Bereiche beschränken, in denen übergreifende Probleme ausgemacht wurden. Dies kann sich insbesondere dort ergeben, wo der entsprechenden Entscheidung Personendaten zugrunde gelegt werden. Ebenfalls noch genauer zu betrachten sein wird die Tatsache, dass trotz

1036 Vgl. SINGLENSTEIN, NStz, 2018, S. 2 betreffend «Predictive Policing».

1037 Für eine detailliertere Gegenüberstellung vgl. RADEMACHER, AöR, 2017 S. 373 ff.

1038 Vgl. MATTER, digma, 2019, S. 17.

der Verwendung von Algorithmen, welche mit dem Versprechen antreten, dass dadurch eine fehlerfreiere Erledigung von Aufgaben möglich ist, weiterhin Fehler geschehen können. Diese können einerseits auf der Eingabe falscher Daten beruhen («garbage in – garbage out»).[1039] Bei menschlichen Entscheidenden können z.B. Vorurteile bewusst oder unbewusst dazu führen, dass gewisse Personen oder Gruppen systematisch gegenüber anderen schlechter gestellt werden. Diese Gefahr besteht auch bei der Berechnung durch Algorithmen, wobei sich hier die Diskriminierung einerseits aus den Daten oder deren Gewichtung ergeben kann oder anderseits eine Schlechterstellung auch gerade durch die Auswertung grosser Mengen an Daten überhaupt erst ersichtlich werden kann.

III. Informationelle Selbstbestimmung

Um sinnvoll funktionieren zu können, brauchen Algorithmen oft spezifische 435
Daten über die Personen, über deren Ansprüche sie zu entscheiden haben. Es liegt auf der Hand, dass etwa der Anspruch auf Sozialhilfeleistung oder die Rückfallwahrscheinlichkeit einer Person auch durch einen Algorithmus nur sinnvoll berechnet werden kann, wenn gewisse Angaben über diese bekannt sind. Wie überall, wo Personendaten bearbeitet werden, sind daher das Recht auf informationelle Selbstbestimmung und die Datenschutzgesetzgebung zu beachten. Die entsprechenden Personendaten können dabei auf zwei verschiedenen Ebenen relevant sein. Einerseits benötigt der Algorithmus gewisse Daten für die Prognose oder die Berechnung selbst, sprich als Input. Vor allem im Bereich der prädiktiven Analytik können jedoch auch intelligente Systeme eingesetzt werden, welche durch maschinelles Lernen die Regeln selbständig entwickeln können, nach denen der Input verarbeitet werden soll. Für diesen Prozess benötigt das System daher anderseits «Trainingsdaten», etwa Daten zur Straffälligkeit oder Rückfallgefahr aus den vergangenen Jahren, um diese zu analysieren und z.B. herauszufinden, welche Indikatoren ein gewisses Resultat massgeblich beeinflussen.[1040] Diese zwei Ebenen sollen im Folgenden separat betrachtet werden.

A. Input

Werden Personendaten bearbeitet, so ist einerseits Art. 17 DSG zu beachten, 436
gemäss dem jede Datenbearbeitung durch ein Bundesorgan eine gesetzliche Grundlage benötigt. Wie bereits ausgeführt, sind an diese gesetzliche Grundlage

1039 GLATTHAAR, SZW, 2020, S. 45.

1040 KNOBLOCH, S. 22; vgl. BRAUN BINDER, SJZ, 2019, S. 473.

hinsichtlich der Bearbeitung keine allzu grossen Anforderungen zu stellen, d.h., es reicht in der Regel aus, wenn eine Informationsbearbeitung im sachlichen Zusammenhang mit der Aufgabe des betreffenden Bundesorgans steht.[1041] Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen gemäss Art. 17 Abs. 2 DSG nur bearbeitet werden, wenn ein Gesetz im formellen Sinn dies vorsieht. Für kantonale Behörden sind diese Voraussetzungen in der Regel analog ausgestaltet.[1042]

437 Zu beachten ist hier, dass die entsprechende Datenbearbeitung oftmals bereits vorgängig zur Verwendung durch Algorithmen durch die jeweilige Behörde vorgenommen wurde. So ist etwa vorausschauende Polizeiarbeit nicht grundsätzlich ein neues Phänomen. Die Polizei besass und bearbeitete die entsprechenden Daten oft bereits vor dem Einsatz entsprechender Algorithmen. Die Regelungen zu den Datenbearbeitungen im Rahmen der vorausschauenden Polizeiarbeit sind daher etwa in den entsprechenden Polizeigesetzen zu suchen.[1043] Dass die Daten nun nicht mehr von einem Polizeimitarbeitenden, sondern von einer Maschine bearbeitet werden, führt nicht zu anderen Voraussetzungen an die gesetzliche Grundlage, zumal das aktuelle Datenschutzrecht die Anforderungen an die Bestimmtheit in erster Linie nach der Sensibilität der jeweiligen Personendaten ausrichtet.[1044]

438 In diesem Zusammenhang ist auf eine Unzulänglichkeit dieser Kategorisierung hinzuweisen, welche in der Lehre an verschiedener Stelle kritisiert wurde. Hierbei wird vertreten, dass nicht nur das Datum allein, sondern auch dessen Verwendung eine besondere Gefahr für die Persönlichkeitsrechte ausmachen kann. Als Beispiel wird oft genannt, dass die Bekanntgabe einer Adresse grundsätzlich kein besonderes Gefahrenpotenzial begründet, jedoch eine Gefährdung begründen kann, wenn sie in die Hände des gewalttätigen Ex-Manns einer Person gerät.[1045] Der Gesetzgeber hat diese Unzulänglichkeit erkannt und sieht de lege ferenda in Art. 30 Abs. 2 lit. c. E-DSG vor, dass sich auch aus der Art und Weise der Datenbearbeitung ein schwerwiegender Eingriff in die Grundrechte der betroffenen Person ergeben kann, welcher eine formell-gesetzliche Grundlage benötigt. Hierbei werden automatisierte Einzelentscheide explizit als Beispiel genannt, wobei auch betont wird, dass nicht

1041 Botschaft DSG, S. 467.

1042 Oft ist gar bereits von Gesetzes wegen vorgesehen, dass es ausreicht, wenn die Bearbeitung zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist; vgl. etwa Art. 9 IDG BL.

1043 Vgl. etwa das Polizeigesetz des Kantons Zürich, welches in Art. 52 PolG ZH die Datenbearbeitung durch die Polizei zur Erfüllung ihrer Aufgaben regelt, zu denen gemäss Art. 3 PolG ZH auch die Prävention gehört.

1044 Botschaft DSG, S. 467; MUND, SHK-DSG, Art. 17, N. 6.

1045 Vgl. etwa RUDIN, SHK-DSG, Art. 3, N. 20 f.

jede automatisierte Einzelfallentscheidung ein schwerwiegendes Risiko darstellen muss.[1046] Aufgrund des Ausgeführten hat dies auch dann zu gelten, wenn ein Entscheid lediglich durch eine Maschine vorbereitet wird, so dass auch hier unter Umständen höhere Anforderungen an die gesetzliche Grundlage zu stellen sind.

439 Relevant sind indes in diesem Zusammenhang immer auch die Grundsätze der Datenbearbeitung, insbesondere der Grundsatz der Zweckbindung (Art. 4 Abs. 3 DSG). Die Daten dürfen nur zu demjenigen Zweck bearbeitet werden, zu welchem sie auch erhoben wurden. Auf diese Weise soll verhindert werden, dass bestehende Daten- oder Datenbanken ohne Weiteres – also ohne Gesetzesanpassung – miteinander verknüpft werden können.[1047]

B. Regeln

440 Wie bereits ausgeführt, werden die Regeln, nach welchen sich der Algorithmus zu richten hat, entweder im Vornherein durch die Programmierer definiert (z.B. gestützt auf wissenschaftliche Theorien wie die «Near repeat»-Theorie bei «Precobs»), oder der Algorithmus wird mit Daten gefüttert, aus welchen er durch maschinelles Lernen herausfindet, welche Parameter einen Einfluss auf die entsprechende Entscheidung haben. Die daraus gewonnene Erkenntnis wird auf die eingegebenen Daten (den Input) angewendet. Auch wenn die meisten der hierzulande verwendeten Systeme (noch) keine maschinellen Lernverfahren verwenden[1048], kamen diese etwa beim ebenfalls genannten Algorithmus, welcher die Asylbewerber nach ihren Berufschancen auf die Kantone verteilt, zumindest versuchsweise bereits zum Einsatz.[1049] Daher soll hier kurz auch auf diese Thematik eingegangen werden.

441 Um die entsprechenden Schlüsse ziehen zu können, brauchen die intelligenten Systeme eine Vielzahl von Trainingsdaten, welche als Referenz für künftige Unterscheidungen dienen sollen.[1050] Um etwa herauszufinden, ob eine Person rückfällig wird, muss der Algorithmus aus den Daten auslesen können, wie viele Personen mit den gleichen Voraussetzungen (z.B. gleiche Straftat, gleiches Alter) ebenfalls rückfällig wurden. Für die Verwendung als Trainingsdaten spielt indes die Person «hinter dem jeweiligen Datum» in der Regel für den Algorithmus keine Rolle mehr, so dass die entsprechenden Daten

1046 Botschaft Rev. DSG 2017, S. 7080.

1047 BRAUN BINDER, SJZ, 2019, S. 475.

1048 Siehe dazu bereits oben Rz. 428.

1049 BANSAK/FERWERDA/HAINMUELLER/DILLON/HANGARTNER/LAWRENCE/WEINSTEIN, Science, 2018, S. 325 ff.

1050 BRAUN BINDER, SJZ, 2019, S. 473.

anonymisiert (also ohne Personenbezug) verwendet werden können. Wie bereits an anderer Stelle ausgeführt kommt das Datenschutzrecht nur dann zur Anwendung, wenn es sich bei den erhobenen Daten um Personendaten i.S. von Art. 3 DSG handelt. Werden Personendaten anonymisiert, so wird deren Personenbezug irreversibel aufgehoben, womit keine Rückschlüsse auf die betroffene Person mehr möglich sind, ohne dass dafür ein unverhältnismässiger Aufwand betrieben werden müsste. Sofern die Daten vor der Verwendung vollständig anonymisiert werden, stellen sie keine Personendaten im Sinne der Datenschutzgesetzgebung mehr dar und können ohne Beachtung von deren Vorgaben verwendet werden.[1051]

442 Findet keine Anonymisierung der verwendeten Daten statt, so sind die Vorgaben des Datenschutzrechts zu beachten, insbesondere das Erfordernis einer gesetzlichen Grundlage und der in Art. 4 Abs. 3 DSG verankerte Zweckbindungsgrundsatz, nach welchem Personendaten nur für den Zweck bearbeitet werden, welcher bei der Beschaffung angegeben wurde oder aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Bestehende Datenbestände, dürfen daher nicht ohne Weiteres miteinander verknüpft werden.[1052] Auch wenn die Polizei Daten eines Straftäters rechtmässig zur Berechnung von dessen Rückfallwahrscheinlichkeit benutzen kann, bedeutet dies nicht, dass sie dieselben Daten nichtanonymisiert auch als Trainingsdaten benutzen darf.

C. Fazit

443 Die bestehenden datenschutzrechtlichen Bestimmungen schränken die Verwendung von Daten für Algorithmen und insbesondere für Vorhersagen im Bereich der polizeilichen Präventionsarbeit grundsätzlich wirksam ein, indem für die Datenbearbeitung eine gesetzliche Grundlage gefordert wird und der Zweckbindungsgrundsatz beachtet werden muss. Dennoch lauern auch Gefahren. Je mehr Daten über eine Person erfasst werden, desto genauer wird potenziell das Ergebnis der Voraussage. Jedoch findet damit auch ein schwererer Eingriff in die informationelle Selbstbestimmung der betroffenen Person statt. Der Gesetzgeber hat diesen Überlegungen Rechnung zu tragen, sofern weitere Datenkategorien für die Verwendung durch Algorithmen – etwa im Hinblick auf die präventive Polizeiarbeit – erhoben werden sollen. Erstellt der Algorithmus die Regeln, denen er folgt, im Rahmen von

1051 HÄRTEL, LKV, 2019, S. 55, s. weiter oben Rz. 181.

1052 BRAUN BINDER, SJZ, 2019, S. 475, vgl. dazu etwa auch das Gesetz über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG), welches in § 4 Abs. 4 explizit eine weitergehende Nutzung von Fluggastdaten für die Erstellung und den Abgleich von Mustern vorsieht, und die Auseinandersetzung mit dieser Bestimmung bei RADEMACHER, AöR, 2017, S. 410 ff.

maschinellen Lernverfahren selbst, so muss zudem auf eine grosse Menge an Daten als Trainingsdaten zurückgegriffen werden. Hierbei ist darauf zu achten, dass diese Daten lediglich anonymisiert verwendet werden und sich daraus auch kein Personenbezug mehr herstellen lässt. Findet keine Anonymisierung statt, so ist die Verwendung der Daten zu Trainingszwecken ohne eigene gesetzliche Grundlage aufgrund des Zweckbindungsgrundsatzes nicht gestattet.

IV. Fehler durch Algorithmen

Eine wichtige Versprechung, welche mit dem Einsatz von Algorithmen als Entscheidungshilfe im Verwaltungsverfahren einhergeht, besagt, dass diese aufgrund ihrer Programmierung weniger fehlerhaft und objektiver sind. Es sind indes bereits mehrere Fälle in den Medien publik geworden, in denen Algorithmen ungewünschte oder falsche Resultate lieferten. Im Rahmen einer Studie ergab sich etwa, dass über zwei Drittel der begutachteten Personen, denen die Software «DyRias» ein hohes Gewaltrisiko attestierte, im Untersuchungszeitraum keine weiteren schweren Gewalttaten begingen.[1053] Dies kann rechtlich relevant sein, da die Polizei aufgrund einer entsprechenden Einordnung durch den Algorithmus zum Schluss kommen kann, dass für die entsprechende Person weitere Massnahmen (etwa eine Vorladung zu einem Gespräch oder gar eine weitere Beobachtung der Person) notwendig werden, und diese auch ergreift. 444

Es ist klar, dass auch Menschen Fehler machen können, wenn sie mit den entsprechenden Entscheidungen konfrontiert werden. Zudem lösen – wie bereits ausgeführt – zumindest in der Schweiz die meisten Algorithmen die entsprechenden Aufgabestellungen nach denselben Regeln wie ein Verwaltungsangestellter (z.B. kriminologischen Erkenntnissen). Darum müsste man betreffend die Fehlertoleranz von Algorithmen mit gleichen Ellen messen. Zumindest darf der Umstand, dass auch ein Algorithmus Fehler machen bzw. zu unzutreffenden Folgerungen verleiten kann, nicht bereits dazu führen, dass diese Technologie nicht eingesetzt werden darf. Dennoch ist an dieser Stelle zu betrachten, wie sich Fehler durch Algorithmen auswirken können und ob die in der Schweizer Rechtsordnung vorgesehenen Korrektive ausreichen, um den zusätzlichen Gefahren zu begegnen. 445

1053 Vgl. dazu etwa: FREI, in: Bedrohungsmanagement in der Schweiz; GERTH/ROSSEGGER/SINGH/ENDRASS, Archives of Forensic Psychology, 2015, siehe auch SRF, News-Beitrag vom 5. April 2018.

A. Datenschutzrechtliche Behelfe

446 Ein Algorithmus ist wesentlich von den Daten abhängig, welche er verarbeiten soll. Dabei ist nicht nur die Quantität (wie viele Datenkategorien werden verarbeitet), sondern auch die Qualität der Daten – insbesondere deren Richtigkeit – für das Ergebnis von grosser Bedeutung.[1054] Dies hat sowohl hinsichtlich der Daten des konkreten Einzelfalls als auch betreffend diejenigen Daten, gestützt auf welche das System die Prognose ausstellt, zu gelten. Werden etwa relevante Straftaten einer Person nicht in die Berechnung aufgenommen, kann ein System zur Einschätzung von deren gewalttätiger Neigung kaum eine zutreffende Prognose stellen. Auch die Definition der zugrundeliegenden Regeln steht und fällt mit der Genauigkeit der eingegebenen Daten. Problematisch ist hierbei, dass die Datenerfassung nur einen kleinen Teil der Aufgaben der Polizistinnen und Polizisten darstellt.[1055] Dieses Problem akzentuiert sich, wenn der Algorithmus durch maschinelle Lernverfahren mit Daten aus der Vergangenheit (z.B. Einbruchsdaten) trainiert wurde. Für den Polizeimitarbeitender, welcher die Daten erfasst hat, war unter Umständen gar noch nicht absehbar, dass die Daten einmal auf diese Weise genutzt werden können. Dies kann ebenfalls zu Unvollständigkeiten und Ungenauigkeiten führen. Gerade diese Trainingsdaten haben aber einen wesentlichen Einfluss auf das Funktionieren des Algorithmus.[1056] Ebenfalls möglich ist es, dass gewisse Datenkategorien nicht beachtet werden, welche sehr wohl einen Einfluss auf das Ergebnis haben.[1057]

447 Das schweizerische Datenschutzgesetz kennt mit Art. 5 DSG eine Bestimmung, wonach der Bearbeiter von Personendaten sich über deren Richtigkeit zu vergewissern und Massnahmen zu treffen hat, damit unvollständige oder unrichtige Daten berichtigt oder vernichtet werden können. Damit die Daten richtig im Sinne dieser Bestimmung sind, müssen sie die Umstände und die Tatsachen, bezogen auf die betroffene Person, sachgerecht wiedergeben.

1054 So lehnte das Bundesgericht z.B. in einem anderen Kontext auch bereits Studien oder Statistiken als Prognosemittel für die Durchsetzung von Ansprüchen aufgrund mangelnder Qualität ab; vgl. BGE 136 I 1, E. 4.4.1; Urteil des BGer 1C_383/2016 vom 13. Dezember 2017, E. 5.6; vgl. ALTWICKER, ZBl, 2018, S. 238.

1055 Wenn dann auch noch die Bedienung der entsprechenden Systeme als wenig nutzerfreundlich erachtet wird, dann ist hier erst recht Vorsicht geboten; vgl. KNOBLOCH, S. 21.

1056 KNOBLOCH, S. 21 f mit Verweis auf einen Bilderkennungsalgorithmus des MIT, welcher mit verschiedenen Daten trainiert wurde und dementsprechend Bilder diametral anders interpretierte: WAKEFIELD, Meet Norman, the psychopathic AI, BBC News, 2. Juni 2018.

1057 Vgl. CAPUS, Die Tyrannei des Wahrscheinlichen in der Justiz, Republik, 19. September 2018.

Daraus kann je nach Sachzusammenhang auch gefordert werden, dass die Daten aktuell und vollständig sind.[1058] Auch wenn ein einzelnes Datum für sich betrachtet richtig ist, kann es im Gesamtzusammenhang durchaus unzutreffend sein.[1059] Art. 5 Abs. 2 DSG gibt dem Einzelnen die Möglichkeit, die falschen Daten berichtigen zu lassen. Ein entsprechender Anspruch ist in Art. 25 DSG gegenüber Bundesorganen verankert. Der Berichtigungsanspruch stellt somit grundsätzlich ein Mittel dar, um Fehlern durch unrichtige Daten vorbeugen zu können. Dieser Berichtigungsanspruch stösst jedoch im vorliegenden Kontext in verschiedenen Bereichen an seine Grenzen. Dies soll im Folgenden beleuchtet werden.

1. Grenzen der datenschutzrechtlichen Behelfe

a) Mangelnde Bekanntheit der Datenbearbeitung

In erster Linie ist den Betroffenen im Vorfeld der Entscheidung oft nicht bewusst, dass die entsprechenden Daten über sie bearbeitet werden und dass diese falsch sind.[1060] Das geltende Datenschutzrecht auf Bundesebene kennt mit Art. 18a DSG zwar eine Pflicht, Personen darüber zu informieren, wenn Daten über diese (auch bei Dritten) beschafft werden. Eine entsprechende Informationspflicht entfällt jedoch unter anderem, wenn die Speicherung oder Bekanntgabe ausdrücklich im Gesetz vorgesehen ist (Art. 18a Abs. 4 DSG). Zur Bearbeitung der Daten und auf welche Weise dies geschieht, besteht keine Informationspflicht. Die Personendaten, welche hierzulande im Rahmen von prädiktiver Analytik benutzt werden, sind in der Regel gestützt auf ein Gesetz im Besitz der Amtsstelle (z.B. Polizei),[1061] so dass diese Informationspflicht nicht greift. Allenfalls kann das datenschutzrechtliche Auskunftsrecht nach Art. 8 DSG beigezogen werden, gemäss welchem alle über die Person vorhandenen Daten und deren Zweck durch den Inhaber der Datensammlung bekanntgegeben werden müssen. Jedoch bleibt auch hier das Problem bestehen, dass die Betroffenen wissen oder zumindest vermuten müssen, dass Daten über sie bearbeitet werden sollen. Auch dieses Recht kann zudem nach den Vorgaben von Art. 9 DSG eingeschränkt werden. Oftmals erfahren die Betroffenen die Verwendung falscher Daten daher erst im Rahmen einer Anhörung zum Erlass einer Verfügung.[1062] 448

1058 MAURER-LAMBROU/SCHÖNBÄCHLER, BSK DSG/BGÖ, Art. 5 DSG, N 5.

1059 MAURER-LAMBROU/SCHÖNBÄCHLER, BSK DSG/BGÖ, Art. 5 DSG, N 6.

1060 Vor dem Erlass einer Verfügung besteht immerhin der Anspruch auf rechtliches Gehör (vgl. etwa Art. 30 VwVG), siehe dazu jedoch sogleich.

1061 Siehe dazu weiter oben Rz. 436.

1062 Siehe dazu sogleich Rz. 455.

b) Begrenzung auf Personendaten

449 Die Datenschutzgesetzgebung und somit auch die soeben genannten Rechtsbehelfe der Betroffenen sind zudem nur dort einschlägig, wo Personendaten bearbeitet werden. Sofern Sachdaten durch einen Algorithmus verarbeitet werden, bietet das Datenschutzrecht keine Handhabe zu deren Berichtigung. Eine Berichtigung kann erst im Rahmen des rechtlichen Gehörs geschehen, falls der Fehler dort entdeckt wird. Weiter problematisch sein kann zudem die Verwendung von falschen Daten als Trainingsdaten. Zu beachten ist, dass es sich hierbei ebenfalls – wie im vorigen Kapitel ausgeführt – aufgrund der Anonymisierung der Daten oftmals nicht um Personendaten handelt. Weiter verliert das einzelne falsche Datum in der Masse der Daten an Relevanz und wirkt sich je nachdem nicht im selben Masse auf den Output aus. Es müssten daher systematisch falsche Daten verwendet werden, was nicht undenkbar, aber dennoch eher unwahrscheinlich ist. Auch an nicht personenbezogen Daten müssten für die Verwendung jedoch Anforderungen an die Richtigkeit gestellt werden.[1063] Gerade bei nicht-personenbezogenen Daten wird daher in der Literatur dafür plädiert, dass die öffentliche Hand Daten verwendet, welche sie auch selber bewirtschaftet und zwecks Nachvollziehbarkeit als Open Government Data verfügbar macht. Es ist jedoch ersichtlich, dass dies nicht immer möglich ist.[1064]

c) Mangelnder Einblick in die Funktionsweise des Algorithmus

450 Ein weiteres Problem stellt dar, dass es für den Betroffenen mit zunehmender Komplexität des Algorithmus in zunehmendem Masse schwierig zu durchschauen ist, in welcher Weise die entsprechenden Daten auf das Resultat eingewirkt haben. In diesen Konstellationen kann der Betroffene zwar vielleicht noch erkennen, dass ein Datum falsch ist, aber nicht, ob und wie sich dies auf das Resultat auswirkt. Das geltende Datenschutzrecht kennt keine Pflicht, dass die Behörden bekanntgeben müssen, wie ein entsprechender Algorithmus zu seinen Schlussfolgerungen gekommen ist.

451 De lege ferenda sieht Art. 19 Abs. 1 E-DSG vor, dass die betroffene Person zu informieren ist über «eine Entscheidung, die ausschliesslich auf einer automatisierten Bearbeitung, einschliesslich ‹Profiling›[1065], beruht und die für

1063 BRAUN BINDER, SJZ, 2019, S. 474.

1064 KNOBLOCH, S. 23.

1065 Unter «Profiling» versteht das neue Datenschutzgesetz in Anlehnung an die DSGVO gemäss Art. 4 lit. f. «die Bewertung bestimmter Merkmale einer Person auf der Grundlage von automatisiert bearbeiteten Personendaten, insbesondere um die Arbeitsleistung, die wirtschaftlichen Verhältnisse, die Gesundheit, das Verhalten, die Vorlieben, den Aufenthaltsort oder die Mobilität zu analysieren oder vorherzusagen».

sie mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt». Bundesorgane müssen entsprechende Entscheidungen gemäss Art. 19 Abs. 4 E-DSG gar kennzeichnen. Art. 23 E-DSG sieht zudem vor, dass die betroffene Person ein Auskunftsrecht hat über das Vorliegen einer automatisierten Einzelfallentscheidung und darüber, auf welcher Logik diese Entscheidung beruht. Zu beachten ist allerdings, dass diese Rechte lediglich für ausschliesslich automatisch gefällte Entscheide gelten.[1066] Entscheide, bei welchen der Mensch das letzte Wort hat und der Algorithmus nur die Entscheidungshilfe darstellt, sind dadurch nicht erfasst, was als sehr unbefriedigend empfunden wird.[1067] Es wäre daher zu prüfen, auch die Verwendung von Algorithmen zur Entscheidungsunterstützung der Informationspflicht gemäss Art. 19 Abs. 1 bzw. Abs. 4 DSG zu unterstellen. Im Sinne der Transparenz wäre es zudem wünschenswert, wenn im Rahmen dieser Informationspflichten ebenfalls Angaben über allenfalls verwendete Trainingsdaten bei maschinellen Lernverfahren gemacht würden.[1068]

Es sei an dieser Stelle noch kurz auf den bereits in Kraft stehenden Art. 22 DSGVO verwiesen, welcher die Zulässigkeit von automatisierten Einzelfallentscheidungen ebenfalls regelt. Die betreffende Bestimmung sieht ein Verbot von automatisierten Einzelfallentscheidungen vor, welches jedoch in verschiedener Weise abgeschwächt wird. Auch diese Regelung gilt nur bei ausschliesslich automatisierten Einzelfallentscheidungen ohne wesentliche Beteiligung des Menschen.[1069] Zudem ist es den Mitgliedstaaten erlaubt, durch Rechtsvorschriften weitere automatisierte Entscheidungen vorzusehen. Immerhin sind gemäss Art. 22 Abs. 2 lit. b und Abs. 3 DSGVO gewisse Vorkehrungen zu treffen, damit die Rechte und Freiheiten der betroffenen Personen gewahrt bleiben. Eine weitergehende Auseinandersetzung mit dieser Bestimmung soll weiter unten in dieser Arbeit erfolgen.[1070] 452

2. Fazit

Dem Gesetzgeber war durchaus bewusst, dass die Richtigkeit der Daten Auswirkungen auf die ergehenden Entscheide haben kann. Er hat den Betroffenen daher Instrumente an die Hand gegeben, um die Richtigkeit der über sie bearbeiteten Daten sicherzustellen. Diese Instrumente stossen indes in der vorliegenden Konstellation an gewisse Grenzen, insbesondere dort, wo durch den Algorithmus nicht nur Personendaten verwendet werden und wo den 453

1066 Botschaft Rev. DSG 2017, S. 7056 f.

1067 WEBER/HENSELER, EuZ, 2020 S. 36 und 41; BRAUN BINDER, SJZ, 2019, S. 475.

1068 Vgl. zum Ganzen: BRAUN BINDER, SJZ, 2019, S. 475.

1069 HLADJK, Ehmann/Selmayr DSGVO, Art. 22, N. 6.

1070 Vgl. weiter unten Rz. 649ff.

Personen gar nicht bewusst ist, dass über sie Daten verwendet werden. Daher kann die Richtigkeit der Daten allenfalls erst, aber immerhin, im Rahmen der Gewährung des rechtlichen Gehörs überprüft werden. Zum jetzigen Zeitpunkt fehlt zudem ein Anspruch darauf, einen Einblick zu erhalten, wie die entsprechenden Algorithmen funktionieren. Dies ist problematisch, da für den Betroffenen allenfalls nicht nachvollziehbar ist, wie sich seine richtigen oder falschen Daten auf das Resultat auswirken. Ein solches Recht sollte grundsätzlich entgegen der Bestimmung des E-DSG auch gewährt werden, wenn der Algorithmus lediglich eine Entscheidungshilfe darstellt. Indes ist auch diese geforderte Nachvollziehbarkeit insbesondere bei komplexen Systemen mit Problemen verbunden, wie im Folgenden gezeigt werden soll.

B. Rechtliches Gehör (insbesondere Anspruch auf Begründung)

1. Vorgaben

454 Nach dem soeben Ausgeführten kommt der Gewährung des rechtlichen Gehörs bei der Verarbeitung der Daten durch Algorithmen ein grosses Gewicht zu. Aus der entsprechenden Verfassungsbestimmung in Art. 29 BV ergibt sich einerseits das bereits vorgängig erwähnte Recht auf Anhörung vor dem Erlass einer Verfügung.[1071] Im vorliegenden Kontext ist zudem noch das Recht auf eine sachgerechte Begründung relevant. Nur dies erlaubt es dem Betroffenen zu überprüfen, ob sich die Behörde nicht von unsachlichen Motiven hat leiten lassen, und soll ihm ermöglichen, den Entscheid gegebenenfalls anzufechten. Eine Begründung erfüllt die an sie gestellten Voraussetzungen dann, wenn sie dem Betroffenen erlaubt, eine Entscheidung oder getroffene Massnahme zu verstehen und sachgemäss Beschwerde zu erheben.[1072]

455 Es gilt zu beachten, dass aus dem Gebrauch algorithmenbasierter Systeme in der Schweiz bis anhin kaum direkte Rechtswirkungen für die Betroffenen entstehen. So weisen «Risiko-Assessment»-Instrumente wie «DyRias», gestützt auf die Input-Daten zur betroffenen Person und die definierten Regeln, lediglich ein Gefahrenpotenzial auf einer abstrakten Skala aus. Erst gestützt auf das Ergebnis dieser Berechnung werden weitere Massnahmen vorgenommen, etwa die Einladung zu einem Gespräch oder strafprozessuale Zwangsmassnahmen. Sofern entsprechende Massnahmen Rechte und Pflichten berühren, müssen sie in der Form einer Verfügung (vgl. Art. 5 VwVG) oder gar eines gerichtlichen Beschlusses ergehen, in deren Rahmen grundsätzlich eine vorgängige Anhörung stattzufinden hat und eine Begründung vorgelegt

1071 Vgl. Art. 30 VwVG, siehe dazu oben Rz. 350 ff.

1072 Vgl. zum Ganzen WALDMANN, BSK BV, Art. 29, N. 57.

werden muss.[1073] In Fällen, in denen keine direkten Rechtswirkungen, sondern lediglich ein Taterfolg herbeigeführt wird, wie z.B. mit der Entscheidung, an einem gewissen Ort zu patrouillieren, ist eine vollständige Gehörsgewährung lediglich nach dem Abschluss der Handlung im Rahmen eines Verfahrens auf eine Verfügung über einen Realakt nach Art. 25a VwVG möglich.[1074] Auch in Fällen, in denen die Bearbeitung der Daten keine rechtliche Aussenwirkungen hat, etwa weil eine Einstufung kein weiteres Gefahrenpotenzial offenbart, sind indes die datenschutzrechtlichen Vorgaben zu beachten.[1075]

Im Rahmen der Gehörsgewährung ist es wichtig, dass die Personenda- 456
ten, welche einer Entscheidung zugrunde liegen, der Person im Rahmen der vorgängigen Anhörung bekanntgemacht werden, so dass diese sich allenfalls dagegen wehren kann, wenn die entsprechenden Angaben falsch sind. Ein zusätzliches Problem bei der Verwendung komplexerer Algorithmen – insbesondere solcher, die auf maschinellen Lernverfahren basieren – kann aber darstellen, dass die Behörde selbst die Entscheidung nicht mehr genau nachvollziehen kann. Begreift der Sachbearbeiter nicht, welche Gründe die «Maschine» zum Entscheid bewogen haben, kann er dies gegen aussen auch nicht sachgerecht begründen. Gewisse Autoren zweifeln daher, ob es unter diesen Umständen überhaupt möglich ist, eine diesen Anforderungen genügende Begründung zu geben.[1076] Jedoch sind auch die einzelnen Beweggründe und Gedankengänge eines Behördenmitglieds für die Parteien nicht zugänglich und nicht notwendig, um das Erfordernis an eine Begründung zu erfüllen.[1077] Daraus lässt sich folgern, dass die entscheidende Person nicht im Detail die Funktionsweise des Algorithmus oder des maschinellen Lernverfahrens nachvollziehen können muss, aber dass sie dennoch in der Lage sein sollte, die wesentlichen Entscheidungsgründe plausibel darzulegen.[1078] Gerade bei komplexen Entscheidungssystemen kann allerdings auch dies bereits problematisch werden.[1079]

1073 Vgl. auch CAMAVDIC, Jusletter IT, 26. September 2019, N. 14, wobei das rechtliche Gehör gemäss Art. 30 Abs. 2 VwVG auch eingeschränkt werden kann.

1074 SUTTER, VwVG-Kommentar, Art. 30, N. 10; kritisch etwa: THURNHERR, recht, 2014.

1075 Siehe dazu oben Rz. 435 ff.; vgl. den Entscheid der Rechtsbank Den Haag vom 5. Februar 2020 betreffend das weiter oben erwähnte SyRI-System, ECLI:NL:RBDHA:2020:1878, E. 6.59.

1076 RECHSTEINER, Jusletter, 26. November 2018, N. 26.

1077 Vgl. etwa: MEYER, ZRP, 2018, S. 237.

1078 BRAUN BINDER, SJZ, 2019, S. 473. Aus Art. 23 E-DSG und Art. 15 Abs. 1 lit. h DSGVO ergibt sich de lege ferenda ein analoger Anspruch, wobei dieser aktuell lediglich auf automatisierte Einzelfallentscheidungen begrenzt ist; siehe dazu weiter oben Rz. 448 ff.

1079 Zu den Grenzen und möglichen Korrektiven de lege ferenda siehe etwa Rz. 639 ff.

457 Als problematisch zu erachten ist, dass die Behörden oder die – teilweise privaten – Programmierer eines Systems sich betreffend das Innenleben oftmals auf das Vorliegen eines Geschäftsgeheimnisses berufen, welches einem genauen Einblick in die Funktionsweise des Algorithmus gegenüberstehen kann.[1080] Es ist nicht zu verhehlen, dass eine gewisses Interesse an der Geheimhaltung der Funktionsweise auch vonseiten der öffentlichen Verwaltung durchaus berechtigt ist, kann doch die vollständige Transparenz über ein System dazu führen, dass dieses von gewissen Personen ausgenutzt wird, etwa indem sie ihr Verhalten anpassen.[1081] Dies darf jedoch nicht dazu führen, dass gar keine Informationen über die Funktionsweise bekanntgegeben werden, da auf diese Weise gänzlich verunmöglicht wird, dass die Person sich gegen die Bearbeitung ihrer Daten oder gar weitere Massnahmen gestützt auf das entsprechende System wehren kann.[1082] Es ist daher m.E. jeweils zu fordern, dass es überprüfbare Einblicke in die Risikoindikatoren, den Aufbau und Ablauf des Risikomodells, einschliesslich der Analysemethode, gibt, wie dies etwa von einem niederländischen Gericht hinsichtlich der Datenbearbeitungen im Fall der System Risk Indication (SyRI) gefordert wurde, welche verschiedene Datenbanken miteinander verknüpfte, um damit automatisch anhand eines Risikomodells Personen zu finden, bei denen ein Risiko auf Sozialbetrug besteht.[1083] Es ist indes fraglich, ob auch andere Gerichte eine derart restriktive Haltung einnehmen.[1084]

458 Aktuell ist indes noch umstritten, wie eine entsprechende Bekanntgabe der Funktionsweise, welche den Betroffenen ermöglicht, die Ergebnisse nachzuvollziehen, aber zugleich nicht den gesamten Algorithmus offenlegt, in der Praxis umgesetzt werden kann. Denkbar ist etwa, dass man einer Person gegenüber Aussagen macht zur Vergleichsgruppe, in welcher die Person eingeordnet wird, oder zu den ausschlaggebenden Besonderheiten.[1085] Ebenfalls angedacht ist eine Begründung durch die Verwendung sogenannter

1080 WISCHMEYER, in: Der Terrorist als Feind?, S. 203 ff.

1081 SINGLENSTEIN, NStz, 2018, S. 5, welcher darauf verweist, dass versierte Täter allenfalls die aufgrund der Funktionsweise des «PRECOBS»-Systems erhöhte Polizeipräsenz an einem Ort ausnutzen können, um an einem anderen Ort zuzuschlagen; s. auch MARTINI, Blackbox, S. 41; Entscheid der Rechtsbank Den Haag vom 5. Februar 2020 betreffend das weiter oben erwähnte SyRI-System, ECLI:NL:RBDHA:2020:1878, E. 6.49.

1082 Entscheid der Rechtsbank Den Haag vom 5. Februar 2020, ECLI:NL:RBDHA:2020:1878, E. 6.90.

1083 Entscheid der Rechtsbank Den Haag vom 5. Februar 2020, ECLI:NL:RBDHA:2020:1878.

1084 Vgl. den Entscheid des Wisconsin Supreme Court, State v. Loomis, Urteil 881 N.W.2d 749 vom 13. Juli 2016, welcher keinen Anlass sah, dass eine Einsicht gewährt werden müsse. Zweifelnd für D etwa FERNER, JENS: Urteil zum Einsatz von Software zur Aufdeckung von Sozialbetrug.

1085 MARTINI, Blackbox, S. 190.

kontrafaktischer Erklärungen, also in dem man der Partei darlegt, welche Fakten sich in ihrem Fall auf welche Weise hätten ändern müssen, um ein anderes Resultat hervorzubringen.[1086]

2. Fazit

Das rechtliche Gehör stellt ein wichtiges Instrument dar, um die Rechte betroffener Personen vor Fehlern, welche auf algorithmischen Entscheidungshilfen basieren, zu schützen. Jedoch können auch das Anhörungsrecht und das Begründungserfordernis durch die zunehmende Komplexität von Algorithmen an ihre Grenzen stossen. Gerade bei selbstlernenden Algorithmen sind unter Umständen auch technisch versierte Personen nicht mehr ohne Weiteres in der Lage, die Funktionsweise und die Entscheidungsgrundlagen des Algorithmus gänzlich nachzuvollziehen, geschweige denn allfällige Fehler zu finden.[1087] In diesen Fällen kann das rechtliche Gehör als Korrektiv nicht ausreichen. Zu beachten ist, dass in den Bereichen, in welchen die prädiktive Analytik in der Schweiz aktuell eingesetzt wird, bisher noch keine technisch derart anspruchsvollen Programme ersichtlich sind. Dennoch bleibt festzuhalten, dass gerade in diesem Bereich noch wesentliche Unklarheiten betreffend den Einsatz von Algorithmen bestehen, die einer Klärung harren. 459

C. Diskriminierungsverbot

Auch wenn vollständige, richtige und aktuelle Daten verwendet werden, können die Resultate einer algorithmenbasierten Datenbearbeitung unter Umständen unerwartete oder nicht beabsichtigte Auswirkungen nach sich ziehen. Eine entsprechende Gefahr besteht insbesondere dort, wo Systeme mithilfe von maschinellen Lernverfahren selbständig die Regeln definieren, nach denen die Daten verarbeitet werden. Diese Systeme neigen dazu, gewisse (allenfalls auch unbewusst vorhandene) Vorurteile als relevante Zusammenhänge zu erkennen und auf diese Weise auf zukünftige Entscheide zu reproduzieren.[1088] Ersichtlich wurde dies etwa beim Algorithmus, welcher die Arbeitsmarktchancen von Arbeitssuchenden in Österreich aufgrund der Daten der Vergangenheit in drei Kategorien einteilt, deren Zugehörige in unterschiedlichem Ausmass von Unterstützungsmassnahmen profitieren. Der Algorithmus bewertet dabei aufgrund der zugrundeliegenden statistischen Daten aus der Vergangenheit die Chancen von Frauen (insbesondere Alleinerziehenden mit Kindern) auf dem Arbeitsmarkt pauschal schlechter als diejenigen von 460

1086 WACHTER/MITTELSTADT/RUSSELL, Jolt, 2018 846 ff.

1087 KROLL/HUEY/BAROCAS/FELTEN/REIDENBERG/ROBINSON/YU, PENN LAW REVIEW, 2017, S. 638; MARTINI, Blackbox, S. 227.

1088 BRAUN BINDER, SJZ, 2019, S. 473.

Männern.[1089] Diese Schlussfolgerung mag aufgrund der zur Verfügung stehenden Daten korrekt sein und bildet wohl auch die gesellschaftliche Realität ab.[1090] Jedoch führt dies auch dazu, dass Frauen gegenüber Männern, welche ansonsten dieselben Voraussetzungen haben, schlechter bewertet werden und somit weniger Unterstützungsmassnahmen erhalten. Dies wiederum hat die Konsequenz, dass diesen Nachteilen nicht entgegengewirkt wird und sie somit perpetuiert werden könnten.[1091]

461 Die Bundesverfassung kennt in Art. 8 Abs. 2 BV ein Diskriminierungsverbot, welches vorsieht, dass eine Person nicht alleine aufgrund ihrer Zugehörigkeit zu einer Gruppe – und Eigenschaften, die dieser Gruppe allenfalls zugeschrieben werden – gegenüber Angehörigen anderer Gruppen benachteiligt werden darf.[1092] Die Bestimmung knüpft an persönliche Eigenschaften an, die nicht oder nur schwer abänderbar sind, und nennt dabei unter anderem auch namentlich die Herkunft, die Rasse oder das Geschlecht.[1093] Im vorliegenden Falle ist insbesondere problematisch, dass Merkmale, welche einer Menschengruppe zugesagt werden, als Ersatz für Informationen über das jeweilige Individuum als Grundlage dieser Prognose dienen. Die entsprechenden Erkenntnisse können sich dabei etwa auf statistische Betrachtungen vergangener Daten stützen. Diese statistische Diskriminierung ist, sofern sie an eine gruppenbezogene Eigenschaft anknüpft, eine Form der direkten Diskriminierung.[1094] Aufgrund der oben ausgeführten Beispiele ist es nicht auszuschliessen, dass gestützt auf die Erkenntnisse eines Algorithmus Menschen aufgurnd anderer Hautfarbe oder des Geschlechts schlechtere Bedingungen antreffen als andere Gruppen.

462 Während das Diskriminierungsverbot also auch Fälle erfassen kann, in denen durch den Algorithmus diskriminiert wird, stellen sich bei der Geltendmachung der entsprechenden Rechte einige Probleme. Problematisch kann in diesem Zusammenhang in erster Linie sein, dass die entsprechenden Diskriminierungen überhaupt entdeckt werden.[1095] Die naheliegende Lösung

1089 CECH/FISCHER/HUMAN/LOPEZ/WAGNER, Dem AMS-Algorithmus fehlt der Beipackzettel, Futurezone, 3. Oktober 2019.

1090 FRÖHLICH/SPIECKER GENANNT DÖHMANN, VerfBlog, 26.12.2018.

1091 BRAUN BINDER, SJZ, 2019, S. 474.

1092 WALDMANN, BSK BV, Art. 8, N. 59.

1093 SCHWEIZER/BIGLER-EGGENBERGER/KÄGI-DIENER, SG Komm. BV, Art. 8, N. 62.

1094 ALTWICKER, ZBl, 2018 S. 640.

1095 Im Beispiel von COMPAS wurde etwa erst im Rahmen einer statistischen Auswertung der Daten nachgewiesen, dass Personen mit schwarzer Hautfarbe systematisch schlechter beurteilt wurden; vgl. ANGWIN/LARSON/MATTU/KIRCHNER, Machine Bias. ProPublica, There's software used across the country to predict future criminals. And it's biased against blacks.

wäre, bei der Ausgestaltung entsprechender diskriminierungsaffiner Algorithmen auf die Berücksichtigung der sensiblen Merkmale im Sinne von Art. 8 Abs. 2 BV (z.B. Hautfarbe) zu verzichten. Dies kann jedoch als alleinige Lösung dann nicht ausreichen, wenn der Algorithmus auf andere Daten zurückgreifen kann, welche direkt oder indirekt vom jeweiligen Merkmal beeinflusst werden, so dass auf diese Weise das entsprechende Merkmal dennoch einen Einfluss auf das Resultat hat.[1096]

Es gilt zu beachten, dass die Algorithmen zudem «nur» diejenigen Vorurteile fortschreiben, welche in der Gesellschaft bereits bewusst oder unbewusst vorhanden sind. Dies ist insbesondere dann der Fall, wenn die Algorithmen aufgrund von systematisch ausgewerteten Daten aus der Vergangenheit trainiert wurden. Wichtig scheint an dieser Stelle zu sein, dass man sich bewusst ist, dass Algorithmen nicht per se neutral sind. Sobald sie an Merkmale anknüpfen und diese in einen Zusammenhang mit anderen stellen, nehmen sie eine Wertung vor.[1097] Diese Merkmale werden ihnen entweder durch die Programmierung oder das Training vorgegeben. Dies allein darf noch nicht gegen den Einsatz von Algorithmen ins Feld geführt werden, kann es doch auch dazu dienen, Missstände – welche bisher nicht bewusst wahrgenommen wurden – sichtbar zu machen, was allenfalls entsprechende Gegenmassnahmen nach sich ziehen kann.[1098] Aus diesen Gründen stösst der verfassungsrechtliche Diskriminierungsschutz als Korrektiv ebenfalls an seine Grenzen. Es ist daher wichtig, dass auch bei Korrektheit der Daten eine Kontrolle der Entscheidungsempfehlungen stattfindet, wobei aktuell noch unklar ist, wie diese stattfinden soll.[1099] 463

D. Menschliche Entscheidung als Korrektiv

Die bisher vorgestellten Korrektive stossen beim Einsatz komplexer Algorithmen an ihre Grenzen und können unter Umständen sachlich falsche Entscheide nicht wirksam verhindern. Im Gegensatz zu vollautomatischen Entscheidungen – welche weiter unten eingehend thematisiert werden – ist es in der öffentlichen Verwaltung in der Schweiz bei den Einsatzbereichen von Algorithmen und prädiktiver Analytik bis anhin immer der Mensch, welcher letztendlich die Entscheidung trifft. Oftmals wird die Vorhersage des Algorithmus lediglich als ein Indiz für den Entscheidungsträger genommen, welches 464

1096 Dabei handelt es sich um sogenannte Proxy-Variablen, vgl. etwa weitergehend: SCHERER, Queen Mary University of London, School of Law, Legal Studies Research Paper, 2019, S. 21.

1097 FRÖHLICH/SPIECKER GENANNT DÖHMANN, VerfBlog, 26.12.2018.

1098 FRÖHLICH/SPIECKER GENANNT DÖHMANN, VerfBlog, 26.12.2018.

1099 BRAUN BINDER, SJZ, 2019, S. 474, vgl. dazu weiter unten Rz. 639 ff.

sich entweder mit seinen eigenen Erkenntnissen und Erfahrungen sowie seinem Bauchgefühl deckt oder nicht.[1100] Zumindest Entscheide, welche den Verantwortlichen krass unrichtig erscheinen, können auf diese Weise korrigiert werden. Problematisch ist dabei, dass viele Fehler für den menschlichen Betrachter nicht auf den ersten Blick ersichtlich sind und dass es gerade bei komplexen Algorithmen immer schwieriger wird, die Beweggründe des Algorithmus nachzuvollziehen, insbesondere wenn die zugrundeliegenden Regeln nicht mehr von einem Menschen programmiert, sondern vom Programm durch maschinelles Lernen aus vergangenen Daten definiert oder weiterentwickelt wurden. In solchen Fällen ist für den Entscheidungsträger allenfalls nicht ersichtlich, welche Daten den Ausschlag für die Entscheidung gegeben haben.

465 Diese eingeschränkte Nachvollziehbarkeit ist nicht nur wegen des bereits angesprochenen Begründungsanspruchs des Betroffenen problematisch. Sie verunmöglicht dem Entscheidungs-tragenden auch, den Algorithmus kritisch zu hinterfragen. Dies darf nicht dazu führen, dass der Entscheidende der Maschine blindlings vertraut, sondern es müssen immer auch andere Faktoren, wie etwa die eigene Intuition oder Erfahrung, miteinbezogen werden.[1101] Zu beachten ist in diesem Fall jedoch auch eine psychologische Komponente, welche es schwierig macht, gegen die Empfehlung des Algorithmus zu entscheiden.[1102] Entscheidet der Mensch entgegen der Einschätzung des Algorithmus, eine Person nicht weiter beobachten zu lassen, und diese begeht dann eine schwere Straftat, muss sich der zuständige Sachbearbeiter für seine Abweichung von der Einschätzung des Algorithmus rechtfertigen, während er ansonsten die Verantwortung zumindest in Teilen auf den Computer abstützen kann.[1103] Dieser Problematik könnte allenfalls dadurch entgegengewirkt werden, dass dem entscheidenden Beamten eine sogenannte «score-blinde» Prognose anhand der durch die Maschine ermittelten, zentralen Faktoren übermittelt wird, ohne ein genaues Urteil vorwegzunehmen, und dass man den Entscheidungstragenden zu seinem eigenen Schluss kommen lässt.[1104]

1100 SRF, News-Beitrag vom 5. April 2018.

1101 Vgl. CAPUS, Die Tyrannei des Wahrscheinlichen in der Justiz, Republik, 19. September 2018.

1102 Vgl. dazu auch MARTINI, Blackbox, S. 48.

1103 SRF, News-Beitrag vom 5. April 2018.

1104 Auch hier ist eine Beeinflussung des Entscheidungsträgers nicht auszuschliessen, da dieser sich durchaus bewusst ist, dass der Algorithmus gewisse Faktoren als erfüllt erachtet, ansonsten hätte er die Daten nicht als auffällig markiert; vgl. RADEMACHER, AöR, 2017 S. 391.

Hierbei ist ebenfalls problematisch, dass im Bereich der prädiktiven Analytik immer (etwa unter Abstützung auf statistische Wahrscheinlichkeiten) eine Prognose über ein ungewisses, zukünftig eintretendes Ereignis erstellt wird.[1105] Es beinhaltet immer nur eine Wahrscheinlichkeit, dass ein gewisses Ereignis auf die vorhergesagte Weise eintritt. Auch wenn der Algorithmus einer Person, ein hohes Risiko attestiert, dass sie erneut eine Straftat begeht, muss dies nicht zwingend geschehen. Dadurch gibt es ein systemimmanentes Risiko, dass die Prognose falsch liegt. Die meisten entsprechenden Systeme sind darauf ausgelegt, möglichst keine der potenziell gefährlichen Personen zu verpassen, weswegen die Parameter entsprechend weit gewählt werden. Dies kann jedoch dazu führen, dass, wie im oben erwähnten Beispiel DyRias, neben den richtig erkannten Delinquenten auch eine Vielzahl an «false positives» existiert, sprich Menschen fälschlicherweise als verdächtig eingestuft werden.[1106] Wie dieser Problematik wirksam begegnet werden soll, ist aktuell nicht absehbar. 466

V. «Predictive policing» als Anschauungsbeispiel

Die Verwendung von Algorithmen und prädiktiver Analytik in der Schweiz ist im Rahmen vorausschauender Polizeiarbeit bereits durchaus verbreitet. Daher sollen die soeben erarbeiteten Grundsätze anhand dieses Praxisbeispiels veranschaulicht werden. 467

A. Datenschutzrechtliche Vorgaben

Nach dem weiter oben Ausgeführten kommt Datenschutzrecht nur dann zur Anwendung, wenn es sich bei den im konkreten Fall verwendeten Daten um Personendaten i.S. von Art. 3 DSG handelt, das heisst um Angaben, durch die eine Person bestimmt oder bestimmbar ist.[1107] 468

1. Input

Das in der Schweiz in verschiedenen Kantonen eingesetzte, raumbezogene «Predictive policing»-System «Precobs» wird mit ortsbezogenen Daten gefüttert, etwa wo der letzte Einbruch geschah. Personendaten – etwa wer im betroffenen Haus wohnt – sind für das System nicht relevant. Da entsprechend keine Bearbeitung von Personendaten stattfindet, wird davon ausgegangen, 469

1105 DREYER, in: Big Data – Regulative Herausforderungen, S. 135; vgl. weiterführend ALTWICKER, ZBl, 2018, S. 231.

1106 Vgl. zum Ganzen etwa: FREI, in: Bedrohungsmanagement in der Schweiz.

1107 Siehe oben Rz. 76.

dass solche Systeme datenschutzrechtlich keine relevanten Risiken mit sich bringen.[1108] Es ist indes sicherzustellen, dass nicht über sehr detaillierte Ortsangaben allenfalls dennoch ein Personenbezug hergestellt werden kann.[1109]

470 Anders ist dies allenfalls im Bereich des personenbezogenen «predictive policing» zu beurteilen, also wenn ein Algorithmus etwa Aussagen treffen soll, ob eine Person straf- oder rückfällig wird. Um darauf eine Antwort zu erhalten, müssen sehr wohl Daten bearbeitet werden, die eine Person bestimmbar machen können, etwa das Alter oder die Herkunft. Unter Umständen sind auch Daten über strafrechtliche Sanktionen relevant, welche als besondere Personendaten nach Art. 3 lit. c. Ziff. 4 DSG gelten. Bei umfangreicheren Datensammlungen lässt sich unter Umständen sogar ein Persönlichkeitsprofil i.S. von Art. 3 lit. d DSG über eine Person erstellen. Gemäss Art. 17 DSG und analogen kantonalen Bestimmungen ist für eine Bearbeitung dieser Daten grundsätzlich eine gesetzliche Grundlage gefordert. Wie weiter oben bereits ausgeführt wurde, handelt es sich bei der vorausschauenden Polizeiarbeit nicht grundsätzlich um ein neues Phänomen. Die Polizei durfte die entsprechenden Daten oftmals bereits vor der Digitalisierung gestützt auf die Polizeigesetzgebung erheben.[1110]

471 Gerade im Bereich der vorausschauenden Polizeiarbeit gilt allerdings: Je mehr Daten über eine Person bekannt sind und in das System eingegeben werden können, desto besser kann eingeschätzt werden, ob und unter welchen Umständen die entsprechende Person ein Risiko darstellen könnte.[1111] Wohin die Reise gehen könnte, zeigt das amerikanische COMPAS-System zur Rückfallgefahr von Straftätern, welches die entsprechende Gefahr anhand von ganzen 137 Attributen einschätzt.[1112] Somit besteht für die Behörden der Anreiz, weitere Kategorien von Personendaten zu erfassen, um Voraussagen robuster zu machen. Sollten dazu neue gesetzliche Grundlagen geschaffen werden, so hat der Gesetzgeber immer auch den Grundsatz der Verhältnismässigkeit zu beachten.[1113] Die Effektivierung der Strafverfolgung und der Gefahrenabwehr stehen durchaus im öffentlichen Interesse und können somit Eingriffe in die Grundrechte rechtfertigen.[1114] Problematisch ist jedoch,

1108 Vgl. etwa KNOBLOCH, S. 5; für die Schweiz auch: LEESE, in: Bulletin 2018 zur schweizerischen Sicherheitspolitik, S. 59; CAMAVDIC, Jusletter IT, 26. September 2019, N. 8.

1109 SINGLENSTEIN, NStz, 2018, S. 6.

1110 Siehe oben Rz. 437.

1111 LEESE, in: Bulletin 2018 zur schweizerischen Sicherheitspolitik, S. 59.

1112 Vgl. etwa ANGWIN/LARSON/MATTU/KIRCHNER, Machine Bias. ProPublica, There's software used across the country to predict future criminals. And it's biased against blacks.

1113 Vgl. weiter oben Rz. 436 ff.

1114 Vgl. HÄRTEL, LKV, 2019, S. 55.

dass die Wirksamkeit gerade von «Predictive policing»-Massnahmen bis anhin nicht eindeutig erwiesen werden konnte. So berichten Kantone, welche «PRECOBS»Systeme einsetzen, zwar durchaus von einem Rückgang an Einbrüchen auf ihrem Gebiet. Es lässt sich aber schwer belegen, dass dies nur mit der Verwendung der Systeme zusammenhängt, da auch andere Aspekte wie die Verdrängung in andere Kantone (ohne PRECOBS) sowie andere polizeiliche Massnahmen diesen Effekt beeinflusst haben können.[1115] Auch bei personenbezogenen Ansätzen sind keine verlässlichen Studien vorhanden, welche etwa aussagen, in welchem Masse diese zusätzlich zur Verhinderung von Straftaten beitragen. Hingegen besteht, wie weiter oben ausgeführt, die Gefahr, dass das von den Personen ausgehende Risiko generell eher überschätzt wird, um möglichst keine «gefährlichen Fälle» zu verpassen.[1116] Somit konnte bisher nicht abschliessend und hinreichend belegt werden, ob diese Systeme überhaupt geeignet sind, die damit verfolgten Ziele zu erreichen.

Im Hinblick auf die Verhältnismässigkeit im engeren Sinne ist zu beachten, dass die Datenbearbeitung im Bereich der polizeilichen Präventivarbeit oftmals an das Vorliegen gewisser Verdachtsmomente gebunden ist.[1117] Bei den in der Schweiz eingesetzten Algorithmen, welche präventive Analytik einsetzen, sind entsprechende Verdachtsmomente in der Regel vorhanden. So basiert etwa «DyRias» darauf, dass für die untersuchten schweren Gewalttaten oder Delikte in der Regel bereits zuvor Anzeichen bestehen.[1118] Die verwendeten Parameter stehen in der Regel im Zusammenhang mit dem Delikt (z.B. spielt der Strafregisterauszug oder eine gewalttätige Neigung durchaus eine Rolle, wenn es um die Berechnung der Rückfallgefahr geht). Je weiter jedoch die Anzahl der erhobenen Parameter gezogen werden soll, desto weniger lässt sich deren Auswahl begründen und desto mehr kann von einer anlasslosen Überwachung gesprochen werden. Als Beispiel kann hier die oben erwähnte «Strategic Subject List» in Chicago (USA) angeführt werden, welche beispielsweise auch die sozialen Kontakte zur Bewertung verwendet, ob eine Person allenfalls in Bandenkriminalität involviert sein könnte. Somit kann es ausreichen, mit einem polizeibekannten Straftäter zu verkehren, um in das Visier dieses Systems zu gelangen.[1119] Eine solche anlasslose Datenspeicherung und -bearbeitung liesse sich nur schwer mit dem Verhältnismässigkeitsgrundsatz vereinbaren. 472

1115 Vgl. etwa LEESE, in: Bulletin 2018 zur schweizerischen Sicherheitspolitik, S. 64 oder HÄRTEL, LKV, 2019, S. 55 f.

1116 Siehe dazu oben Rz. 466.

1117 HÄRTEL, LKV, 2019, S. 56, CAMAVDIC, Jusletter IT, 26. September 2019, N. 11 ff.

1118 Vgl. etwa den Projektbeschrieb der Software DyRiAS.

1119 LEESE, in: Bulletin 2018 zur schweizerischen Sicherheitspolitik, S. 59.

473 Ebenfalls kritisch zu betrachten ist die Verknüpfung von Datenbeständen verschiedener Behörden, um neue Erkenntnisse zu gewinnen. Bei der Schaffung entsprechender Gesetzesgrundlagen im Sinne von Art. 17 DSG spielen die oben genannten Prinzipien der Verhältnismässigkeit und der Zweckbindung eine wichtige Rolle. So hat etwa ein niederländisches Gericht entschieden, dass der Einsatz des «SyRI»-Systems zur Einschätzung des Risikos für Sozialhilfebetrug in der vorliegenden Ausgestaltung nicht rechtskonform sei.[1120] Dabei wurde insbesondere argumentiert, dass sich aus dem Schutz der Privatsphäre beim Einsatz von neuen Techniken eine spezielle Verantwortung ergebe, die Balance zwischen dem Interesse an deren Verwendung und der potenziellen Verletzung der Grundrechte der Betroffenen zu wahren. Diese Balance sei im zugrundeliegenden Fall aufgrund der Vielzahl an verknüpften Daten und der Nichtpreisgabe der Funktionsweise des Algorithmus nicht gegeben.[1121]

2. Regeln

474 Bei den in der Schweiz bestehenden Einsatzbereichen des «predictive policing» beruhen die Regeln, nach denen die Algorithmen entscheiden, soweit ersichtlich auf wissenschaftlichen Erkenntnissen (z.B. der «Near repeat»-Theorie).[1122] Somit werden zur Definition der Regeln in keiner Weise Personendaten bearbeitet, womit sie datenschutzrechtlich unbedenklich sind. Sollten im Rahmen eines «Predictive policing»-Projekts dereinst Trainingsdaten eingesetzt werden, welche ihrer Natur nach einen Personenbezug enthalten, so ist dieser entweder vollständig und irreversibel zu entfernen (Anonymisierung) oder es ist eine gesetzliche Grundlage für die entsprechende Zweckänderung der betreffenden Daten zu schaffen.

B. Schwachstellen bei Algorithmen

475 Auch «Predictive policing»-Algorithmen können Fehler produzieren. Betreffend die datenschutzrechtlichen Behelfe, welche den Betroffenen offenstehen, und deren Grenzen kann auf das oben Ausgeführte verwiesen werden.[1123] Sofern die Behörde sich aufgrund der Schlussfolgerungen des Systems entschliesst, Massnahmen gegenüber dem Betroffenen zu ergreifen, so ist diesem das rechtliche Gehör zu gewähren. Dabei ist insbesondere darauf zu achten, dass die Entscheidung für die Behörde und die Adressaten nachvollziehbar ist.

1120 Entscheid der Rechtsbank Den Haag vom 5. Februar 2020, ECLI:NL:RBDHA:2020:1878, E. 6.90.

1121 Entscheid der Rechtsbank Den Haag vom 5. Februar 2020, ECLI:NL:RBDHA:2020:1878, E. 6.6 und 6.49.

1122 Siehe oben Rz. 426.

1123 Siehe oben Rz. 446.

Im Zusammenhang mit «predictive policing» können sich spezifische Probleme hinsichtlich des Diskriminierungsverbots stellen. Gerade in diesem Zusammenhang ist zu erwarten, dass Fälle der statistischen Diskriminierung auch im verwaltungsrechtlichen Bereich eine grössere Rolle spielen können.[1124] Medienwirksam publik wurde dies etwa im Falle des COMPAS-Systems, welches Delinquenten mit schwarzer Hautfarbe hinsichtlich ihrer Rückfallprognose schlechter bewertete als solche mit weisser Hautfarbe und dadurch eine erhebliche Zahl an «false positives» lieferte.[1125] Ähnliche Effekte wurden auch bei personenbezogenen «Predictive policing»-Systemen in den USA beobachtet.[1126] Bei ortsbezogenen Systemen findet zwar nicht in erster Linie eine Diskriminierung der einzelnen Person aufgrund eines Merkmals statt, jedoch können die Erkenntnisse beispielsweise zu einer erhöhten Polizeipräsenz in einem gewissen Gebiet führen. Die erhöhte Polizeipräsenz könnte wiederum dazu führen, dass die Polizei an diesen Orten mehr Straftaten entdeckt, wodurch sie wiederum vermehrt in diese Gebiete patrouilliert. Somit bestätigen sich diese Vorurteile als «selbst erfüllende Prophezeiung».[1127] 476

Ein Ausschluss von sensiblen Merkmalen kann wiederum Auswirkungen auf den Wert der Prognose haben, einerseits indem die Prognosekraft dadurch verringert wird, dass die ausgeschlossenen Faktoren einen wesentlichen Einfluss auf das Endresultat haben.[1128] Anderseits kann es unter Umständen auch nicht ausreichen, lediglich das sensible Merkmal auszuschliessen, da dies durch andere Merkmale, welche von diesem indirekt beeinflusst werden, dennoch wieder Eingang in die Prognose finden kann. So war etwa im Falle des COMPAS-Systems die Hautfarbe der Betroffenen explizit als Kategorie ausgeschlossen. Dies hielt den Algorithmus nicht davon ab, aufgrund anderer Daten, welche zumindest mit von der Hautfarbe beeinflusst waren, zum selben Schluss zu kommen und somit diese Person mittelbar dennoch wegen ihrer Hautfarbe zu diskriminieren. So kann gerade in Gegenden mit einer ausgeprägten Trennung zwischen Bevölkerungsschichten oder Ethnien auch der Wohnort dennoch Rückschlüsse auf die Hautfarbe zulassen.[1129] 477

1124 ALTWICKER, ZBl, 2018, S. 640; siehe dazu oben Rz. 460.

1125 ANGWIN/LARSON/MATTU/KIRCHNER, Machine Bias. ProPublica, There's software used across the country to predict future criminals. And it's biased against blacks.

1126 KNOBLOCH, S. 12.

1127 KNOBLOCH, S. 12 und 24; auch im Zusammenhang mit dem Asylalgorithmus wurde die Gefahr einer Ghettoisierung der Asylbewerbenden betont, vgl. SRF, News-Beitrag vom 11. Mai 2018.

1128 RADEMACHER, AöR, 2017, S. 393

1129 Wohnt etwa eine Person schwarzer Hautfarbe in einem Viertel mit hoher Kriminalitätsrate, kann sich dies für sie auch dann in der Berechnung negativ auswirken, wenn die Hautfarbe nicht als Kategorie vorhanden ist; vgl. etwa BRAUN BINDER, SJZ, 2019 S. 474.

Dies zeigt, dass gerade in den Bereichen sensibler Merkmale erhöhte Vorsicht beim Einsatz von «predictive policing» geboten ist.

C. Zwischenfazit

478 Der Einsatz von «predictive policing», wie er in der Schweiz aktuell erfolgt, kann als mit der Rechtsordnung vereinbar beurteilt werden. Bei allfälligen Weiterentwicklungen (etwa durch die Verwendung weiterer Personendaten) hat indes jeweils eine neue Bestandesaufnahme zu erfolgen, ob die dadurch versprochenen Vorteile die damit verbundenen Nachteile überwiegen.[1130] Dies insbesondere, da die bestehenden rechtlichen Möglichkeiten der Betroffenen umso mehr an ihre Grenzen stossen, je komplexer die entsprechenden Systeme ausgestaltet sind.

VI. Zusammenfassung

479 Die Rechtsordnung steht einer Verwendung von Algorithmen als Entscheidungshilfe im Verwaltungsverfahren nicht entgegen, da die Mittel, welche die Behörden bei der Erledigung ihrer Aufgaben benutzen, grundsätzlich frei gewählt werden können. Eingeschränkt wird die Verwendung von Algorithmen durch datenschutzrechtliche Bestimmungen, indem Personendaten nur verwendet werden dürfen, wenn dies gesetzlich vorgesehen ist. Da vor allem im Bereich von datengestützten Vorhersagen neben der Datenqualität auch die Datenquantität grossen Einfluss auf die Resultate hat, besteht der Anreiz, neue gesetzliche Grundlagen zu schaffen, um immer mehr zusätzliche Daten erheben zu können. Daher ist bei der Einführung neuer Datenbearbeitungsgrundlagen immer auch das Verhältnismässigkeitsprinzip zu beachten.

480 Problematisch ist auch, dass Algorithmen als Entscheidungsunterstützung Fehler machen können. Dies allein kann nicht als Argument für ein Verbot von deren Einsatz ausreichen, da auch menschliche Verwaltungsangestellte Fehler machen. Jedoch bietet die Verwendung von Algorithmen Raum für zusätzliche Fehlerquellen. Die Rechtsordnung sieht einige Korrektive vor. Wichtig ist einerseits die Richtigkeit der zugrundeliegenden Daten. Für die betroffenen Personen existieren datenschutzrechtliche Behelfe, um etwa Daten berichtigen zu können. Dazu muss die betroffene Person wissen, dass und wie Daten über sie bearbeitet werden. Ein erster Schritt wäre hier, die in Art. 19 E-DSG neu vorgesehenen Pflichten bei automatisierten Einzelfallentscheidungen auch auf Einsatzbereiche auszudehnen, in welchen Algorithmen lediglich zur Entscheidungshilfe angewendet werden. Zudem besteht in gewissen

1130 Im Ergebnis gleich: CAMAVDIC, Jusletter IT, 26. September 2019 N. 17 f.

Einsatzbereichen die Gefahr, dass versteckte Vorurteile perpetuiert werden und sich diskriminierend auf betroffene Bevölkerungsgruppen auswirken. Dieser Gefahr kann durch den Verzicht auf die entsprechenden Datenkategorien nicht immer wirksam begegnet werden. Eine wichtige Rolle kommt auch dem Anspruch auf rechtliches Gehör zu, welcher ein Recht auf Anhörung und Begründung umfasst. Um dies zu gewährleisten, ist es umso wichtiger, dass die Menschen die Entscheidungsempfehlungen, welche ihnen entsprechende Systeme geben, nachvollziehen und auch gegen aussen begründen können. Je nach Komplexität des Systems ist dies ebenfalls nicht einfach zu gewährleisten.

All diese Korrektive können mögliche Risiken durch die Verwendung 481
von Algorithmen nicht gänzlich verhindern, sondern sie lediglich eingrenzen. Wichtig scheint daher auch, dass sich der Entscheidungsträger (aber auch allenfalls weitere Instanzen) bewusst ist, dass die Computerprognose nur ein Entscheidungskriterium neben weiteren darstellt. Dieser Prognose sollte daher nicht blindlings gefolgt werden und sie darf durchaus auch kritisch hinterfragt werden. Daher sollen Algorithmen vor allem in Bereichen, welche hier spezifische Risiken (etwa hinsichtlich der Diskriminierung sensibler Gruppen) bieten, mit Bedacht eingesetzt werden. Zudem wird in der Literatur nach alternativen Korrektivmöglichkeiten Ausschau gehalten. Da diese aktuell allerdings noch «Zukunftsmusik» darstellen, sollen entsprechende Überlegungen im nächsten Teil der Arbeit eingehender behandelt werden.

Teil 3: Absehbare Entwicklungen und verfassungsrechtlicher Kontext

Wie im vorangegangenen Teil dargelegt wurde, bestehen sowohl für das rechtliche als auch für das tatsächliche Verwaltungshandeln der Behörden Rechtsgrundlagen, welche digitales Handeln durch die Verwaltung im Großen und Ganzen ermöglichen bzw. zu legitimieren vermögen. Es wurde indes aufgezeigt, dass gewisse Gesetzeslücken und Rechtsunsicherheiten bestehen bleiben. Zu beachten ist, dass in gewissen Bereichen zwar die Rechtsgrundlagen bestehen, aber allfällige digitale Angebote noch wenig genutzt werden (etwa im elektronischen Rechtsverkehr). Hierzu lässt sich die Frage stellen, ob und welche Vorkehrungen unternommen werden müssten, um entsprechenden Angeboten zum Durchbruch zu verhelfen. Zudem zeichnen sich weitere technologische Errungenschaften oder Weiterentwicklungen bestehender Technologien ab, welche das Verwaltungshandeln ebenfalls beeinflussen können. 482

Im vorliegenden Teil soll daher untersucht werden, welche möglichen Entwicklungen sich im Bereich der Digitalisierung des Verwaltungshandelns in den nächsten Jahren ergeben könnten. Dabei soll untersucht werden, ob diese sich in die bestehende Rechtsordnung einpassen lassen oder ob neue Grundlagen geschaffen werden müssen und welche allfälligen rechtlichen Probleme entsprechende Weiterentwicklungen mit sich bringen könnten. Da nicht verlässlich vorhergesagt werden kann, welche Technologien sich in welchem Bereich durchsetzen, soll hier eine selektive Auswahl getroffen werden. Berücksichtigt werden in erster Linie technologische oder technologiebedingte Neuerungen, zu welchen es entweder bereits Regulierungsbestrebungen gibt oder deren Einsatz im Bereich der öffentlichen Verwaltung durch die Lehre als erstrebenswert oder wahrscheinlich angesehen wird. 483

§7 Digitalisierung des tatsächlichen Verwaltungshandelns

Ausserhalb von Verfahren ist es bereits weitgehend Realität, dass Behörden über das Internet informieren und kommunizieren. Wie bereits ausgeführt, 484

bringt die behördliche Informationstätigkeit via Internet durchaus Vorteile mit sich und kann als effiziente Alternative zu den bisherigen Formen der Informationstätigkeit beurteilt werden. Allerdings sind gewisse Aspekte noch nicht vollends geklärt, etwa betreffend die Haftung für Aussagen im Internet oder auf sozialen Medien oder betreffend die Sperrung von Personen in den sozialen Medien. Beispiele aus anderen Ländern oder der Privatwirtschaft belegen, dass es auch in diesem Bereich noch Entwicklungsmöglichkeiten gibt. So erledigen – wie weiter oben ausgeführt – in Dänemark 90 % der Einwohner sämtliche Kommunikation mit den Behörden online.[1131] Vermehrt setzen öffentliche Einrichtungen zum Kontakt mit der Bevölkerung sogenannte Chatbots ein, welche aufgrund vorprogrammierter Antwortmöglichkeiten unabhängig von menschlicher Intervention Anfragen beantworten können.[1132] Im vorliegenden Kapitel sollen diese möglichen Weiterentwicklungen im Bereich der behördlichen Information und Kommunikation betrachtet werden, welche in anderen Ländern bereits umgesetzt wurden. Dabei soll ihre Vereinbarkeit mit der schweizerischen Rechtsordnung ergründet werden. Zudem soll die Frage thematisiert werden, ob die gesamte Informationstätigkeit oder zumindest Teile davon aus rechtlicher Sicht ausschliesslich online erbracht werden dürfte.

I. Behördliche Informationstätigkeit ausschliesslich über Internet

485 Im Rahmen der geltenden Rechtsordnung steht den Behörden die Möglichkeit offen, über das Internet oder soziale Medien ihre Informationstätigkeit zu erfüllen. Es ist als verhältnismässig zu erachten und kann unter Umständen gar geboten sein, eine Information auch auf diesen Kanälen zu verbreiten, um möglichst rasch eine möglichst grosse Menge oder einen gezielten Kreis von Adressaten zu erreichen. Auch amtliche Publikationen dürfen grundsätzlich über das Internet erfolgen. Einschränkungen sind dabei in erster Linie dann denkbar, wenn durch die Information Personendaten bekanntgegeben werden sollen.[1133] Weiter oben wurde bereits dargelegt, unter welchen Umständen es zulässig sein kann, dass eine Behörde Informationen zumindest in einem gewissen Bereich (vorliegend stellte sich die Frage insbesondere hinsichtlich der amtlichen Publikation) nur noch online erbringen darf. Soweit ersichtlich hat indes noch kein Gemeinwesen eine Umstellung dahingehend gewagt, dass umfassend nur noch online informiert wird. Da dies zumindest

1131 Vgl. etwa Agency for Digitisation, Digital Post.

1132 Vgl. etwa den Govbot der Stadt Bonn.

1133 Vgl. zum Ganzen oben Rz.155.

vorstellbar ist – und wie oben beschrieben gewisse Doppelspurigkeiten beheben könnte –, soll an dieser Stelle untersucht werden, ob eine reine Online-Informationstätigkeit der Verwaltung im geltenden rechtlichen Rahmen zulässig wäre.

A. Betroffene Grundrechte

1. Informationelle Selbstbestimmung

Weiter vorne wurde bereits ausgeführt, dass bei der behördlichen Informationstätigkeit über Internet insbesondere die informationelle Selbstbestimmung gewisse Regelungen, etwa hinsichtlich der Bekanntgabe von Personendaten, notwendig macht. Die an früherer Stelle angestellten Überlegungen zu diesem Thema haben auch zu gelten, sofern die Informationstätigkeit ausschliesslich über das Internet erfolgt. Indes ergibt sich für die Betroffenen in dieser Hinsicht keine andersartige oder grössere Bedrohung dadurch, dass die Publikation nun ausschliesslich online anstatt zusätzlich über andere Kanäle stattfindet. Daher sei für diese Aspekte auf den vorangegangenen Teil der Arbeit verwiesen.[1134] 486

2. Diskriminierungsverbot

Bereits aus der Verfassungsbestimmung in Art. 180 BV ergibt sich, dass die Öffentlichkeit und somit die gesamte Bevölkerung und nicht bloss spezifische gesellschaftliche Zielgruppen als Adressatin der Behördeninformation zu verstehen ist.[1135] Entscheidet sich eine Behörde daher, ihre Informationstätigkeit nur noch online zu erbringen, so könnten dadurch gewisse Gruppen benachteiligt werden. Gemäss Art. 8 Abs. 2 BV darf niemand 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. Es ergibt sich zudem auch aus der Informationsfreiheit, dass die Informationstätigkeit der Behörden rechtsgleich und willkürfrei zu erfolgen hat.[1136] 487

In der Schweiz hat – wie bereits an früherer Stelle ausgeführt – nach wie vor nicht jede Person einen Internetzugang oder regelmässigen Zugang zum Internet. Weiter vorne wurde bereits erwähnt, dass Personen ohne Internetzugang keine sensible Gruppe im Sinne von Art. 8 Abs. 2 BV darstellen.[1137] 488

1134 Siehe oben Rz. 155.

1135 Vgl. MÜLLER, BSK BV, Art. 180, N. 10.

1136 HERTIG, BSK BV, Art. 16, N. 28; vgl. etwa BGE 104 Ia 377, E. 2.

1137 Siehe dazu oben Rz. 218.

Stellt eine Behörde gewisse Informationen nur über ihre Website zur Verfügung, können allenfalls auch weitere Gruppen einer Benachteiligung ausgesetzt sein. Zu denken ist hier neben älteren Personen vor allem an sprachliche Minderheiten und Menschen mit Behinderung, welche in Art. 8 Abs. 2 BV ebenfalls explizit als sensible Gruppen genannt werden. Auch wenn diese Gruppen nicht unmittelbar durch die entsprechende Regelung benachteiligt sind, also keine unmittelbare Diskriminierung vorliegt, so können sie doch allenfalls mittelbar schlechter gestellt sein.[1138]

i) Alter

489 Dem Umstand, dass zum Zeitpunkt der Fertigstellung dieser Arbeit ältere und insbesondere hochaltrige Personen teilweise keine Computer oder andere technische Geräte besitzen oder nicht über genügend technisches Knowhow verfügen, um diese zu bedienen, könnte der Staat entgegenwirken, indem er diese Personen etwa mit den entsprechenden Geräten ausstattet[1139] oder Kurse anbietet, um die entsprechenden Kenntnisse aufzubauen (sog. digital literacy).[1140] Verweigert sich eine Person indes aus irgendwelchen Gründen dem Internet ganz, so ist keine Handhabe ersichtlich, um dagegen vorzugehen. Aus diesem Grund ist es wohl zumindest aus Gründen des Diskriminierungsverbots nicht ohne Weiteres denkbar, dass Informationen lediglich über das Internet verbreitet werden können. Gerade wichtige Informationen, etwa Warnungen vor einer gefährlichen Viruserkrankung, müssen daher neben dem Internet etwa auch noch über Radio und Fernseher, Medienkonferenzen oder Medienmitteilungen bekanntgegeben werden, so dass sie zumindest über diese Kanäle auch für diejenigen Bevölkerungsteile zugänglich bleiben, welche keinen Internetzugang haben.[1141] Dies hat insbesondere dort zu gelten, wo die entsprechende Information mit der Ausübung von Rechten verbunden ist, etwa beim Versand des «Abstimmungsbüchleins» an sämtliche Stimmberechtigten.[1142]

1138 Siehe dazu ebenfalls oben Rz. 461.

1139 Auch wenn hierauf kein einklagbarer Anspruch besteht, vgl. Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 4.2.

1140 Vgl. etwa in Dänemark, wo entsprechende Kurse angeboten werden, da im Rahmen der E-Government-Strategie nur noch digital mit dem Staat kommuniziert werden soll; vgl. NATIONAL INTEROPERABILITY FRAMEWORK OBSERVATORY, E-Government in Denmark, S. 21.

1141 LANGER, AJP, 2014, S. 951 und 958.

1142 LANGER, AJP, 2014, S. 951 und 958; siehe dazu sogleich weiter unten Rz. 495.

ii) Sprache

Die Websites des Bundes, der Kantone und – sofern sie solche haben – der Gemeinden und die Informationen, welche auf diesen verfügbar sind, werden oftmals nur in gewissen Sprachen zugänglich gemacht.[1143] Personen, welche diese Sprachen nicht verstehen, könnten daher allenfalls aufgrund ihrer Sprache diskriminiert sein. Art. 180 Abs. 2 BV macht keine Vorgaben darüber, welche Sprachen die Behörden in ihrer Informationstätigkeit verwenden müssen. Es besteht lediglich die Verpflichtung, dass die Information verständlich sein, das heisst von den Adressaten auch verstanden werden können muss.[1144] Daraus ergibt sich wohl zumindest implizit, dass sie in einer Sprache zu erfolgen hat, welche von den Adressaten verstanden werden kann. Auf Bundes- und auf kantonaler Ebene wird in der Regel in Verfahrens- oder speziellen Sprachengesetzen[1145] festgelegt, dass die Kommunikation mit den Behörden in den jeweiligen Amtssprachen zulässig ist.[1146] 490

Mit Blick auf eine allfällige Diskriminierung können bei der Informationstätigkeit wohl keine höheren Standards verlangt werden. Es ist davon auszugehen, dass sich die meisten Personen zumindest in einer Amtssprache verständigen, diese grob verstehen oder sich entsprechende Erklärungen verschaffen können. Daher sollte es unter diesem Gesichtspunkt als ausreichend gelten, wenn die entsprechenden Informationsangebote in den jeweiligen Amtssprachen verfügbar sind. Die Übersetzung der Website in weitere Sprachen wird zwar teils angeboten, kann aber aus Verhältnismässigkeitsgründen wohl nicht gefordert werden.[1147] Meines Erachtens sprechen jedoch bei sehr wichtigen Informationen, welche die gesamte Bevölkerung erreichen müssen, auch Verhältnismässigkeitsüberlegungen dafür, dass diese etwa in die Sprachen grösserer Sprachminderheiten übersetzt oder mittels leicht verständlicher Piktogramme erklärt werden.[1148] 491

1143 So ist etwa die Website des Bundes (www.admin.ch) aktuell in Deutsch, Französisch, Italienisch, Rumantsch und Englisch verfügbar.

1144 MÜLLER, BSK BV, Art. 180, N. 18.

1145 Vgl. für den Bund etwa das Bundesgesetz über die Landessprachen und die Verständigung zwischen den Sprachgemeinschaften (Sprachengesetz, SpG, SR 441.1) vom 5. Oktober 2007.

1146 Derartige Einschränkungen sind in erster Linie unter dem Aspekt der Sprachenfreiheit (Art. 18 BV) zu betrachten und werden grundsätzlich als zulässig erachtet, vgl. CARONI/HEFTI, BSK BV, Art. 18, N. 23.

1147 LANGER, AJP, 2014, S. 951 f.

1148 So wurden etwa im Rahmen der Coronavirus-Pandemie wichtige Informationen auch in diversen weiteren Sprachen bereitgestellt (Albanisch, Polnisch etc.) und mit Piktogrammen versehen; vgl. etwa die COVID Informationen des Bundesamts für Gesundheit.

iii) Behinderung

492 Zu guter Letzt könnte auch Menschen mit Behinderungen bis zu einem gewissen Grad der Zugang zu Informationen erschwert oder verunmöglicht werden, wenn dieser nur noch über das Internet erfolgen würde. Auch Personen mit Behinderungen stellen eine durch Art. 8 Abs. 2 BV geschützte Gruppe dar. Gemäss Art. 8 Abs. 4 BV hat das Gesetz Massnahmen zur Beseitigung der Benachteiligung von Behinderten vorzusehen. Konkretisiert wird dieser Gesetzgebungsauftrag in erster Linie durch das Behindertengleichstellungsgesetz. Dieses verpflichtet den Bund, seine Dienstleistungen benachteiligungs- bzw. barrierefrei anzubieten (Art. 3 lit. e i.V.m. Art. 2 Abs. 4, 11 und 12 Abs. 3 BehiG). Art. 14 Abs. 2 BehiG sieht darüber hinaus gar explizit die Pflicht vor, dass Dienstleistungen, welche der Bund im Internet anbietet, für Sehbehinderte zugänglich zu machen sind. Die ausführende Bestimmung in Art. 10 BehiV weitet diese Verpflichtung aus und konkretisiert, dass Information sowie die Kommunikations- und Transaktionsdienstleistungen über das Internet grundsätzlich für Sprach-, Hör- und Sehbehinderte sowie motorisch Behinderte zugänglich sein müssen.[1149] Die Betreiber der Websites haben im Rahmen dieser Gesetze also gewisse Vorkehrungen zu treffen, um die Angebote diskriminierungsfrei auszugestalten. Ihre Grenze findet diese Pflicht allerdings in der Verhältnismässigkeit. Dies bedeutet vorliegend, dass eine Massnahme im vorliegenden Zusammenhang nicht ergriffen werden muss, wenn der wirtschaftliche Aufwand im Verhältnis zum erzielbaren Nutzen klar überwiegt.[1150] Auch dies dürfte wohl hinsichtlich sehr wichtiger Informationen, welche die ganze Bevölkerung erreichen müssen, allerdings anders zu beurteilen sein.

iv) Fazit

493 Eine Erbringung der gesamten Informationstätigkeit über das Internet dürfte wohl insbesondere hinsichtlich wichtiger und mit der Ausübung weiterer Rechte verbundener Informationen im jetzigen Zeitpunkt und auf absehbare Zeit kaum mit dem Diskriminierungsverbot vereinbar sein. Hinsichtlich der Diskriminierung wegen der Sprache oder Behinderungen setzt die konkretisierende Gesetzgebung zwar durch das Verhältnismässigkeitsprinzip gewisse Grenzen, jedoch dürfte auch hier bei sehr wichtigen Informationen ein überwiegendes Interesse der Betroffenen an der Information allfällige Wirtschaftlichkeitsüberlegungen klar überwiegen.

1149 BOLFING/HEINSER/GIUDICE/RITTER, Schweizer Accessibility-Studie 2016, S. 53; vgl. weiterführend: SCHEFER/HESS-KLEIN, S. 285 ff.

1150 LANGER, AJP, 2014, S. 952.

3. Informationsfreiheit

Weiter oben wurde ausgeführt, dass die ausschliessliche Online-Publikation gegen die Informationsfreiheit gemäss Art. 16 Abs. 3 BV verstossen kann, sofern dadurch Informationen aus allgemein zugänglichen Quellen betroffen sind.[1151] Ein Eingriff kann insbesondere dann vorliegen, wenn staatliche Informationspflichten bestehen. Diese können sich z.B. aus grundrechtlichen Überlegungen ergeben. So anerkennt der EGMR aus Art. 8 EMRK gewisse grundrechtliche Schutzpflichten des Staates, welche auch eine Informationspflicht hinsichtlich von technologischen Gefahren oder Naturgefahren beinhalten können.[1152] Dies umfasst die Pflicht, dass die Betroffenen aktiv und rechtzeitig über die entsprechenden Risiken informiert werden.[1153] In der Schweiz geht die Lehre weitgehend davon aus, dass sich eine solche Pflicht auch aus Art. 10 BV bzw. Art. 13 BV ergibt.[1154] Im Weiteren garantiert Art. 34 Abs. 2 BV die freie Willensbildung vor Volksabstimmungen. Diese umfasst auch eine Pflicht in der Vorbereitung des Urnengangs, den Bürgern aufgrund der Beratungsfunktion der Regierung bzw. ihrer Verwaltung amtliche Erläuterungen über den Abstimmungsgegenstand zur Verfügung zu stellen.[1155] Das Bundesgericht hatte sich bisher lediglich betreffend die Online-Publikation amtlicher Publikationsorgane unter dem Aspekt der Informationsfreiheit mit dieser Frage zu befassen. Dabei hat es den damit verbundenen Eingriff in die Informationsfreiheit als leicht eingestuft.[1156] Gerade für den Fall, dass indes zusätzlich andere Grundrechtspositionen betroffen sind, etwa weil ein Kanton die Verteilung von Abstimmungsinformationen lediglich noch über einen Internetkanal durchführen möchte, ist diese Einschätzung m.E. nicht in Stein gemeisselt. 494

B. Information über Social Media

Das soeben Ausgeführte hat auch zu gelten, falls der Staat ausschliesslich über seine Social-Media-Plattformen informieren möchte. Hier sind indes noch einige zusätzliche Überlegungen anzustellen. 495

1151 Siehe dazu oben Rz. 221.

1152 Vgl. etwa Urteil des EGMR vom 19. Februar 1998, 14967/89, Guerra/Italien, N. 60; Urteil des EGMR vom 30. November 2004, 48939/99, Öneryildiz/Türkei (wobei hier Art. 2 EMRK als verletzt erachtet wurde).

1153 MEYER-LADEWIG/NETTESHEIM, Meyer/Ladewig EMRK, Art. 8, N. 19, mit Hinweisen auf die Rechtsprechung in FN 55.

1154 SCHWEIZER, SG Komm. BV, Art. 10, N. 53; DIGGELMANN, BSK BV, Art. 13, N. 28.

1155 TSCHANNEN, BSK BV, Art. 34, N. 33.

1156 Vgl. zum Ganzen: Urteil des BGer 1C_137/2018 vom 27. November 2018, E. 4.2.

1. Diskriminierungsverbot

496 Betreffend das Diskriminierungsverbot ist neben dem bereits Ausgeführten zu beachten, dass auf diesem Kanal der Unterschied in der Verbreitung zwischen Jung und Alt ohne Zweifel noch deutlich grösser ist, was eine Diskriminierung wegen des Alters wahrscheinlich erscheinen lässt. Erschwerend kommt zudem hinzu, dass der Staat bei seinen Websites selbst bestimmen kann, in welchen Sprachen er deren Inhalte anbietet und welche Massnahmen er zur Barrierefreiheit vorsieht. Bei der Informationstätigkeit über eine Social-Media-Plattform ist er nur ein weiterer Benutzer, der sich mit der Registrierung den Regeln des jeweiligen Anbieters unterstellt. Dieser Betreiber kann grundsätzlich selbst entscheiden, in welchen Sprachen er die Plattform anbietet und ob er diese barrierefrei ausgestaltet.[1157]

497 Wie weiter oben ausgeführt, ist das schweizerische Recht dabei grundsätzlich auch für die Social-Media-Plattformen anwendbar, wobei diese in der Regel nicht direkt an die Grundrechte gebunden sind, sich eine indirekte Drittwirkung jedoch aus dem Gesetzesrecht ergeben kann.[1158] So verwirklicht etwa das Behindertengleichstellungsgesetz in einem gewissen Masse das Diskriminierungsverbot auch gegenüber Privaten, indem Art. 6 BehiG vorsieht, dass öffentlich angebotene Dienstleistungen diskriminierungsfrei zugänglich sein müssen.[1159] Das Problem ist indes – wie bereits beschrieben – die Rechtsdurchsetzung gegenüber den Betreibern.[1160] Anzumerken ist an dieser Stelle, dass die bekanntesten sozialen Netzwerke heutzutage in verschiedenen Sprachen verfügbar und teilweise auch barrierefrei ausgestaltet sind.[1161] Hinsichtlich der Sprache der eigenen Beiträge auf Social-Media-Plattformen ist jedoch immer noch der Staat verantwortlich und hat sich daher an die oben genannten Vorgaben zu halten.[1162] Zusammenfassend lässt sich indes festhalten, dass Social-Media-Plattformen aus Sicht des Diskriminierungsverbots noch weniger als das Internet an sich als alleinige Informationsplattform des Staates geeignet sind. Das Argument, dass durch die Information über Social-Media-Angebote ein Adressatenkreis angesprochen werden kann, welcher ansonsten nicht erreicht wird, und somit keine Diskriminierung geschaffen, sondern diese viel mehr abgebaut wird,[1163] überzeugt nicht. Es ist aktuell und

1157 LANGER, AJP, 2014, S. 952.
1158 Siehe dazu oben Rz. 191 ff.
1159 Botschaft VI Gleiche Rechte, S. 1780.
1160 Siehe oben Rz. 120.
1161 Vgl. etwa für Facebook.
1162 Siehe oben Rz. 490.
1163 Vgl. LANGER, AJP, 2014, S. 958.

wäre in naher Zukunft unter dem Aspekt des Diskriminierungsverbots nicht zulässig, dass der Staat seine gesamte Informationstätigkeit nur über das Internet oder gar über soziale Medien wahrnimmt.

2. Informationsfreiheit

Bezüglich eines Eingriffs in die Informationsfreiheit lässt sich feststellen, dass die Nutzung dieser Plattformen in der Regel zwar ebenfalls kostenfrei möglich ist und somit für viele Personen wie die Information über die Website der Behörde eine Erleichterung des Informationszugangs gegenüber der Zeitung oder dem Amtsblatt darstellt. Erschwerend ist jedoch zu beachten, dass viele der sozialen Medien eine Registrierung vorsehen. Zwar ist diese – wie bereits an anderer Stelle ausgeführt – in der Regel nicht obligatorisch, um die entsprechenden Inhalte angezeigt zu erhalten. Eine gewisse Ermutigung zur Registrierung findet durch die ständig präsente Werbung der Plattformen und die zusätzlichen Möglichkeiten («Liken» oder Kommentieren von Beiträgen) nach der Registrierung aber dennoch statt. Anderseits besitzen viele der Nutzenden bereits aus anderen Gründen ein entsprechendes Konto. Dennoch ist mehr noch als bei der grundsätzlichen Informationstätigkeit über das Internet auch hier von einem Eingriff in die Informationsfreiheit auszugehen. 498

Sehen spezielle gesetzliche Grundlagen eine Publikation etwa des Amtsblatts lediglich noch per Internet vor, so verweisen sie in der Regel explizit auf die Internetsite des Kantons.[1164] Es ist höchst fraglich, ob darunter auch dessen Social-Media-Präsenz subsumiert werden kann. Meines Erachtens müssen die entsprechenden Bestimmungen restriktiv ausgelegt werden und nur den Internetauftritt des Kantons im eigentlichen Sinne umfassen. Dies insbesondere, weil sich bei einer Publikation über ein soziales Medium auch weitere Fragen hinsichtlich der Datensicherheit und des Datenschutzes stellen müssten, welche die Behörden nicht alleine gewährleisten können.[1165] Wo keine spezielle Grundlage eine entsprechende Einschränkung vorsieht, wäre gestützt auf die allgemein gehaltenen gesetzlichen Grundlagen eine Information lediglich über die sozialen Medien grundsätzlich zulässig. Einschränkend wirkt sich – wie soeben ausgeführt – aus, wenn die Information mit der Wahrnehmung von Rechten verbunden ist. Im Rahmen der Verhältnismässigkeit sprechen unter anderem die bereits weiter oben ausgeführten datenschutzrechtlichen Bedenken gegen eine exklusive Nutzung von Social-Media-Plattformen. Eine Information lediglich über Social Media ist unter dem Gesichtspunkt der Informationsfreiheit daher – falls überhaupt – lediglich bei 499

1164 Vgl. etwa den oben erwähnten § 15 Abs. 1 und Abs. 3 PublG ZH (Rz. 217).

1165 Vgl. dazu weiter oben Rz. 195 und 211.

oberflächlichen Informationen bedenkenlos zulässig (etwa beim Teilen von Landschaftsbildern aus dem Kanton), wobei sich hier wiederum die Frage nach dem praktischen Nutzen stellt.[1166]

C. Fazit

500 Eine Information über das Internet kann in gewissen Bereichen helfen, Informationen für ein grösseres Publikum und vor allem einfacher und rascher zugänglich zu machen. Wird jedoch ausschliesslich über das Internet informiert, kann dies für diejenigen Personen, welche keinen Zugriff auf dieses Medium haben, einerseits eine Diskriminierung und anderseits einen Eingriff in die Informationsfreiheit darstellen. Genauer zu betrachten ist dabei jeweils der Aspekt der Verhältnismässigkeit. Insbesondere dort, wo weitere Grundrechtspositionen oder die Ausübung anderer Rechte betroffen sein könnten, hat eine sorgfältige Abwägung stattzufinden. Während es durchaus zulässig scheint, gewisse Daten, welche nicht direkt mit der Ausübung von Rechten verbunden sind, lediglich über das Internet zu publizieren, müssen wichtige Informationen – etwa die Warnung der Bevölkerung oder Abstimmungsinformationen – zwingend alle Bewohner erreichen können, was bei der Internetkommunikation zum aktuellen Zeitpunkt noch nicht gewährleistet ist. Es bleibt zu beachten, dass es sich beim hier getroffenen Fazit um eine Momentaufnahme handelt. Es ist gut möglich, dass dies etwa in fünf oder zehn Jahren aufgrund der steigenden Verbreitung des Internets und der wachsenden Fähigkeiten der Bevölkerung im Umgang damit anders beurteilt werden kann.

II. Behördenkommunikation über das Internet

501 Es ist zulässig, dass Behörden und Bürgern ausserhalb geregelter Verwaltungsverfahren über das Internet – etwa per E-Mail oder über Social-Media-Plattformen – kommunizieren. Sofern dabei jedoch Personendaten betroffen sind, sind die Datenschutzgesetzgebung und insbesondere der Aspekt der Datensicherheit zu beachten. Dies gilt einerseits für E-Mails, welche nicht per se als sicherer Kanal gewertet werden können und daher gegebenenfalls einer zusätzlichen Verschlüsselung benötigen. Im vermehrten Masse gilt dies anderseits auch für soziale Medien. Hier ist der Staat bekanntermassen lediglich ein Nutzer des Plattformangebots und hat sich wie auch die Nutzenden den Regeln dieser Plattformen etwa hinsichtlich der Datennutzung zu unterwerfen.[1167]

1166 Vgl. WEWER, ZRP, 2016, S. 25.

1167 Vgl. zum Ganzen oben Rz. 122.

Die elektronische Kommunikation hat aber auch für beide Seiten Vorteile gegenüber der hergebrachten schriftlichen Kommunikation, indem die Kommunikation beschleunigt wird und sich etwa Kosten für Postsendungen sparen lassen. Daher ist es vorstellbar, dass eine Behörde Kommunikation auch ausserhalb des Verfahrens lediglich noch über E-Mail zulassen möchte und sich etwa vorbehält, auf briefliche Anfragen nicht mehr zu antworten. Während dies in der Schweiz soweit ersichtlich bei keiner Behörde der Fall ist, haben andere Länder wie Dänemark entsprechende Umstellungen bereits vorgenommen.[1168] Im Folgenden soll daher geprüft werden, welche rechtlichen Schwierigkeiten damit verbunden sein könnten. 502

A. Behördenkommunikation ausschliesslich über Internet

Eine Regelung, welche eine Kommunikation mit den Behörden nur noch über einen bestimmten Kanal zulässt, könnte unter Umständen gewisse Gruppen, welche nicht über diesen Kanal verfügen, von der Kommunikation ausschliessen. In diesem Fall wäre sie nicht mit dem Diskriminierungsverbot (Art. 8 Abs. 2 BV) vereinbar. Weiter oben wurde dargestellt, dass die Behörden wichtige Informationen, welche etwa mit der Ausübung von Rechten verbunden sind, nicht ausschliesslich über das Internet verbreiten dürfen. Diese Informationen müssen auch für Personen zugänglich bleiben, welche keinen Internetzugang haben oder diese Technologie nicht bedienen können.[1169] Dasselbe hat a fortiori auch für die Kommunikationstätigkeit zu gelten. Es muss für alle Personen möglich sein, mit den Behörden zu kommunizieren. Lässt eine Behörde nur noch die Kommunikation per E-Mail zu, so könnte sie unter Umständen durch gewisse Personen nicht mehr erreicht werden. Wie bereits an früherer Stelle ausgeführt wurde, sind verschiedene Anknüpfungspunkte denkbar, in denen durch das Diskriminierungsverbot geschützte Gruppierungen speziell betroffen sein könnten (Alter, Behinderung, Sprache).[1170] 503

Für die betroffenen Personen muss Abhilfe geschaffen werden, damit ihnen die Kommunikation mit der Behörde weiterhin möglich bleibt. Die in Dänemark getroffene Regelung sieht etwa vor, dass gewisse Bevölkerungsgruppen davon befreit sind, das «digitale Postfach» nutzen zu müssen, etwa wenn sie aufgrund einer Behinderung dazu nicht in der Lage oder obdachlos sind bzw. aus anderen Gründen keinen Internetanschluss haben.[1171] Es besteht jedoch kein Rechtsanspruch darauf, das System nicht nutzen zu 504

1168 Siehe dazu oben Rz. 485.

1169 Siehe dazu oben Rz. 490 ff.

1170 Siehe dazu weiter oben Rz. 492 ff.

1171 Siehe etwa Life in Denmark, Digital Post.

müssen.[1172] Sollte in der Schweiz eine entsprechende Regelung eingeführt werden, müssten ebenfalls Übergangs- und Ausnahmeregelungen vorgesehen werden, damit keine unzulässige Diskriminierung gewisser Bevölkerungsgruppen stattfindet, welche dadurch von der Kommunikation mit den Behörden ausgeschlossen wären.

B. Sperrung von Benutzern auf Social-Media-Plattformen

505 Bei der staatlichen Behördenkommunikation über Social-Media-Plattformen stellt sich das spezifische Problem, dass gewisse Beiträge auf den jeweiligen Sites unter Umständen andere Personen in ihren Rechtsgütern verletzen oder dem Staat aus anderen Gründen nicht genehm sind. Die Plattformen sehen die Möglichkeit vor, entsprechende Beiträge zu löschen und die betreffenden Personen von der Site auszuschliessen. Während straf- oder zivilrechtlich relevante Äusserungen auch durch staatliche Stellen gestützt auf die jeweilige Strafnorm gelöscht werden dürfen, gibt es Beiträge («Posts»), bei welchen dieser Schutz nicht greift. Mangels einer entsprechenden gesetzlichen Grundlage dürfen staatliche Stellen hierzulande diese Beiträge nicht löschen oder die Personen nicht sperren und müssen daher auf ein Handeln der Plattformbetreiber hoffen.[1173]

506 Das Problem, wie der Staat mit rechtswidrigen Inhalten und Fake News auf Plattformen der sozialen Medien umgehen soll, stellt sich weltweit. Inhalte, die etwa zur Gewalt aufrufen, oder rassendiskriminierende Mitteilungen, gelten als sogenannte «Hate Speech» und sind in den meisten Ländern ebenfalls illegal.[1174] Jedoch ist nicht immer klar erkennbar, wann die entsprechenden Grenzen überschritten sind. Des Weiteren müssen gerade bewusste Falschaussagen nicht zwingend straf- oder zivilrechtlich relevant sein. Es besteht ein weiter Konsens, dass die Verbreitung von «Fake News» über soziale Medien ein Problem für die Demokratie darstellen kann.[1175] Dies hat dazu geführt, dass in vielen Ländern Gesetze verabschiedet wurden, um diese Phänomene in den Griff zu bekommen, wobei verschiedene Herangehensweisen gewählt wurden. Im Folgenden sollen nun diese Regelungen vorgestellt und es soll dargelegt werden, ob diese für die Schweiz allenfalls als Vorbild dienen können.

1172 Vgl. etwa IT-Politisk Forening, New Danish law will make digital communication with the public sector mandatory.

1173 Siehe zum Ganzen oben Rz. 273 ff.

1174 Bericht Social Media 2017, S. 17.

1175 OSZE, Joint declaration on freedom of expression and "fake news", disinformation and propaganda.

1. Regulierung in anderen Ländern

In Deutschland werden die Betreiber von Social-Media-Plattformen bei der Bekämpfung von unerlaubten Inhalten durch das Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz, NetzDG) stärker in die Pflicht genommen. Dieses Gesetz sieht vor, dass die Plattformen ein Verfahren einbauen, durch das Benutzende rechtswidrige Inhalte melden können. Die Betreiber müssen dafür sorgen, dass gemeldete Beiträge innerhalb einer gewissen Frist gelöscht werden. Was als rechtswidriger Inhalt gilt, wird dabei anhand gewisser Delikte des Strafgesetzbuchs definiert.[1176] In Frankreich wurde ein Gesetz verabschiedet, welches in Wahlkampfzeiten Politikern und Politikerinnen sowie Kandidierenden eine einfache Möglichkeit einräumen soll, gegen Inhalte vorzugehen, welche sie betreffen. Zudem wurden den Plattformbetreibern ebenfalls zusätzliche Pflichten auferlegt.[1177] Weiter gehen Länder etwa in Südostasien, welche das Verbreiten von Fake News mit Gefängnisstrafen oder hohen Geldbussen bestrafen wollen, wobei es z.B. in Singapur der Regierung obliegt festzulegen, was als «Fake News» gilt und was nicht.[1178] Die EU geht ihrerseits einen anderen Weg und hat mit dem «Code of Practice on Disinformation» ein Regelungswerk zur Selbstregulierung der grössten Anbieter von Online-Plattformen und sozialen Medien geschaffen, welche sich verpflichten, Falschinformationen effizient zu löschen und ihre Anstrengungen im Kampf gegen Fake News nachzuweisen.[1179] 507

2. Rechtlich Bewertung der bestehenden Regelungen

Die meisten dieser Gesetze wurden bereits bei ihrer Verabschiedung hinsichtlich ihrer Vereinbarkeit mit der Meinungsfreiheit kritisch betrachtet.[1180] Der «UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression» beurteilt staatliche Regulierungsvorhaben, wie sie aktuell gelten oder in Planung sind, generell als kritisch im Hinblick auf die Meinungsfreiheit.[1181] Die in Straftatbeständen oft nur vage definierten Begriffe wie Terrorismus oder «Fake News» können aus seiner Sicht als Vorwand verwendet werden, um einen legitimen Diskurs zu 508

1176 KALSCHEUER/HORNUNG, NVwZ, 2017, S. 1722.

1177 Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

1178 UKROW, MMR-Aktuell, 2019.

1179 Vgl. eta den Code of Practice on Disinformation der EU.

1180 Vgl. etwa für Deutschland KALSCHEUER/HORNUNG, NVwZ, 2017, für Frankreich: CUENI, ex ante, 2019, S. 13 ff.

1181 KAYE, Report Mai 2016; KAYE, Report April 2018.

unterbinden.[1182] Da die Staaten die Deutungshoheit darüber haben, was unter den jeweiligen Begriff fällt, könnte dies dazu führen, dass Private oder Unternehmen aus Vorsichtsgründen auch Inhalte zensieren, die nicht unter den jeweiligen Tatbestand fallen, und somit Selbstzensur üben.[1183] Als fraglich wird zudem erachtet, ob entsprechende Regelungen mit dem Bestimmtheitsgrundsatz vereinbar sind.[1184] Auch die Schaffung zusätzlicher Pflichten für die Betreiber der Plattformen (wie etwa im deutschen NetzDG) ist nicht unbedenklich, da ebenfalls die Gefahr besteht, dass eigentlich nicht rechtswidrige Inhalte aus Angst vor einer Busse gesperrt werden.[1185] Ein weiteres Problem ist die oftmals globale Ausrichtung der Social-Media-Unternehmen. Dies führt dazu, dass Staaten ungeachtet der Staatsgrenzen Löschungen verlangen und somit auch ausserhalb ihres Staatsgebiets Handlungen vornehmen können, die geeignet sind, in die Meinungsfreiheit einzugreifen.[1186]

509 Diese Kritikpunkte haben den «Special Rapporteur» dazu bewogen, verschiedene Empfehlungen zuhanden der UN-Mitgliedstaaten zu verfassen, bei deren Beachtung entsprechende Regulierungen mit der Meinungsfreiheit vereinbar sind. So sollen keine Gesetze erlassen werden, welche Meinungsäusserungen kriminalisieren oder unangemessen einschränken. Es soll zudem nicht den Verwaltungsbehörden obliegen zu bestimmen, was eine rechtmässige Meinungsäusserung darstellt. Im Weiteren sollen staatliche Löschungen von Inhalten nur zulässig sein, wenn sie durch eine unabhängige Gerichtsbehörde nach dem Durchlaufen eines fairen Prozesses angeordnet wurden.[1187] Vielmehr solle auf die Unternehmen so eingewirkt werden, dass sie von sich aus in ihrem Handeln den Menschenrechten mehr Beachtung schenken.[1188] Das französische Gesetzesvorhaben geht hier teilweise in die richtige Richtung, indem es Transparenzvorschriften hinsichtlich politischer Werbung und Geldflüsse schafft. Doch auch bei diesem Gesetz können die Massnahmen, welche Politikern und Kandidaten im Vorfeld der Wahlen offenstehen, um missliebige Beiträge löschen zu lassen, im Widerspruch zum Grundsatz einer freien und ungehinderten Diskussion stehen.[1189] In diesem Zusammenhang sind die «Guiding Principles on Business and the Human Rights»[1190]

1182 KAYE, Report April 2018, S. 6.
1183 KAYE, Report Mai 2016, S. 11.
1184 STAFFLER, MMR-Aktuell, 2017.
1185 KAYE, Report April 2018, S. 7.
1186 KAYE, Report April 2018, S. 7 f.
1187 KAYE, Report April 2018, S. 19 f.
1188 KAYE, Report Mai 2016, S. 22.
1189 CUENI, ex ante, 2019, S. 13.
1190 UN doc A/HRC/17/31.

zu erwähnen. Diese setzen einen globalen Standard des menschenrechtskonformen Verhaltens für Unternehmen und enthalten Vorgaben an die Mitgliedsstaaten und Unternehmen zur Vorbeugung und Bekämpfung von Menschenrechtsverletzungen. Zu beachten ist indes, dass dieses Regularium keine rechtsverbindlichen Vorgaben enthält und somit «soft law» darstellt.[1191] Allenfalls in die richtige Richtung gehen könnte der Ansatz zur Selbstregulierung, wie ihn die EU mit dem «Code of Practice on Disinformation» verfolgt, findet hier doch immerhin im Code selber eine Definition des Begriffs der Desinformation statt und wird die Wichtigkeit der Meinungsfreiheit betont.[1192] Jedoch wird auch hier kritisiert, dass das entsprechende Regelungswerk aufgrund seines weiten Anwendungsbereichs nicht unproblematisch ist.[1193] Zudem ist der Rechtsschutz der von einer Löschung Betroffenen ebenfalls nicht stark ausgebaut.[1194]

3. Fazit

Es bleibt festzustellen, dass ein Gesetz, welches die staatliche Löschung von (nicht eindeutig illegalen) Äusserungen auf sozialen Plattformen oder die gesetzliche Verpflichtung der Betreiber zur Löschung vorsieht, aus Sicht der Meinungsfreiheit in jedem Fall problematisch bleibt. Ein entsprechendes Gesetz wandert immer auf dem schmalen Grat zwischen Meinungsfreiheit und staatlicher Zensur. Der Fokus der Staaten sollte darauf liegen, die Unternehmen zur Transparenz und zum Vorsehen interner Verfahren zu bewegen.[1195] Eine bessere Einhaltung der Menschenrechte durch vor allem global tätige Unternehmen, wie sie die nicht verbindlichen «Guiding Principles» vorsehen, wäre auf jeden Fall wünschenswert. Unter diesem Aspekt ist der im Social-Media-Bericht 2017 des Bundesrats bezugnehmend auf Europarats-Generalsekretär Jaagland gezogene Schluss, dass es in erster Linie an den Betreibern der sozialen Medien liegt, mehr Verantwortung zu übernehmen, anstatt staatliche Regelungen vorzusehen, durchaus und meines Erachtens mit Nachdruck vertretbar.[1196] 510

Inwiefern dies aufgrund der grossen Marktmacht von Facebook und weiteren Social-Media-Betreibern realistisch ist, muss an dieser Stelle dahingestellt bleiben. Immerhin hat etwa Facebook im Rahmen der Corona-Virus-Pandemie 2020 durchaus Bereitschaft gezeigt, von sich aus strikter gegenüber 511

1191 KAYE, Report April 2018, S. 5.

1192 GLOBAL PARTNERS DIGITAL, The EU's Code of Practice on Disinformation: First thoughts.

1193 CUENI, ex ante, 2019, S. 16.

1194 GLOBAL PARTNERS DIGITAL, The EU's Code of Practice on Disinformation: First thoughts.

1195 KAYE, Report April 2018, S. 19.

1196 Bericht Social Media 2017, S. 17.

Falschmeldungen vorgehen zu wollen und können, wenn dies der Umgang mit dem Thema aus seiner Sicht erfordert.[1197] Hervorgehoben sei in diesem Zusammenhang auch die Rolle und Verpflichtung der Medien, welche als «public watchdog» Falschmeldungen entgegenwirken sollen.[1198]

C. Einsatz von Chatbots

1. Einsatzbereiche

512 Algorithmen werden nach dem bereits Ausgeführten inzwischen vielfältig eingesetzt, um einfache, sich wiederholende Verwaltungsaufgaben zu automatisieren und zu vereinfachen. Auch im Bereich der Kommunikation mit der Bevölkerung sind Behörden oft mit wiederkehrenden Fragestellungen konfrontiert und publizieren daher Merkblätter oder «FAQ» auf den jeweiligen Websites. Algorithmen können hier zusätzliche Möglichkeiten eröffnen, indem sogenannte «Chatbots» angeboten werden können, um mit der Bevölkerung zu kommunizieren.[1199] Hierbei handelt es sich um einen Software-Code, der so geschrieben ist, dass er sich wiederholende und klar definierte Abläufe auf Befehl hin automatisch vollziehen und diese Abläufe in einer Konversation mit einem realen Gegenüber ausführen kann.[1200] Die entsprechenden Systeme führen dabei aufgrund von vorprogrammierten Regeln und Dialogdefinitionen durch das Gespräch und können basierend auf den Eingaben des Benutzers Rückfragen stellen oder Antworten erteilen.[1201] In vielen Bereichen der Verwaltung bestehen für häufig gestellte, einfach zu beantwortende Fragen in der Regel oft bereits umfassende Entscheidungsbäume, welche technisch mit wenig Aufwand in eine Konversationsumgebung eingebaut werden können.[1202]

513 Dies bietet den Beteiligten verschiedene Vorteile. Einerseits können wiederkehrende Fragen durch den Algorithmus allenfalls effizienter beantwortet werden, was zu einer Entlastung des Personals führt, welches sich somit auf komplexere Aufgaben konzentrieren kann.[1203] Zudem bietet der Bot einen

1197 Vgl. Etwa THEILE, Facebook verschärft Kampf gegen Corona-Fake-News, Frankfurter Allgemeine Zeitung, 16. April 2020.

1198 HOLZNAGEL, MMR, 2018, S. 21; Bericht Social Media 2017, S. 18.

1199 Vgl. etwa den Chatbot der SVA St. Gallen.

1200 RINGEISEN/BERTOLOSI-LEHR/DEMAJ, Swiss Yearbook of Administrative Sciences, 2018, S. 53.

1201 FELFERING/STETTINGER/WUNDARA/STANIK, in: Handbuch E-Government, S. 501.

1202 RINGEISEN/BERTOLOSI-LEHR/DEMAJ, Swiss Yearbook of Administrative Sciences, 2018, S. 52.

1203 RINGEISEN/BERTOLOSI-LEHR/DEMAJ, Swiss Yearbook of Administrative Sciences, 2018, S. 54, MARTINI, in: Verwaltungspraxis und Verwaltungswissenschaft, S. 49.

wichtigen Vorteil gegenüber der Information z.B. über FAQ auf der Website, indem es beiden Seiten in einer laufenden Interaktion möglich ist, Nachfragen zu stellen, falls etwas unklar ist.[1204] Sollte die Beantwortung einer Frage durch den Chatbot nicht möglich sein, so kann die Anfrage immer noch an einen menschlichen Bearbeitenden weitergegeben werden, welcher damit bereits im Besitz der relevanten Informationen aus der Interaktion mit dem Chatbot ist. Anderseits kennt der Chatbot keine Büroöffnungszeiten, ist für die Rechtssuchenden also grundsätzlich rund um die Uhr verfügbar.[1205] Denkbar ist zudem, dass aufgrund von früheren Anfragen und dem Abruf von nutzerspezifischen Daten entsprechende Systeme auch für den jeweiligen Nutzer massgeschneiderte Empfehlungen aussprechen[1206] oder gar zugrundeliegende Emotionen verarbeiten und berücksichtigen können.[1207] Technisch realisierbar und in der Privatwirtschaft bereits praktiziert wird, dass entsprechende Chat-Systeme aus den Eingaben der Benutzenden lernen und sich somit durch maschinelles Lernen weiterentwickeln.[1208] Schliesslich ist es bei entsprechenden Softwarelösungen in der Regel möglich, dass diese auf verschiedenen Plattformen eingebaut werden können, etwa auf der eigenen Website oder über Facebook, was die potenzielle Reichweite des Chatbots erhöht.[1209]

Entsprechende Anwendungen sind bisher wie erwähnt in erster Linie in 514
der Privatwirtschaft verbreitet. In der Verwaltung finden sich noch nicht viele Beispiele. Im Rahmen der eidgenössischen Parlamentswahlen 2019 beantwortete der Chatbot «Parli» Fragen rund um die Wahlen.[1210] Dabei konnte indes lediglich auf vorgefertigte Fragen zurückgegriffen werden.[1211] Weiter gehen die Pilotprojekte der SVA St. Gallen und der Stadt Adliswil ZH, die einen Chatbot einsetzen, welcher auch auf Benutzerfragen reagieren kann.[1212] In anderen Ländern werden entsprechende Systeme bereits in verschiedenen Bereichen flächendeckend eingesetzt.[1213]

1204 FELFERING/STETTINGER/WUNDARA/STANIK, in: Handbuch E-Government, S. 502.

1205 Ringeisen/Bertolosi-Lehr/Demaj, Swiss Yearbook of Administrative Sciences, 2018, S. 54.

1206 HILL, VM, 2018, S. 289.

1207 FELFERING/STETTINGER/WUNDARA/STANIK, in: Handbuch E-Government, S. 502.

1208 MARTINI, in: Verwaltungspraxis und Verwaltungswissenschaft, S. 49.

1209 RINGEISEN/BERTOLOSI-LEHR/DEMAJ, Swiss Yearbook of Administrative Sciences, 2018, S. 55.

1210 Bundesversammlung, Wahlbot Parli.

1211 BRAUN BINDER, SJZ, 2019, S. 471.

1212 RINGEISEN/BERTOLOSI-LEHR/DEMAJ, Swiss Yearbook of Administrative Sciences, 2018, S. 58 f.

1213 Vgl. etwa den Chatbot «Amelia», welcher in einem britischen Bezirk mit einem gewissen Erfolg Bürgeranfragen beantwortet, BITKOM E. V., KI Gipfelpapier S. 51.

2. Rechtliche Probleme

515 Wie bereits ausgeführt, sind die Behörden in der Ausgestaltung ihrer Kommunikation grundsätzlich frei, sofern diese allen Personen in gleicher Weise offensteht. Wenn also ein Chatbot als zusätzliche Möglichkeit angeboten wird, um mit der Verwaltung in Kontakt zu treten, ohne dass andere Kanäle wie Telefon oder persönlicher Kontakt nicht mehr zugelassen werden, ist dessen Nutzung durchaus zulässig.[1214] Indes können sich bei der Nutzung von Chatbots durchaus rechtliche Fragen stellen, welche weiteren Regelungsbedarf nach sich ziehen.

a) Informationelle Selbstbestimmung

516 Bei der Kommunikation mit einem «Chatbot» werden in verschiedener Weise auch Personendaten bearbeitet, so dass die Vorgaben der Datenschutzgesetzgebung zu beachten sind. Einerseits können oder müssen die Benutzenden je nach Ausgestaltung des Bots und der Fragestellungen, welche damit beantwortet werden sollen, Daten über sich selbst eingeben. Auf diese Weise kann der Bot ihnen bestenfalls direkt helfen, ein Formular auszufüllen, welches danach an die zuständige Stelle weitergeleitet wird.[1215] Ebenfalls ist es möglich, dass die von den Benutzenden auf diese Weise eingegebenen Daten zwischengespeichert werden, um an den zuständigen Sachbearbeiter weitergegeben werden zu können, falls der Chatbot die Frage nicht zufriedenstellend beantworten kann. Im Gegensatz zur Datenbearbeitung über Online-Formulare oder Behördenportale stellen sich hierbei keine zusätzlichen Probleme, so dass auf die weiter vorne erfolgten Ausführungen verwiesen werden kann.[1216]

517 Relevant sein können für Verwaltungsstellen, welche entsprechende Chatbots anbieten, unter Umständen auch die jeweiligen Hintergrunddaten, also etwa, von wem, mit welchem Browser und wie lange entsprechende Angebote in Anspruch genommen werden. Wie weiter oben bereits abgehandelt wurde, setzen sie zu diesem Zweck oft Webtracking-Programme ein. Wie ebenfalls bereits im Laufe dieser Arbeit betont, ist der Einsatz entsprechender Applikationen datenschutzrechtlich zumindest dann fragwürdig, wenn keine genügend klare gesetzliche Grundlage für die Datenbearbeitung besteht.[1217] Ebenfalls denkbar ist insbesondere bei Chatbots, welche sich mithilfe von maschinellem Lernen weiterentwickeln, dass Daten und

1214 Siehe weiter oben Rz. 248.

1215 Vgl. BITKOM E. V., KI Gipfelpapier, S. 51.

1216 Siehe oben Rz. 155 ff. und 320 ff.

1217 Siehe dazu weiter oben Rz. 190 ff.

Eingaben der Benutzenden als Trainingsdaten weiterverwendet werden sollen. Eine Weiterverwendung der Daten zu Trainingszwecken, auch wenn sie ursprünglich rechtmässig erhoben und bearbeitet wurden, ist dabei zumindest ohne vorgängige Anonymisierung nicht mit dem Zweckbindungsgrundsatz vereinbar.[1218]

Zudem ist es technisch möglich, entsprechende Chatbots neben der eigenen Website auch über andere Plattformen wie Facebook zur Verfügung zu stellen.[1219] Hierbei stellen sich die Probleme, dass die Kommunikation auf diese Weise nur denjenigen möglich ist, welche über ein Facebook-Konto verfügen, was unter dem Aspekt des Diskriminierungsverbots problematisch sein könnte. Hierbei ist indes zu beachten, dass es sich lediglich um ein Zusatzangebot handelt und die Fragen auch weiterhin auf normalen Weg per E-Mail, Telefon oder persönlichem Kontakt beantwortet werden können.[1220] Im Weiteren ist zu beachten, dass die Interaktion mit dem «Verwaltungsbot» bei einer Einbindung auf einer entsprechenden Plattform auch den jeweiligen Datenschutzrichtlinien (etwa von Facebook) untersteht.[1221] Da Betreiber von Social-Media-Plattformen sich – wie weiter oben bereits ausgeführt – aufgrund ihrer Nutzungsbedingungen weitgehende Datennutzungsrechte einräumen lassen, stellt sich insbesondere bei sensiblen Vorgängen indes die Frage, ob eine Implementierung auf Facebook etc. datenschutzrechtlich vertretbar ist.[1222] Auch wenn die entsprechenden Daten allenfalls an den Betreibern «vorbeigeschleust» werden könnten,[1223] ist daher von einer Verwendung auf einer entsprechenden Plattform aus datenschutzrechtlicher Warte abzusehen. Im Weiteren gilt es für die Speicherung und Bearbeitung der entsprechenden Daten selbstverständlich auch die Grundsätze des Datenschutzrechts zu beachten, wobei insbesondere die Sicherheit der Nutzerdaten jederzeit gewährleistet sein muss (Art. 7 DSG). Die entsprechenden rechtlichen Probleme können indes kaum abstrakt beurteilt werden, ohne die Ausgestaltung entsprechender Lösungen im Einzelfall zu kennen. Abschliessend lässt sich resümieren, dass der Einsatz von Chatbots durchaus datenschutzkonform

518

1218 Siehe oben Rz. 191.

1219 Dies wurde im Rahmen der bereits erwähnten Pilotprojekte anfänglich auch gemacht; vgl. RINGEISEN/BERTOLOSI-LEHR/DEMAJ, Swiss Yearbook of Administrative Sciences, 2018, S. 59 und 60.

1220 Für eine weitere Diskussion dieses Aspekts siehe weiter oben Rz. 218 ff.

1221 RINGEISEN/BERTOLOSI-LEHR/DEMAJ, Swiss Yearbook of Administrative Sciences, 2018, S. 61; siehe zu dieser Problematik ausführlich bereits weiter oben Rz. 122 f.

1222 RINGEISEN/BERTOLOSI-LEHR/DEMAJ, Swiss Yearbook of Administrative Sciences, 2018, S. 61.

1223 RINGEISEN/BERTOLOSI-LEHR/DEMAJ, Swiss Yearbook of Administrative Sciences, 2018, S. 55.

erfolgen kann, wenn die oben genannten Kautelen etwa hinsichtlich des Einsatzes von Webtracking oder der Verwendung von Trainingsdaten beachtet werden.

b) Haftung

519 Von den «Chatbots» verspricht man sich in der Literatur neben Effizienzgewinnen eine fehlerfreiere und diskriminierungsfreie Kommunikation.[1224] Dies ist durchaus denkbar, da der Chatbot immer anhand derselben vordefinierten Regeln handelt. Dennoch ist nicht ausgeschlossen, dass ein Chatbot eine fehlerhafte Auskunft erteilt, welche bei der jeweiligen Person zu einem Schaden führt, sei es aufgrund von fehlerhafter Programmierung des Chatbots oder aufgrund eines kommunikativen Missverständnisses. Nicht zuletzt besteht bei maschinell lernenden Systemen auch ein Missbrauchspotenzial. Dies zeigt etwa das Beispiel von Microsofts Chatbot «Tay», welcher von den Benutzenden innerhalb von wenigen Stunden mit gezielten Fragen und Aussagen zum Rassisten «umerzogen» wurde und danach deaktiviert werden musste.[1225] In diesem Zusammenhang ergibt sich die Frage, inwiefern der Staat für Schäden haften muss, welche er durch den Einsatz von Algorithmen oder künstlicher Intelligenz verursacht.

520 Problematisch ist dabei, dass die Verwaltung zwar von den entsprechenden Technologien profitiert, aber teilweise gar nicht mehr die Kontrolle darüber hat, wie ein entsprechender Algorithmus handelt. Die Frage nach der Haftung für künstliche Intelligenz wurde bisher insbesondere im privatrechtlichen oder strafrechtlichen Zusammenhang bearbeitet.[1226] Eine Auseinandersetzung mit den Auswirkungen auf die Staatshaftung fand bisher kaum statt. Indes sind im hier vorliegenden Zusammenhang aufgrund des aktuellen Stands der Technik zumindest für den Autor keine Anwendungsbeispiele ersichtlich, in denen die Aussage eines staatlichen Chatbots zu einer direkten Schädigung der Betroffenen führen kann, weswegen eine ausführliche Diskussion dazu hier unterbleiben soll.

521 Wohl häufiger als ein direkt durch den Chatbot verursachter Schaden wird es vorkommen, dass eine Person sich aufgrund der Kommunikation mit einem Chatbot zu einer Disposition entschliesst, die ihr einen finanziellen Nachteil einbringt. Dies etwa, indem der Chatbot eine falsche Information

1224 Vgl. etwa FELFERING/STETTINGER/WUNDARA/STANIK, in: Handbuch E-Government, S. 501.

1225 Vgl. etwa VINCENT, Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day, The Verge, 24. März 2016.

1226 Vgl. etwa GORDON/LUTZ, SZW, 2020; HORNER/KAULARTZ, InTeR, 2016; SIMMLER/MARKWALDER, Zeitschrift für die gesamte Strafrechtswissenschaft, 2017.

erteilt, welche die Person dann zur Einreichung eines ungültigen kostenpflichtigen Gesuchs verleitet. Entsprechende Konstellationen sind – wie weiter oben ausgeführt wurde – unter dem Titel des Vertrauensschutzes zu behandeln und sorgen dafür, dass Betroffene unter Umständen in ihrem Vertrauen auf eine behördliche Auskunft geschützt werden, wenn ihnen dadurch ein Schaden erwuchs.[1227] Generell lässt sich eine Auskunft durch einen Chatbot in vielen Punkten nicht von der konventionellen Auskunft durch einen Verwaltungsangestellten unterscheiden. Zu beachten ist in diesem Zusammenhang, ob die entsprechende Behörde für die Auskunft zuständig war oder der Betroffene dies zumindest nach Treu und Glauben annehmen durfte. In jedem Fall spricht der Einsatz des jeweiligen Chatbot-Systems auf der Website deutlich dafür, dass die Behörde für die Fragen, welche dieser beantworten kann, eine Zuständigkeit übernimmt. Es liegt auch an der Behörde sicherzustellen, dass der Chatbot lediglich Fragen beantworten kann, für welche die Behörde auch zuständig ist. Meist wird bereits durch die vorgegebene Programmierung – welche, wie weiter oben ausgeführt, auf Entscheidungsbäumen basiert – verhindert, dass er auf nicht themenbezogene Fragen verbindlich antworten kann, und dafür gesorgt, dass er in diesen Fällen oder bei Unklarheiten auf eine menschliche Beratung verweist. Bei fortschrittlichen KI-Systemen wäre es denkbar, dass das System selbständig aufgrund der verarbeiteten Daten lernt, auf eine bestimmte Frage eine Auskunft zu geben. Dabei stellt sich die Frage, inwiefern die jeweilige Amtsstelle diese Antwort im Nachhinein noch nachvollziehen kann. Diese Thematik könnte unter Umständen eine beträchtliche Ausweitung staatlicher Vertrauenshaftung nach sich ziehen. Auch selbstlernende Systeme müssten daher in der Programmierung so ausgestaltet sein, dass es ihnen nicht möglich ist, auf Fragen eine Antwort zu geben, welche nicht im Zuständigkeitsbereich der jeweiligen Behörde liegen.

Zusätzliche Probleme einer haftungsrechtlichen Zuweisung kann das 522
Erfordernis bereiten, dass die entsprechende Auskunft eine konkrete Angelegenheit betreffen und vorbehaltslos erfolgen muss. Hier kann im Gegensatz zu «FAQ» oder Formularen auf der Website eine Chatbot-Konversation durchaus eine konkrete Angelegenheit betreffen und ist entsprechend weniger problematisch. Bei der Vorbehaltslosigkeit ist wohl ebenfalls damit zu rechnen, dass die verantwortliche Behörde einen Haftungsausschluss oder «Disclaimer» einbaut, um zu signalisieren, dass sie nicht an die Aussagen des Chatbots gebunden sein möchte. Wie weiter oben ausgeführt, stellt sich indes die

1227 Für eine genauere Auseinandersetzung insbesondere mit den Voraussetzungen des Vertrauensschutzes siehe oben Rz. 287 ff.

Frage, ob entsprechende Disclaimer rechtskonform die Haftung ausschliessen können.[1228]

3. Fazit

523 Ein Einsatz von Chatbots durch die öffentliche Verwaltung ist zulässig, sofern es sich dabei um ein Zusatzangebot handelt. Je nach Ausgestaltung des Chatbots können sich indes Fragestellungen ergeben, welche eine zusätzliche rechtliche Regelung notwendig machen oder noch ungelöste rechtliche Probleme mit sich bringen. Insbesondere müssen entsprechende Chatbots datenschutzkonform ausgestaltet sein. Dazu zählt, dass die in Frage stehenden Personendaten durch die Behörde erhoben werden dürfen und wie sie allenfalls für eine weitere Verwendung gespeichert werden. Werden entsprechende Angebote in eine Facebook-Site eingebunden, so können sich aufgrund der zusätzlichen Datenflüsse weitere, rechtlich noch nicht zufriedenstellend gelöste Probleme ergeben. Ebenfalls noch ungeklärt sind Fragen nach der Haftung und dem Vertrauensschutz. Hierbei gilt zu beachten, dass Betroffene in der Regel auch bei der Aussage eines Chatbots in ihrem Vertrauen geschützt sein können. Meines Erachtens lassen sich diese noch offenen rechtlichen Aspekte indes vor dem Hintergrund der allgemeinen Rechtsgrundsätze, der einschlägigen Gesetzgebung, Praxis und Literatur zum Haftungsrecht lösen. Je technisch fortgeschrittener entsprechende Angebote werden, desto schwieriger dürfte es zudem werden, sie von realen Beamten zu unterscheiden. Auch aus diesem Grund wird richtigerweise gefordert, dass Bots explizit als solche gekennzeichnet werden sollen, um Vorbehalte von Privaten gegenüber den digitalen Assistenten abzubauen.[1229]

III. Zusammenfassung

524 Die Digitalisierung der Behördeninformation und -kommunikation ist bereits fortgeschritten und akzeptiert, auch wenn – wie in § 3 ersichtlich – noch einige offene Rechtsfragen existieren. Zusätzliche Problematiken können sich stellen, wenn ein Gemeinwesen sich entschliesst, ausschliesslich online informieren oder kommunizieren zu wollen. Dies ist insbesondere aufgrund des Diskriminierungsverbots aktuell noch nicht übergreifend zulässig, da zumindest die wichtigsten Informationen (etwa Wahl- und Abstimmungsbüchlein oder die Warnung vor Naturgefahren) der gesamten Bevölkerung zugänglich bleiben müssen. Eine entsprechende Ausgestaltung der Information würde

1228 Siehe dazu oben Rz. 290 ff.

1229 Vgl. GUCKELBERGER, S. 120.

aktuell in erster Linie ältere Menschen betreffen. Jedoch können sich auch aus den Bedürfnissen von anderssprachigen Menschen oder Personen mit Behinderung gewisse Anforderungen an die Ausgestaltung entsprechender Webangebote ergeben. Bei weniger wichtigen Informationen dürfen hier allerdings Verhältnismässigkeitsüberlegungen miteinbezogen werden. Auch die Behördenkommunikation sollte aus ähnlichen Überlegungen aktuell nicht auf den Online-Kanal beschränkt werden. Diese Aussage basiert auf einer Momentaufnahme, welche sich aufgrund neuer technischer Möglichkeiten und der wachsenden «digital literacy» wohl in einigen Jahren anders präsentieren dürfte. Auch dann werden jedoch für Personen, welchen die digitalen Kanäle nicht offenstehen, Übergangs- oder Ausweichlösungen gefordert sein.

Noch ungelöst ist das Problem der Sperrung von Benutzenden auf Social- 525
Media-Plattformen durch staatliche Stellen. Bisher verabschiedete Regelungen in anderen Staaten bewegen sich oft am Grat zur staatlichen Zensur und zeigen, wie schwierig es ist, eine Regelung zu finden, welche die Meinungsfreiheit vollständig wahrt. Eine entsprechende Regelung müsste den Betroffenen in jedem Fall einen klar ersichtlichen Rechtsweg bieten. Gefordert sein dürften in diesem Zusammenhang indes auch die privaten und oft mächtigen Betreibenden der entsprechenden Dienste, welche ihre bestehenden Richtlinien mit Nachdruck durchsetzen sollen. Zunehmend relevant wird auch der Einsatz von Chatbots. Während sich dieser zumindest bei datenschutzkonformer Ausgestaltung mit der Rechtsordnung vereinbaren lässt, sind Fragen betreffend etwa die Haftung noch nicht abschliessend geklärt. Je potenter entsprechende Dienste werden, desto wichtiger ist es auch, darauf hinzuweisen, dass der Private sich gerade mit einer Maschine statt einem Menschen unterhält.

§8 Elektronischer Rechtsverkehr

Das VwVG erlaubt – wie bereits ausgeführt wurde – seit der Revision vom 526
17. Juni 2005 die Möglichkeit der elektronischen Einreichung von Eingaben. Eine Übergangsbestimmung sah vor, dass der Bundesrat während zehn Jahren nach dem Inkrafttreten die Möglichkeit, Eingaben den Behörden elektronisch zuzustellen, auf Verfahren vor bestimmten Behörden beschränken kann. Diese Übergangsfrist ist mittlerweile abgelaufen.[1230] Grundsätzlich ist der elektronische Rechtsverkehr auf Bundesebene seit 2011 flächendeckend

1230 Vgl. dazu die Schlussbestimmungen zur Änderung des VwVG vom 17. Juni 2005, welche per 1. Januar 2007 in Kraft traten; AS 2006 2197, S. 2228.

zulässig.[1231] Auch auf kantonaler Ebene lässt inzwischen ein beträchtlicher Anteil der Kantone die Möglichkeit zu, Verfahrenshandlungen elektronisch vorzunehmen.[1232] Zu beachten ist dabei, dass zur Identifikation der jeweiligen Person unter Umständen weitere Vorkehrungen, wie etwa eine elektronische Unterzeichnung ihrer Eingabe oder die Eingabe eines Passworts im Rahmen eines Behördenportals, notwendig sein können.[1233]

527 Betrachtet man genauer, wie stark einzelne Verfahren bereits online abgewickelt werden, so lassen sich gemäss der nationalen E-Government-Studie erhebliche Unterschiede feststellen. Dienstleistungen wie das Ausfüllen von Steuererklärungen oder das Bestellen von Registerauszügen werden bereits von einem grossen Teil der Bevölkerung online durchgeführt oder zumindest in Betracht gezogen. Hingegen geben viele der befragten Personen an, komplexere Anträge wie Baubewilligungen oder Arbeitsbewilligungen nicht online abzuwickeln.[1234] Zu beachten ist dabei zweifellos, dass viele Bürger mit diesen Dienstleistungen wesentlich weniger in Berührung kommen als mit der jährlich einzureichenden Steuererklärung. Sobald die Betroffenen sich in einem formellen Verfahren befinden, ist indes davon auszugehen, dass die Kommunikation in erster Linie nicht elektronisch geschieht. Beim Bundesgericht etwa wurden lediglich ca. 50 von 8'000 jährlichen Beschwerden elektronisch eingereicht.[1235] Somit muss festgestellt werden, dass viele Bürger bzw. Fachleute die bestehenden Möglichkeiten nicht oder nur teilweise nutzen.[1236]

528 Dabei können verschiedene Gründe dazu führen, dass die Verbreitung des elektronischen Behördenkontakts nicht in gewünschtem Masse erreicht wurde und von vorhandenen Möglichkeiten kein Gebrauch gemacht wird. Im Rahmen der Studie befragte Personen geben insbesondere mangelndes Vertrauen in die Datensicherheit und eine schlechte Einbindung und Dokumentation der jeweiligen Angebote als Grund für die Nichtnutzung an. Ein weiterer wichtiger Faktor ist, dass die Verwendung in vielen Fällen an weitere Voraussetzungen gebunden ist, um die Identität der jeweiligen Person sicherzustellen, etwa eine Registrierung oder eine elektronische Signatur.[1237] Dies ist zwar mit Blick auf die Anforderungen an die Echtheit und die Integrität

1231 Vgl. etwa die Übersicht der Bundeskanzlei zum elektronischen Rechtsverkehr.

1232 Vgl. etwa für eine Übersicht per Ende 2016: Elektronischer Behördenverkehr im Kanton Bern.

1233 Siehe weiter oben Rz. 318.

1234 BUESS/RAMSDEN/BIERI, S. 28.

1235 Vgl. Geschäftsbericht BGer 2019, S. 11; andere Gerichte wie das BVGer erfassen die elektronischen Beschwerden im Jahresbericht nicht separat.

1236 Bericht Bischof, S. 3.

1237 Vgl. BUESS/RAMSDEN/BIERI, S. 34.

der Daten durchaus richtig, erschwert aber insbesondere Laien die Benutzung der entsprechenden Kanäle. Ebenfalls gegen eine Verwendung entsprechender Dienste sprechen können damit verbundene Zusatzkosten oder das Risiko hinsichtlich der Fristenwahrung.[1238]

Der zweite Grund, welcher weiter oben bereits angesprochen wurde, ist 529
die Rechtszersplitterung im Bereich des Verwaltungsrechts. Gerade für Laien ist nicht ersichtlich, ob im jeweiligen Rechtsbereich oder in ihrem Kanton eine elektronische Einreichung überhaupt zulässig ist. Sie müssen daher schlimmstenfalls damit rechnen, dass eine elektronische eingereichte Akte oder Beschwerde aus formellen Gründen nicht entgegengenommen wird.[1239] Dadurch, dass die entsprechenden Angebote durch die Privaten nur schwach genutzt werden, besteht drittens auch für die Behörden kein Anreiz, den elektronischen Rechtsverkehr wirksam voranzutreiben.[1240]

I. Ansätze zur Förderung des elektronischen Rechtsverkehrs in anderen Ländern

Es wird als unbefriedigend empfunden, dass die Möglichkeiten zu einer wei- 530
tergehenden Digitalisierung des Verwaltungsverfahrens bestehen, aber kaum genutzt werden.[1241] Andere Länder zeigen indes auf, dass den Gründen dieser Zurückhaltung entgegengewirkt und ein flächendeckender Einsatz von elektronischer Kommunikation erreicht werden kann. So ist in Dänemark durch den «Act on Public Digital Post» vorgeschrieben, dass jede Einwohnerin und jeder Einwohner über ein digitales Postfach zu verfügen hat, über das sämtliche Kommunikation mit den Behörden abgewickelt werden muss.[1242] Dies hat dazu geführt, dass über 90 % der Bevölkerung von Dänemark ihre Kommunikation mit den Behörden digital erledigen.[1243]

Der Kritik, dass viele Behördendienstleistungen nur mit einer aufwen- 531
digen Registrierung möglich seien, sind viele Länder mit übergreifenden staatlichen Identifikationslösungen begegnet, welche in erster Linie für E-Government-Dienste, unter Umständen aber auch für weitere Einsatzzwecke benutzt werden können. In Dänemark ist aus einer Kooperation zwischen den Banken und staatlichen Stellen ein Angebot namens «NemID» hervorgegangen,

1238 Siehe dazu weiter oben Rz. 317 und 342.

1239 Siehe dazu weiter oben Rz. 343.

1240 Vgl. Bericht Bischof, S. 6.

1241 Vgl. etwa PIESBERGEN, Justice – Justiz – Giustizia, 2018, S. 2.

1242 NATIONAL INTEROPERABILITY FRAMEWORK OBSERVATORY, E-Government in Denmark, S. 15.

1243 Vgl. oben Rz. 484.

welches nach dem Prinzip der Zwei-Faktor-Authentifizierung funktioniert, d.h., der Benutzende loggt sich mit Name und Passwort bei einer staatlichen oder privatwirtschaftlichen Dienstleistung ein und erhält dann via eine Codekarte oder App einen Zahlencode, um das Login zu komplettieren. Dieses Angebot wird von über 70 % der Einwohner Dänemarks genutzt.[1244] In Estland ist es gar grundsätzlich obligatorisch, eine elektronische Identität zu besitzen, weswegen 90 % der Esten deren Funktionen nutzen. Dabei gibt es verschiedene Ausgestaltungen der elektronischen Identität. Diese Lösungen können sowohl zur digitalen Authentifizierung gegenüber Behörden als auch für diverse private Zwecke (Reisedokument, Online-Einkauf) benutzt werden.[1245] Auch in Deutschland wird seit 2010 der Personalausweis mit einem eingebauten Chip ausgegeben, mit welchem die Authentifizierung im Internet gegenüber Behörden ermöglicht wird. Die entsprechende Option muss indes zuerst durch den Bürger aktiviert werden, was bisher bloss eine Minderheit getan hat.[1246]

532 Auch eine einheitliche Identifizierungslösung allein kann das Problem der mangelnden Verbreitung nicht lösen, wenn die entsprechenden Angebote nicht aufgefunden werden können, etwa weil sie über die jeweilige Website oder gar über Websites verschiedener Gemeinwesen verteilt sind. Daher sehen einige Staaten zentrale Portallösungen vor, welche die online verfügbaren Dienstleistungen sämtlicher Staatsebenen an einem Ort im Internet zentral zugänglich machen. Entsprechende Dienstleistungen können oftmals mit einem Login durch eine elektronische Identifizierungsmöglichkeit genutzt werden. So existiert in Österreich z.B. die Site «www.oesterreich.gv.at» (ehemals HELP.gv.at) als zentrale Anlaufstelle für sämtliche Bürger. Diese stellt einen behördenübergreifenden «One Stop Shop» für Online-Dienstleistungen dar, welcher anhand von verschiedenen Lebenssituationen Informationen, Dokumente und Formulare anbietet. Auf der Website sind verschiedene Dienstleistungen in einem durch ein «Single Sign-on» geschützten Bereich online durchführbar.[1247] Grossbritannien verfügt mit der Plattform GOV.uk ebenfalls über ein zentrales Portal, welches für alle vom Staat angebotenen Dienstleistungen

1244 NATIONAL INTEROPERABILITY FRAMEWORK OBSERVATORY, E-Government in Denmark, S. 27.

1245 NATIONAL INTEROPERABILITY FRAMEWORK OBSERVATORY, E-Government in Estonia, S. 27 f.

1246 Botschaft BGEID, S. 3941. Auch aus diesem Grund wurde im Jahr 2017 ein Gesetz zur Förderung des elektronischen Personalausweises beschlossen, welches unter anderem vorsieht, dass die elektronische Identifizierungsmöglichkeit standardmässig aktiviert ist; vgl. DIETRICH/MÜLLER/AKKAYA TÜRKAVCI/KRCMAR/BOBERACH/EXEL, S. 25.

1247 NATIONAL INTEROPERABILITY FRAMEWORK OBSERVATORY, E-Government in Austria, S. 25.

als «single point of contact» dient und laufend ergänzt wird.[1248] In Deutschland wurde im Jahr 2017 durch Art. 91c Abs. 5 des Grundgesetzes und das zugehörige Onlinezugangsgesetz (OZG) ebenfalls eine Grundlage für einen derartigen Portalverbund geschaffen.[1249]

533 Die bisher erwähnten Massnahmen können der Bevölkerung die Nutzung entsprechender Dienstleistungen erleichtern. Indes steht es den Bürgern immer noch frei, entsprechende Angebote nicht zu nutzen, wenn aus ihrer Sicht die Nachteile der Nutzung weiter überwiegen. Deswegen sind die Behörden gefordert, jene Angebote attraktiv und insbesondere datenschutzkonform auszugestalten. Zu beachten ist dabei, dass, wenn nicht eine kritische Grösse an Nutzenden erreicht wird, unter Umständen auch für die Behörde kein richtiger Nutzen darin besteht, die vorhandenen Angebote auszubauen. Hier könnte allenfalls ein Nutzungszwang für entsprechende Angebote Abhilfe schaffen. So besteht etwa in Dänemark – wie bereits erwähnt – grundsätzlich die Pflicht, dass sämtlicher Kontakt mit den Behörden über ein digitales Postfach erfolgt. Durch diese Vorgaben waren die Behörden auch gezwungen, ein möglichst grosses Portfolio an Online-Dienstleistungen zu schaffen.[1250] Auch andere Länder kennen Vorschriften, welche die Nutzung des elektronischen Kanals zumindest für gewisse Bevölkerungsgruppen (in der Regel Anwälte) vorschreiben. So wurde in Deutschland etwa das besondere elektronische Anwaltspostfach (beA) eingeführt.[1251] Seit 2018 besteht für Anwälte eine Pflicht, die für die Nutzung dieses Postfachs notwendigen Einrichtungen bereitzuhalten und auf diesem Wege an sie gerichtete Mitteilungen zur Kenntnis zu nehmen (passive Nutzungspflicht). Ab 2020 (bzw. je nach Bundesland 2022) soll eine aktive Nutzungspflicht folgen, d.h., dass Anwälte nur noch elektronisch mit Gerichten kommunizieren dürfen.[1252]

534 Nach dem soeben Ausgeführten bestehen verschiedene Anhaltspunkte, wie man den elektronischen Rechtsverkehr in der Schweiz voranbringen kann. Einerseits müssen die bestehenden rechtlichen und tatsächlichen Nutzungshindernisse abgebaut werden. Anderseits können Behörden und Private dazu gezwungen werden, gewisse Kanäle zu benutzen oder Voraussetzungen zu schaffen, damit diese effektiv genutzt werden können. Im Folgenden

1248 NATIONAL INTEROPERABILITY FRAMEWORK OBSERVATORY, E-Government in the UK, S. 28.

1249 Vgl. dazu etwa GUCKELBERGER, S. 306 ff; SCHLIESKY/HOFFMANN, DÖV, 2018; SIEGEL, DÖV, 2018.

1250 Siehe dazu weiter oben Rz. 530.

1251 Vgl. etwa: LUMMEL/FENSKE/BOYN, Jusletter IT, 25. Februar 2016.

1252 SIEGMUND, NJW, 2017, S. 3134. Diese Pflicht wurde in der Lehre lange kritisch betrachtet, vgl. etwa BROSCH, NJW, 2015.

soll betrachtet werden, welche Anstrengungen in der Schweiz in diese Richtungen unternommen werden bzw. ob und wie allenfalls im Ausland bewährte Lösungen in die Schweizer Rechtsordnung übernommen werden können.

II. Abbau tatsächlicher Hindernisse

535 Viele kantonale Stellen und Bundesstellen sehen bereits vor, dass man gewisse Dienstleistungen online auf der Website vornehmen oder beziehen kann. Teilweise verfügen sie dazu über einen mit einem Login geschützten Bereich, in welchem die Nutzenden Daten speichern oder den Stand ihrer Anliegen verfolgen können. Dieses Login kann dabei auf verschiedene Arten geschehen, etwa über die Eingabe eines Benutzernamens und eines Passworts oder aber über eine Zwei-Faktor Authentifizierung, bei welcher nach Eingabe der Logindaten zusätzlich ein Code auf das Smartphone gesendet wird. Hierbei kann jedes Gemeinwesen (und unter Umständen jede eine einzelne Dienststelle) eigene Lösungen vorsehen.[1253] Dies kann dazu führen, dass für verschiedene Dienstleistungen mehrere Konten erstellt werden. In einer Zeit, in welcher jede Person in der Regel bereits eine Vielzahl von Konten für die Nutzung privater Dienstleistungen hat, kann dies durchaus abschreckend wirken. Diesem Hindernis kann, wie der Blick ins Ausland zeigt, auf zwei verschiedene Weisen begegnet werden.

536 Einerseits kann für sämtliche verfügbaren Dienstleistungen eines Gemeinwesens oder sogar gesamtschweizerisch ein gemeinsames zentrales Anlaufportal geschaffen werden. Idealerweise sollten dabei alle Dienste über dieselben Zugangsdaten erreicht werden können, damit die Betroffenen sich nicht für jeden Dienst ein separates Kennwort merken müssen. Hierbei können die soeben vorgestellten zentralen Behördenportale anderer Länder als Vorbild genommen werden. Dieses Modell wird von seinen Befürwortern als besonders bürgerfreundlich propagiert, weil es unabhängig davon, ob eine Gemeinde-, Kantons- oder Bundesbehörde zuständig ist, nur noch eine Anlaufstelle geben soll.[1254] Es gilt zu beachten, dass die hier vorgeschlagenen Lösungen auch ausserhalb förmlicher Verwaltungsverfahren Einsatzmöglichkeiten haben. Da dadurch jedoch insbesondere eine Förderung des elektronischen Rechtsverkehrs anvisiert wird, sollen sie an dieser Stelle behandelt werden.

1253 Vgl. etwa Merkblatt Online-Portale.

1254 Vgl. dazu das Interview mit dem E-Government-Experten KONRAD WALSER in: FLÜCKIGER, «Die Daten sollen laufen, nicht die Bürger», Neue Zürcher Zeitung, 21. Februar 2015.

A. Zentrale Behördenportale

Verschiedene Kantone sehen bereits Behördenportale für kantonale (und teilweise auch kommunale) Dienstleistungen vor. Deren Einsatz und Ausgestaltung wird teilweise auch in spezifischen Gesetzen geregelt.[1255] Da diese jedoch immer nur gewisse Gemeinwesen umfassen, muss, z.B. wenn Dienstleistungen eines Gemeinwesen einer anderen Stufe in Anspruch genommen werden sollen, ein weiteres Konto für das andere Portal eröffnet werden, was aus Nutzendensicht verbesserungswürdig ist. Ein zentrales Behördenportal, wie in den genannten Beispielen aus anderen Ländern, existiert in der Schweiz in dieser Form noch nicht. In der Schweiz besteht mit «www.ch.ch» lediglich ein umfassendes Informationsangebot der Bundeskanzlei, welches den Einwohnern Informationen zu verschiedenen Rechtsbereichen bietet. Darunter sind auch Rechtsgebiete wie die Einbürgerung zu finden, bei welchen der Bund gemeinsam mit Kantonen und Gemeinden zuständig ist.[1256] Das Portal bietet indes keinen mit einem Login geschützten Bereich, in welchem beispielsweise Formulare direkt ausgefüllt und Verfahren angestossen werden können. Es erschöpft sich darin, generelle Informationen zur Verfügung zu stellen und für konkrete Anträge auf die zuständigen (auch kantonalen oder kommunalen) Behörden zu verweisen. Das Portal ist in seiner heutigen Form sehr heterogen, jedoch bestehen Bestrebungen, es zu einem erkennbaren Informationsverbund zusammenzufassen.[1257] Es ist noch nicht ersichtlich, ob dieser auch eine zentrale Login-Möglichkeit umfassen und z.B. direkt Formulare bereitstellen soll. 537

Im Hinblick auf ein entsprechendes Vorhaben könnte sich allenfalls problematisch erweisen, dass aufgrund des föderalistischen Staatsaufbau der Schweiz die jeweiligen Staatsebenen (Bund, Kanton, Gemeinden) je nach Rechtsbereich über unterschiedliche Kompetenzen verfügen. Die Errichtung einer einzigen zentralen Portallösung könnte für die Betroffenen Probleme hinsichtlich der Gewährleistung individueller Rechte nach sich ziehen. Es ist daher zu untersuchen, inwiefern sich eine zentrale, staatsebenenübergreifende Portallösung im bestehenden Rechtsrahmen überhaupt realisieren liesse. 538

Aktuell findet das Portal «ch.ch» seine rechtliche Grundlage in der «Öffentlich-rechtlichen Rahmenvereinbarung über die E-Government Zusammenarbeit in der Schweiz» zwischen Bund und Kantonen sowie der darauf 539

1255 Vgl. etwa das Gesetz über das Behördenportal des Kantons Solothurn (BehöPG, BGS 116.1).

1256 GLASER, ZSR, 2015, S. 264.

1257 Vgl. E-Government Schweiz, Zugang zu elektronischen Behördenleistungen.

basierenden Leistungsvereinbarung.[1258] Während diese Grundlage für die aktuelle Version als reines Informationsportal ausreicht, müssten für ein zentrales Portal mit Login-Möglichkeit insbesondere aus datenschutzrechtlichen Überlegungen gesetzliche Grundlagen geschaffen werden, welche Fragen wie den Aufbau, die Rechte und Pflichten von Nutzern und Behörden und die Verantwortlichkeit für oder die Speicherung der Daten verbindlich regeln.[1259] Aufgrund der Tatsache, dass eine entsprechende Lösung sowohl kommunale und kantonale als auch Bundeskompetenzen betreffen könnte, wäre zusätzlich die Frage der datenschutzrechtlichen Verantwortlichkeit für eine entsprechende Lösung zu regeln, also wer etwa für die Gewährung der Betroffenenrechte verantwortlich ist.[1260]

540 Eine entsprechende Regelung könnte mangels umfassender Kompetenz des Bundes im Verwaltungsrecht, welche es ihm erlaubt, organisatorische oder technische Vorgaben im Bereich des E-Government zu machen, nicht durch ein Bundesgesetz erfolgen.[1261] Sofern keine umfassende Bundeskompetenz geschaffen würde, ist es daher zielführender, die entsprechenden Punkte weiterhin in einer Vereinbarung zwischen Bund und Kantonen zu regeln, an welcher beide Seiten im Rahmen ihrer Kompetenzen mitwirken.[1262] Dabei könnte auf die bestehende Rahmenvereinbarung aufgebaut werden oder eine neue Vereinbarung geschaffen werden, welche die notwendigen Bereiche umfassend regelt. Welcher Lösung der Vorzug zu geben ist, müsste dabei je nach Ausgestaltung und Umfang des Portals entschieden werden. Im Rahmen einer entsprechenden Vereinbarung sind die beteiligten Parteien gleichberechtigt bei der Ausarbeitung des Portals, jedoch wäre eine solche vertragliche Regelung exekutivlastig und eine Änderung auch aus diesem Grund aufwendig.[1263]

541 Gegen eine solche Lösung werden auch aus rechtsstaatlicher Sicht Vorbehalte angebracht. Die bisher klar geregelte, behördliche Zuständigkeitsordnung soll die Bürger vor Machtmissbrauch durch den Staat schützen. Wird ein einheitlicher Ansprechpartner geschaffen, so kann dies dazu führen, dass Verantwortungszusammenhänge verschleiert werden.[1264] Für den

1258 Vgl. Öffentlich-rechtliche Rahmenvereinbarung über die E-Government Zusammenarbeit in der Schweiz 2020, 1.8 und 3.

1259 Vgl. weiter oben Rz. 324.

1260 Vgl. dazu Art. 16 Abs. 2 DSG, gemäss dem der Bundesrat die Verantwortlichkeit regeln kann, wenn Bund und Kantone gemeinsam Personendaten bearbeiten.

1261 Siehe dazu oben Rz. 67 ff.

1262 Rechtsgrundlagen IKT-Zusammenarbeit, S. 15.

1263 Rechtsgrundlagen IKT-Zusammenarbeit, S. 16.

1264 GUCKELBERGER S. 343.

betroffenen Privaten wäre allenfalls nicht mehr ersichtlich, an wen er sich etwa für die Erhebung von Rechtsmitteln wenden müsste oder wer haftbar ist für ihm durch staatliches Handeln zugefügten Schaden.[1265] Nach dem soeben Geschriebenen müsste also zumindest die Abwicklung des Verfahrens auf einer solchen Portalseite bei den Kantonen verbleiben, in deren Zuständigkeit das entsprechende Rechtsgebiet liegt.[1266] Zweifellos müsste dies indes in technischer Sicht entsprechend programmiert werden können, was ebenfalls einen Zusatzaufwand darstellt. Die entsprechenden Fragen und technischen Vorkehrungen müssten geklärt werden, bevor eine weitergehende Zentralisierung stattfindet. Indes bleibt zu beachten, dass die aktuellen Vorhaben im Rahmen der E-Government-Strategie bis 2023 in erster Linie darauf abzielen, das Portal «ch.ch» als Informationsportal zugänglicher und umfassender zu machen, ohne eine Zentralisierung der Angebote vorzusehen.[1267]

B. Erleichterung der elektronischen Identifizierung und Zertifizierung

Eine baldige Schaffung eines zentralen Behördenportals nach dem Vorbild anderer Staaten erscheint folgerichtig noch einige Jahre entfernt, was sich mit gewissen kompetenzrechtlichen Bedenken aufgrund des föderalistischen Staatsaufbaus der Schweiz begründen lässt, welche andere Staaten nicht in diesem Masse kennen. Solange weiterhin jeder Kanton eigene Portallösungen betreibt, könnte immerhin die elektronische Identifizierung dadurch erleichtert werden, dass übergreifende Login-Möglichkeiten im Sinne einer einheitlichen digitalen Identität geschaffen werden, anstatt dass jede Dienstleistung ein eigenes Login vorsieht. 542

Einige Kantone sehen bereits vor, dass man sich für deren Dienstleistungen mit der «Swiss ID» einloggen kann, welche sich nebenbei auch für gewisse private Angebote nutzen lässt.[1268] Sollen Dokumente rechtsgültig signiert werden müssen, bestehen zum jetzigen Zeitpunkt vier verschiedene Anbieter.[1269] Die Nutzung der entsprechenden Lösungen ist dabei für die Nutzenden mit einem Zusatzaufwand verbunden, sei es über zusätzlich notwendige Hardware oder über einen Registrierungsprozess. Es erstaunt daher nicht unbedingt, dass die entsprechenden Lösungen in der Schweiz nicht flächendeckend genutzt werden. [1270] 543

1265 GLASER, ZSR, 2015, S. 326.

1266 SCHLEISS, S. 319.

1267 Vgl. etwa die Abschlusspublikation zur E-Government-Strategie 2016–2019.

1268 Vgl. etwa den Produktbeschrieb der SwissID.

1269 Vgl. etwa Kühn in Digital Business Law Bites #1: Die elektronische Unterschrift.

1270 Vgl. DIETRICH/MÜLLER/AKKAYA TÜRKAVCI/KRCMAR/BOBERACH/EXEL, S. 29.

544 In anderen europäischen Ländern haben sich elektronische Identifizierungsdienste im Gegensatz zur Schweiz schon in grösserem Masse durchgesetzt. Daher hat der Bundesgesetzgeber erkannt, dass im Bereich der elektronischen Identifizierungsdienste Verbesserungspotenzial besteht und zu diesem Zweck ein Bundesgesetz über elektronische Identifizierungsdienste (BGEID) erarbeitet. Damit soll eine Basis für die Herausgabe von elektronischen Identifizierungsmitteln geschaffen werden, die es den Einzelnen ermöglichen, sich aufgrund staatlich bestätigter Daten im digitalen Raum zu identifizieren. Das Gesetz soll der Förderung des elektronischen Geschäftsverkehrs unter Privaten und Behörden dienen und auch den Behördenkontakt über virtuelle Schalter erleichtern.[1271] Die angestrebte Lösung basiert auf einem Zusammenwirken von Staat und Privaten. Es soll privaten Anbietern überlassen bleiben, die entsprechenden technischen Lösungen zur elektronischen Identifizierung zu kreieren, da sich der Staat dazu aufgrund des schnellen technologischen Wandels nicht in der Lage sieht. Es bleibt jedoch weiterhin den staatlichen Stellen vorbehalten, die Identität der beantragenden Personen im Rahmen der Ausstellung der E-Identität zu überprüfen und zu bestätigen. Weiter muss der Staat die Anbieter von entsprechenden Identifizierungsdiensten in einem strengen Verfahren anerkennen und regelmässigen Prüfungen unterziehen.[1272]

545 Da für die entsprechenden elektronischen Identifizierungsdienste verschiedene Einsatzbereiche sowohl im privaten Bereich als auch für den Kontakt mit Behörden vorgesehen sind, welche nicht alle dieselben Sicherheitsanforderungen erfüllen müssen, bestimmt der Gesetzesentwurf verschiedene Sicherheitsniveaus. Diese unterscheiden sich in erster Linie durch die mit dem Ausweis verknüpften Daten und die Anforderungen an die jeweiligen Login-Verfahren.[1273] Betont wird dabei, dass es sich bei den E-ID-Lösungen nicht um einen digitalen Pass handeln soll.[1274] Weitergehende Dienste, wie die elektronische Signatur, können von den zertifizierten Diensten ebenfalls angeboten werden, bleiben jedoch weiterhin im ZertES geregelt.[1275]

546 Das BGEID wurde von der Bundesversammlung am 27. September 2019 verabschiedet. Verschiedene Gruppen kündigten daraufhin an, das Referendum dagegen zu ergreifen, welches im Februar 2020 zustande kam. Entsprechend werden die Stimmbürger das letzte Wort zu diesem Gesetzesvorhaben

1271 Vgl. zum Ganzen: Botschaft BGEID, S. 3916.

1272 Botschaft BGEID, S. 3923.

1273 Botschaft BGEID, S. 3926 ff.

1274 Vgl. dazu die FAQ zur E-ID: BUNDESAMT FÜR JUSTIZ, FAQ E-ID.

1275 Botschaft BGEID, S. 3922.

sprechen.[1276] Die Ergreifung des Referendums lässt darauf schliessen, dass die Vorlage auch in rechtlicher Hinsicht nicht unbestritten ist. In den folgenden Kapiteln wird aufzeigt, welche rechtlichen und tatsächlichen Probleme sich bei der Gesetzesvorlage stellen. Zudem soll, auch mit Blick auf die Lösungen in anderen Ländern, betrachtet werden, ob der angedachten Lösung zur Schaffung digitaler Identitäten im BGEID Erfolg beschieden sein kann.

1. Elektronische Identität als Staatsaufgabe

Ein Hauptkritikpunkt derjenigen Gruppen, welche das Referendum ergriffen 547
haben, betraf die Aufgabenteilung zwischen Staat und Privaten. Da bei einer Ausstellung der digitalen Identitäten durch Private zur Identitätsfeststellung diverse – unter Umständen auch besonders schützenswerte – Personendaten an diese Aussteller bekanntgegeben werden müssten, solle der Identitätsnachweis und die Herausgabe von entsprechenden Ausweisen eine Staatsaufgabe darstellen und nicht an Private ausgelagert werden dürfen.[1277] Diese Frage war bereits im Rahmen des Vernehmlassungsverfahrens höchst umstritten.[1278] Der Gesetzgeber entschied sich trotz teilweise kritischer Rückmeldungen, die vorgesehene Aufgabenaufteilung zwischen Staat und Privaten zu belassen. In der Botschaft führte er dazu aus, dass die Überprüfung der Identität einer Person weiterhin Sache des Staates bleibe. Lediglich die Ausstellung der digitalen Identitäten würde durch die privaten Betreiber vorgenommen.[1279] Weiter verweist er auf die Probleme in anderen Staaten. Dort standen aufgrund von beschaffungsrechtlichen Vorgaben und der allfällig notwendigen Anpassung rechtlicher Grundlagen oftmals langwierige Verfahren im Kontrast zum raschen technologischen Wandel. Zudem seien entsprechende Projekte oft mit hohen Investitionskosten verbunden, wobei es auch bei staatlichen Lösungen keine Garantie für die Akzeptanz und Nutzung der entsprechenden Dienste gebe.[1280]

Der Begriff der staatlichen Aufgabe ist in der Bundesverfassung nicht 548
konkretisiert. Darunter zu verstehen sind im Wesentlichen alle Tätigkeitsfelder, die dem Gemeinwesen durch Verfassung oder darauf basierende Gesetzgebung zur Erfüllung zugewiesen werden.[1281] Was eine staatliche Aufgabe ist, kann sich aus dem Staatszwecke von Art. 2 BV, weiteren Zielbestimmungen

1276 Vgl. dazu die Mitteilung über das Zustandekommen des Referendums BGEID, BBl 2020 1285.

1277 Vgl. dazu die Website des Referendumskomitee E-ID.

1278 Vernehmlassungsbericht BGEID, S. 5 f.

1279 Botschaft BGEID, S. 3923.

1280 Botschaft BGEID, S. 3933 f.

1281 WALDMANN, BSK BV, Art. 35, N. 20.

der Verfassung oder konkreten Gesetzgebungsaufträgen oder Zweckbestimmungen ergeben. Auch die Menschenrechte können hierzu Vorgaben erhalten.[1282] Der Staat muss die ihm übertragenen Aufgaben grundsätzlich selbst wahrnehmen. Unter gewissen Umständen ist es jedoch zulässig, dass staatliche Aufgaben an Private übertragen werden können (sogenannte Privatisierung).[1283] Auf Bundesebene sieht Art. 178 Abs. 3 BV vor, dass Verwaltungsaufgaben durch Gesetz an Organisationen und Personen des öffentlichen oder des privaten Rechts übertragen werden können, die ausserhalb der Bundesverwaltung stehen. Die Bundesverfassung sieht dabei zumindest explizit keine materielle Schranke für die Aufgabenübertragung vor. Lehre und Praxis stehen einer derart schrankenlosen Aufgabenauslagerung indes überwiegend ablehnend gegenüber.[1284] Es wird argumentiert, dass gewisse Aufgabenbereiche dem Staat aufgrund seiner Souveränität zukommen und nicht zur freien Disposition stehen können. Es handelt sich dabei um sogenannte genuine oder notwendige Staatsaufgaben.[1285] Unterschieden werden diese genuinen Staatsaufgaben von den Gewährleistungspflichten. Während der Staat Erstere selbst ausführen muss, hat er bei Letzteren lediglich sicherzustellen, dass diese erfüllt werden. Kann er dies gewährleisten, so ist eine Übertragung an Private zulässig.[1286]

549 Beim Ausweis in Papierform weist die Gesetzgebung in der Form des Ausweisgesetzes die Herausgabe von Ausweispapieren und die damit verbundene Überprüfung der Identität von Personen dem Staat als Aufgabe zu. Das Ausweisgesetz stützt sich dabei auf die Kompetenz des Bundes zur Regelung des Erwerbs und Verlusts des Bürgerrechtes, aus welcher der Gesetzgeber die Kompetenz zur Ausgabe eines Ausweises ableitet, der die Staatsangehörigkeit nachweist.[1287] Auch wenn die Herausgabe der Ausweise in Papierform eine staatliche Aufgabe darstellt, muss nicht abgeleitet werden, dass auch die Herausgabe einer digitalen Identität zwingend Aufgabe des Staates ist. Während das Ausweisgesetz den Erwerb oder Verlust des Bürgerrechts regelt, handelt es sich bei den im BGEID geregelten digitalen Identitäten nicht um einen digitalen Pass.[1288] Daher kann man auch mehrere entsprechende

1282 SCHWEIZER, SG Komm. BV, Art. 35, N. 35.

1283 Vgl. etwa MÜLLER, BSK BV, Art. 178 N. 34.

1284 BIAGGINI, SG Komm. BV, Art. 178, N. 34.

1285 ZÜND/ERRASS, S&R, 2012, S. 175.

1286 KÄLIN/LIENHARD/WYTTENBACH, S. 78.

1287 Botschaft Ausweisgesetz, S. 4775. Diese Einordnung wird allerdings als fraglich erachtet; vgl. BIAGGINI, OFK BV, Art. 38, N. 7. Für Ausländerausweise ist die gesetzliche Grundlage wohl in Art. 41 AiG zu finden.

1288 Siehe oben Rz. 542.

digitale Identitäten besitzen, welche etwa über verschiedene Sicherheitsniveaus verfügen.[1289] Das E-ID-Gesetz regelt in seinem Verständnis in erster Linie das Verhältnis zwischen Staat und Privaten im Bereich der digitalen Identitäten.[1290]

Der Gesetzgeber geht davon aus, dass es sich beim Identitätsnachweis 550
über Personen, welche einen entsprechenden Ausweis beantragen, und der Herausgabe entsprechender Ausweise um zwei separate Teilaufgaben handle. Die erste Aufgabe erfülle der Staat weiterhin selbständig, sei doch eine neu zu schaffende Identitätsprüfungsstelle für die Überprüfung der Identität anhand von Registern des Bundes zuständig. Lediglich die Herausgabe der Ausweise als zweite Teilaufgabe werde von Privaten wahrgenommen.[1291] Dadurch, dass detaillierte Regelungen bestehen, unter welchen die jeweiligen Anbieter von Identitätsdienstleistungen anerkannt werden und Ausweise ausstellen dürfen, kann davon ausgegangen werden, dass der Bund indes auch in diesem Bereiche zumindest die Gewährleistung der ordentlichen Aufgabenerfüllung wahrnehmen will.

Die Übertragung dieser Aufgabe zur Erfüllung durch Private ist nach 551
dem soeben Geschriebenen unter den Voraussetzungen von Art. 178 Abs. 3 BV zulässig. Eine Übertragung wäre ausgeschlossen, wenn es sich bei der Herausgabe von digitalen Identitäten um eine genuine Staatsaufgabe handeln würde. Nach der hier vertretenen Ansicht gehört die Ausstellung digitaler Identitäten in der vorgesehenen Form, welche also nicht als digitaler Pass zu verstehen ist, nicht zur staatlichen Kernverwaltung. Insbesondere ist mit der Übertragung dieser Aufgabe kein Übergang staatlicher Zwangsbefugnisse an Private verbunden.[1292] Nach dem bisher Ausgeführten wird es daher als zulässig erachtet, dass lediglich die Überprüfung der Identität als staatliche Aufgabe verbleibt, während die Herausgabe durch Private vorgenommen wird.

Art. 178 Abs. 3 BV fordert explizit, dass die Übertragung einer Aufgabe in 552
einem referendumsfähigen Erlass geregelt sein muss.[1293] Darüber hinaus enthält die Bestimmung keine weiteren expliziten Voraussetzungen. Diese ergeben sich jedoch aus allgemeinen rechtsstaatlichen Prinzipien. So muss

1289 Vgl. Botschaft BGEID, S. 3927.

1290 Aus diesem Grund nennt es als Verfassungsgrundlage Art. 95 BV, welcher dem Bund erlaubt, wirtschaftspolizeiliche Vorschriften über die Ausübung privatwirtschaftlicher Erwerbstätigkeit zu machen, sowie die Art. 96 (Kompetenz zum Erlass im Bereich des Kartellschutzes) und Art. 97 BV (Konsumentenschutz); vgl. Botschaft BGEID, S. 3978.

1291 Botschaft BGEID, S. 3923.

1292 MÜLLER, BSK BV, Art. 178, N. 55.

1293 MÜLLER, BSK BV, Art. 178, N. 37.

die Übertragung einem öffentlichen Interesse dienen und verhältnismässig sein. Zudem ergibt sich aus dem Grundsatz der Wettbewerbsneutralität, dass die Auswahl der Adressaten der Aufgabenübertragung in einem allen offenstehenden Verfahren erfolgt. Letztlich müssen die übrigen Grundrechte und der Rechtsschutz der Betroffenen gewahrt bleiben.[1294]

553 Im vorliegenden Fall würde das BGEID die geforderte Gesetzesgrundlage für eine Aufgabenübertragung darstellen. Das öffentliche Interesse dürfte etwa darin bestehen, dass Private entsprechende Lösungen schneller und benutzerorientierter entwickeln können als der Staat, zumal dieser etwa aufgrund beschaffungsrechtlicher Vorgaben und notwendiger gesetzlicher Anpassungen regelmässig langwierige (und kostspielige) Verfahren durchlaufen muss.[1295] Die Auslagerung der Ausgabe digitaler Identitäten darf als geeignet erachtet werden, um ein entsprechendes Ziel zu erreichen, und es ist auch kein milderes Mittel ersichtlich, um diesen Zweck zu verfolgen. Schliesslich erscheint es zumutbar, dass die Aufgabe an Private übergeben wird, zumal der Staat durch das Verfahren zur Anerkennung von Identitätsprovidern weiterhin die Gewährleistung der Aufgabenerfüllung vornimmt. Dieses Anerkennungsverfahren soll auch sicherstellen, dass alle Anbieter von digitalen Identitäten gleich behandelt werden. Zudem müssen bei einer Auslagerung der Aufgabenerfüllung auch die Grundrechte der Betroffenen beachtet und gewahrt werden. In diesem Zusammenhang ergeben sich insbesondere hinsichtlich des Rechts auf informationelle Selbstbestimmung Fragen, welche im nächsten Kapitel genauer betrachtet werden sollen.

554 Es lässt sich zusammenfassend feststellen, dass die Übertragung einer Ausgabe digitaler Identitäten an Private nicht grundsätzlich unzulässig ist, zumal der Staat auch in diesem Bereich die Gewährleistungspflicht beibehält. Dennoch bleibt zu bedenken, dass die geltend gemachten Vorbehalte bezüglich einer derartigen Aufteilung der Legitimation und der Akzeptanz des Systems schaden könnten.[1296] Immerhin gaben gemäss dem Referendumskomitee gegen das BGEID in einer repräsentativen Umfrage 87 % der Befragten an, dass sie einen digitalen Pass lieber vom Staat beziehen möchten.[1297] Daher gab es auch im Vernehmlassungsverfahren diverse Vorschläge dahingehend, dass beispielsweise eine Trägerschaft aus verschiedenen öffentlichen Organen (allenfalls auch unter dem Beizug von privaten Anbietern) die Herausgabe

1294 Vgl. etwa BIAGGINI, SG Komm. BV, Art. 178, N. 34 f.

1295 Botschaft BGEID, S. 3934.

1296 Vgl. etwa SP SCHWEIZ, S. 1.

1297 Vgl. etwa Digitale Gesellschaft, Newsbeitrag vom 3. Juli 2019, Entscheidung für eine vertrauenswürdige staatliche E-ID.

verantworten solle oder je nach Verwendungszweck private oder öffentliche Organe mit der Aufgabe betraut werden sollten.[1298] Immerhin lässt der Bund mit Art. 10 BGEID eine Hintertür für ein staatlich entwickeltes E-ID-System der Sicherheitsniveaus «substanziell» und «hoch» offen, falls kein Marktteilnehmender ein solches entwickeln will.[1299]

2. Datenschutz

Ein Grund für das in der Bevölkerung vorhandene offensichtliche Misstrauen gegenüber der vorgeschlagenen Lösung sind datenschutzrechtliche Bedenken. Unbehagen bereitet etwa dem Referendumskomitee in erster Linie, dass private Unternehmen als anerkannte Identitätsprovider (IdP) im Sinne des Gesetzes Zugriff auf die entsprechenden Daten der Bürger erhalten und auch für deren Speicherung und Verwendung zuständig sind. Der Staat gebe somit in einem gewissen Masse die Kontrolle über diese Daten ab, lautet der Vorwurf.[1300] Im Folgenden soll überprüft werden, ob die Regelungen des BGEID sich mit den datenschutzrechtlichen Vorgaben des Bundes vereinbaren lassen. 555

Im vorliegenden Kontext enthalten die elektronischen Identitäten gemäss Art. 5 des Entwurfs zwingend gewisse Personenidentifizierungsdaten, wobei der Umfang der geforderten Daten je nach Sicherheitsniveau verschieden ist. Beantragt eine Person eine elektronische ID, so findet eine Überprüfung ihrer Identität statt, in deren Rahmen das Bundesamt für Polizei (fedpol), welches die neu geschaffene Identitätsstelle führt, dem IdP diese Daten mit Einwilligung des Betroffenen bekanntgibt.[1301] Diese Personenidentifizierungsdaten umfassen den Namen, das Geburtsdatum sowie allenfalls zusätzlich das Geschlecht, den Geburtsort, die Staatsangehörigkeit und das Gesichtsbild. Diese Daten können eine Person durchaus bestimmen und sind somit als Personendaten im Sinne der Datenschutzgesetzgebung zu betrachten. Deswegen sind die Vorgaben des Datenschutzgesetzes und dabei insbesondere Art. 17 und 19 DSG zu beachten, welche grundsätzlich eine gesetzliche Grundlage für die Bearbeitung und Bekanntgabe von Personendaten durch Bundesorgane fordern. Im Weiteren sind die Grundsätze der Datenbearbeitung für die Bundesorgane verbindlich. Die Privaten, welche die Daten bearbeiten, sind gemäss Art. 2 Abs. 1 lit. a DSG ebenfalls durch das Datenschutzrecht gebunden. Für sie ist insbesondere Art. 12 DSG zu beachten, gemäss dem, wer Personendaten bearbeitet, dabei die Persönlichkeit der betroffenen 556

1298 Vernehmlassungsbericht BGEID, S. 7.

1299 Botschaft BGEID, S. 3954.

1300 Vgl. dazu das Argumentarium des Referendumskomitees.

1301 Botschaft BGEID, S. 3925.

Personen nicht widerrechtlich verletzen darf. Auch für private Datenbearbeiter sind gemäss Art. 12 Abs. 2 DSG die Grundsätze des Datenschutzgesetzes einschlägig.

557 Der Gesetzgeber statuiert bereits im Zweckartikel in Art. 1 Abs. 2 lit. b BGEID, dass die Grund- und Persönlichkeitsrechte der Personen geschützt werden sollen, über die im Rahmen dieses Gesetzes Daten bearbeitet werden.[1302] Das Gesetz regelt für die Beteiligten, unter welchen Umständen sie welche Personendaten bearbeiten oder bekanntgeben dürfen. Das fedpol ist beispielsweise gemäss Art. 6 Abs. 2 BGEID berechtigt, den IdP die Personenidentifizierungsdaten bekanntzugeben, sofern die betroffene Person gemäss dem jeweiligen Sicherheitsniveau identifiziert wurde und in eine Übermittlung eingewilligt hat. Zu diesem Zweck führt das fedpol gemäss Art. 24 BGEID ein Informationssystem. In diesem Artikel sind die betreffenden Daten und der Zweck ihrer Bekanntgabe geregelt, so dass davon ausgegangen werden kann, dass die Vorgaben von Art. 17 und Art. 19 DSG erfüllt sind.[1303] Die IdP erhalten vom Gesetz in Art. 7 BGEID die Berechtigung bzw. die Pflicht, die entsprechenden Personenidentifizierungsdaten beim fedpol mittels automatisierter Abfrage regelmässig zu aktualisieren. Betreffend die Datenbearbeitung und -haltung durch die IdP sieht das Gesetz in Art. 9 BGEID gewisse Regelungen vor. So dürfen von fedpol übermittelte Personenidentifizierungsdaten nur bearbeitet werden, bis die E-ID widerrufen wird, und nur für Identifizierungen nach dem Gesetz verwendet werden. Gegenüber den die E-ID verwendenden Diensten darf ein IdP gemäss Art. 16 BGEID nur diejenigen Personenidentifizierungsdaten bekanntgeben, welche dem geforderten Sicherheitsniveau entsprechen, für die Identifizierung im Einzelfall notwendig sind und in deren Übermittlung der Inhaber eingewilligt hat. Gegenüber Dritten ist die Weitergabe von Personenidentifizierungs- und Nutzungsdaten gemäss Art. 16 Abs. 2 des Gesetzes verboten. Zu erwähnen ist ebenfalls noch Art. 15 BGEID, welcher die Pflichten der IdP festhält und insbesondere in Art. 15 Abs. 1 lit. i BGEID einen Online-Zugang für die Nutzenden zu ihren mit der Benutzung verbundenen Personenidentifizierungsdaten und Nutzungsdaten vorsieht.

558 Im Rahmen der Vernehmlassung wurden dabei wesentliche datenschutzrechtliche Kritikpunkte beseitigt. So wurde etwa der ursprünglich in Art. 7 VE-BGEID vorgesehene nicht abschliessende Katalog der Personenidentifizierungsdaten, welche an die IdP weitergegeben werden, als zu umfassend und somit nicht verhältnismässig befunden und daher reduziert. Auch auf die vorgesehene Verwendung der AHV-Versichertennummer als Personen-

1302 Botschaft BGEID, S. 3981.

1303 Botschaft BGEID, S. 3983.

identifizierungsdatum gegenüber den IdP wurde verzichtet.[1304] Stattdessen wird eine zufallsgenerierte E-ID-Registernummer verwendet, welche keinen Rückschluss auf die AHV-Nummer zulässt.[1305]

559 Dennoch bleiben einige datenschutzrechtliche Befürchtungen bestehen. So wird der Verzicht auf die AHV-Versicherungsnummer als Identifikator begrüsst. Es wird jedoch darauf hingewiesen, dass auch die geschaffene E-ID-Registernummer von den Behörden uneingeschränkt als Identifizierungsmerkmal verwendet werden könne, um Personendatensätze aus unterschiedlichen Systemen miteinander zu vernetzen.[1306] Im Weiteren seien zwar die Rechte und Pflichten der IdP detailliert geregelt, jedoch nicht diejenigen der Dienste, welche die E-ID verwenden können. Auf diese Weise sei ein ausreichender Schutz der Daten nicht gewährleistet. Es müssten dabei insbesondere Aspekte wie Datensparsamkeit, die Sperrung der E-ID, die Vernichtung und die Weitergabe von Informationen, der Speicherort und der Umgang mit Auftragsdatenbearbeitung sowie Mindestanforderungen zum Sicherheitsniveau und zu technischen und organisatorischen Massnahmen geregelt werden.[1307] Zu beachten sein wird in diesem Rahmen sicherlich auch der Aspekt der Datensicherheit, d.h., dass bei allen Beteiligten genügende technische und organisatorische Massnahmen getroffen werden, um die Sicherheit der Daten zu gewährleisten. Dabei handelt es sich indes um Aspekte der Umsetzung, welche zum jetzigen Zeitpunkt nicht schlüssig beurteilt werden können.

560 Insgesamt lässt sich feststellen, dass die vorgeschlagene Lösung des Gesetzgebers sich im Rahmen der datenschutzrechtlichen Vorgaben bewegt. Gewichtige Kritikpunkte wurden aufgrund der Rückmeldungen im Vernehmlassungsverfahren behoben. Die Datenbearbeitung durch Bundesbehörden ist im Rahmen dieses Gesetzes weitgehend beschränkt. Auch die Befugnisse der IdP sind gesetzlich eingeschränkt. Allenfalls sind hinsichtlich der Betreiber von E-ID verwendenden Diensten noch klarere Vorgaben zu wünschen. Wichtig ist insbesondere, dass zahlreiche der Datenbearbeitungen durch Private im Rahmen des Gesetzes explizit nur mit der Einwilligung der Betroffenen zulässig sind.

1304 Als problematisch erachtet wurde, dass die AHV-Nummer über den Bereich der Sozialversicherungen hinaus durch die Schaffung neuer gesetzlicher Grundlagen in immer weiteren Rechtsbereichen als Identifizierungsdatum eingesetzt werde und somit zu einem allgemeinen Personenidentifikator werde; vgl. etwa PRIVATIM, Stellungnahme zum E-ID-Gesetz im Rahmen des Vernehmlassungsverfahrens; kritisch zur Verwendung der AHV-Nummer als allgemeiner Personenidentifikator: BASIN.

1305 Botschaft BGEID, S. 3936. Die AHV-Nummer wird nun gemäss Art. 24 E-BGEID lediglich noch dort verwendet, wo das fedpol zum Abgleich der Identifizierungsdaten mit anderen Registern von Behörden kommunizieren muss.

1306 Vgl. Stellungnahme BGEID .

1307 Vgl. die Stellungnahme von privatim zum Gesetzesentwurf BGEID.

561 Zu beachten bleibt, dass es sich bei der E-ID zum Zeitpunkt ihrer Einführung um ein freiwilliges Angebot handeln wird, welches durch die Bevölkerung nicht in Anspruch genommen werden muss. Datenschutzrechtliche Bedenken oder Schwachstellen bei der Nutzung können allerdings für die Nutzenden auch durch die Freiwilligkeit nicht ausgemerzt werden und könnten dazu führen, dass sich die Verwendung des Angebots nicht wie gewünscht entwickeln wird.

562 Sollte die E-ID nicht die gewünschte Verbreitung finden, könnten Anbieter (insbesondere auch staatliche Behörden) zu deren Förderung versucht sein, gewisse Angebote nur noch mit der E-ID zuzulassen, womit ein faktischer Nutzungszwang bestehen würde.[1308] Gerade Behörden müssten in diesem Fall dem Diskriminierungsverbot Rechnung tragen. Dementsprechend müsste für Personen, welche eine E-ID nicht benutzen können (oder wollen), Übergangsfristen oder alternative Möglichkeiten zur Nutzung von Behördendienstleistungen vorgesehen werden.[1309]

3. Fazit und Ausblick

563 Grundsätzlich passt sich die geplante Gesetzgebung zu den elektronischen Identitäten in die aktuelle Rechtsordnung ein. Es ist nach der hier vertretenen Auffassung rechtlich zulässig, dass der Staat die Entwicklung und Herausgabe von digitalen Identitäten an private Partner auslagert, während er selbst lediglich die Gewährleistungsverantwortung für diese Aufgabe übernimmt. Bei der Übertragung der Aufgabe an Private sind auch der Rechtsschutz und die Grundrechte der Betroffenen zu wahren. Im vorliegenden Kontext ist insbesondere die informationelle Selbstbestimmung zu beachten. Die Datenschutzbestimmungen des Gesetzes schränken die Datenbearbeitung durch staatliche Stellen und IdP – nach einigen Nachbesserungen aufgrund der Ergebnisse der Vernehmlassung – wirksam ein. Restzweifel bestehen indes hinsichtlich der Rechte und Pflichten von Betreibern von E-ID-Diensten, welche genauer geregelt werden sollten.

564 Auch aufgrund der augenscheinlich vorhandenen Vorbehalte gegenüber der vorgesehenen Aufgabenteilung ist die Frage zu stellen, ob sich die E-ID auf die vorgesehene Weise durchsetzen wird. Das Vorliegen einer entsprechenden Gesetzgebung allein garantiert noch nicht, dass das Angebot auch benutzt wird, wie Erfahrungen aus anderen Ländern zeigen. Während in Estland 90 % eine digitale Identität haben und nutzen, besitzen in Deutschland zwar bereits viele Personen einen Personalausweis mit integriertem Chip, jedoch

1308 Vgl. die Stellungnahme von privatim zum Gesetzesentwurf BGEID.

1309 Vgl. analog für die Information ausschliesslich über das Internet, Rz. 237.

machten sie sich über lange Zeit kaum das entsprechende Angebot zunutze bzw. liessen den Chip überhaupt nicht aktivieren. Seit einer Gesetzesrevision im Jahr 2017 ist die entsprechende Funktion indes standardmässig aktiviert und muss von den Benutzenden deaktiviert werden.[1310]

565 Analysiert man die Erfahrungen anderer Länder und die Literatur, so lassen sich verschiedene mögliche Erfolgsfaktoren finden. Eine staatliche Trägerschaft allein bietet keine Garantie für eine Verbreitung einer entsprechenden E-ID-Lösung, wie auch das soeben genannte Beispiel aus Deutschland zeigt.[1311] Hingegen kann auch eine in Kooperation von Staat und Privaten entwickelte Lösung wie in Dänemark sich einer grossen Verbreitung erfreuen.[1312] Die populären Lösungen anderer Länder kommen zudem in verschiedenen Ausgestaltungen daher, sei es als App auf dem Smartphone oder als persönliches Identitätsdokument mit einem Zusatzchip. Somit dürfte für den Erfolg einer Lösung keine oder eine eher untergeordnete Rolle spielen, in welcher Form die elektronische Identität angeboten wird, zumindest solange sie nicht mit der kostspieligen Anschaffung zusätzlicher Hard- oder Software verbunden ist.[1313]

566 Nicht zielführend sein dürfte unter diesem Aspekt für die Akzeptanz einer E-ID-Lösung ein Nutzungszwang,[1314] zumal sich diesfalls Fragen hinsichtlich der Diskriminierung gewisser Gruppen stellen könnten. Eher noch könnte die Akzeptanz durch das Anbieten gewisser Vorteile erhöht werden. So musste etwa die estnische Bevölkerung zu Beginn durch gewisse Anreize zur Nutzung der E-ID ermutigt werden (verbilligte Bustickets, Aufzeigen von Vorteilen).[1315] Aus den Erfahrungen anderer Länder zeigt sich zudem, dass es eine Verbreitung entsprechender Lösungen begünstigt, wenn die elektronische Identität in verschiedenen Bereichen – allenfalls auch im privaten Rechtsverkehr oder beispielsweise als elektronische Signatur – eingesetzt werden kann. Hierfür sind die Ausbaufähigkeit und die Integrierbarkeit der E-ID massgebend. Ebenfalls als grundlegend erachtet werden Aspekte wie Sicherheit, Nutzungskomfort und Datenschutz.[1316]

1310 Gesetz zur Förderung des elektronischen Identitätsnachweises vom 7. Juli 2017, Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 46, 2310 f.

1311 Botschaft BGEID, S. 3923.

1312 Siehe oben Rz. 531.

1313 KRCMAR/MÜLLER/SCHEIBER/EXEL/MOTZET/BASTIN, S. 4.

1314 Botschaft BGEID, S. 3934.

1315 JACCARD, Jusletter, 30. April 2018, N. 70 ff.

1316 Vgl. etwa BRIAN/WEISSENFELD, Sicherheit, Nutzungskomfort und Datenschutz – die einzigen Erfolgsfaktoren einer nationalen eID?.

567 Das BGEID sieht zwar Regelungen zum Datenschutz vor, welche die Datenbearbeitung durch staatliche und private Stellen einschränken. Hierbei scheint jedoch wie bereits oben erwähnt ein Unbehagen gewisser Bevölkerungsteile hinsichtlich der Auslagerung der Datenbearbeitung an Private zu bestehen, welches sich negativ auf das in der Bevölkerung entgegengebrachte Vertrauen auswirken kann. Gerade dieser Aspekt ist indes von essenzieller Bedeutung. Es lässt sich wohl erst anhand konkreter E-ID-Lösungen inskünftig abschätzen, wie es beispielsweise um den Nutzungskomfort und das verfügbare Angebot steht. Den Entwicklern entsprechender Lösungen sind insbesondere diese Aspekte ans Herz zu legen. Problematisch sein könnte in dieser Hinsicht auch, dass viele Länder, in denen E-IDs weit verbreitet sind, nur ein einziges System kennen. In der Schweiz kann es aufgrund der gesetzlichen Grundlagen auch für die höheren Sicherheitsniveaus potenziell mehrere Systeme geben, was eine Verbreitung hemmen dürfte. Es ist daher zum jetzigen Zeitpunkt meines Erachtens als fraglich zu erachten, ob die mit dem BGEID gewählte Lösung die dadurch geweckten Erwartungen erfüllen kann.

568 Ebenfalls relevant sein könnte gerade im von Natur aus grenzenlosen Internet die Möglichkeit einer Verwendbarkeit im Ausland.[1317] Der Gesetzgeber hat daher im Rahmen der Ausarbeitung des Gesetzesvorschlags diesen Aspekten ebenfalls Beachtung geschenkt. So wurden etwa die verschiedenen Sicherheitsniveaus und ihre Voraussetzungen in Anlehnung an die relevante eIDAS-Verordnung der EU gewählt.[1318]

III. Nutzungszwang

569 Wie weiter oben ausgeführt sind alle Bundesbehörden inzwischen verpflichtet, elektronisch eingereichte Dokumente anzunehmen, wobei diese Möglichkeit von Privatpersonen aktuell noch selten genutzt wird. In anderen Ländern wurden aufgrund einer gesetzlichen Pflicht für die Bevölkerung oder zumindest gewisse Bevölkerungsgruppen, elektronische Medien zum Behördenverkehr zu nutzen, zahlenmässige Fortschritte in der Verbreitung des elektronischen Rechtsverkehrs erzielt.[1319] In der Schweiz besteht bisher für Privatpersonen soweit ersichtlich nirgends eine entsprechende rechtliche Verpflichtung, Eingaben im Verfahren elektronisch zu tätigen. Im Jahr 2018 wurde das Projekt «Justitia 4.0» angestossen, welches vorsieht, schweizweit den elektronischen Rechtsverkehr und das rechtsgültige elektronische Dossier

1317 Botschaft BGEID, S. 3943.

1318 JACCARD, Jusletter, 30. April 2018, N. 64 ff., Botschaft BGEID, S. 3934.

1319 Siehe oben Rz. 527 ff.

einzuführen.[1320] Es soll dabei auf Bundesebene gesetzlich der elektronische Rechtsverkehr mit den Gerichten geregelt werden und die Verwendung der E-Justizakte zumindest für professionelle Prozessteilnehmende als obligatorisch erklärt werden.[1321] Juristische Laien sollen weiterhin wählen dürfen, ob sie in einem Verfahren elektronisch oder herkömmlich per Briefpost kommunizieren möchten.[1322] Parallel dazu soll eine einzige Gerichtsplattform für sämtliche beteiligten Gerichte geschaffen werden, um die Kommunikation zwischen den einzelnen Stellen zu erleichtern. Die gesamte Planung ist auf acht Jahre ausgelegt.[1323] Es ist vorgesehen, dass die Beschaffung des Systems ab 2022 begonnen werden und spätestens ab 2026 das Obligatorium greifen soll.[1324]

570 Um das Obligatorium durchsetzen zu können, sollen im Rahmen eines Mantelerlasses auf Bundesebene (Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz, BEKJ) die jeweiligen Verfahrensordnungen für die einzelnen Justizbereiche entsprechend angepasst werden. Dieses Gesetzeswerk befindet sich aktuell noch in der Ausarbeitung.[1325] Die Einführung des obligatorischen elektronischen Rechtsverkehrs soll in erster Linie die Gerichte auf Bundesebene betreffen. Da jedoch beispielsweise auch das VwVG überarbeitet werden soll, ist es vorstellbar, dass ein entsprechendes Obligatorium auch im erstinstanzlichen bundesrechtlichen Verwaltungsverfahren eingeführt wird.[1326]

571 Hinsichtlich der Durchsetzung des elektronischen Rechtsverfahrens auf kantonaler Ebene kann der Bund – wie bereits weiter oben ausgeführt – im Rahmen seiner Kompetenzen keine Vorgaben an die Kantone machen. Es kann kantonalen Instanzen grundsätzlich durch den Bundesgesetzgeber nicht aufgezwungen werden, ihre Akten elektronisch zu führen.[1327] Ob das Projekt «Justitia 4.0» auch auf kantonaler Ebene zu einer vermehrten Einführung von elektronischem Rechtsverkehr und elektronischer Akte führt, ist in

1320 Vgl.anstatt vieler: TSCHÜMPERLIN, SJZ, 2018; PIESBERGEN, Justice – Justiz – Giustizia, 2018; RHYNER, Justice – Justiz – Giustizia, 2019.

1321 Vgl. etwa RALL, Anwaltsrevue, S. 148. Zu denken in erster Linie an Anwälte, aber wohl auch Treuhänder oder Steuerexpertinnen, vgl. HÄNER, Justice – Justiz – Giustizia, 2018, S. 2.

1322 PIESBERGEN, Justice – Justiz – Giustizia, 2018, S. 3.

1323 TSCHÜMPERLIN, SJZ, 2018, S. 321.

1324 Vgl. die Projektübersicht (Roadmap) zum Projekt Justitia 4.0.

1325 Vgl. etwa die Präsentation von HOLENSTEIN anlässlich des Magglinger Rechtsinformatikseminars 2019.

1326 Vgl. HÄNER, Justice – Justiz – Giustizia, 2018, N. 19 f.

1327 S. dazu auch weiter oben Rz. 67 ff.; vgl. HÄNER, Justice – Justiz – Giustizia, 2018, N. 19.

erster Linie den Kantonen überlassen. Um etwa elektronische Akteneinsicht zu ermöglichen, müssen aber auch die gerichtlichen Vorinstanzen des Bundesgerichts ihre Akten elektronisch übermitteln. Eine entsprechende gesetzliche Regelung auf Bundesebene könnte daher zumindest die direkten Vorinstanzen des Bundesgerichts (darunter also auch die Verwaltungsgerichte der Kantone) dazu zwingen, mit diesem elektronisch zu verkehren. Diese erzwungene Umstellung bei den Verwaltungsgerichten könnte dazu führen, dass diese darauf angewiesen sind, dass ihre eigenen Vorinstanzen – also etwa die verfügenden Behörden oder vorinstanzliche Rechtsmittelbehörden – den elektronischen Rechtsverkehr ebenfalls einführen, da sie ansonsten die elektronische Erfassung selber übernehmen müssten.[1328] So würde also der Druck auf diejenigen Kantone steigen, welche den elektronischen Rechtsverkehr noch nicht flächendeckend eingeführt haben. Dieser indirekte Zwang zur Einführung des elektronischen Rechtsverkehrs in den Kantonen wird in der Literatur teilweise aus rechtsstaatlicher Warte als problematisch angesehen, da auf diese Weise die Organisationsautonomie der Kantone umgangen werde.[1329]

572 Indes ist hierzu festzuhalten, dass die Konferenz der kantonalen Justiz- und Polizeidirektoren sich einstimmig für die obligatorische Einführung einer entsprechenden gesetzlichen Grundlage auf Bundesebene ausgesprochen hat. Dadurch hat sie den damit verbundenen Eingriff in ihre Organisationshoheit explizit akzeptiert.[1330] Somit scheint ein entsprechender Wunsch zumindest auf exekutiv-politischer Ebene breit abgestützt zu sein. Es scheint auch in den Kantonen, welche den elektronischen Rechtsverkehr bisher noch nicht eingeführt haben, ein Konsens zu bestehen, dass in ihrem Zuständigkeitsbereich, etwa bei der Verwaltungsgerichtsbarkeit, die notwendigen gesetzgeberischen Schritte unternommen werden sollen.[1331] Vieles wird indes auf die Umsetzung der jeweiligen Bestimmungen ankommen, welche zur Zeit noch nicht absehbar ist.

573 Auch in grundrechtlicher Hinsicht wurden in der Diskussion zum Projekt «Justitia 4.0» in der Literatur einige Aspekte angesprochen, welche an dieser Stelle ebenfalls skizziert werden sollen. Da zum Zeitpunkt der Erarbeitung

1328 Vgl. zum Ganzen HÄNER, Justice – Justiz – Giustizia, 2018, N. 20.

1329 Vgl BREITENMOSER/HOFMANN, Justice – Justiz – Giustizia, 2019, S. 4.

1330 TSCHÜMPERLIN, SJZ, 2018, S. 318. Es dürfte m.E. allerdings an dieser Stelle die Frage nach der demokratischen Legitimation der entsprechenden Beschlüsse gestellt werden. Basiert die auf kantonaler Ebene gefasste Zustimmung auf entsprechenden Regierungsratsbeschlüssen? Sind die Regierungen überhaupt kompetent, dies zu bestimmen?

1331 TSCHÜMPERLIN, SJZ, 2018, S. 319.

dieser Arbeit die Gesetzesvorlage noch nicht verabschiedet wurde, kann indes keine detaillierte Untersuchung hinsichtlich ihrer Rechtskonformität erfolgen.

A. Diskriminierung

574 Wie in anderen Bereichen, in denen der Zwang besteht, dass die Betroffenen nur über einen bestimmten Kanal mit der Verwaltung kommunizieren können, stellt sich die Frage, ob dadurch das Diskriminierungsverbot gemäss Art. 8 Abs. 2 BV betroffen sein könnte. Gemäss Art. 8 Abs. 2 BV darf – wie weiter oben bereits behandelt – niemand aufgrund eines sensiblen Merkmals diskriminiert werden.[1332] Im vorliegenden Fall soll sich das Obligatorium – zumindest in einem ersten Schritt – auf Anwender beschränken, welche berufsmässig mit den Gerichten verkehren (insbesondere Anwälte). Wie bereits festgestellt wurde, sind Personen ohne Computer oder Internetanschluss in diesem Zusammenhang nicht als sensible Gruppe zu verstehen. Auch das Ausüben eines bestimmten Berufs (z.B. Anwalt) kann nicht als Anknüpfungsmerkmal für eine Diskriminierung dienen, da es nicht an eine persönliche Eigenschaft anknüpft, welche nur schwer veränderbar ist.[1333] Denkbar ist allenfalls, dass durch den Zwang zur Nutzung einer bestimmten Softwarelösung gewisse Anwender aufgrund ihres Alters oder einer Behinderung diskriminiert werden, da sie dieses System aufgrund mangelnder technischer Fähigkeiten oder aufgrund einer nicht behinderungskonformen Ausgestaltung nicht nutzen können. Es ist jedoch gerade im beruflichen Umfeld davon auszugehen, dass die meisten Anwälte ihre Geschäfte bereits zu einem weiten Teil computergestützt erledigen und daher über technologisches Know-how oder zumindest entsprechende Mittel und Vorkehrungen innerhalb ihrer Organisation verfügen. Um die Frage nach einer möglichen Diskriminierung schlüssig beantworten zu können, wird indes die konkrete Ausgestaltung des Obligatoriums abzuwarten sein.

575 Wie in anderen Bereichen, in denen der Staat nur noch auf eine gewisse Weise oder über einen gewissen Kanal mit den Privaten interagieren will, sollte bei der Ausarbeitung der gesetzlichen Grundlagen darauf geachtet werden, dass für die Betroffenen Ausweichmöglichkeiten oder Übergangsregelungen vorgesehen werden, welche diesen hinreichend Zeit für die Umstellung lassen.[1334] In diesem Zusammenhang ist zu erwähnen, dass die Einführung

1332 Vgl. oben Rz. 218 und 453.

1333 Siehe dazu weiter oben Rz. 453.

1334 Siehe dazu auch die Urteile des BGer 1C_137/2018, 1C_139/2018 vom 27. November 2018, E. 5.4, welche sich mit den Voraussetzungen für eine elektronische Publikation des Amtsblatts befassen.

des Obligatoriums schrittweise frühestens ab 2022 erfolgt, womit für die Betroffenen durchaus Zeit bleibt, sich auf diese Umstellung vorzubereiten.[1335] Zudem sollten allenfalls auch weitere flankierende Massnahmen (etwa Schulungs- oder Supportmöglichkeiten) angedacht werden, um den entsprechenden Übergang verhältnismässig zu gestalten.

576 Sofern eines Tages vorgesehen werden sollte, dass die Verwendung des elektronischen Kanals für alle Personen im Kontakt mit der Verwaltung und Gerichten obligatorisch wird, könnte dies ebenfalls für gewisse sensible Gruppen im Sinne von Art. 8 Abs. 2 BV diskriminierend wirken. Es ist erschwerend anzunehmen, dass in der breiten Bevölkerung, im Gegensatz zu Personen, welche professionell mit Gerichten verkehren, gerade im höheren Alterssegment das Know-how im Umgang mit Computern und insbesondere Spezial-Applikationen noch wenig ausgeprägt ist. Diese Bevölkerungsgruppe wäre somit wesentlich mehr betroffen als andere. Zudem wäre es Angehörigen dieser Bevölkerungsgruppe bei einem allgemeinen Obligatorium nicht mehr möglich, mit den Behörden innerhalb eines Verfahrens zu kommunizieren, ohne sich dabei auf die Hilfe anderer zu verlassen und beispielsweise einen Anwalt zu mandatieren. Dies wäre wiederum mit zusätzlichen Kosten und Umständen für die Betroffenen verbunden, welche sich nicht jeder Rechtssuchende leisten kann.

577 Immerhin ergibt sich aus den allgemeinen Verfahrensgarantien gemäss Art. 29 Abs. 3 BV ein Anspruch auf unentgeltliche Rechtspflege, welches auch die Bestellung eines Anwalts beinhalten kann, wenn dies für die Wahrung der Rechte der Betroffenen notwendig ist.[1336] Dies könnte hier durchaus der Fall sein. Eine entsprechende Regelung könnte daher für die Staatskasse zu zusätzlichen Mehrkosten führen und die Einsparungen durch die elektronische Akte zumindest in Teilen tilgen. Wäre es den Betroffenen aufgrund eines entsprechenden Obligatoriums nicht mehr möglich, eine gerichtliche Instanz anzurufen, so könnte dies auch eine Verletzung der Rechtsweggarantie gemäss Art. 29a BV darstellen.

578 Auch aus diesem Grund ist es zu begrüssen, das vorab von einem allgemeinen Obligatorium abgesehen wird und ein solches auf professionelle Anwender beschränkt bleibt. Sollte ein entsprechendes Obligatorium allerdings dereinst eingeführt werden, ist aus Gründen des Diskriminierungsverbots und der Rechtsweggarantie sicherzustellen, dass Personen aus betroffenen Gruppen durch Übergangsregelungen und Ausweichmöglichkeiten (etwa

1335 FREIBURGHAUS, Justice – Justiz – Giustizia, 2018, N. 2; PIESBERGEN, Justice – Justiz – Giustizia, 2018, N. 10.

1336 WALDMANN, BSK BV, Art. 29, N. 60 f.

unentgeltliche Unterstützung bei der elektronischen Einreichung) ebenfalls die Möglichkeit erhalten, weiterhin ohne Beschränkungen mit den Behörden und den Gerichten zu kommunizieren.

B. Wirtschaftsfreiheit

579 Durch ein Obligatorium, ihre Akten elektronisch einzureichen, wird professionellen Vertretern und insbesondere Anwälten eine Vorgabe darüber gemacht, wie sie ihren Beruf auszuüben haben. Somit könnte vorliegend allenfalls eine Verletzung der Berufsfreiheit geltend gemacht werden, wie dies ein Anwalt in Deutschland betreffend das dortige Obligatorium tat.[1337] In der Schweiz ist die Berufsausübungsfreiheit als Teilgehalt der Wirtschaftsfreiheit in Art. 27 BV statuiert.[1338] Unter diesem Aspekt ist etwa die freie Wahl der Mitarbeitenden, der Organisation, der sachlichen Mittel oder der Geschäftsbeziehungen geschützt.[1339] Im vorliegenden Fall könnte insbesondere ein Eingriff in die freie Wahl der sachlichen Mittel vorliegen, ist es doch dem Betroffenen grundsätzlich vorbehalten, jede mögliche Maschine oder Technik zur Ausübung seiner professionellen Aktivität zu wählen.[1340] Der Anwaltsberuf fällt ohne Zweifel ebenfalls unter den Schutz der Wirtschaftsfreiheit.[1341] Wird einem Anwalt nun vorgeschrieben, dass er seine Eingaben nur noch via ein gewisses Computerprogramm vornehmen darf, so kann dies durchaus als Einschränkung dieser Berufsausübungsfreiheit angesehen werden.

580 Ein Eingriff in die Wirtschaftsfreiheit muss neben den allgemeinen Voraussetzungen von Art. 36 BV auch mit dem Grundsatz der Wirtschaftsfreiheit gemäss Art. 94 BV vereinbar sein. Nicht mit diesem Grundsatz in Einklang zu bringen sind staatliche Massnahmen, welche entweder von ihrem Eingriffsmotiv her unzulässig sind oder sich zwar nicht primär gegen den Wettbewerb richten, diesen aber derart verzerren, dass dies nicht mehr tragbar erscheint.[1342] Abweichungen vom Grundsatz der Wirtschaftsfreiheit sind nur zulässig, wenn sie in der Bundesverfassung vorgesehen oder durch kantonale Regalrechte begründet sind (vgl. Art. 94 Abs. 4 BV). Die Einführung eines Obligatoriums zum elektronischen Rechtsverkehr mit den Gerichten bezweckt in erster Linie die Förderung desselben. Dadurch sollen eine rechtssichere und schnelle Kommunikation mit diesen ermöglicht und auf beiden

1337 Vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 20. Dezember 2017 - 1 BvR 2233/17 -, N. 1-19.

1338 Vgl. etwa BGE 128 I 92 E. 2a; BGE 128 I 19 E. 4c.

1339 VALLENDER, SG Komm. BV, Art. 27, N. 22.

1340 BGE 63 I 213 E. 1.

1341 BIAGGINI, OFK BV, Art. 27, N. 14.

1342 UHLMANN, BSK BV, Art. 94, N. 7.

Seiten Kosten (z.B. für Druck und Versand) gespart werden.[1343] Der Eingriff ist somit nicht auf eine Beeinflussung des Wettbewerbs gerichtet. Auch sind allfällige Auswirkungen auf den Wettbewerb nicht derart gravierend, dass sie dem Grundsatz der Wirtschaftsfreiheit entgegenstehen.

581 Die gesetzliche Grundlage für den Eingriff soll durch die Änderungen der Verfahrensgesetze im Rahmen des geplanten Mantelerlasses geschaffen werden. Eine abschliessende Beurteilung dieser Rechtsgrundlagen ist daher erst möglich, wenn ein entsprechender Gesetzesentwurf vorliegt. Das öffentliche Interesse am vorliegenden Grundrechtseingriff ist in der Durchsetzung des elektronischen Rechtsverkehrs zu suchen, welcher zu mehr Effizienz und Kosteneinsparungen im Rechtsverkehr sorgen soll. Hinsichtlich der Verhältnismässigkeit ist wohl die Ausgestaltung der Regelung abzuwarten, damit etwa absehbar wird, welche Zusatzkosten (z.B. für die Anschaffung neuer Geräte) auf die betroffenen Anwälte zukommen, wobei die sich ergebenden Kosteneinsparungen ebenfalls in die Kalkulation einzubeziehen sind. Zu beachten gilt hier allerdings, dass die meisten Anwälte erfahrungsgemäss ihre Rechtsschriften bereits elektronisch verfassen und sich daher lediglich die Modalitäten des Versands ändern würden. Unter diesen Umständen ist wohl davon auszugehen, dass das Obligatorium für Anwälte grundsätzlich zumutbar ist.

582 Zu keinem anderen Schluss kam auch das deutsche Bundesverfassungsgericht, welches die erwähnte Beschwerde abwies. Zur Begründung brachte es vor, dass der Beschwerdeführer eine Verletzung der Berufsfreiheit (gemäss Art. 12 GG) nicht genügend substanziiert dargelegt habe. Insbesondere habe er nicht aufzeigen können, dass es sich bei den Motiven der Regelung nicht um geforderte berufsbezogene Gemeinwohlgründe handle. Zudem habe er zwar behauptet, dass die entsprechende Regelung nicht zu Einsparungen, sondern zu zusätzlichen Kosten für ihn führe, habe dies jedoch ebenfalls nicht substanziieren können.[1344] Nach dem soeben Ausgeführten ist eine Einschränkung der Wirtschaftsfreiheit durch den Zwang zur elektronischen Einreichung von Beschwerden m.E. als zulässig zu beurteilen.

C. Datenschutz

583 Bei der konkreten Umsetzung eines entsprechenden Nutzungszwangs sind zudem noch spezifische Fragen hinsichtlich des Datenschutzes und der Datensicherheit im Zusammenhang mit der Einführung einer einheitlichen Portallösung für die Gerichte des Bundes und die obersten Gerichte der Kantone

1343 Vgl. dazu für Deutschland: BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 20. Dezember 2017 – 1 BvR 2233/17, N. 12 f.

1344 Vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 20. Dezember 2017 - 1 BvR 2233/17 -, N. 13.

zu klären, welche den Datenaustausch zwischen den Gerichten sicherstellen soll. Eine Datenbearbeitung und -bekanntgabe über dieses Portal betrifft dabei in erster Linie hängige Gerichtsverfahren, womit das Datenschutzgesetz gemäss Artikel 2 Abs. 2 lit. c nicht anwendbar ist. Dies ist dadurch begründet, dass die jeweiligen Verfahrensordnungen in der Regel eigene Bestimmungen zum Schutz der Persönlichkeitsrechte Betroffener (etwa Mitwirkungs- oder Akteneinsichtsrechte) vorsehen.[1345] Von einer gewissen Relevanz bleiben allerdings auch hier die Grundsätze des Datenschutzrechts, insbesondere hinsichtlich der Datensicherheit, handelt es sich doch bei den betroffenen Daten zum Teil um besondere schützenswerte Personendaten.[1346]

584 Wie wichtig dieser Aspekt ist, zeigen gerade auch die Erfahrungen aus Deutschland, wo das besondere elektronische Anwaltspostfach (beA) aufgrund von Sicherheitslücken während mehrerer Monate offline gestellt werden musste. Die entsprechenden Lücken betrafen insbesondere die End-zu-End-Verschlüsselung zwischen der Software des Anwaltspostfachs und der Postfachlösung der Gerichte.[1347] Ein entsprechendes Risiko kann in der Schweiz insofern reduziert werden, als hier eine einheitliche Lösung vorgesehen ist, über welche die Kommunikation zwischen den Gerichten und den Parteien erfolgen soll. Gerade dies kann jedoch auch Nachteile erzeugen, da auf diese Weise potenziell eine Vielzahl von Akteuren Zugriff auf die entsprechenden Daten haben kann. Aus diesem Grund ist es wichtig, dass entsprechende Regelungen zu den Zugangsberechtigungen möglichst klar und restriktiv verfasst werden.[1348] Zu beachten bleibt, dass bei allen Vorkehrungen hinsichtlich der Datensicherheit der Mensch selber ebenfalls einen, wenn nicht gar den grössten Unsicherheitsfaktor darstellt, etwa durch das Wählen schwacher Passwörter.[1349] Dieser Gefahr kann kaum bzw. nicht vollständig mit gesetzgeberischen Massnahmen begegnet werden, jedoch ist die Schaffung eines Datenschutzbewusstseins bei den betroffenen Stellen und Benutzern unerlässlich.

D. Fazit

585 Ein Obligatorium des elektronischen Rechtsverkehrs (zumindest für professionelle Parteivertreter) lässt sich mit der bestehenden Rechtsordnung

1345 Botschaft DSG, S. 442.

1346 Etwa hinsichtlich administrativer oder strafrechtlicher Verfolgungen und Sanktionen; vgl. Art. 3 lit. c. Abs. 4 DSG.

1347 SECUNET AG, S. 13.

1348 SCHULER, plädoyer, 2019, S. 14.

1349 Vgl. etwa JAQUELINE FEHR, Eröffnungsrede anlässlich der Kick-off-Veranstaltung Justitia 4.0 vom 4. Februar 2019.

grundsätzlich vereinen. Sofern sich das Obligatorium lediglich auf die oben genannten Gruppen beschränkt, bleibt dies unter dem Gesichtspunkt des Diskriminierungsverbots wohl unbedenklich und ein Eingriff in die Berufsausübungsfreiheit als Teilgehalt der Wirtschaftsfreiheit wäre nach den obigen Ausführungen als gerechtfertigt zu bezeichnen. Dennoch lauern aus rechtlicher und technischer Sicht einige Stolpersteine bei der Einführung des Obligatoriums und insbesondere einer einheitlichen Portallösung, welche bei der Ausarbeitung zu beachten sein werden. Vorbehalte werden in der Literatur auch betreffend den im Vergleich mit bereits umgesetzten Projekten in Kantonen oder anderen Staaten ambitionierten Zeitplan und die mit der Einführung verbundenen Kosten angebracht.[1350] Aus rechtlicher Hinsicht wird insbesondere die Datensicherheit einer einheitlichen Portallösung zu gewährleisten sein. Für eine abschliessende Beurteilung sind die konkrete gesetzliche Regelung und auch die technische Umsetzung abzuwarten. Wichtig wird dabei sein, aus den in anderen Ländern gemachten Erfahrungen zu lernen und die entsprechenden Lösungen vor ihrem produktiven Einsatz im Rechtsverkehr gründlich zu testen, um peinliche technische Pannen zu verhindern. So war etwa die in Deutschland eingesetzte Lösung nicht in der Lage, Umlaute zu verarbeiten. Dies führte dazu, dass gewisse Beschwerden nicht fristgerecht beim Gericht eintrafen, ohne dass die Benutzenden dies bemerken konnten.[1351]

IV. Zusammenfassung

586 Von Mitteln wie zentralen Behördenportalen und elektronischen Identitäten, welche in anderen Ländern bereits existieren, verspricht man sich auch in der Schweiz eine Förderung des E-Government und des elektronischen Rechtsverkehrs. Ein einziges zentrales Behördenportal für alle Staatsebenen ist aktuell insbesondere aus Gründen des Föderalismus noch weit entfernt. Immerhin sehen einzelne Kantone bereits Behördenportale vor, welche auch Dienstleistungen der Gemeinden beinhalten und in ihrem Umfang stetig ausgebaut werden. Entsprechende Nutzungshindernisse durch eine Vielzahl an Portalen könnte auch die Einführung staatlich anerkannter elektronischer Identitäten beseitigen, wie diese im Bundesgesetz über elektronische Identifizierungsdienste vorgesehen sind. Das Gesetzgebungsprojekt ist allerdings

1350 SCHULER, plädoyer, 2019, S. 12 f.; BREITENMOSER/HOFMANN, Justice – Justiz – Giustizia, 2019, S. 3.

1351 Vgl. etwa BFH, Beschluss vom 5.6.2019 – IX B 121/18; kritischer Kommentar bei: MÜLLER, NZA, 2019.

politisch umstritten, was das dagegen ergriffene Referendum zeigt. Die vorgesehenen Regelungen des BGEID sind mit der bestehenden Rechtsordnung vereinbar, jedoch steht und fällt der Erfolg entsprechender Dienste auch damit, ob die Bevölkerung diese akzeptiert, was beim BGEID in dieser Form zumindest zweifelhaft erscheint. Ein Nutzungszwang für elektronische Kommunikation mit der Verwaltung ist insbesondere aus Gründen des Diskriminierungsverbots aktuell noch problematisch. Sollte eine entsprechende Verpflichtung vorgesehen werden, so sind Übergangsregelungen und Ausweichmöglichkeiten für diejenigen Personen zu schaffen, welche die entsprechenden Dienste nicht nutzen können (z.B. wegen Alter oder Behinderung). Ein Obligatorium für bestimmte Bevölkerungsgruppen (etwa Anwälte, wie dies das kommende BEKJ vorsieht) ist zudem auf seine Vereinbarkeit mit der Wirtschaftsfreiheit zu untersuchen, dürfte aber je nach Ausgestaltung unter diesem Aspekt zulässig sein.

§9 Bearbeitung des Sachverhalts

Bei der Bearbeitung des Sachverhalts durch die Behörden sind auch in Zukunft 587
erhebliche Neuerungen denkbar, indem etwa neue Mitwirkungspflichten geschaffen werden sollen oder zusätzliche Gesetzesgrundlagen zur Datenbekanntgabe der Behörden untereinander. Eine umfassende Betrachtung schon nur der aktuell geplanten oder diskutierten Neuerungen in diesen Bereichen würde den Rahmen dieser Arbeit sprengen. Aus diesem Grund soll hier betreffend die Schaffung neuer Mitwirkungspflichten ein besonders aufsehenerregender Gesetzentwurf aus dem Bereich des Asylrechts anhand der weiter oben aufgestellten Grundsätze betrachtet werden. Im Bereich der Amtshilfe übernehmen insbesondere Art. 17 und Art. 19 DSG eine begrenzende Funktion. Sofern der Gesetzgeber eine entsprechende gesetzliche Grundlage schafft, welche den obigen Vorgaben genügt, ist grundsätzlich die Speicherung aller denkbaren Daten zulässig.[1352] Da jedes Jahr eine Vielzahl an neuen Gesetzesgrundlagen zur Bearbeitung und Bekanntgabe von Daten geschaffen wird, welche teilweise mehr oder weniger umstritten sind, und einige dieser bestehenden oder geplanten Gesetzesgrundlagen hier auch bereits unter dem Aspekt der informationellen Selbstbestimmung kritisch betrachtet wurden bzw. noch werden[1353], soll sich die Betrachtung an dieser

1352 Siehe dazu oben Rz. 414 ff.

1353 Siehe dazu etwa Rz. 379 ff. (Social-Media-Recherche) oder Rz. 423 ff. (Einsatz von Algorithmen).

Stelle auf die Grundsätze beschränken und keine Auseinandersetzung mit einzelnen geplanten Rechtsnormen beinhalten.

I. Neue Mitwirkungspflichten aufgrund von technologischem Fortschritt

588 Durch neue technologische Möglichkeiten können sich unter Umständen auch neue Möglichkeiten ergeben, auf welche Weise die Verfahrensparteien ihre Mitwirkungspflichten erfüllen können. So ist es etwa denkbar, dass in Verwaltungsverfahren inskünftig Mobiltelefone nach konkreten Hinweisen durchsucht werden können, wie dies aktuell bereits im Strafverfahren unter gewissen Voraussetzungen der Fall ist.[1354] Unter diesem Aspekt befindet sich aktuell eine Revision des Asylgesetzes in der Ausarbeitung, welche es im Rahmen der Mitwirkungspflichten der Asylbewerbenden gemäss Art. 8 Abs. 1 Bst. g. AsylG erlauben soll, dass dem SEM elektronische Datenträger ausgehändigt werden sollen, wenn die Identität, die Nationalität oder der Reiseweg der Betroffenen nicht gestützt auf Identitätsausweise oder in anderer zumutbarer Weise festgestellt werden kann. Als elektronische Datenträger sind dabei im Rahmen eines offenen Katalogs gemäss Art. 8a AsylG etwa Mobiltelefone, Computer und Laptops oder Speichermedien zu verstehen.[1355] Die entsprechenden Daten sollen dabei gemäss Art. 8a Abs. 3 und 4 AsylG beim EJPD zwischengespeichert und in Anwesenheit der asylsuchenden Person ausgewertet werden. Diese neue Mitwirkungspflicht wird dadurch begründet, dass bei 70 bis 80 % der Asylsuchenden die Identität nicht bekannt ist oder nicht zweifelsfrei festgestellt werden kann. Indes führen die meisten Asylsuchenden mittlerweile elektronische Geräte mit sich, welche potenziell eine Vielzahl von Daten enthalten, die Aufschluss über Identität oder Reiseweg geben können.[1356] Viele andere Länder (unter anderem Deutschland, Dänemark, Finnland oder Belgien) kennen ebenfalls gesetzliche Grundlagen, welche eine Durchsuchung mobiler Datenträger Asylsuchender erlauben.[1357] So ist in Deutschland gemäss Art. 15a des dortigen Asylgesetzes die Auswertung von Datenträgern zulässig, soweit dies für die Feststellung der Identität und Staatsangehörigkeit des Ausländers erforderlich ist und der Zweck der Massnahme nicht durch mildere Mittel erreicht werden kann. Die entsprechende Regelung soll dabei als «ultima ratio» ausgestaltet sein, wobei die Auswertung von Datenträgern

1354 Vgl. Art. 263 StPO.

1355 Vernehmlassungsbericht Mitwirkung Asyl, S. 7.

1356 Vernehmlassungsbericht Mitwirkung Asyl, S. 3.

1357 Vernehmlassungsbericht Mitwirkung Asyl, S. 4.

zu unterbleiben habe, wenn anzunehmen sei, dass dadurch Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden.[1358]

Wie weiter oben bereits ausgeführt, steht der offene Katalog an möglichen Beweismitteln technologischen Neuerungen nicht entgegen. Begrenzt werden die Mitwirkungspflichten in erster Linie durch Geheimhaltungspflichten der Betroffenen und durch Verhältnismässigkeitsüberlegungen.[1359] 589

A. Betroffene Grundrechte

Durch die entsprechende Massnahme könnte ein Eingriff in verschiedene Grundrechtspositionen der Betroffenen vorliegen. Problematisch ist dabei in erster Linie, dass sich auf den Smartphones neben den allenfalls relevanten Daten auch weitere persönliche Daten befinden, welche im vorliegenden Zusammenhang keine Relevanz haben. Zu denken ist dabei etwa an den privaten Nachrichtenverkehr oder an persönliche Fotos und Videos.[1360] Dadurch, dass der Staat Zugriff auf diese Daten erhalten soll, ist ein Eingriff in die durch Art. 13 BV garantierten Ansprüche auf Privatsphäre und auf Achtung des Brief-, Post- und Fernmeldegeheimnisses denkbar. Indem Daten über die betroffene Person bearbeitet werden, ist immer auch das Recht auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV zu beachten. Diesbezüglich wird bereits in der Gesetzesvorlage explizit darauf hingewiesen, dass unter Umständen besondere Personendaten bearbeitet werden, welche etwa mit der Gesundheit oder den religiösen Ansichten in Verbindung stehen.[1361] Durch die auf den Smartphones enthaltenen Daten ist es unter Umständen sogar möglich, Einblick in wesentliche Aspekte über diese Person zu erhalten, was ein Persönlichkeitsprofil im Sinne von Art. 3 lit. d. DSG darstellt. Nicht vergessen werden darf, dass durch entsprechende Kontrollen auch unbeteiligte Dritte (etwa Personen, mit denen der Asylbewerbende kommuniziert hat) in diesen grundrechtlichen Positionen betroffen sein können.[1362] 590

1. Gesetzliche Grundlage

Die soeben vorgestellten Artikel sollen die gesetzliche Grundlage für den Eingriff in die Privatsphäre und das Recht auf informationelle Selbstbestimmung darstellen. Dabei sieht Art. 8a E-AsylG Vorgaben zur Datenbearbeitung etwa 591

1358 Auch diese Regelung wurde verschiedentlich kritisiert, mitunter wurde gar vom «gläsernen Flüchtling» geschrieben; vgl. BERGMANN, Beck-Komm. Ausländerrecht-D, Art. 15a, N. 2 ff.; vgl. die Stellungnahme.

1359 Siehe oben Rz. 406 ff.

1360 Vgl. etwa SCHWEIZER FLÜCHTLINGSHILFE, Fakten statt Mythen N° 78, 5. April 2017.

1361 Vernehmlassungsbericht Mitwirkung Asyl, S. 13.

1362 SCHWEIZER FLÜCHTLINGSHILFE, Fakten statt Mythen N°78, 5. April 2017.

hinsichtlich ihrer Formalitäten, der beteiligten Personen oder der Speicherung der Daten vor. Kritisiert wird von den Teilnehmenden der Vernehmlassung indes, dass keine abschliessende Definition der durchsuchbaren Geräte stattfindet.[1363] Dies ist vom Gesetzgeber so gewollt, damit auch zukünftige Technologien allenfalls darunterfallen.[1364] Meines Erachtens ist es wohl an dieser Stelle nicht zu vermeiden, dass eine gewisse technologische Offenheit besteht, wobei anzumerken gilt, dass zumindest auf kurze Sicht auch keine wesentlichen Technologien zu erwarten sind, welche für die Betroffenen im vorliegenden Zusammenhang zusätzliche Risiken bedeuten würden. Nach dem soeben Ausgeführten ist die Gesetzesgrundlage als genügend bestimmt zu erachten.

2. Öffentliches Interesse

592 Die Feststellung der Identität von Asylbewerbenden stellt einen wichtigen Teil des Asylverfahrens dar, da nur eruiert werden kann, ob eine Person den durch den Flüchtlingsstatus gewährten Schutz benötigt, wenn ihre Identität oder zumindest gewisse Informationen zu ihrer Person feststehen.[1365] Die Identitätsfeststellung dient somit der Rechtsverwirklichung und liegt folglich im öffentlichen Interesse.

3. Verhältnismässigkeit

593 Der Gesetzgeber erachtet die Regelung als verhältnismässig, da keine Abnahme bzw. zwangsweise Einziehung des Datenträgers gegen den Willen der betroffenen Person stattfindet. Zudem erfolgt die Auswertung der mobilen Datenträger nur, wenn andere Mittel zur Identitätsfeststellung ausgeschöpft sind. Die Datenauswertung geschieht überdies nur im Beisein der betroffenen Person, ausser diese verzichtet explizit darauf. Bis zum Zeitpunkt des Beizugs der Betroffenen findet kein Zugriff auf die Daten statt. Schliesslich wird den Asylbewerbenden immer zuerst die Gelegenheit eingeräumt, von sich aus Angaben zur Nationalität, zur Identität oder zum Reiseweg zu machen.[1366]

594 Verschiedene Vernehmlassungsteilnehmende stellten indes die Verhältnismässigkeit in Frage, wobei bereits die Eignung der Massnahme als fraglich

1363 Vgl. etwa DIGITALE GESELLSCHAFT, Stellungnahme zur Mitwirkungspflicht im Asylverfahren: Überprüfungsmöglichkeit bei Mobiltelefonen (17.423n Pa.Iv.) S. 5.

1364 Vernehmlassungsbericht Mitwirkung Asyl, S. 7.

1365 Vgl. etwa bereits: Botschaft Rev. AsylG 1996, S. 29.

1366 Vernehmlassungsbericht Mitwirkung Asyl, S. 6.

erachtet wurde.[1367] Die Daten, welche sich aus den Smartphones der Asylbewerbenden gewinnen lassen, können zwar für die Feststellung des Sachverhalts durchaus relevant sein, wenn sich entsprechende Erkenntnisse über die Identität oder Herkunft einer Person nicht auf anderem Wege feststellen lassen. Im Rahmen des oben erwähnten Pilotprojekts konnten damit indes nur in 15 % der Fälle nützliche Hinweise auf die Identität oder den Fluchtweg gewonnen werden.[1368] Auch in Deutschland wurde im Rahmen einer Studie festgestellt, dass bei den ausgewerteten Datenträgern in 33 % der Fälle die Identität belegt und in 2 % der Fälle die Identität widerlegt werden konnte.[1369]

Im Weiteren wird darauf verwiesen, dass es für die Migrationsbehörden 595
durchaus mildere Möglichkeiten gibt, um die Identität festzustellen, womit der entsprechende Grundrechtseingriff nicht erforderlich ist. Zu denken ist etwa an die detaillierte Befragung der Asylbewerbenden zu ihrer Herkunft und ihrer Flucht oder an LINGUA-Sprachanalysen.[1370] Der Vernehmlassungsbericht führt dazu aus, dass mildere Massnahmen dann angezeigt seien, wenn sie im Vergleich zur Datenauswertung mit geringerem Aufwand möglich seien, etwa durch präzise Angaben der Betroffenen, oder wenn andere eindeutige Dokumente (Führerschein, Geburtsurkunde) vorliegen. Eine sogenannte Herkunftsanalyse bzw. ein «LINGUA-Gutachten» wird jedoch als nicht verhältnismässig erachtet, da diese Mittel mit einem grossen zeitlichen und organisatorischen Aufwand verbunden sind.[1371] Dieser Ansicht ist aus zweierlei Gründen zu widersprechen. Einerseits spielen entsprechende Überlegungen hinsichtlich der Erforderlichkeit eine geringere Rolle, da es hier in erster Linie darum gehen soll, welcher Eingriff für den Betroffenen weniger invasiv ist.[1372] Anderseits dürfte auch die Speicherung und Auswertung der Daten zeitlich und organisatorisch anspruchsvoll sein, zumal Letztere grundsätzlich nur in Anwesenheit der Betroffenen (und allfälliger Übersetzer) durchgeführt werden darf.

1367 Vgl. etwa SFH, Stellungnahme Rev. AsylG, S. 7 oder DIGITALE GESELLSCHAFT, Stellungnahme zur Mitwirkungspflicht im Asylverfahren: Überprüfungsmöglichkeit bei Mobiltelefonen (17.423n Pa.Iv.),S. 5.

1368 SDA, Bund wertet Handydaten von Flüchtlingen aus, FM1 today, 10. August 2019.

1369 Vgl. etwa DPA, Auswertung der Handydaten von Flüchtlingen hilft kaum, Süddeutsche Zeitung, 16. Februar 2019 mit Verweis auf eine Studie des Bundesinnenministeriums.

1370 Vgl. DIGITALE GESELLSCHAFT, Stellungnahme zur Mitwirkungspflicht im Asylverfahren: Überprüfungsmöglichkeit bei Mobiltelefonen (17.423n Pa.Iv.), S. 7; MEYER, Kriminalistik. Unabhängige Zeitschrift für die kriminalistische Wissenschaft und Praxis, 2006.

1371 Vernehmlassungsbericht Mitwirkung Asyl, S. 6.

1372 SGK, Art. 36, N. 39; ähnlich SFH, Stellungnahme Rev. AsylG, S. 9.

596 Fraglich ist zudem, ob die entsprechende Mitwirkungspflicht für den Asylbewerber in Anbetracht der konkreten Umstände zumutbar ist. Dabei ist nach dem oben Ausgeführten unbeachtlich, dass sich aus der Mitwirkungspflicht allenfalls negative Auswirkungen für den Asylbewerbenden hinsichtlich der Behandlung seines Gesuchs ergeben können, indem sich etwa herausstellt, dass er die Behörden über seine Herkunft getäuscht hat.[1373] Zu beachten sind hinsichtlich der Zumutbarkeit indes die möglichen Eingriffe in die dargestellten Grundrechtspositionen der Betroffenen und allfälliger Dritter. Diese sind mit dem genannten öffentlichen Interesse abzuwägen.

597 Dabei kann es als schwerer Eingriff zu werten sein, dass auf höchstpersönliche Aufzeichnungen Zugriff genommen wird und besondere Personendaten bearbeitet werden. Dem gegenüber steht ein – nach dem soeben Geschriebenen – offenbar eher ungewisser Nutzen.

598 Weiter wird ein Vergleich zum Strafprozessrecht und zur Überwachung von Fernmeldediensten gemäss Art. 269 ff. StPO gezogen, welche nur unter strengen Voraussetzungen zulässig ist, etwa wenn eine schwere Straftat und ein konkreter Tatverdacht vorliegen, und für welche zudem gemäss Art. 272 StPO eine gerichtliche Genehmigung verlangt wird.[1374] Es erscheint kaum vertretbar, dass im Falle von Schutzsuchenden dieselben oder gar einschneidendere Regelungen zur Anwendung kommen sollen.[1375] Bereits nach dem Wortlaut von Art. 270 StPO umfasst diese Überwachung jedoch nur die Postadresse und den Fernmeldeanschluss eines Beschuldigten oder einer Drittperson und ist somit im hier interessierenden Kontext nicht anzuwenden. Die vorliegend zu beurteilende Durchsuchung ist m.E. eher mit der in Art. 246 ff. StPO geregelten Durchsuchung von Aufzeichnungen zu vergleichen, welche bereits gemäss dem Wortlaut von Art. 246 StPO «Schriftstücke, Ton-, Bild- und andere Aufzeichnungen, Datenträger sowie Anlagen zur Verarbeitung und Speicherung von Informationen» umfasst. Auch hier stehen den Betroffenen allerdings ein Recht auf vorgängige Äusserung (Art. 247 Art. 1 StPO) oder die Möglichkeit der Siegelung (Art. 248 StPO) und somit eine gerichtliche Überprüfung offen.

599 Auch wenn die Durchsuchung der Datenträger im Asylverfahren nach dem Ausgeführten im Gegensatz zu den soeben genannten strafprozessualen Massnahmen nicht erzwungen werden darf und es den Betroffenen jederzeit möglich ist, diese durch Vorbringen anderweitiger Beweise zu verhindern,

1373 Siehe oben Rz. 405.

1374 Vgl. DIGITALE GESELLSCHAFT, Stellungnahme zur Mitwirkungspflicht im Asylverfahren: Überprüfungsmöglichkeit bei Mobiltelefonen (17.423n Pa.Iv.), S. 10 f.

1375 Vgl. SCHWEIZER FLÜCHTLINGSHILFE, Fakten statt Mythen N°78, 5. April 2017.

ist zu beachten, dass eine Verweigerung im Rahmen der Glaubwürdigkeitsprüfung berücksichtigt wird und somit trotz fehlender Erzwingbarkeit der Mitwirkung nicht wirklich von Freiwilligkeit gesprochen werden kann.[1376]

Unter Abwägung all dieser Argumente ist es höchst fraglich, ob die vorgesehene Regelung in einer für den Asylbewerbenden zumutbaren Weise in seine Grundrechte auf Privatsphäre und informationelle Selbstbestimmung eingreift. Schliesslich ist auch der Eingriff in die Grundrechtspositionen unbeteiligter Dritter zu beachten, auf deren Daten ebenfalls Zugriff besteht. Auch wenn im Vernehmlassungsbericht ausgeführt wird, dass auf entsprechende Daten kein Zugriff erfolgen soll,[1377] stellt sich in der Praxis die unbeantwortete Frage, wie dies mit Blick auf den verfolgten Zweck sowie bei einer grossen Menge an Daten technisch und organisatorisch durchgeführt werden kann.[1378] 600

4. Fazit

Nach dem soeben Ausgeführten ist in Frage zu stellen, ob die Durchsuchung von elektronischen Geräten, in der Form, in welcher sie aktuell vorgesehen ist, verhältnismässig ausgestaltet ist. Probleme stellen sich hierbei insbesondere betreffend die Zumutbarkeit für die Betroffenen, aber auch für allfällige Drittpersonen. Die Regelung im deutschen Asylgesetz ist noch stärker als «ultima ratio» ausgestaltet, und es hat zudem eine Bearbeitung zu unterbleiben, wenn der Kernbereich privater Lebensgestaltung betroffen ist, womit diese Regelung wohl eher als verhältnismässig erachtet werden kann. Indes halten Kritiker aufgrund des unbestimmten Begriffs des Kernbereichs privater Lebensgestaltung auch diese Regelung für verfassungswidrig.[1379] 601

II. Neue Rechtsgrundlagen im Bereich der Amtshilfe

Das Erfordernis einer Gesetzesgrundlage zur Datenbearbeitung und -bekanntgabe nach Art. 17 und Art. 19 DSG führte im Laufe der letzten Jahre zu einer Vielzahl an neuen Gesetzesgrundlagen und Registern. Im Ausländerrecht wurde im Rahmen einer kürzlich ergangenen Revision des AiG zur Vielzahl an bereits bestehenden Datenbanken etwa ein «eRetour» geschaffen, welches die Arbeitsprozesse der Migrations- und Strafbehörden im Rückkehrbereich 602

1376 SFH, Stellungnahme Rev. AsylG, S. 11.

1377 Vernehmlassungsbericht Mitwirkung Asyl, S. 8.

1378 DIGITALE GESELLSCHAFT, Stellungnahme zur Mitwirkungspflicht im Asylverfahren: Überprüfungsmöglichkeit bei Mobiltelefonen (17.423n Pa.Iv.), S. 4.

1379 Vgl. etwa Stellungnahme; a.M. BERGMANN, Beck-Komm. Ausländerrecht-D, Art. 15a, N. 5.

verbessern soll.[1380] Zu beachten ist auch, dass Kantone und Gemeinden eigene Datenbanken oder Registerlösungen vorsehen, welche oft organisch gewachsen sind. Dies hat zu einer kaum mehr überblickbaren Registerlandschaft geführt, welche hier nicht weiter vorgestellt werden soll.[1381] Es stellt sich daher die Frage, warum nicht einfach eine Datenbank geschaffen wird, welche z.B. sämtliche relevanten Daten zum Ausländerrecht zusammenfasst. Im Folgenden soll die Frage erläutert werden, welche Grenzen einer Schaffung neuer gesetzlicher Grundlagen gesetzt sind.

A. Schaffung neuer gesetzlicher Grundlagen

603 Dem Aufbau neuer Datenbanken durch Gesetz sind gewisse Grenzen gesetzt. Diese ergeben sich einerseits aus allgemeinen rechtsstaatlichen Prinzipien und anderseits aus den Grundsätzen des Datenschutzes. Relevant ist dabei insbesondere der Grundsatz der Verhältnismässigkeit, welcher sowohl in Art. 5 Abs. 2 BV als auch in der Datenschutzgesetzgebung eine wichtige Rolle spielt. So ist stets zu fragen, ob die Beschaffung von Daten nicht auch mit einer anderen oder milderen Massnahme zu erreichen ist.[1382] Gemäss dem Grundsatz der Verhältnismässigkeit in Art. 4 Abs. 2 DSG darf der Datenbearbeiter nur diejenigen Daten erheben und bearbeiten, welche für den verfolgten Zweck geeignet sind und welche von ihm auch tatsächlich benötigt werden.[1383] Bei der Planung einer neuen gesetzlichen Grundlage für eine Datenbekanntgabe oder ein Abrufverfahren hat der Gesetzgeber immer abzuwägen, ob dies aus rechtlicher, finanzieller und organisatorischer Sicht Sinn macht.[1384] Insbesondere ist zu fragen, ob die Daten nicht auf eine grundrechtsschonendere Art und Weise, z.B. bei der betroffenen Person, besser oder zuverlässiger beschafft werden können.[1385]

604 Gerade weil der Gesetzgeber – nach dem bisher Ausgeführten – grosse Macht darüber hat, welche neuen Datenbanken und Register geschaffen werden, spielen die demokratische Kontrolle und Legitimation eine wichtige Rolle. Möglichkeiten dazu bieten in erster Linie das Vernehmlassungsverfahren und eine allfällige Referendumsabstimmung. Hierbei ist zu beachten, dass für die Bearbeitung von Personendaten grundsätzlich ein Gesetz im

1380 Vgl. Botschaft Rev. AuG 2018, S. 1685 ff.

1381 Vgl. etwa die Übersicht über die Registerlandschaft Schweiz von E-Government Schweiz.

1382 Vgl. zum Ganzen: Bericht Lustenberger, S. 683.

1383 BOLLIGER/FÉRAUD, S. 21.

1384 Vgl. Bericht Lustenberger, S. 683; siehe auch die Abwägungen im Statusbericht Datenaustausch, S. 7 ff.

1385 Vgl. Bericht Lustenberger, S. 655.

materiellen Sinn ausreichen kann, dieses also unter Umständen auch auf Verordnungsstufe erlassen werden kann. Das Vernehmlassungsverfahren ist dabei gemäss Art. 3 VlG unter anderem nur bei Gesetzesvorlagen oder Verordnungen und anderen Vorhaben anwendbar, die von grosser politischer, finanzieller, wirtschaftlicher, ökologischer, sozialer oder kultureller Tragweite sind. Auch das obligatorische und fakultative Referendum schliesst auf Bundesebene Verordnungen generell nicht ein (vgl. Art. 140 und 141 BV). Dies hat zu bedeuten, dass in diesen Fällen die Stimmbürger keine Möglichkeit haben, sich gegen eine aus ihrer Sicht zu weit gehende Datenbearbeitung zu wehren. Es ist daher auch aus diesem Grund richtig, dass die Bearbeitung besonderes schützenswerter Personendaten nach Art. 17 Abs. 2 DSG eine formell-gesetzliche Grundlage benötigt. Unabhängig davon, ob besonders schützenswerte Personendaten bearbeitet werden, ist daher richtigerweise auch bei sonstigen schwerwiegenden Eingriffen in die Persönlichkeitsrechte eine gesetzliche Grundlage im formellen Sinn zu fordern.[1386]

B. Besondere Voraussetzungen bei Abrufverfahren

Die Voraussetzungen für das Errichten neuer Abrufverfahren sind nach dem weiter oben Ausgeführten sehr streng.[1387] Dies führt dazu, dass aufgrund der langen Zeit, bis ein Gesetz oder eine Revision den Gesetzgebungsprozess durchlaufen hat, sowie aufgrund fehlender vorgängiger Evaluationsmöglichkeiten die entsprechenden Berechtigungen oftmals sehr grosszügig bemessen werden (etwa hinsichtlich des Kreises der Zugriffberechtigten oder der abrufbaren Daten).[1388] Es versteht sich von selbst, dass eine derart weite Umschreibung nicht sinnvoll ist und sich mit dem Zweckbindungsgebot nicht vereinbaren lässt. Aus diesem Grund wurde mit Art. 17a DSG eine gesetzliche Grundlage geschaffen, die es ermöglicht, dass der Bundesrat im Rahmen eines Pilotversuchs vor Inkrafttreten eines Gesetzes im formellen Sinn die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen für eine Dauer von bis zu fünf Jahren bewilligen kann. Dies soll es ermöglichen, die Auswirkungen einer geplanten Regelung während einer Pilotphase zu überprüfen und gestützt darauf die gesetzliche Grundlage entsprechend genauer auszuformulieren.[1389]

605

1386 Vgl. EPINEY/CIVITELLA/ZBINDEN PATRIZIA, S. 42; vgl. de lege ferenda immerhin Art. 30 Abs. 2 lit. c DSG, welcher eine gesetzliche Grundlage im formellen Sinn auch erforderlich macht, wenn der Zweck oder die Art und Weise der Bearbeitung zu einem schwerwiegenden Eingriff in die Grundrechte der Betroffenen führen.

1387 Siehe dazu oben Rz. 417.

1388 Vgl., Botschaft Rev. DSG 2003, S. 2142.

1389 Vgl. Botschaft Rev. DSG 2003, S. 2142 f. Entsprechende Regelungen bestehen oft auch auf kantonaler Stufe; vgl. etwa Art. 9a IDG BS.

III. Zusammenfassung

606 Die technologieneutrale Formulierung der Verwaltungsverfahrensgesetzgebung im Zusammenhang mit möglichen Beweismitteln lässt Möglichkeiten offen, um technologische Neuerungen in Verfahren nutzbar zu machen, wie etwa die Smartphones von Asylbewerbenden zu durchsuchen, um beispielsweise Auskünfte über ihre Herkunft zu erhalten. Die entsprechenden Möglichkeiten sind indes durch die Grundrechte der Betroffenen, insbesondere die informationelle Selbstbestimmung und das rechtliche Gehör, wiederum eingeschränkt und müssen insbesondere verhältnismässig ausgestaltet sein. Bezüglich der Amtshilfe werden vermehrt neue Gesetzesgrundlagen geschaffen, welche die Datenbekanntgabe von einer Behörde an die andere, unter Umständen gar mit Abrufverfahren, erlauben. Um den vollständig «gläsernen Bürger» zu verhindern, ist bei der Erstellung neuer Gesetzesgrundlagen immer auch die Verhältnismässigkeit zu beachten. In diesem Zusammenhang kommt auch der demokratischen Kontrolle durch Vernehmlassungsverfahren und Referenden ein grosses Gewicht zu.

§ 10 Automatisierte Einzelfallentscheidungen

I. Ausgangslage

A. Automatisierte Einzelfallentscheidungen in der Schweiz

607 Weiter vorne in dieser Arbeit wurde aufgezeigt, dass in der Schweiz in gewissen Bereichen bereits Entscheide durch Algorithmen vorbereitet werden. Dabei kommen teilweise und inskünftig wohl vermehrt komplexe maschinelle Lernverfahren zum Einsatz. Dies ist im Rahmen des geltenden Rechts grundsätzlich zulässig, wobei sich in gewissen dieser Anwendungsszenarien durchaus Probleme ergeben können, für welche die aktuelle Rechtsordnung noch keine befriedigende Lösung bereitstellt.[1390]

608 In den weiter oben vorgestellten Einsatzbereichen sind mit Rechtswirkungen für die Betroffenen verbundene Entscheide indes immer noch menschlichen Bearbeitern vorbehalten. Zumindest aus technischer Sicht wäre es nur noch ein kurzer Weg dahin, dass ein Computerprogramm anhand von vorprogrammierten (oder durch «Machine Learning» aufgestellten) Regeln basierend auf dem Dateninput eine Verfügung oder einen Entscheid selbständig fällt und direkt an den Betroffenen versendet, ohne dass ein Mensch diesen jemals zu Gesicht erhält. Daher kann die Frage gestellt werden, inwiefern

1390 Siehe zum Ganzen oben Rz. 423 ff.

dieser «Umweg» über den Menschen überhaupt noch notwendig ist. Die Vorteile, welche man sich aus der Entscheidungshilfe durch Algorithmen verspricht, könnten auf diese Weise noch in verstärktem Masse realisiert werden. Denkbar ist etwa, dass einfach strukturierte, gleichartige Verfahrensvorgänge sich auf diese Weise kosten- und zeiteffizient durch die Maschine erledigen lassen, während sich die menschlichen Bearbeitenden auf wenige, komplexere Fälle konzentrieren können.[1391] Es fragt sich indes, ob es rechtlich auch zulässig wäre, wenn der dafür eingesetzte Computer entsprechende Entscheidungen mit rechtlichen Konsequenzen vollständig und ausschliesslich selbst fällen würde.

609 In der Schweiz werden zum Zeitpunkt der Fertigstellung dieser Arbeit Algorithmen bereits in einem wachsenden Masse eingesetzt, um Entscheide vorzubereiten. Allerdings ist es soweit ersichtlich in Bund und Kantonen noch in keinem Bereich vorgesehen, dass «der Computer» vollständig allein entscheiden und verfügen kann. Anzumerken ist an dieser Stelle immerhin die automatisierte Grenzkontrolle bei der Ausreise aus dem Schengen-Raum an Schweizer Flughäfen. Hierbei werden die biometrischen Daten der Person erfasst und automatisiert mit den Daten im Pass sowie mit den zur Fahndung ausgeschriebenen Personen im Fahndungssystem (RIPOL) oder im Schengener Informationssystem (SIS) abgeglichen. Stimmen die Daten überein, so kann die Person die Grenze passieren, was eine automatisierte (formlose) positive Verfügung darstellt. Ergeben sich im Rahmen der Prüfung Auffälligkeiten, so wird ein automatisierter Grenzübertritt nicht zugelassen und es hat eine Grenzkontrolle durch einen Beamten zu erfolgen, welche allenfalls in einer nicht automatisierten Wegweisungsverfügung münden kann.[1392]

B. Internationale Bestrebungen

610 Nicht nur in der Schweiz stellt sich aufgrund der beschriebenen Vorzüge die Frage nach den Einsatzbereichen entsprechender automatisierter Einzelfallentscheidungen. In verschiedenen Ländern werden dabei bereits automatisierte Einzelfallentscheidungen eingesetzt oder es wurden zumindest entsprechende gesetzliche Grundlagen geschaffen. Gewisse Bereiche scheinen dabei insbesondere entsprechenden Bestrebungen offenzustehen, etwa das Steuerrecht. In Deutschland wurden etwa per 1. Januar 2017 die Rechtsgrundlagen für den ausschliesslich automationsgestützten Erlass von Steuerbescheiden geschaffen.[1393] Dazu wurde die Abgabenordnung um eine Bestimmung

1391 Siehe zum Ganzen bereits oben Rz. 424.

1392 Vgl. zum Ganzen RECHSTEINER, Jusletter, 26. November 2018, N. 8; Art. 45 Abs. 2 und 3 VEV; Bericht Smart Borders, S. 14 ff und 20.

1393 BRAUN BINDER, in: Digitalisierte Verwaltung – Vernetztes E-Government, S. 313, N. 6.

ergänzt, welche erlaubt, dass die Finanzbehörden «Steuerfestsetzungen sowie Anrechnungen von Steuerabzugsbeträgen und Vorauszahlungen auf der Grundlage der ihnen vorliegenden Informationen und der Angaben des Steuerpflichtigen ausschließlich automationsgestützt vornehmen, berichtigen, zurücknehmen, widerrufen, aufheben oder ändern, soweit kein Anlass dazu besteht, den Einzelfall durch Amtsträger zu bearbeiten»[1394]. Ein entsprechender Anlass kann etwa in der Meldung eines Risikomanagementsystems, durch Auswahl des Amtsträgers oder in einem Eintrag der steuerpflichtigen Person in ein dafür vorgesehenes Datenfeld bestehen.[1395]

611 Ebenfalls empfänglich für Automatisierung scheinen gewisse Bereiche der Leistungsverwaltung zu sein. In verschiedenen Ländern erfolgt beispielsweise die Auszahlung von Sozialleistungen (z.B. in Dänemark[1396] oder Finnland[1397]) oder Stipendien[1398] automatisch. In Estland wird im Rahmen der Subventionsverteilung mittels Luftaufnahmen geprüft, ob lokale Bauern ihre Felder dem Gesetz entsprechend geschnitten haben, und wenn dies der Fall ist, werden automatische Subventionszahlungen ausgelöst.[1399]

612 Es ist zu beachten, dass der Einsatz von Algorithmen in vielen Ländern kaum in umfassenden Gesetzen geregelt ist. Oftmals umfassen Regulierungsbestrebungen in erster Linie Einzelaspekte wie etwa die datenschutzrechtliche Behandlung des Einsatzes von automatisierten Einzelfallentscheidungen. Während internationale Verträge hinsichtlich dieses Themas aufgrund der Komplexität weitgehend fehlen, ist zu beachten, dass verschiedene internationale Organisationen hinsichtlich der Verwendung von «künstlicher Intelligenz» Richtlinien ausgearbeitet haben und dabei auch Handlungsempfehlungen an die Staaten abgeben.[1400] Entsprechende Richtlinien beruhen aber grundsätzlich auf dem Freiwilligkeitsprinzip, was damit erklärt wird, dass die Chancen und Risiken entsprechender KI-Systeme aktuell noch zu

1394 Art. 155 Abs. 4 Abgabeordnung.

1395 BRAUN BINDER, in: Digitalisierte Verwaltung – Vernetztes E-Government, S. 314, N 8.

1396 ALFTER, in: Automating Society – Taking Stock of Automated Decision-Making in the EU, S. 53.

1397 RUCKENSTEIN/VELKO, in: Automating Society – Taking Stock of Automated Decision-Making in the EU, S. 60 f.

1398 So etwa in Dänemark, vgl. ALFTER, in: Automating Society – Taking Stock of Automated Decision-Making in the EU, S. 49.

1399 NIILER, Can AI Be a Fair Judge in Court? Estonia Thinks So, WIRED, 25. März 2019.

1400 Vgl. zum Ganzen: WEBER/HENSELER, EuZ, 2020, S. 32 f.; Zu denken ist etwa an die Empfehlungen des Rats der OECD zu künstlicher Intelligenz oder an die Ethik-Leitlinien für eine vertrauenswürdige KI der Expertengruppe für Künstliche Intelligenz der Hochrangigen Expertengruppe KI; diese thematisieren jedoch den staatlichen Einsatz von KI kaum.

wenig bekannt sind und eine Überregulierung vermieden werden soll.[1401] Im Weiteren befasst sich auch die DSGVO unter anderem in Artikel 22 umfassend mit dem Einsatz automatisierter Einzelfallentscheidungen.[1402]

Im Folgenden soll überprüft werden, ob automatisierte Einzelfallentscheidungen wie in den genannten Beispielen auch in der Schweiz zulässig wären und welche Anpassungen allenfalls an der Rechtsordnung gemacht werden müssten. 613

II. Zulässigkeit automatisierter Einzelfallentscheidungen

A. Bedarf einer gesetzlichen Grundlage

Zumal es grundsätzlich nicht relevant ist, welche Mittel die Behörde zur Erreichung des jeweiligen Zwecks einsetzt, wird für den Einsatz von Algorithmen als Entscheidungshilfe, wie weiter vorne ausgeführt, nicht grundsätzlich eine spezifische gesetzliche Grundlage benötigt. Der Einsatz ist oft durch die allgemeine gesetzliche Grundlage für die jeweilige Aufgabe gedeckt. Gesetzliche Grundlagen können indes aus anderen Gründen relevant sein, etwa hinsichtlich der Verwendung der Daten, welche durch den jeweiligen Algorithmus bearbeitet werden.[1403] Es ist daher die Frage zu stellen, inwiefern automatisierte Einzelfallentscheidungen ohne menschliche Einflussnahme sich von der Entscheidungsunterstützung unterscheiden und ob diese für die Betroffenen allenfalls zusätzliche Gefahren mit sich bringen, welche deren Einsatz verbieten bzw. eine explizite gesetzliche Grundlage als notwendig erscheinen lassen. 614

1. Abgrenzung zu Algorithmen als Entscheidungshilfe

Bei der blossen Verwendung von Algorithmen als Entscheidungshilfe liegt die Entscheidungsverantwortung immer beim Menschen. Automatisierte Einzelfallentscheidungen zeichnen sich hingegen dadurch aus, dass sie ausschliesslich automatisiert gefällt werden. Dies bedeutet, dass sowohl die inhaltliche Bewertung des Sachverhalts und der sich stellenden Rechtsfragen als auch die Subsumtion durch einen Algorithmus erfolgen. Es findet keine inhaltliche Beurteilung des konkreten Falles durch eine natürliche Person statt.[1404] Keine automatisierte Einzelfallentscheidung liegt vor, wenn die natürliche 615

1401 GUCKELBERGER, S. 125.

1402 Siehe dazu im Detail weiter unten Rz. 648 ff.

1403 Vgl. zum Ganzen weiter oben Rz. 435 ff.

1404 Botschaft Rev. DSG 2017, S. 7056 f.; vgl. etwa auch BUCHNER, Beck-Komm. DSGVO, Art. 22, N. 15.

Person eine Entscheidungsbefugnis hat und diese im Einzelfall auch ausübt.[1405] Der zulässige menschliche Einfluss auf eine automatisierte Entscheidung beschränkt sich grundsätzlich auf die Programmierung und Instandhaltung des Systems.[1406] Es ist unbestritten, dass eine automatisierte Einzelfallentscheidung auch vorliegen kann, wenn der automatisiert gefällte Entscheid durch eine Person den Betroffenen mitgeteilt wird, sofern diese Person keinen sonstigen Einfluss auf den Entscheid hat.[1407] Auch wenn eine natürliche Person die Arbeit des Algorithmus lediglich überwacht und stichprobenweise oder auf Bitte des Betroffenen eingreifen kann, so wird davon ausgegangen, dass es sich gleichwohl um eine automatisierte Einzelfallentscheidung handelt.[1408]

2. Rechtlich relevante Unterschiede

616 Wie weiter oben ausführlich untersucht wurde, bringt der Einsatz von Algorithmen als Entscheidungshilfe gewisse Nachteile oder Risiken für die betroffenen Personen mit sich, etwa hinsichtlich des vermehrten Bedarfs an Personendaten zur Errechnung genauer Vorhersagen oder hinsichtlich der Gehörsgewährung bei komplexen Entscheidungen. Vollständig automatisierte Verfahren sind nicht allein dadurch per se datenschutzrechtlich gefährlicher für das Individuum, dass die Daten nun vollständig von einer Maschine bearbeitet werden. Vielmehr ist die datenschutzrechtliche Zulässigkeit anhand der weiter oben genannten Kriterien im jeweiligen Anwendungsfall zu beurteilen. Auch vollständig automatisierten Entscheidungen können in ihren Berechnungen die oben genannten Fehlerarten unterlaufen, wobei die Korrektive wie das rechtliche Gehör oder das Diskriminierungsverbot denselben Einschränkungen unterliegen, wie wenn ein Entscheid durch die Maschine nur vorbereitet wird. Bei vollständig automatisierten Einzelfallentscheidungen besteht allerdings eine zusätzliche Gefahr für die Betroffenen dadurch, dass der menschliche Einfluss als Korrektiv wegfällt. Ein menschlicher Entscheidungsträger kann, zumindest wenn ihm ein Entscheid krass unrichtig erscheint, die Maschine überstimmen und einen abweichenden Entscheid treffen oder untersuchen (lassen), wieso die Maschine einen aus seiner Sicht unzutreffenden Rat erteilt. Automatisierte Einzelfallentscheide zeichnen sich hingegen durch die Abwesenheit jeglichen menschlichen Einflusses aus.

1405 MARTINI, Paal/Pauly DSGVO, Art. 22, N. 19; RECHSTEINER, Jusletter, 26. November 2018, N. 6.

1406 RECHSTEINER, Jusletter, 26. November 2018, N. 5.

1407 Botschaft Rev. DSG 2017, S. 7057.

1408 MARTINI, Paal/Pauly DSGVO, Art. 22, N. 19; RECHSTEINER, Jusletter, 26. November 2018, N. 6.

Diese Überlegungen zeigen auf, dass Grundrechtspositionen der Betroffenen durch eine automatisierte Einzelfallentscheidung unter Umständen stärker betroffen sein können, als wenn Algorithmen lediglich zur Unterstützung eingesetzt werden. Der aus rechtlicher Sicht wichtigste Unterschied besteht jedoch darin, dass beim Einsatz von Algorithmen zur Entscheidungsunterstützung aus dem Befund der Maschine keine direkten Rechten und Pflichten für den Betroffenen begründet werden. Es obliegt der jeweiligen Behörde, ob gestützt auf die Entscheidung der «Maschine» weitere Schritte unternommen werden. So kann etwa das «DyRias»-System ausweisen, dass von einer Person ein Gefahrenpotenzial ausgeht. Der zuständige Polizeibeamte muss allerdings gestützt auf diese Prognose selbständig entscheiden, ob er die Person z.B. zu einem Gespräch einlädt oder strafprozessuale Zwangsmassnahmen gegen sie ergreifen will. Die entsprechenden Massnahmen müssen sich, wie jedes staatliche Handeln, bereits aufgrund des Legalitätsprinzips auf eine gesetzliche Grundlage stützen können.[1409] 617

Bei einer vollständig automatisierten Entscheidung entfällt dieser Zwischenschritt über den Menschen. Die Verfügung, welche beim Betroffenen Rechte und Pflichten begründen kann, muss indes dennoch auf eine gesetzliche Grundlage gestützt werden können. Aus verschiedenen Überlegungen dürfte sogar eine gesetzliche Grundlage im formellen Sinn zu fordern sein. Dies kann einerseits aus datenschutzrechtlichen Gründen der Fall sein. Nach aktuellem Recht fordert Art 17 Abs. 2 DSG eine Grundlage in einem formellen Gesetz zumindest bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen. De lege ferenda sieht Art. 30 Abs. 2 lit. c E-DSG vor, dass eine entsprechende gesetzliche Grundlage auch notwendig ist, wenn der Zweck oder die Art und Weise der Bearbeitung geeignet sind, schwerwiegend in die Persönlichkeitsrechte der Betroffenen einzugreifen, wobei automatisierte Einzelfallentscheidungen in der Botschaft explizit als Beispiel genannt werden.[1410] Anderseits ergibt sich bereits aus Art. 164 Abs. 1 BV, dass alle wichtigen rechtsetzenden Bestimmungen in der Form eines Bundesgesetzes erlassen werden.[1411] Als wichtig gelten dabei insbesondere Bestimmungen, welche massgeblich in die bestehende Rechtsstellung der Adressaten eingreifen, eine grosse Anzahl von Adressaten oder Sachverhalten erfassen und die Organisation und das Verfahren betreffen.[1412] Automatisierte 618

1409 EPINEY, BSK BV, Art. 36 N. 40.

1410 Botschaft Rev. DSG 2017, S. 7080.

1411 Viele kantonale Verfassungen sehen ähnliche Bestimmungen vor; vgl. RECHSTEINER, Jusletter, 26. November 2018, N. 40.

1412 WYTTENBACH/WYSS, BSK BV, Art. 164, N. 9.

Entscheidungen sind geeignet, Rechte und Pflichten bei den Betroffenen festzulegen und sie – nach dem soeben Geschriebenen – erheblich in Grundrechtspositionen zu treffen. Zudem betreffen sie die Organisation und das Verfahren einer Bundesbehörde und haben potenziell einen grossen Adressatenkreis bzw. können eine grosse Zahl von Lebenssachverhalten betreffen, was ebenfalls für die Wichtigkeit im Sinne von Art. 164 BV spricht.[1413]

3. Fazit

619 Der Einsatz von vollautomatisierten Einzelfallentscheidungen bringt für die Grundrechtspositionen der Betroffenen aus verschiedenen Gründen ein erhebliches Schädigungspotenzial mit sich, gerade auch im Vergleich zum unterstützenden Einsatz von Algorithmen. Insbesondere wäre auf diese Weise der Computer in der Lage, ohne menschlichen Einfluss sowie ohne Gewährung des rechtlichen Gehörs Rechte und Pflichten bei den Betroffenen zu begründen und damit Eingriffe in Grundrechtspositionen zu verursachen. Da entsprechende Entscheidungen zudem eine Vielzahl an Personen betreffen können, ist für den Einsatz von automatisierten Einzelfallentscheidungen zum Erlass einer Verfügung nach geltendem Recht eine gesetzliche Grundlage im formellen Sinn zu fordern. Wo keine solche besteht, darf auch keine automatisierte Einzelfallentscheidung vorgenommen werden.

B. Automatisierbare Entscheide

620 Nach dem soeben Ausgeführten könnte, eine entsprechende gesetzliche Grundlage vorausgesetzt, jeder Entscheid grundsätzlich auch automatisiert erfolgen. Es lässt sich allerdings fragen, ob in technischer Hinsicht jeder Entscheid in einer Art und Weise automatisiert werden kann, dass den rechtlichen Anforderungen Genüge getan wird. Automatisierte Einzelfallentscheidungen basieren auf durch die Entwickler oder ein maschinelles Lernprogramm vorgegebenen Kriterien, nach welchen die jeweiligen Input-Daten verarbeitet werden. Die Programme können dabei nicht von den jeweiligen vorgängig programmierten Regeln abweichen, was mitunter zu stossenden oder diskriminierenden Ergebnissen führen kann.[1414]

621 Hierbei ist die generelle Frage zu stellen, inwiefern sich das Recht durch IT abbilden lässt.[1415] Dabei ist festzuhalten, dass bei richterlichen Entscheidungen die individuellen Erfahrungen der Richter und deren soziales Umfeld

1413 RECHSTEINER, Jusletter, 26. November 2018, N. 15.

1414 Siehe dazu oben Rz. 460 ff.

1415 Für eine Abbildung der hierzu in der deutschen Literatur vertretenen Postionen vgl. GUCKELBERGER S. 369 ff.

immer auch eine Rolle spielen und richterliches Urteilen somit keine mechanische Tätigkeit darstellt. Dies würde umfassend gegen eine Automatisierbarkeit von Entscheiden sprechen. Allerdings gilt es zu beachten, dass auch menschliche Entscheidungen in der Verwaltung etwa durch interne Verwaltungsvorschriften, Dienstanweisungen oder Formulare in der Regel bis zu einem gewissen Grad vorstrukturiert werden, um einen einheitlichen Gesetzesvollzug sicherstellen zu können.[1416] Aber gerade um stossende Ergebnisse zu verhindern und eine Einzelfallgerechtigkeit zu ermöglichen, lässt der Gesetzgeber den Behörden in vielen Bereichen Ermessens- und Beurteilungsspielräume etwa durch Kann-Vorschriften oder die Aufzählung möglicher Rechtsfolgen.[1417] Diese Ermessensspielräume lassen die aktuell noch bestehenden Leistungsschranken von Algorithmen offenbar werden.[1418] Sie können durch regelbasierte Algorithmen nicht ausgefüllt werden, da sich diese an die programmierten Regeln halten und die Einzelfallgerechtigkeit gerade der Möglichkeit zur Abweichung von der Regel bedarf.[1419] Bei Algorithmen, welche auf maschinellen Lernverfahren basieren, besteht zwar keine vorgängige, starre Regelbindung, jedoch beruht hier die Entscheidung auf einer Auswertung vergangener Entscheidungen. Dies steht einer dem Einzelfall gerecht werdenden Beurteilung eines noch nicht bekannten Sachverhalts entgegen.[1420]

In Deutschland wird daher in § 35a VwVfG für das Verwaltungsverfahren explizit vorgesehen, dass automatisierte Einzelfallentscheidungen nur zulässig sind, sofern kein Ermessen oder kein Beurteilungsspielraum besteht.[1421] Wesentliche Überlegungen sprechen auch in der Schweiz dafür, dass Entscheide, welche einen Ermessensspielraum vorsehen, nicht Gegenstand von automatisierten Einzelfallentscheidungen bilden sollen. Räumt der Gesetzgeber einer Behörde einen Ermessensspielraum ein, so ist diese in ihrer Entscheidung nicht gänzlich frei, sondern muss dieses Ermessen pflichtgemäss ausüben. Im Gegensatz zu einem bloss unangemessenen Entscheid, welcher zwar innerhalb des eingeräumten Ermessensspielraums liegt, bei dem aber das Ermessen unzweckmässig gehandhabt wurde, stellt eine Ermessensunterschreitung eine Rechtsverletzung dar. Dies ist insbesondere deshalb relevant, weil Verwaltungsbehörden in der Regel einen Entscheid 622

1416 BERGER, NVwZ, 2018, S. 1262; GUCKELBERGER, S. 383.

1417 RECHSTEINER, Jusletter, 26. November 2018, N. 29.

1418 MARTINI/NINK, NVwZ-Extra, 2017, S. 2.

1419 MARTINI/NINK, NVwZ-Extra, 2017, S. 2; SIEGEL, DVBl, 2017, S. 26; siehe auch BRAUN BINDER, NVwZ, 2016, S. 963.

1420 RECHSTEINER, Jusletter, 26. November 2018, N. 29.

1421 Vgl. BERGER, NVwZ, 2018, S. 1263, welche dieses Unterscheidungskriterium allerdings nicht für gänzlich überzeugend hält.

auch auf seine Angemessenheit überprüfen können, Verwaltungsgerichte jedoch in der Regel nur eine Rechtskontrolle vornehmen und somit überprüfen, ob eine Unter- oder Überschreitung bzw. ein Missbrauch des Ermessens vorliegt.[1422]

623 Falls nun eine Behörde einen Algorithmus einsetzt, so verzichtet sie ganz oder teilweise auf ein Ermessen, das ihr eingeräumt wurde, da die algorithmische Entscheidfindung – zumindest nach dem aktuellen Stand der Technik – dieses Ermessen nicht korrekt abzubilden vermag.[1423] Ein entsprechender Entscheid müsste also sowohl von einer verwaltungsinternen als auch von einer gerichtlichen Rechtsmittelinstanz aufgehoben werden, da es sich um eine unzulässige Ermessensunterschreitung handelt. Es ist daher als folgerichtig zu erachten, dass zum jetzigen Zeitpunkt das Vorliegen eines Ermessensspielraums einer automatisierten Einzelfallentscheidung entgegensteht.

III. Regelung der automatisierten Einzelfallentscheidung «de lege ferenda»

624 Bis anhin kennt das geltende Recht weder auf Bundes- noch auf kantonaler Ebene eine gesetzliche Grundlage für automatisierte Einzelfallentscheidungen. Der Gesetzgeber hat erkannt, dass aufgrund der Art und Weise der Datenbearbeitung gerade auch automatisierte Einzelfallentscheidungen einen schweren Eingriff in die Grundrechte der betroffenen Person darstellen können.[1424] Er hat daher entschieden, im Rahmen der Revision des Datenschutzgesetzes einige allgemeinverbindliche Regelungen zu automatisierten Einzelfallentscheidungen aufzunehmen.[1425]

625 Art. 19 E-DSG sieht aus diesem Grund neu eine Informationspflicht bei automatisierten Einzelfallentscheidungen vor, sofern diese für die Betroffenen mit einer Rechtsfolge verbunden sind oder sie erheblich beeinträchtigen. Damit die Beeinträchtigung als erheblich im Sinne dieses Gesetzes gilt, muss die Person auf nachhaltige Weise, etwa in ihren wirtschaftlichen Belangen, eingeschränkt werden. Im öffentlich-rechtlichen Bereich ist die Voraussetzung regelmässig durch das Eintreten einer Rechtsfolge, insbesondere durch die Eröffnung der Verfügung, erfüllt.[1426] Als automatisierte Einzelfallentscheidungen gelten dabei, wie bereits ausgeführt, nur diejenigen Entscheide, bei

1422 Vgl. zum Ganzen: HÄFELIN/MÜLLER/UHLMANN, N. 439 ff.

1423 RECHSTEINER, Jusletter, 26. November 2018, N. 29.

1424 Botschaft Rev. DSG 2017, S. 7080.

1425 Vgl. Art. 19 E-DSG; Botschaft Rev. DSG 2017, S. 7056.

1426 Botschaft Rev. DSG 2017, S. 7057.

welchen keine inhaltliche Bewertung und keine Entscheidung durch eine natürliche Person stattgefunden haben.[1427] Gemäss Art. 19 Abs. 2 E-DSG muss der betroffenen Person auf Antrag die Möglichkeit gegeben werden, ihren Standpunkt darzulegen und zu verlangen, dass die Entscheidung von einer natürlichen Person gefällt wird. Diese Einschränkung gilt allerdings unter Umständen nach Art. 19 Abs. 4 E-DSG für Bundesorgane nicht.[1428] Dafür trifft das Bundesorgan gemäss dieser Bestimmung zusätzlich die Pflicht, die Entscheidung entsprechend zu kennzeichnen.

626 Weitere Bestimmungen befassen sich ebenfalls mit automatisierten Einzelfallentscheidungen. So erteilt Art. 23 Abs. 2 lit. f E-DSG betroffenen Personen unter anderem das Recht, über das Vorliegen einer automatisierten Einzelfallentscheidung sowie die Logik, auf der die Entscheidung beruht, Auskunft zu erhalten. Dieses Auskunftsrecht umfasst keinen Anspruch auf eine Einsicht in die detaillierte Funktionsweise der Algorithmen, welche – wie bereits an anderer Stelle erwähnt – den meisten Betroffenen mangels Programmierkenntnissen wohl auch kaum weiterhelfen würde und zudem oftmals dem Geschäftsgeheimnis unterstehen kann. Gefordert sind lediglich Informationen über die grundlegenden Funktionen des Algorithmus.[1429] Im Weiteren ist Art. 30 E-DSG zu beachten, welcher den bestehenden Art. 17 DSG übernimmt und für jede Datenbearbeitung eine gesetzliche Grundlage fordert. Nach dem weiter oben Ausgeführten, wird gerade bei automatisierten Einzelfallentscheidungen gemäss Art. 30 Abs. 2 lit. c. E-DSG oftmals gar eine gesetzliche Grundlage im formellen Sinn zu fordern sein.[1430]

627 Zudem hat der Gesetzgeber die Gelegenheit der Revision des Datenschutzgesetzes genutzt und schlägt in diesem Rahmen Änderungen an anderen Erlassen vor, welche in den jeweiligen Rechtsbereichen automatisierte Einzelfallentscheidungen ermöglichen sollen. Vorgesehen ist die automatisierte Festsetzung bei der Schwerverkehrsabgabe, bei der Berechnung des Steuerbetrags nach Tabaksteuergesetz und Mineralölsteuergesetz sowie bei der Veranlagung nach dem Zollgesetz und dem Biersteuergesetz. Zudem sollen im Bereich der Unfall- und der Militärversicherung die verantwortlichen Organe pauschal dazu ermächtigt werden, automatisierte Verfügungen zu erlassen (Art. 96 Abs. 2 E-UVG, Art. 94*a* Abs. 2 E-MVG).[1431]

1427 Siehe dazu weiter oben Rz. 42.

1428 Der entsprechende Artikel wurde im Laufe des Gesetzgebungsverfahrens mehrmals verändert und soll weiter unten eingehender betrachtet werden, siehe sogleich Rz. 628 ff.

1429 Botschaft Rev. DSG 2017, S. 7067.

1430 Vgl. oben Rz. 616.

1431 RECHSTEINER, Jusletter, 26. November 2018, N. 16.

IV. Vereinbarkeit der Regelungen «de lege ferenda» mit übergeordnetem Recht

A. Rechtliches Gehör

628 Bereits im Zusammenhang mit der Verwendung von Algorithmen als Entscheidungsunterstützung wurde auf die Wichtigkeit der vorgängigen Anhörung der Betroffenen vor Erlass einer Verfügung und auf die Begründungspflicht hingewiesen, welche sich beide aus dem Anspruch auf rechtliches Gehör gemäss Art. 29 BV ergeben. Daher ist es nicht erstaunlich, dass dieser Aspekt auch in die Revision des Datenschutzgesetzes Eingang gefunden hat, indem etwa Artikel 19 Abs. 2 DSG der von einer automatisierten Einzelfallentscheidung betroffenen Person die Möglichkeit gibt, ihren Standpunkt vor Erlass einer Entscheidung darzulegen. Zu beachten ist hierbei die Ausnahme für Bundesorgane in Art. 19 Abs. 4 E-DSG, gemäss der diese Möglichkeit des «menschlichen Gehörs» wegfallen kann, «wenn die betroffene Person nach Artikel 30 Absatz 2 des Verwaltungsverfahrensgesetzes vom 20. Dezember 1968 oder nach einem anderen Bundesgesetz vor dem Entscheid nicht angehört werden muss». Es wird im Folgenden zu untersuchen sein, ob diese Ausnahme von einer Gehörsgewährung auch im automatisierten Entscheidungsverfahren mit dem grundsätzlichen Anspruch auf rechtliches Gehör vereinbar ist.

629 Die Bestimmung in Art. 19 Abs. 4 E-DSG hat eine bewegte Entstehungsgeschichte und wurde vom Vorentwurf über die Parlamentsberatungen mehrfach geändert. So sah Art. 15 Abs. 3 des VE-DSG vor, dass die Informationspflicht und das Anhörungsrecht nicht gelten, wenn ein Gesetz eine automatisierte Einzelfallentscheidung vorsieht. Im E-DSG wurde die Bestimmung dahingehend abgeändert, dass kein Anspruch auf «menschliches Gehör» bestehe, wenn der betroffenen Person gegen die Entscheidung ein Rechtsmittel zur Verfügung stehe. Gemäss der aktuellen Fassung von Art. 19 Abs. 4 E-DSG besteht nun grundsätzlich eine Pflicht zur vorgängigen Anhörung gemäss Art. 30 VwVG, es sei denn, diese sei explizit durch Art. 30 Abs. 2 VwVG oder ein anderes Bundesgesetz ausgeschlossen.

630 Bereits anlässlich des Vorentwurfs wurde davon ausgegangen, dass die Informationspflicht und das Anhörungsrecht, welche Art. 15 VE-DSG vorsah, sich vollständig mit den sich aus dem rechtlichen Gehör ergebenden Ansprüchen auf Anhörung vor dem Erlass einer Verfügung decken. Auch das in Art. 20 Abs. 2 lit. e und Art. 20 Abs. 3 VE-DSG enthaltene Auskunftsrecht über das Vorliegen, Zustandekommen, Ergebnis und die Auswirkungen der Entscheidung, wird als Teilgehalt des rechtlichen Gehörs betrachtet.[1432] Eine Wiederholung

1432 ROTH, digma, 2017, S. 105.

dieser Ansprüche im Datenschutzgesetz wurde vereinzelt als problematisch angesehen aufgrund der Frage, in welchem Verhältnis der aus einer entsprechenden widerrechtlichen Datenbearbeitung ergebende Berichtigungsanspruch zum Anspruch aus der Gehörsverletzung steht.[1433]

631 Da der Anspruch auf rechtliches Gehör nicht zu bürokratischen Leerläufen führen soll, sieht bereits Art. 30 Abs. 2 VwVG einige Ausnahmen vor, in denen von einer vorgängigen Anhörung abgesehen oder diese auf eine andere Weise nachgeholt werden kann.[1434] Zumal der aus Art. 19 Abs. 4 E-DSG resultierende Anspruch auf Anhörung sich nach dem soeben Geschriebenen nicht vom Anspruch auf rechtliches Gehör unterscheidet, ist es sinnvoll, dass die entsprechenden Einschränkungen auch für Ersteren gelten. Problematisch wäre unter diesem Aspekt jedoch die ursprünglich vorgesehene Variante in Art. 19 Abs. 4 E-DSG gewesen, welche einen Verzicht auf «menschliches Gehör» vorsah, wenn der betroffenen Person gegen die Entscheidung ein Rechtsmittel zur Verfügung steht. Dies wurde in der Botschaft damit begründet, dass es der Person durch die Ergreifung des Rechtsmittels möglich bleibt, ihren Standpunkt darzulegen und einen Entscheid durch eine natürliche Person zu erwirken.[1435]

632 Die Begründung, dass eine entsprechende Anhörung auf Rechtsmittelstufe nachgeholt werden kann, greift indes mit Blick auf die Praxis zum rechtlichen Gehör zu kurz.[1436] Es ist in der Lehre und Rechtsprechung anerkannt, dass Verfahrensgrundrechte wie das Recht auf Äusserung in anderer als der üblichen Form gewährt werden können, etwa im Rahmen eines Einspracheverfahrens.[1437] Hierbei befasst sich dieselbe Behörde erneut mit der Sache und nicht erst die Rechtsmittelinstanz. Zudem ist ein Einspracheverfahren in der Regel kostenlos und weniger formalisiert als ein Rechtsmittelverfahren.[1438] Eine Gehörsverletzung kann ausnahmsweise geheilt werden, wenn sie nicht besonders schwer wiegt und die betroffene Person sich in einem Rechtsmittelverfahren vor einer Instanz mit derselben Kognition wie die verfügende Behörde äussern kann oder wenn durch die Rückweisung an die Vorinstanz ein formalistischer Leerlauf entstehen würde.[1439] Letzteres kann indes nur

1433 Zum Ganzen ROTH, digma, 2017, S. 105; vgl. die Diskussion zum Verhältnis von Art. 25 DSG und der Ergreifung eines Rechtsmittels: BANGERT, BSK DSG/BGÖ, Art. 25 DSG, N. 66.

1434 WALDMANN/BICKEL, PK VwVG, Art. 30, N. 9 f.

1435 Botschaft Rev. DSG 2017, S. 7059.

1436 RECHSTEINER, Jusletter, 26. November 2018, N. 20 ff.

1437 Vgl. etwa STEINMANN, SG Komm. BV, Art. 29, N. 8 und 51 f.

1438 RECHSTEINER, Jusletter, 26. November 2018, N. 21 f.

1439 Vgl. etwa BGE 142 II 218, E. 2.8.1 (Pra 106/2017 Nr. 2), 137 I 195, E. 2.3.2; BIAGGINI, OFK BV, Art. 29, N. 9.

für den konkreten Einzelfall beurteilt und gerade bei einer automatisierten Einzelfallentscheidung nicht grundsätzlich angenommen werden.[1440]

633 Durch die Abänderung der Bestimmungen im Rahmen der parlamentarischen Beratungen haben die Räte dieses Problem beheben können. Nach dem soeben Geschriebenen ist im Rahmen automatisierter Einzelfallentscheidungen zulässig, den Anspruch auf vorgängige Anhörung zu beschränken, wenn dieser auch bei einer nicht automatisiert erlassenen Verfügung lediglich einen Leerlauf darstellen würde und deswegen aufgrund von Art. 30 Abs. 2 VwVG oder einer spezialgesetzlichen Regelung eingeschränkt ist bzw. in einem späteren Verfahrensschritt ohne Nachteile für den Betroffenen nachgeholt werden kann. Entsprechend diesen Erkenntnissen wird im «Leitfaden der Konferenz der Kantonsregierungen betreffend Anpassungsbedarf bei den kantonalen (Informations- und) Datenschutzgesetzen aufgrund der EU-Datenschutzreform und der Modernisierung der Europaratskonvention 108» festgehalten, dass in den kantonalen Gesetzen keine Regelung zum Thema der automatisierten Einzelfallentscheidungen notwendig ist, sofern sichergestellt ist, dass die Person über die Entscheidung informiert wird und die Möglichkeit hat, sich zum Entscheid zu äussern.[1441] Gestützt auf diese Empfehlung verzichten viele Kantone daher im Rahmen der Anpassung ihrer Datenschutzgesetze an die DSGVO und das totalrevidierte Datenschutzrecht darauf, spezifische Regelungen zu dieser Thematik aufzunehmen.[1442]

634 Dies entbindet sie nach dem oben Ausgeführten indes nicht davon, dass etwa aufgrund der Art und Weise der Datenbearbeitung dennoch eine gesetzliche Grundlage für den jeweiligen Einsatzbereich geschaffen werden muss.[1443] Eine gewichtige Einschränkung wird zudem angebracht, falls in Zukunft automatisierte Entscheidungen vorgesehen werden sollten, die nicht in der Form einer Verfügung erlassen werden, aber dennoch rechtliche Wirkungen für die betroffene Person erzeugen sollen, da in solchen Fällen die oben beschriebenen Schutzvorrichtungen für die betroffene Person wegfallen. In solchen Fällen müssen im jeweiligen Rechtsbereich im Rahmen einer ausdrücklichen und formell-gesetzlichen Grundlage für die betreffenden Entscheidungen geeignete Massnahmen zum Schutz der Rechte der jeweiligen Person vorgesehen und ihr insbesondere die Möglichkeit gegeben werden, sich zur automatisierten Einzelfallentscheidung zu äussern.[1444] Eine Lehrmeinung vertritt indes, dass das durch Art. 15 VE-DESG (bzw. Art. 19 E-DSG)

1440 RECHSTEINER, Jusletter, 26. November 2018, N. 21.

1441 Leitfaden, S. 15.

1442 Vgl. etwa Vorlage Rev. IDG BL, S. 10.

1443 Siehe oben Rz. 616 ff.

1444 Leitfaden, S. 15; PRIVATIM, Zusammenfassung Stellungnahme DSG, S. 8 f.

postulierte Anhörungsrecht nicht über den durch Art. 25a VwVG gewährten Rechtsschutz bei Realakten hinausgeht und somit bereits gestützt auf diese Bestimmung ein genügender Schutz besteht.[1445]

B. Ermessensspielraum

Im Rahmen der Revision des Datenschutzrechts wurden neben den soeben vorgestellten Vorgaben an das Verfahren und die Betroffenenrechte bereits erste Grundlagen geschaffen, welche in gewissen Rechtsbereichen automatisierte Entscheidungen im Einzelfall ermöglichen sollen. Der Schweizer Gesetzgeber sieht dabei im Gegensatz zum deutschen § 35a VwVfG zumindest im Rahmen der Revision des Datenschutzgesetzes keine grundsätzliche Einschränkung der Zulässigkeit von automatisierten Einzelverfahren auf Entscheidungen ohne Ermessens- oder Beurteilungsspielraum vor. Somit stünden grundsätzlich alle Verwaltungsentscheidungen der Automatisierung offen, sofern eine entsprechende formell-gesetzliche Grundlage geschaffen wird. Nach dem weiter vorne Ausgeführten ist indes zum jetzigen Zeitpunkt davon auszugehen, dass Algorithmen Rechtsfragen, welche der jeweiligen Behörde einen Ermessensspielraum zugestehen, noch nicht vollständig beurteilen können und daher entsprechende Entscheide aufgrund einer Ermessensunterschreitung stets von der Gefahr einer gerichtlichen Anfechtung begleitet werden. 635

Betrachtet man die im Rahmen der Revision geschaffenen formell-gesetzlichen Grundlagen, welche automatisierte Einzelfallentscheidungen ermöglichen sollen, so wird ersichtlich, dass es sich dabei in erster Linie um steuer- und abgaberechtliche (Veranlagungs-)Verfügungen handelt. So darf etwa gemäss Art. 38 Abs. 2 ZG die Zollstelle die Veranlagungsverfügung als automatisierte Einzelfallentscheidung nach Artikel 19 E-DSG erlassen. In diesem Bereich kommt der verfügenden Behörde grundsätzlich kaum ein Ermessens- oder Beurteilungsspielraum zu. Dies vorausgesetzt, sind die entsprechenden Grundlagen wohl unter diesem Gesichtspunkt unproblematisch.[1446] 636

Darüber hinaus sollen auch die mit der Durchführung oder mit der Kontrolle bzw. Beaufsichtigung der Durchführung der Unfallversicherungsgesetzgebung und der Militärversicherungsgesetzgebung betrauten Organe zur Erfüllung ihrer Aufgaben zum Erlass von automatisierten Einzelfallentscheidungen nach Art. 19 DSG befugt werden.[1447] Dabei enthält die entsprechende 637

1445 Vgl. ROTH, digma, 2017, S. 106 f.

1446 Vgl. zum Ganzen: RECHSTEINER, Jusletter, 26. November 2018, N. 31. Auch im Bereich der Steuern gibt es aber durchaus Entscheide, welche einen Beurteilungsspielraum lassen; vgl. BRAUN BINDER, Jusletter IT, 25. Mai 2016, N. 15.

1447 Botschaft Rev. DSG 2017, S. 7146 ff, vgl. Art. 96 Abs. 2 UVG, Art. 94a Abs. 2 MVG.

Gesetzgebung neben einigen Bereichen, welche sich durchaus für die Automatisierung eignen, auch Normen, welche den Behörden einen Ermessensspielraum einräumen.[1448] Nach den Vorgaben des E-DSG wären automatisierte Einzelfallentscheidungen auch in diesen Rechtsfragen zulässig. Sie würden jedoch vor einer Rechtsmittelinstanz aufgrund der Ermessensunterschreitung bei einer Anfechtung nicht standhalten. Art. 96 Abs. 2 E-UVG und Art. 94a Abs. 2 E-MVG sind somit zu weit formuliert und auch mit Blick auf das Legalitätsprinzip fragwürdig. Um mit dem Legalitätsprinzip konform zu gehen, müsste spezifiziert werden, welche Rechtsfragen in diesen Bereichen automatisiert entschieden werden dürfen.[1449] Andernfalls müssten die Gesetzesgrundlagen derjenigen Entscheide, welche einen Ermessensspielraum offenlassen, so umformuliert werden, dass sie ohne Ermessensspielraum abgebildet werden können. Gerade Letzteres dürfte indes m.E. mit grossem Zusatzaufwand verbunden und kaum praktikabel sein.

C. Zusätzliche Korrektive «de lege ferenda»

638 Im früheren Verlauf der Arbeit wurde beschrieben, mit welchen Korrektiven den Gefahren von Algorithmen als Entscheidungshilfe begegnet wird. Hervorzuheben sind dabei insbesondere gewisse Rechtsbehelfe des Datenschutzrechts (Auskunfts- und Berichtigungsrecht), das rechtliche Gehör und das Diskriminierungsverbot. Die entsprechenden Korrektive gelten auch im Rahmen von automatisierten Einzelfallentscheidungen, können allerdings im Zusammenhang mit komplexen Algorithmen an ihre Grenzen stossen.[1450] Beim Einsatz von automatisierten Einzelfallentscheidungen gilt dies unter Umständen gar in verstärktem Masse, zumal der Mensch als zusätzliche Kontrollinstanz wegfällt oder nur dann tätig wird, wenn die Betroffenen dies verlangen.[1451] Dies kann dazu führen, dass etwa diskriminierende Algorithmen unter Umständen erst nach einiger Zeit bemerkt werden.[1452] Auch wenn das rechtliche Gehör – wie soeben ausgeführt – bei automatisierten Einzelfallentscheidungen ebenfalls gewährt werden muss, ist insbesondere bei komplexen Entscheidungen oft problematisch, dass diese durch die Betroffenen nicht mehr nachvollzogen werden können. Aus diesen Gründen ist es gerechtfertigt, gewisse zusätzliche Kontrollmechanismen zu fordern, welche teilweise im Rahmen

1448 Vgl. etwa Art. 46 Abs. 2 UVG, gemäss welchem die Leistung verweigert werden kann, wenn absichtlich eine falsche Unfallmeldung eingereicht wurde; vgl. RECHSTEINER, Jusletter, 26. November 2018, N. 31 mit Verweisen auf die Rechtsprechung.

1449 RECHSTEINER, Jusletter, 26. November 2018, N. 16 und 31.

1450 Vgl. oben Rz. 455 ff.

1451 Siehe soeben Rz. 616.

1452 Vgl. das Beispiel COMPAS, weiter oben Rz. 476 ff.

der Revision des Datenschutzgesetzes vorgesehen sind, teilweise aber auch lediglich in der Literatur diskutiert werden.[1453] Im Folgenden soll thematisiert werden, inwiefern die vorgesehenen Korrektive «de lege ferenda» allenfalls Probleme der Nutzung von Algorithmen entschärfen können.

1. Rechte des Einzelnen

Aus Art. 19 Abs. 2 E-DSG ergibt sich der Anspruch darauf, seinen eigenen Standpunkt zu einer automatisierten Einzelfallentscheidung darlegen zu können. Der Anspruch geht – wie soeben ausgeführt – nicht weiter als der Anspruch auf rechtliches Gehör. Damit dieser Anspruch indes wirksam wahrgenommen werden kann, muss die betroffene Person zumindest in Grundzügen verstehen können, wie der entsprechende Algorithmus funktioniert bzw. wie dieser zum jeweiligen Entscheid geführt hat.[1454] Im Weiteren erlaubt es Art. 23 Abs. 2 lit. f. E-DSG dem Einzelnen, eine Auskunft über Informationen zu verlangen betreffend das Vorliegen einer automatisierten Einzelfallentscheidung sowie die Logik, auf der diese Entscheidung beruht. Mitgeteilt werden muss den Betroffenen dabei nicht der Quellcode der betreffenden Algorithmen.[1455] Dies wäre oft auch nicht zielführend, da der entsprechende Code oftmals komplex und für des Programmierens unkundige Laien ohne Erkenntniswert ist. Zudem können sich die Entwickler allenfalls auch auf das Vorliegen von Geschäftsgeheimnissen berufen, welche einer vollständigen Offenlegung der Wirkungsweise entgegenstehen.[1456] Es reicht daher bereits aus, wenn die Grundannahmen der Algorithmus-Logik, die Art und Menge der verwendeten Informationen sowie deren Gewichtung genannt werden.[1457] 639

Die datenschutzrechtlichen Rechtsbehelfe erlauben den Betroffenen somit keine umfassende Einsicht in die Algorithmen, führen aber immerhin zur Offenlegung der jeweiligen Funktionsweise. Nichtsdestotrotz kann bereits eine derartige Begründung unter Umständen – und dies je komplexer der zugrundeliegende Mechanismus ist, desto naheliegender – alles andere als trivial sein.[1458] Zwar folgt jeder Algorithmus einer inneren Logik, doch muss diese immer zuerst erkannt und so aufbereitet werden, dass sie dem 640

1453 Vgl. insbesondere zusammenfassend bei MARTINI, Blackbox, S. 157 ff.

1454 Vgl. weiter oben Rz. 454.

1455 Botschaft Rev. DSG 2017, S. 7067.

1456 Vgl. etwa: WEBER, in: Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, S. 15; GLATTHAAR, SZW, 2020, S. 49; SCHEJA, CR, 2018, S. 487.

1457 Botschaft Rev. DSG 2017, S. 7067.

1458 MARTINI, Blackbox, S. 193; KNIGHT, The Dark Secret at the Heart of AI, MIT Technology Review, 11. April 2017; GUNNING/AHA, AI Magazine, 2019, S. 44 ff.

Betroffenen weiterhilft.[1459] So kann z.B. ein Algorithmus, welcher die Erfolgsaussichten von Beschwerden hinsichtlich der Gewährung der unentgeltlichen Rechtspflege prüft, aufgrund des ihm zur Verfügung stehenden Fallmaterials zum Schluss kommen, dass eine Laienbeschwerde im Ausländerrecht ohne anwaltliche Vertretung nur in 10 % erfolgreich und das Begehren somit aussichtslos ist. Würde jedoch bloss diese Korrelation als Begründung bekanntgegeben werden, so würde dies dem Betroffenen kaum ermöglichen, den Entscheid in voller Kenntnis der wesentlichen Entscheidungsgründe wirksam anzufechten.[1460]

641 Daher muss einerseits bereits bei der Programmierung entsprechender Algorithmen als Systemanforderung darauf geachtet werden, dass die entsprechenden Resultate nachvollziehbar gestaltet werden können. Insbesondere bei maschinellen Lernverfahren ist unter Umständen auch für die Programmierer nicht mehr nachvollziehbar, wie ein Programm zu gewissen Schlussfolgerungen gekommen ist. Eine lückenlose und nachvollziehbare Dokumentation der Programmierung ist demnach unabdingbar. Hierbei wurde bis zum jetzigen Zeitpunkt noch keine alleine zufriedenstellende Lösung gefunden. Aktuell beschäftigen sich indes zahlreiche Forschende mit dem Bereich der «explainable AI», also dem Verständlichmachen von KI-Entscheidungen[1461] Dies kann auf verschiedene Weise geschehen, etwa indem KI so programmiert wird, dass sie die Entscheidungsfindung von vorneherein transparent macht oder dass das Programm angibt, wie sicher es sich seiner Entscheidung ist und welche Quellen verwendet wurden. Denkbar ist auch eine bessere Visualisierung für die Betroffenen, indem etwa einzelne Variablen aus der Berechnung herausgelöst werden und angezeigt wird, inwiefern dies das Ergebnis verändert.[1462]

2. Kollektive Mittel

642 Die Mittel und Möglichkeiten, welche dem Einzelnen gemäss dem Datenschutzrecht offenstehen, können den Betroffenen zwar im jeweiligen Einzelfall teilweise genügend Einsicht geben, um ihm zu erlauben, das Ergebnis nachzuvollziehen. Es gibt indes auch Fälle, in denen sich die Mängel einer automatisierten Einzelfallentscheidung nicht durch die Betrachtung eines Einzelfalls offenbaren. Angeführt sei hier erneut das COMPAS-System, bei welchem erst im Rahmen einer Wirkungskontrolle aufgedeckt werden konnte,

1459 MARTINI, Blackbox, S. 194, m.w.H.

1460 Vgl. RECHSTEINER, Jusletter, 26. November 2018, N. 27.

1461 MARTINI, Blackbox, S. 194.

1462 GUCKELBERGER, S. 528.

dass Personen mit dunkler Hautfarbe wesentlich schlechtere Rückfallprognosen gestellt wurden als Personen mit weisser Hautfarbe.[1463] Insbesondere das Diskriminierungspotenzial von algorithmischen Entscheidungen lässt sich oft naheliegenderweise nicht aus der Betrachtung eines Einzelfalls eruieren. Zwar kann auch in diesen Fällen das Auskunftsrecht nach Art. 23 E-DSG geltend gemacht werden, jedoch stösst es in diesem Kontext an seine Grenzen. Wenn es – wie soeben ausgeführt – bereits für den Einzelnen aufgrund der Komplexität und allenfalls gegenüberstehender privaten Interessen schwierig sein kann, komplexe Systeme nachzuvollziehen, so ist es noch beschwerlicher, aus der Logik ohne konkrete Fallbeispiele allfällige Diskriminierungsgefahren zu erkennen. Aus diesem Grund ist die Implementierung allfälliger weiterer Kontrollmechanismen in Betracht zu ziehen. Diese können entweder präventiv oder begleitend zum Einsatz des Algorithmus wirken.[1464]

a) Präventive Massnahmen

Ein erstes Instrument, welches bereits im geltenden Recht im Ansatz vorgesehen ist und in diesem Kontext allenfalls vermehrt zu beachten sein wird, stellt die Datenschutz-Folgeabschätzung dar. De lege lata müssen Bundesorgane gemäss Art. 20 VDSG dem Datenschutzverantwortlichen oder dem Beauftragten unverzüglich alle Projekte zur automatisierten Bearbeitung von Personendaten melden. Art. 20 E-DSG schreibt bei jeder Bearbeitung, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann, eine Folgeabschätzung über die geplante Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie Massnahmen zu deren Schutz vor (Art. 20 Abs. 1 und 3 E-DSG). Auf diese Weise können Risiken allenfalls präventiv erkannt und behoben werden.[1465] Gemäss Art. 21 E-DSG ist der Datenschutzbeauftragte zu konsultieren, wenn sich ohne Massnahmen des für die Bearbeitung Verantwortlichen ein hohes Risiko ergäbe. Dieses Instrument kann gegebenenfalls wirksam sein, um Gefahrenherde frühzeitig zu identifizieren und zu beheben. Allerdings bleibt zu beachten, dass es von einer korrekten Handhabung durch den jeweiligen Verantwortlichen abhängig ist. Irrt dieser über Art oder Ausmass des Risikos, so bleiben allfällige Gefahren unentdeckt oder werden falsch behandelt, zumal der Beauftragte von der fraglichen Bearbeitung nicht erfährt. Um diese Lücke zu beheben, müsste

643

1463 ANGWIN/LARSON/MATTU/KIRCHNER, Machine Bias. ProPublica, There's software used across the country to predict future criminals. And it's biased against blacks, MARTINI, Blackbox, S. 250.

1464 Vgl. zum Ganzen MARTINI, Blackbox, S. 168 ff.

1465 Vgl. zum Ganzen Botschaft Rev. DSG 2017, S. 7060.

die Datenschutz-Folgeabschätzung allenfalls dergestalt abgeändert werden, dass sie etwa in grundrechtlich sensiblen Fällen durch Dritte erfolgen kann oder dass die Verantwortlichen die Ergebnisse der Folgeabschätzung gegenüber den Betroffenen veröffentlichen müssen.[1466] Aus den erwähnten Gründen kann die Datenschutz-Folgeabschätzung alleine noch nicht einen wirksamen Schutz darstellen.

644 Als weiteres Instrument denkbar wäre etwa die Einführung eines staatlichen Prüfverfahrens, welches zumindest Algorithmen durchlaufen müssen, die Entscheidungen in besonders persönlichkeits-sensiblen Anwendungsfeldern treffen, um diese auf ihre Vereinbarkeit mit den normativen Anforderungen zu prüfen.[1467] Während dem privaten Betroffenen – wie oben beschrieben – nur ein begrenztes Einsichtsrecht zusteht, können durch eine öffentliche Prüfstelle ungeachtet allfälliger Geheimhaltungsinteressen tiefere Einblicke in die Funktionsweise der Algorithmen vorgenommen werden.[1468] Die Implementierung einer solchen Kontrolle ist indes ebenfalls mit Schwierigkeiten verbunden. Aufgrund der Komplexität entsprechender Systeme sind hohe technische Fähigkeiten für eine entsprechende Kontrolle notwendig. Unter diesen Umständen lassen sich auch diskriminierende Faktoren oder Ähnliches im Quellcode verschleiern.[1469] Nicht zuletzt kann zwar der Algorithmus an sich fehlerfrei sein, jedoch können unvollständige oder unzutreffende Trainingsdaten Fehler oder Unzulänglichkeiten produzieren. Aus diesem Grund haben sich verschiedene Autoren für eine Standardisierung von Entwicklungs- und Trainingsprozessen maschineller Lernverfahren ausgesprochen.[1470]

645 Ein probates Mittel könnte auch eine Zertifizierungspflicht für entsprechende Algorithmen darstellen.[1471] Eine dafür zu errichtende, öffentliche Kontrollstelle müsste dazu jedoch ebenfalls hohe Anforderungen erfüllen und unter Umständen auch auf externe Unterstützung zurückgreifen können.[1472]

1466 Vgl. zum Ganzen: MARTINI, Blackbox, 209 f. Immerhin hat der Verantwortliche gemäss Art. 35 Abs. 9 DSGVO gegebenenfalls den Standpunkt der Betroffenen einzuholen und über das Verfahren zu informieren, vgl. MARTINI, Paal/Pauly DSGVO, Art. 35, N. 60.

1467 MARTINI, JZ, 2017, S. 1021.

1468 MARTINI, Blackbox, S. 226.

1469 MARTINI, Blackbox, S. 227 ff.

1470 GEUTER, Machines Of Loving Grace / Brauchen wir einen Leinenzwang für Algorithmen?, WIRED, 11. Juni 2015; HOFFMANN-RIEM, in: Wissensregulierung und Regulierungswissen, S. 148: WACHTER/MITTELSTADT/FLORIDI, International Data Privacy Law, 2017, S. 98.

1471 Diese Pflicht wird teilweise auch als «Algorithmen-TÜV» bezeichnet; vgl, MARTINI/NINK, NVwZ-Extra, 2017, S. 12; LEWINSKI, InTeR, 2018, S. 174.

1472 MARTINI, Blackbox, S. 228 f.

b) Begleitende Kontrolle

Eine rein präventive Kontrolle der Algorithmen kann insbesondere bei selbstlernenden Systemen zu kurz greifen oder an ihre Grenzen gelangen. Da sich entsprechende Algorithmen unter Umständen an neue Entwicklungen oder Trainingsdaten anpassen können, ist eine fortlaufende Rechtmässigkeitsprüfung notwendig.[1473] Diese kann etwa durch eine nachträgliche Kontrolle der Ergebnisse erfolgen, welche im Beispielfall COMPAS systematische Ungleichheiten zu Tage brachte.[1474] Probat wäre allenfalls auch der Einsatz von Kontrollalgorithmen, welche die Entscheidungsergebnisse der Codes auf Auffälligkeiten, insbesondere Diskriminierungen, überprüfen und deren Gründe ausfindig machen können.[1475] Zudem könnte der Verarbeitungsprozess durch weitergehende behördliche Rechte zur Einsicht etwa in den Programmcode oder in den Datenbearbeitungsprozess kontrolliert werden.[1476] Eine weitere Möglichkeit, um Persönlichkeitsverletzungen vorzubeugen, könnte die Verpflichtung zur Führung sogenannter Risikomanagementsysteme beim Einsatz von Algorithmen in besonders sensiblen Bereichen darstellen.[1477] Diese könnten dafür sorgen, dass etwa im Falle einer Anknüpfung an besonders sensible Daten oder bei sonstigen Unklarheiten eine (menschliche) Kontrolle der automatisierten Entscheidung ausgelöst wird.[1478] Eine entsprechende Pflicht besteht etwa in Deutschland im automatisierten Besteuerungsverfahren, wo die manuelle Überprüfung der Steuererklärung auch nach dem Willen der betroffenen Person durch einen Eintrag in ein qualifiziertes Freitextfeld angestossen werden kann.[1479] 646

3. Fazit

Die soeben vorgestellten präventiven und begleitenden Kontrollmechanismen stellen durchaus Möglichkeiten dar, um Persönlichkeitsverletzungen durch automatisierte Einzelfallentscheidungen vorzubeugen. Allerdings verfügen auch diese Mechanismen über gewisse Einschränkungen. Im Weiteren wurden alle Konstruktionen bisher vorderhand in der (deutschen) Literatur 647

1473 MARTINI, JZ, 2017, S. 1021; zustimmend BUSCH, S. 65.

1474 Vgl. MARTINI, Blackbox, S. 250.

1475 MARTINI/NINK, NVwZ-Extra, 2017, S. 12 m.w.H.; vgl. Entschliessung des Europäischen Parlaments vom 14. März 2017, 2016/2225(INI), Punkt 11; KROLL/HUEY/BAROCAS/FELTEN/REIDENBERG/ROBINSON/YU, PENN LAW REVIEW, 2017.

1476 MARTINI, Blackbox, S. 253 ff.

1477 MARTINI, JZ, 2017, S. 1022.

1478 Vgl. dazu BRAUN BINDER, NVwZ, 2016, S. 962.

1479 BRAUN BINDER, NVwZ, 2016, S. 961.

diskutiert. Eine entsprechende Implementierung ist bis anhin noch nicht absehbar und ebenfalls mit Problemen verbunden, etwa hinsichtlich der Frage, welche Behörde eine entsprechende Kontrollfunktion übernehmen könnte.[1480] In der Schweizer Literatur wurden diese Konstrukte bisher kaum je aufgegriffen, geschweige denn auf ihre Machbarkeit im hiesigen Rechtsrahmen überprüft.[1481] Die entsprechenden Überlegungen bzw. Anwendungen sind daher noch relativ weit von einer Realisierung entfernt. Meines Erachtens gilt es, sich der zusätzlichen Gefahren von automatisierten Einzelfallentscheidungen bewusst zu sein und daher die entsprechenden Möglichkeiten zumindest ergebnisoffen zu diskutieren.

V. Vereinbarkeit mit den Regelungen in der Europäischen Union

648 Einen wesentlichen Grund für die Revision der Datenschutzgesetzgebung in der Schweiz stellt – wie bereits an anderer Stelle ausgeführt – die Anpassung an das EU-Recht dar. Dies mit dem Ziel, ein aus der Sicht der EU angemessenes Datenschutzniveau zu erhalten. Ob ein entsprechendes angemessenes Datenschutzniveau vorliegt, muss von der EU-Kommission regelmässig überprüft und mit einem Angemessenheitsbeschluss gewährleistet werden.[1482] In diesem Zusammenhang sind insbesondere die DSGVO und das SEV-Übereinkommen 108 zu beachten. Diese Regelwerke enthalten neue oder zumindest überarbeitete Vorgaben zu automatisierten Einzelfallentscheidungen. Da sie inhaltlich sehr ähnlich sind, die Datenschutzgrundverordnung jedoch etwas detailliertere Regelungen vorsieht, soll Letztere an dieser Stelle im Fokus der Betrachtung stehen.[1483] In einem weiteren Schritt wird ergründet, ob die bestehenden und vorgesehenen Schweizer Regelungen die Vorgaben der DSGVO im Bereich der automatisierten Einzelfallentscheidungen angemessen umsetzen.

A. Regelungen in der DSGVO

649 Es ist zu bedenken, dass die Regelung von automatisierten Einzelfallentscheidungen kein gänzlich neues Phänomen darstellt. Bereits im Jahr 1978 sah das französische Datenschutzgesetz ein Verbot automatisierter Entscheidungen bezüglich der Beurteilung menschlichen Verhaltens vor. Auch die europäische Datenschutzrichtlinie (RL 95/46/EG) enthielt in Art. 15 ein Verbot entsprechender Entscheidungen, welche rechtliche Folgen nach sich ziehen

1480 Vgl. MARTINI, Blackbox, S. 268.

1481 Vgl. immerhin BRAUN BINDER, SJZ, 2019, S. 475.

1482 Botschaft Rev. DSG 2017, S. 6965.

1483 Botschaft Rev. DSG 2017, S. 6966.

oder die betroffene Person anderweitig erheblich beeinträchtigen.[1484] Art. 22 DSGVO basiert im Wesentlichen auf dieser Bestimmung, welche allerdings um zusätzliche Garantien ergänzt und in ihrem Anwendungsbereich wesentlich erweitert wurde.[1485]

650 Gemäss Art. 22 DSGVO hat jede Person das Recht, nicht einer «ausschliesslich auf einer automatisierten Verarbeitung – einschliesslich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt»[1486]. Damit statuiert auch diese Bestimmung ein grundsätzliches Verbot automatisierter Einzelfallentscheidungen.[1487] Dieses wird allerdings durch eine grosse Menge an Einschränkungen aufgeweicht. Einerseits gilt die Regelung von Art. 22 DSGVO nur bei ausschliesslich auf einer automatisierten Verarbeitung basierenden Entscheidungen. Es darf somit kein menschlicher Einfluss auf den Entscheidungsprozess vorliegen. Prozesse, in denen Algorithmen nur als Entscheidungshilfe benutzt werden, sind also auch von dieser Bestimmung nicht erfasst.[1488] Anderseits muss die Entscheidung rechtliche Wirkung auf die Person haben oder diese auf eine andere Weise erheblich beeinträchtigen. Dies bedeutet, dass in Fällen, in welchen keine rechtliche Beeinträchtigung vorliegt, eine automatisierte Einzelfallentscheidung zulässig ist. Die Handlungen von Behörden sind indes in der Regel auf rechtliche Wirkungen ausgerichtet und somit grundsätzlich von Art. 22 DSGVO erfasst.[1489]

651 Im Weiteren sieht die Bestimmung in Art. 22 Abs. 2 DSGVO weitgehende Ausnahmen vom grundsätzlichen Verbot vor. Im vorliegenden Kontext ist insbesondere Art. 22 Abs. 2 lit. b DSGVO relevant, welcher entsprechende Entscheidungen auch aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten erlaubt, sofern diese Rechtsvorschriften angemessene Massnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen enthalten. Durch diese Konkretisierungsklausel soll es den Mitgliedstaaten in einem gewissen Rahmen möglich bleiben, automatisierte Verfahren vorzusehen oder beizubehalten, sofern die Rechte der betroffenen Personen gewahrt sind.[1490] Zu diesen Rechten zählen insbesondere die Unterrichtung der betroffenen Person, welche in

1484 THOUVENIN/FRÜH/GEORGE, Jusletter, 26. November 2018, N. 21.

1485 HLADJK, Ehmann/Selmayr DSGVO, Art. 22, N. 1 ff.

1486 Art. 22 DSGVO.

1487 DOVAS, digma, 2017, S. 100.

1488 HLADJK, Ehmann/Selmayr DSGVO, Art. 22, N. 6; ARTIKEL-29-DATENSCHUTZGRUPPE, Guidelines ADM, S. 10.

1489 ARTIKEL-29-DATENSCHUTZGRUPPE, Guidelines ADM, S. 11.

1490 DOVAS, digma, 2017, S. 101.

Art. 13 Abs. 1 lit. f. und Art. 14 Abs. 2 lit. g DSGVO geregelt ist, und das Recht auf *Erwirkung des Eingreifens* einer Person beim Verantwortlichen («menschliches Gehör») sowie die Möglichkeit der *Darlegung des eigenen Standpunkts* und der *Anfechtung* der Entscheidung.[1491]

652 Im europarechtlichen Kontext ist zudem hinsichtlich automatisierter Entscheidungen das Auskunftsrecht gemäss Art. 15 Abs. 1 lit. h DSGVO zu beachten, welches den betroffenen Personen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person gewähren soll. Es wird mittlerweile davon ausgegangen, dass Art. 15 Abs. 1 lit. h DSGVO kein vollständiges Recht auf eine Ex-post-Erklärung über eine spezifische Entscheidung (oder gar die vollständige Offenlegung des Algorithmus) beinhaltet, sondern dass die Betroffenen verständlich über die involvierte Logik aufgeklärt werden sollen, damit sie die Entscheidungsgründe verstehen können.[1492] Wie eine entsprechende Information am besten bewerkstelligt werden kann, ist allerdings – wie weiter oben bereits ausgeführt – aktuell noch ungeklärt.[1493] Im Weiteren sieht die DSGVO auch keine probateren Schutzvorkehrungen vor, wie gruppen- und gesellschaftsbezogene Interessen, etwa der Schutz vor Diskriminierung, besser erreicht werden können.[1494] Aufgrund dieser zahlreichen Einschränkungen bestehen in der Lehre berechtigte Zweifel daran, ob Art. 22 DSGVO ein wirksames Instrument darstellt, um die Rechte der Betroffenen bei automatisierten Einzelfallentscheidungen wirksam zu schützen.[1495]

653 Zudem müssen die entsprechenden Normen der DSGVO hinsichtlich der vorgesehenen Schutzmechanismen auf nationaler Ebene konkretisiert werden. In einem gewissen Rahmen steht es den Mitgliedstaaten dabei frei, über die von der DSGVO garantierten Rechte hinauszugehen.[1496] In Deutschland wird diese Konkretisierung für das Verwaltungsverfahren durch § 35a VwVfG und durch § 24 Abs. 1 Ziff. 3 VwVfG vorgenommen.[1497] Gemäss dem

1491 HLADJK, Ehmann/Selmayr DSGVO, Art. 22, N. 12.

1492 WACHTER/MITTELSTADT/FLORIDI, International Data Privacy Law, 2017; ARTIKEL-29-DATENSCHUTZGRUPPE, Guidelines ADM, S. 25.

1493 Siehe oben Rz. 460.

1494 DREYER/SCHULZ, S. 39.

1495 PENNER, in: Automating Society – Taking Stock of Automated Decision-Making in the EU, S. 22; WACHTER/MITTELSTADT/FLORIDI, International Data Privacy Law, 2017. S. 96, welche auch konkrete Vorschläge bringen, wie Art. 22 DSGVO allenfalls verbessert werden kann.

1496 Vgl. im Detail: MALGIERI, Computer Law & Security Review, 2019. S. 1 ff.

1497 PRELL, Kommentar VwVfG-D, Art. 35a VwVfG, N. 11a; vgl. auch BERGER, NVwZ, 2018, S. 1262.

bereits vorgestellten § 35a VwVfG kann ein Verwaltungsakt vollständig durch automatische Einrichtungen erlassen werden, sofern dies durch Rechtsvorschrift zugelassen ist und weder ein Ermessen noch ein Beurteilungsspielraum besteht. § 24 Abs. 1 Ziff. 3 VwVfG ergänzt zudem den Untersuchungsgrundsatz dahingehend, dass die Behörde, welche automatische Einrichtungen zum Erlass von Verwaltungsakten einsetzt, für den Einzelfall bedeutsame tatsächliche Angaben des Beteiligten berücksichtigt, die im automatischen Verfahren nicht ermittelt würden. Parallel zu dieser Bestimmung wurden auch im Zehnten Buch des Sozialgesetzbuchs (SGB X) und in der Abgabeordnung (AO) entsprechende Bestimmungen verankert, welche die Verwendung von automatisierten Entscheidungen unter gewissen Umständen zulassen.[1498]

B. Vereinbarkeit der vorgesehenen Schweizer Regelung mit der DSGVO

Nun stellt sich die Frage, inwiefern die in der Schweiz vorgesehene Regelung ein hinsichtlich der Datenschutzgrundverordnung angemessenes Schutzniveau zu garantieren vermag. Die inhaltliche Konzeption spricht auf den ersten Blick klar dagegen, geht Art. 22 DSGVO doch von einem grundsätzlichen Verbot von automatisierten Entscheidungen aus, während Art. 19 E-DSG diese im Grundsatz zulässt und lediglich eine Informationspflicht vorsieht.[1499] Wie soeben ausgeführt, eröffnet die in der DSGVO vorgesehene Norm indes viele Ausnahmen von diesem grundsätzlichen Verbot und lässt automatisierte Einzelfallentscheidungen etwa zu, sofern diese durch die Mitgliedstaaten in einer Rechtsvorschrift vorgesehen werden, welche angemessene Massnahmen zur Wahrung der Betroffenenrechte enthält. Im Rahmen dieser Schutzmassnahmen muss die Person – dies sei hier nochmals erwähnt – zumindest über die automatisierte Natur der Entscheidung in Kenntnis gesetzt werden, und es muss vorgesehen werden, dass sie ihren Standpunkt einbringen und eine Entscheidung oder Überprüfung durch einen Menschen verlangen kann. Wenn die Regelungen in einem Mitgliedstaat diese Vorgaben einhalten müssen, so haben diese wohl auch für Drittstaaten zu gelten, wenn diese ein angemessenes Datenschutzniveau erreichen wollen. 654

Die geplante Regelung im E-DSG sieht für automatisierte Entscheidungen gemäss Art. 19 DSG grundsätzlich eine Informationspflicht über automatisierte Einzelfallentscheidungen vor, welche für die betroffene Person mit einer Rechtsfolge verbunden sind oder sie erheblich beeinträchtigen. Zum Vergleich geht hier die DSGVO, welche in Art. 13 Abs. 2 lit. f, Art. 14 Abs. 2 lit. f 655

1498 PRELL, Kommentar VwVfG-D, Art. 35a VwVfG, N. 21 ff.

1499 THOUVENIN/FRÜH/GEORGE, Jusletter, 26. November 2018, N. 27.

und Art. 15 Abs. 1 lit. h ebenfalls eine Informationspflicht bzw. ein Auskunftsrecht bei automatisierten Einzelfallentscheidungen vorsieht, nicht grundsätzlich weiter. Auch dieses Recht erschöpft sich darin, dass der Inhalt der Entscheidung zu erklären ist, aber nicht strukturell die Gründe der Entscheidung in allen Einzelheiten offenzulegen sind.[1500] Im Weiteren sieht der Gesetzesentwurf in Art. 23 Abs. 2 lit. f E-DSG analog zu Art. 15 DSGVO ebenfalls ein Auskunftsrecht hinsichtlich der integrierten Logik vor. Art. 19 Abs. 2 E-DSG gibt der Person die Möglichkeit, ihren Standpunkt darzulegen und zu verlangen, dass die Entscheidung von einer natürlichen Person überprüft werden kann.[1501] Dieses Recht entfällt indes gemäss Absatz 4 der Bestimmung, wenn das rechtliche Gehör nicht gewährt werden muss.[1502] Trotz dieser Einschränkung kann davon ausgegangen werden, dass ein der DSGVO angemessenes Niveau in diesem Punkt erreicht wird.[1503]

VI. Zusammenfassung

656 Die Verwendung von Algorithmen durch die öffentliche Verwaltung birgt bereits dann gewisse Gefahren, wenn sie nur zur Unterstützung verwendet werden. Daher sind entsprechende Lösungen in den betreffenden Bereichen (z.B. bei möglichen Diskriminierungen) mit Bedacht einzusetzen. Je komplexer die zugrundeliegenden Algorithmen aufgebaut sind, desto schwieriger gestaltet sich deren Nachvollziehbarkeit für die Vollzugsverantwortlichen und auch für die Betroffenen, was vor allem hinsichtlich des rechtlichen Gehörs problematisch ist. Wird eine Entscheidung vollständig automatisiert und ohne relevanten menschlichen Einfluss gefällt, so bestehen diese Gefahren ebenso und werden durch das Fehlen eines menschlichen Einflusses auf die Entscheidung, welcher ein im Einzelfall stossendes Ergebnis korrigieren könnte, gar noch verstärkt.

657 Das revidierte Datenschutzgesetz sieht einige zusätzliche Schutzvorkehrungen vor, um die Rechte Betroffener bei automatisierten Einzelfallentscheidungen zu schützen. Wichtig ist bei automatisierten Entscheiden, dass es den Betroffenen möglich ist, ihren Standpunkt darzulegen und allenfalls eine menschliche Überprüfung zu verlangen. Da behördliche automatisierte

1500 MARTINI, Blackbox, S. 191; THOUVENIN/FRÜH/GEORGE, Jusletter, 26. November 2018, N. 24 ff.; ARTIKEL-29-DATENSCHUTZGRUPPE, Guidelines ADM, S. 14; a.M. aber WACHTER/MITTELSTADT/FLORIDI, International Data Privacy Law, 2017.

1501 THOUVENIN/FRÜH/GEORGE, Jusletter, 26. November 2018, N. 27 ff.

1502 Siehe dazu weiter oben Rz. 569 ff.

1503 Vgl. bereits hinsichtlich des Vorentwurfs: ROSENTHAL, Jusletter, 20. Februar 2017, N. 58 ff.

Einzelfallentscheide in der Regel im Rahmen eines Verfahrens ergehen, ist bereits gestützt auf das Verwaltungsverfahrensgesetz das rechtliche Gehör zu gewähren. Es ist indes möglich, dass die Gewährung des Anspruchs auf andere Weise – z.B. im Rahmen eines Einspracheverfahrens – stattfindet. Unzulässig wäre es indes, das rechtliche Gehör bei automatisierten Einzelfallentscheidungen komplett auf die nächste Instanz zu verschieben. Die Gewährung des rechtlichen Gehörs kann indes auch mit praktischen Schwierigkeiten verbunden sein, zumal der jeweilige Entscheid für die Behörde und die Betroffenen nachvollziehbar sein muss, was unter Umständen bei komplexen Algorithmen nicht mehr der Fall ist. Hier stossen die gewährten Rechte an ihre Grenzen, so dass allenfalls an zusätzliche Möglichkeiten zur Überprüfung und Kontrolle von Algorithmen vor oder begleitend zu ihrem Einsatz zu denken ist.

Aus diesen Gründen und weil automatisierte Einzelfallentscheidungen 658
direkt Rechten und Pflichten der Betroffenen berühren können, ist ohne Zweifel davon auszugehen, dass ihr Einsatz eine gesetzliche Grundlage im formellen Sinn benötigt. Im Rahmen der Revision des Datenschutzgesetzes werden einige entsprechende Grundlagen geschaffen. Zu beachten ist, dass zumindest im jetzigen Zeitpunkt nicht alle Entscheidungen der Automatisierung offenstehen sollten. In allen Fällen, in denen der Gesetzgeber den rechtsanwendenden Behörden einen Ermessensspielraum belässt, kann dieser durch automatisierte Einzelfallentscheidungen (noch) nicht wahrgenommen werden. Ein Verzicht darauf, im Rahmen automatisierter Entscheidungen dieses Ermessen auszuüben, würde entsprechende Entscheide aufgrund der damit verbundenen Ermessensunterschreitung anfechtbar machen.

§11 Blockchain

I. Anwendungsbereiche in der öffentlichen Verwaltung

Die Blockchain-Technologie kann grundsätzlich überall eingesetzt werden, 659
wo sich verschiedene Parteien im Rahmen einer Transaktion gegenüberstehen. Ihre weiter oben erwähnten Eigenschaften, wie Unveränderbarkeit oder Verzicht auf vertrauensbildende Intermediäre, machen die zugrundeliegende Technologie auch für die öffentliche Verwaltung interessant. Gerade der Staat dient in vielen Fällen als vertrauensbildender Intermediär, etwa wenn es darum geht, Eigentumsverhältnisse zu regeln oder die Echtheit von Dokumenten zu gewährleisten.[1504] Zu diesem Zweck kennt er verschiedene Instrumente,

1504 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 18.

wie öffentliche Register oder Urkunden.[1505] Eine Technologie, welche nun glaubwürdig verspricht, derartige vertrauensbildende Intermediäre als Zwischenschritte überflüssig zu machen, bietet etwa unübersehbare Chancen, die Verwaltung effizienter zu machen.[1506] Im Folgenden sollen daher einige Nutzungs- bzw. Anwendungsmöglichkeiten der Blockchain für die öffentliche Verwaltung genauer vorgestellt werden.[1507]

660 Aufgrund der Entstehungsgeschichte der Blockchain als Basis für Kryptowährungen ist wohl deren Einsatz als Möglichkeit zur Bezahlung von Verwaltungsgebühren am offensichtlichsten (etwa via Bitcoin).[1508] Dies wird etwa im Kanton Zug bereits auf diese Weise praktiziert.[1509] Neben der Bezahlung von Gebühren in einer bestehenden Währung experimentieren Staaten auch mit spezifischen eigenen Währungen.[1510]

661 Da auf der Blockchain sämtliche getätigten Transaktionen dauerhaft, transparent und unveränderbar gespeichert werden, ähnelt sie in ihrer Funktionsweise der Registerführung,[1511] welche in vielen Bereichen eine zentrale Aufgabe des Staates bildet.[1512] Es erscheint daher naheliegend, dass entsprechende Register durch auf Blockchain basierte Anwendungen ersetzt werden können. Grundsätzlich eignen sich dazu alle Register, die über eine öffentlich überprüfbare Transaktionshistorie verfügen und manipulationssicher sein müssen sowie das Prinzip des öffentlichen Glaubens kennen, also etwa Grundbuch-, Personen- oder Handelsregister.[1513] Durch eine entsprechende Umstellung wird insbesondere eine verbesserte Integrität und Transparenz des gesamten Prozesses erhofft.[1514] In der Schweiz sieht etwa der Kanton Genf vor, dass Registerauszüge via Blockchain bestellt werden können. Im Kanton Zug ist die Gründung von Aktiengesellschaften inklusive Handelsregistereintrag

1505 DAPP/BALTA/KRCMAR, S. 6.

1506 Vgl. zu dieser Diskussion vertiefend: ATZORI, 1. Dezember 2015; vgl. SIMMCHEN, MMR, 2017, S. 162.

1507 Die jeweiligen Einsatzbereiche können sich dabei teilweise überschneiden; vgl. BERRYHILL/BOURGERY/HANSON, S. 24.

1508 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 18

1509 ASCHWANDEN, Stadt Zug wird weltweit zum Bitcoin-Pionier, Neue Zürcher Zeitung, 10. Mai 2016.

1510 BERRYHILL/BOURGERY/HANSON, S. 25.

1511 Vgl. WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 30.

1512 SPICHIGER, Die Volkswirtschaft, 2019, S. 23.

1513 DAPP/BALTA/KRCMAR, S. 4; SPICHIGER, Die Volkswirtschaft, 2019, S. 23.

1514 Gerade in Ländern ohne funktionierendes Registersystem wird dadurch auch eine verbesserte Effizienz und Vorbeugung von Korruption erwartet; vgl. etwa SPICHIGER, Die Volkswirtschaft, 2019, S. 23; WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 18; WILSCH, DNotZ, 2017, S. 762 ff.

auf Basis der Blockchain möglich. In beiden Fällen basiert jedoch das eigentliche Register weiterhin nicht auf der Blockchain-Technologie.[1515] In anderen Ländern wurden hingegen auf Blockchain basierte Grundbuchregisterlösungen eingeführt oder zumindest getestet.[1516]

662 Durch ihre Fälschungssicherheit können auf Blockchain basierte Anwendungen auch zur Verifizierung der Echtheit von Dokumenten eingesetzt werden. Heute kann – wie an anderer Stelle bereits ausgeführt – ein Dokument digital signiert werden, um dessen Echtheit zu bestätigen. Dazu wird grundsätzlich eine vertrauenswürdige Instanz benötigt.[1517] Einem zu signierenden Dokument kann indes auch ein sogenannter «Hashwert»[1518] zugeteilt werden, welcher sich verändert, wenn das Dokument auch bereits geringfügig verändert wird. Dieser Hashwert kann nun auf der Blockchain hinterlegt und somit nicht mehr verändert werden. Dadurch ist der Nachweis möglich, dass ein Dokument der jeweiligen Person oder Organisation zu einem Zeitpunkt «X» in einer bestimmten Fassung vorlag. Entsprechende Systeme könnten etwa im Bildungsbereich zur Verifizierung von Abschluss- oder Qualifikationsnachweisen dienen.[1519]

663 Auf dieselbe Weise, wie die Echtheit von Dokumenten via Blockchain bestätigt werden kann, ist es auch möglich, einen Nachweis über die Identität einer Person zu erbringen. Dabei kann aus verschiedenen Attributen ein Hashwert gebildet und in einer Blockchain unveränderbar abgelegt werden.[1520] Auf diese Weise können digitale Identitäten für Einwohner oder Unternehmen gebildet werden, welche dem Nutzer eine Identifikation bei Internetdiensten (etwa im Bereich des E-Government) ermöglichen und deren Nutzung somit vereinfachen können.[1521] In der Schweiz hat etwa die Stadt Zug im Rahmen eines Pilotprojekts eine digitale Identitätslösung auf Basis der Blockchain eingeführt. Dabei können sich die Benutzer in einer «App» registrieren und verschiedene für ihre Identitätsfeststellung benötigte Daten eingeben. Diese werden daraufhin von der Einwohnerkontrolle verifiziert und diese Verifikation wird auf der Blockchain gespeichert. Die Daten der Person verbleiben dabei auf dem jeweiligen Gerät. Nach erfolgter Verifikation kann sich die Person bei Anwendungen der Stadt Zug online mit ihrer elektronischen Identität

1515 SPICHIGER, Die Volkswirtschaft, 2019, S. 24.

1516 Vgl. dazu etwa FAVROD-COUNE, S. 178 f.; BERRYHILL/BOURGERY/HANSON, S. 26.

1517 Siehe dazu weiter oben Rz. 43 ff; vgl. auch WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 19.

1518 Zur Definition siehe oben Rz. 51.

1519 Vgl. zum Ganzen: WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 19.

1520 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 20.

1521 BERRYHILL/BOURGERY/HANSON, S. 25; zur digitalen Identität siehe auch weiter oben Rz. 542.

authentifizieren.[1522] Neben der Benutzung für E-Government-Dienstleistungen kann diese E-Identität auch im privaten Bereich genutzt werden.[1523]

664 Auch Wahlen und Abstimmungen werden als möglicher Einsatzbereich von Blockchain-Lösungen gesehen. So könnte beispielsweise bei Wahlen jeder Kandidat eine «Wallet» – quasi als Wahlurne – erhalten, und der Stimmberechtigte erhält einen «Coin» oder «Token» als Stimme, welchen er an den Kandidaten seiner Wahl übergibt.[1524] Eine entsprechende Lösung verspricht eine unmittelbare Stimmauswertung und eine hohe Datenintegrität, da die Auswertung nicht mehr manuell erfolgen muss.[1525] Auch wird dadurch eine grössere Transparenz erwartet, indem der Stimmberechtigte verifizieren kann, ob seine Stimme gezählt wurde.[1526] Aufgrund des Fokus der Arbeit soll an dieser Stelle eine detaillierte Betrachtung der zweifellos relevanten und sehr interessanten Frage ausbleiben, ob ein entsprechendes Stimm- bzw. Wahlverfahren mit den in Art. 34 BV garantierten politischen Rechten, insbesondere hinsichtlich der Anforderungen an die Nachvollziehbarkeit, vereinbar ist.[1527]

665 Die Blockchain wird auch als naheliegendes Mittel gesehen, um sogenannte «Smart Contracts» ausführen zu können, also Verträge, bei denen Leistungen und Gegenleistungen durch ein Programm abgewickelt werden.[1528] Auch für die Verwaltung können sich dadurch neue Möglichkeiten ergeben, etwa im Kontext von Smart Cities.[1529] Allerdings ist noch zu ergründen, welche Verträge und Prozesse sich für eine entsprechende Abwicklung wirklich eignen.[1530] Vordergründig werden dabei Einsatzmöglichkeiten in den Bereichen Steuer- oder Sozialhilfewesen vorgebracht.[1531] So erscheint es etwa denkbar, dass die Mehrwertsteuer inskünftig direkt mithilfe eines «Smart Contract» zwischen der Steuerverwaltung und dem betreffenden Geschäft verrechnet wird.[1532]

1522 Vgl. etwa KOHLHAAS, Zug ID: Exploring the First Publicly Verified Blockchain Identity, uPort, 7. Dezember 2017.

1523 So können etwa in der Stadt Zug digital Velos mithilfe der E-ID ausgeliehen werden, vgl. zentralplus, News-Beitrag vom 27. August 2018.

1524 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 21 f. In der Stadt Zug fand im Jahr 2018 im Rahmen einer Konsultativabstimmung bereits ein entsprechender Versuch statt; für eine eingehendere Betrachtung vgl. STADT ZUG/LUXOFT/FH ZENTRALSCHWEIZ INFORMATIK.

1525 SIMMCHEN, MMR, 2017, S. 163.

1526 Vgl. etwa NOIZAT, in: Handbook of digital currency, S. 453 ff.

1527 Vgl. dazu SIMMCHEN, MMR, 2017, S. 163.

1528 Siehe oben Rz. 56.

1529 DAPP/BALTA/KRCMAR, S. 6.

1530 VOSHMGIR, S. 27.

1531 SCHLATT/SCHWEIZER/URBACH/FRIDGEN, S. 30; SIMMCHEN, MMR, 2017, S. 162 f.

1532 WALPORT, S. 70.

II. Rechtliche Grundlagen in der Schweiz

Aufgrund ihres dezentralen Wesens kann eine Blockchain grundsätzlich überall auf der Welt «Nodes» (Netzknoten) haben und somit in verschiedenen Ländern Anknüpfungspunkte für das jeweilige Recht bieten, was auch zu rechtlichen Überschneidungen oder Unklarheiten führen kann.[1533] Aus diesem Grund wäre eine multilaterale staatliche Regulierung des Phänomens erstrebenswert, womit indes aus realpolitischen Gründen in naher Zukunft nicht zu rechnen ist.[1534] Auch wenn sich internationale und supranationale Organisationen mit der Blockchain-Technologie befassen und eine Vereinheitlichung der Rechtsordnung mitunter gar für zielführend halten, sind bis zum Zeitpunkt der Fertigstellung dieser Arbeit noch keine konkreten Regulierungsvorschläge ersichtlich.[1535] Im Vordergrund der regulatorischen Bemühungen stehen daher die Tätigkeiten von privaten Organisationen, insbesondere die Selbstregulierungen durch Standardisierungsorganisationen.[1536] Auch haben bereits verschiedene Länder sich mit dem Thema befasst und gegebenenfalls gesetzliche Anpassungen vorgenommen. Die wenigsten gehen dabei soweit wie das Fürstentum Liechtenstein, dass ein spezifisches Blockchain-Gesetz geschaffen hat.[1537] 666

In der Schweiz hat sich die Benutzung der Blockchain-Technologie in verschiedenen Ausgestaltungen bis zu einem gewissen Grad etabliert und unser Land wird in dieser Hinsicht gerade im Finanzsektor zu einem der führenden «Player» gezählt.[1538] Aufgrund der vielen möglichen Anwendungsbereiche, welche mit der Verwendung der «Distributed Ledger»-Technologie (DLT) nicht nur in diesem Bereich einhergehen, ist es wenig verwunderlich, dass auch der Gesetzgeber sich mit der Frage beschäftigte, ob zusätzliche Regulierungen der Blockchain-Technologie notwendig sind. Aus diesem Grund hat der Bundesrat eine Expertengruppe damit beauftragt, einen «Bericht zu den rechtlichen Rahmenbedingungen für Blockchain und DLT» zu verfassen, welcher am 14. Dezember 2018 verabschiedet wurde.[1539] Der Bericht kommt zum Schluss, dass die bestehenden rechtlichen Rahmenbedingungen grundsätzlich geeignet 667

1533 NAVES/AUDIA/BUSSTRA/HARTOG/VAN HEUKELOM-VERHAGE, Innovations Technology Governance Globalization, 2019, S. 88 ff.

1534 WEBER, CRi, 2017, S. 1 f.; WEBER, Jusletter IT, 18. Mai 2017, N. 14.

1535 EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM., S. 33.

1536 Für eine Übersicht vgl. WEBER, CRi, 2017; Bericht Zukunft, S. 148 ff.; Bericht DLT.

1537 Vgl. etwa: WANGER/JOHANN, in: Blockchain and cryptocurrency regulation, S. 372 ff.

1538 Bericht DLT, S. 8.

1539 Bundesrat, Medienmitteilung vom 14.12.2018: Bundesrat will Rahmenbedingungen für Blockchain/DLT weiter verbessern.

sind, um mit den Phänomenen «Blockchain» und «DLT» umzugehen. Dennoch verwies er darauf, dass gewisse zusätzliche Regelungen notwendig seien, da sich die Blockchain oder die Kryptowährungen im geltenden Recht nicht vollständig einordnen lassen. Dementsprechend wurden im Bericht einige Handlungsempfehlungen formuliert, welche sich im Rahmen des «Bundesgesetzes zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register» aktuell im Gesetzgebungsprozess befinden.[1540]

668 Dabei handelt es sich insbesondere um Anpassungen im Bereich des Privatrechts, etwa hinsichtlich der obligationenrechtlichen Einordnung von «Token» oder der Behandlung von kryptobasierten Vermögenswerten im Konkurs.[1541] Im öffentlich-rechtlichen Bereich werden vor allem Anpassungen im Bereich des Finanzmarktrechts und des Geldwäschereigesetzes geprüft.[1542] Die betreffenden Änderungen sollen aufgrund des Fokus dieser Arbeit nicht weiter ausgeführt und beleuchtet werden. Mit der Anwendung von «Distributed Ledger»-Technologie oder Blockchain im Bereich der öffentlichen Verwaltung befasst sich der Bericht nur am Rande. So weist er darauf hin, dass eine Vielzahl an öffentlichen Registern grundsätzlich über die Blockchain geführt werden könnte, was aber aufgrund des damit verbundenen Aufwands und bestehender Unsicherheiten nicht favorisiert wird.[1543] Es bleibt somit festzustellen, dass in der Schweiz zumindest für den öffentlich-rechtlichen Einsatz von DLT/Blockchain aktuell noch keine spezifischen Rechtsgrundlagen bestehen.

669 Es ist durchaus fraglich, ob eine gesetzliche Grundlage für die Verwendung von DLT grundsätzlich benötigt wird. Gemäss Art. 5 BV benötigt jedes staatliche Handeln, welches in Rechtspositionen des Individuums eingreift, eine gesetzliche Grundlage.[1544] Oftmals hat der Staat für die Führung von Registern und die damit verbundenen Datenbearbeitungen bereits gesetzliche Grundlagen geschaffen.[1545] Wie weiter oben dargelegt, kann die Verwaltung grundsätzlich selbst entscheiden, welcher Mittel sie sich zur Erfüllung ihrer Aufgaben bedient.[1546] Je nach Anwendungsbereich ist es daher denkbar, dass die Verwendung von Distributed-Ledger-Technologien nicht zwingend eine gesetzliche Grundlage benötigt. Im Folgenden soll daher ergründet

1540 Bericht DLT, S. 8.

1541 Bericht Rechtsanpassung DLT, S. 11 und 14.

1542 Bericht Rechtsanpassung DLT, S. 7 ff.

1543 Bericht DLT, S. 83, siehe dazu auch weiter unten Rz. 699.

1544 EPINEY, BSK BV, Art. 5, N. 40 f.

1545 Vgl. etwa die Grundbuchverordnung vom 23. September 2011 (GBV, 211.432.1), welche sich in Art. 27 GBV gar explizit mit der elektronischen Auskunft und Einsichtnahme befasst.

1546 Siehe dazu etwa oben Rz. 222.

werden, inwiefern die Verwendung von Distributed-Ledger-Technologien in grösserem Masse in Grundrechtspositionen eingreifen kann und ob die entsprechenden Eingriffe die Schaffung zusätzlicher gesetzlicher Regelungen notwendig machen.

III. Informationelle Selbstbestimmung

In vielen der oben genannten Anwendungsbereiche spielen Daten eine Rolle, welche Personen bestimmen oder bestimmbar machen. So können etwa in einem auf Blockchain basierten Register Daten über eine Person gespeichert werden. Zu denken ist bei einer rechtlichen Untersuchung dieser Technologie daher aus grundrechtlicher Sicht in erster Linie an das Recht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV. Es gilt zu beachten, dass es – wie einleitend in dieser Arbeit ausgeführt – verschiedene Ausgestaltungen von Blockchains gibt. Zu unterscheiden ist in erster Linie nach dem Benutzerkreis (öffentliche und private Blockchains) und den Verwaltungsbefugnissen («permissioned» oder «permissionless» Blockchains).[1547] Diese Unterscheidung kann auch in Bezug auf die datenschutzrechtliche Einordnung Unterschiede nach sich ziehen.[1548] Eine finale Einordnung einer möglichen Anwendung von Blockchain oder DLT kann daher nur anhand des konkreten Einsatzbereichs und der jeweiligen Ausgestaltung vorgenommen werden. An dieser Stelle soll daher lediglich eine grundsätzliche Einordnung der Blockchain-Technologie hinsichtlich allfälliger datenschutzrechtlicher Probleme vorgenommen werden, wobei den Unterschieden zwischen den verschiedenen Arten der Blockchain Rechnung getragen wird. 670

A. Anwendbarkeit der Datenschutzgesetzgebung

Die Datenschutzgesetzgebung von Bund und Kantonen ist grundsätzlich nur anwendbar, wenn Personendaten bearbeitet werden. Ein Bearbeiten von Personendaten ist dabei gemäss Art. 3 lit. e DSG jeder Umgang mit Personendaten, unabhängig von Mitteln und Verfahren. Wie bereits ausgeführt, zeichnet sich die Blockchain-Technologie dadurch aus, dass jede Transaktion grundsätzlich unveränderbar und für alle Beteiligten öffentlich einsehbar ist. Dadurch werden die Daten zumindest gespeichert und allenfalls weiteren Personen bekanntgegeben. Wie an anderer Stelle ausgeführt, ist der Begriff des Bearbeitens weit gefasst, womit grundsätzlich auch die blosse Speicherung 671

1547 Vgl. oben Rz. 52.

1548 Vgl. etwa GUGGENBERGER, ZD, 2017, S. 49 f., siehe dazu konkret auch weiter unten Rz. 672 und 687.

eine Bearbeitung im Sinne des Gesetzes darstellen kann.[1549] Zu beachten ist jedoch auch, dass es in vielen Anwendungsbereichen der Technologie (etwa bei Bitcoin-Transaktionen) nicht auf die genaue Identität des Gegenübers ankommt.[1550] Daher sind die entsprechenden Daten oft verschlüsselt gespeichert und die Identität des Betroffenen wird nicht offengelegt.[1551] Es stellt sich daher die Frage, ob es sich überhaupt um Personendaten im Sinne des Datenschutzgesetzes handelt.

1. Daten auf der Blockchain als Personendaten

672 Personendaten sind gemäss Art. 3 lit. a DSG Daten, welche eine Person bestimmen oder bestimmbar machen. Wie bereits an anderer Stelle ausgeführt, gilt eine Person dann als bestimmbar, wenn sich aufgrund der Daten und der Umstände auf die jeweilige Person schliessen lässt. Personendaten, welche anonymisiert sind, stellen somit grundsätzlich keine Personendaten mehr dar.[1552] Es ist jedoch zu beachten, dass auch vermeintliche anonyme Personendaten unter Umständen wieder reidentifiziert werden können, wenn sie mit anderen Daten kombiniert werden.[1553] Die Anwendbarkeit der Datenschutzgesetzgebung kann daher nur vollständig ausgeschlossen werden, wenn die Re-Identifizierung durch Dritte unmöglich oder mit einem so hohen Aufwand verbunden ist, dass diesen kein Interessierter auf sich nehmen würde.[1554]

673 Hinsichtlich der Frage, ob Daten im Rahmen der Blockchain Personendaten darstellen können, wird oft auf die Rechtsprechung des Bundesgerichts und des Europäischen Gerichtshofs zur Kategorisierung von IP-Adressen als Personendaten zurückgegriffen.[1555] Wie weiter oben im Rahmen dieser Arbeit ausführlich erläutert, ist für diese Einordnung in erster Linie der massgebliche Kontext relevant. Wenn es einer staatlichen Stelle beispielsweise – allenfalls auch unter Zuhilfenahme von Zusatzinformationen Dritter – mit einem vernünftigen Aufwand möglich ist, die Person zu identifizieren, so gelten die Daten als Personendaten.[1556]

674 Übertragen auf die Blockchain, bedeutet dies in erster Linie, dass betrachtet werden muss, welche Daten in diesem Rahmen bearbeitet werden

1549 ISLER, Jusletter, 4. Dezember 2017, N. 29.
1550 SCHREY/THALHOFER, NJW, 2017, S. 1433.
1551 ISLER, Jusletter, 4. Dezember 2017, N. 3.
1552 Vgl. RUDIN, SHK-DSG, Art. 3, N. 13.
1553 Vgl. weiter oben Rz. 230 ff.
1554 Botschaft Rev. DSG 2017, S. 7019.
1555 Vgl. insb. BGE 136 II 508, siehe dazu oben Rz. 353 ff.
1556 Siehe oben Rz. 353 ff.

können. Der Inhalt von Daten, welche auf der Blockchain gespeichert werden, unterscheidet sich dabei je nach Anwendungsfall. So werden bei Transaktionen die Daten etwa in sogenannten «Token» gespeichert. Die Daten können dabei im Klartext abgespeichert sein. Befinden sich darunter Daten mit einem Personenbezug, handelt es sich um Personendaten, welche für jeden einsehbar sind.[1557] Es gibt jedoch auch Möglichkeiten, die Daten auf der Blockchain verschlüsselt zu speichern.[1558] Denkbar ist es etwa, dass die jeweiligen Personendaten «off-chain», also auf dem lokalen Gerät oder auf einem anderen Server, gespeichert werden.[1559] Auf die jeweiligen Daten wird dann auf der Blockchain in verschlüsselter Weise referenziert, womit sie in erster Linie der Verifizierung dienen.[1560] Soweit ersichtlich verwendet etwa die Stadt Zug betreffend ihre E-ID-Lösung eine entsprechende Herangehensweise.[1561]

Werden die Daten nicht im Klartext gespeichert, stellt sich die Frage, ob 675
es sich aufgrund der Verwendung entsprechender Verschlüsselungstechniken um anonymisierte Daten handelt, welche einen Personenbezug entfallen lassen. Grundsätzlich wird davon ausgegangen, dass eine Verschlüsselung der Re-Identifizierung nicht prinzipiell im Wege steht.[1562] Entsprechende technische Lösungen werden weitgehend als Pseudonymisierung bewertet, da weiterhin die Möglichkeit besteht, dass die Daten mit der Person in Verbindung gebracht werden.[1563] Nach dem Geschriebenen ist davon auszugehen, dass die Transaktionsdaten, welche Personendaten enthalten, auch dann noch als Personendaten gelten müssen, wenn sie entsprechend verschlüsselt wurden.[1564] Eine konkrete Einschätzung, ob Personendaten vorliegen, ist indes lediglich für den jeweiligen Einzelfall leistbar.

Neben den Transaktionsdaten gibt es allerdings im Zusammenhang mit 676
der Blockchain noch weitere relevante Daten. Zu beachten sind einerseits die Schlüssel, mittels welcher der Zugriff auf die Daten in der Blockchain möglich ist. Wie weiter oben beschrieben, gibt es hierbei immer ein Schlüsselpaar,

1557 STENGEL/AU, sic!, 2018, S. 445.

1558 Für eine Übersicht etwa ERBGUTH, Jusletter IT, 22. Februar 2018, S. 1 ff.

1559 EBERHARD/TAI, ESOCC (European Conference on Service-Oriented and Cloud Computing), 2017.

1560 STENGEL/AU, sic!, 2018, S. 451; BERGHOFF/GEBHARDT/LOCHTER/MASSBERG, S. 36.

1561 Vgl. für die E-ID-Lösung der Stadt Zug: Consensys, Case Study.

1562 Vgl. etwa FINCK, EDPL, 2018, S. 22 ff. Einzig, wenn der Nachweis gelänge, dass sämtliche Kopien des Schlüssels gelöscht sind (sog. Crypto-Shredding), könnte man dies in Erwägung ziehen, wobei zu bedenken ist, dass eine Entschlüsselung theoretisch auch ohne Schlüssel möglich (wenn auch sehr aufwendig) ist; vgl. ERBGUTH, Jusletter IT, 22. Februar 2018, S. 4.

1563 Vgl. ARTIKEL-29-DATENSCHUTZGRUPPE, Opinion 5/2014, S. 20.

1564 STENGEL/AU, sic!, 2018, S. 445.

welches aus einem öffentlichen Public Key und einem geheimen Private Key besteht.[1565] Der Public Key stellt eine Art Kontonummer dar, an welche z.B. Transaktionen gerichtet werden können. Der private Schlüssel ist dagegen eher eine Art Passwort, welches etwa für die Verifikation der Transaktionen benötigt wird.[1566] Der Private Key lässt sich dabei mittel kryptographischer Funktion aus dem Public Key herleiten.[1567] Während davon ausgegangen werden kann, dass der Private Key aufgrund seiner Funktion als Passwort in der Regel einzig dem Benutzer bekannt ist, ist der Public Key öffentlich zugänglich.[1568] Mittlerweile haben mehrere Studien gezeigt, dass es mithilfe der Transaktionsdaten möglich ist, Rückschlüsse auf die IP-Adresse zu ziehen, von welcher aus die jeweilige Transaktion getätigt wurde, womit auch Rückschlüsse auf den Nutzer möglich sein können.[1569] Es wird daher in der Lehre davon ausgegangen, dass bei öffentlichen (public) Blockchains aus den Schlüsseln ein Personenbezug grundsätzlich hergestellt werden kann, weshalb diese als Personendaten im Sinne des Datenschutzgesetzes verstanden werden können.[1570] Bei Blockchain-Systemen mit geschlossenem Benutzerkreis (private Blockchain) ist oft zusätzlich relevant, dass zumindest für die Stelle, welche etwa ein auf Blockchain basiertes Register betreibt, aufgrund des Public Key ein Rückschluss auf die dahinterstehenden Personen möglich bleibt, etwa anhand eines entsprechende Verzeichnisses. Daher sind die Daten hier in jedem Fall als Personendaten einzuordnen.[1571]

677 Nach dem soeben Ausgeführten kann also bei Blockchains ein Personenbezug nicht grundsätzlich ausgeschlossen werden. Bei der Verwendung im Rahmen der öffentlichen Verwaltung wird es sich dabei regelmässig um geschlossene Systeme handeln, welche durch die jeweilige Stelle verwaltet werden. Dabei ist es etwa gerade bei Registern wesensimmanent, dass die Behörde die Identität der Transaktionsbeteiligten kennt.[1572] Auch für Identitätsnachweise etwa im Rahmen der digitalen Identität ist es geradezu notwendig, dass die jeweiligen Personendaten zumindest den Betreibern bekannt sind. Daher ist davon auszugehen, dass in vielen Fällen, in welchen die

1565 Vgl. oben Rz. 49.

1566 VOSHMGIR, S. 13.

1567 ANTONOPOULOS, S. 63; HESS/LIENHARD, Jusletter, 4. Dezember 2017, N. 4.

1568 STENGEL/AU, sic!, 2018, S. 445.

1569 BIRYUKOV/KHOVRATOVICH/PUSTOGAROV, Proceedings of the 2014 ACM SIGSAC Conference; REID/HARRIGAN, An Analysis of Anonymity in the Bitcoin System.

1570 Bericht DLT, S. 83, m.W.h.; vgl. STENGEL/AU, sic!, 2018, S. 445 f.; ISLER, Jusletter, 4. Dezember 2017, N. 4, 24.

1571 SCHREY/THALHOFER, NJW, 2017, S. 1433.

1572 SCHREY/THALHOFER, NJW, 2017, S. 1433.

Blockchain durch die öffentliche Verwaltung eingesetzt wird, zumindest für die jeweilige Stelle die Person bestimmbar ist und somit Personendaten im Sinne des Datenschutzgesetzes vorliegen.

2. Anwendbares Recht

Das dezentrale Wesen der Blockchain macht es möglich, dass sich die Beteiligten eines Netzwerks überall auf der Welt befinden und somit potenziell auch überall die jeweiligen Daten bearbeitet werden können. Dementsprechend ergibt sich gerade bei offenen Blockchain-Systemen (private Blockchain) eine Vielzahl an möglichen Anknüpfungspunkten.[1573] Daraus resultiert die Frage, ob das schweizerische Datenschutzrecht überhaupt anwendbar ist. In erster Linie kommt es darauf an, wie ein konkretes Blockchain-Projekt ausgestaltet ist. Befinden sich sämtliche Rechner oder Geräte, auf denen eine entsprechende Lösung betrieben wird, in der Schweiz, so ist hinsichtlich des anwendbaren Rechts keine weitergehende Problematik festzustellen. 678

Sobald jedoch ein grenzüberschreitender Zusammenhang vorliegt, bestimmt sich die räumliche Anwendbarkeit des schweizerischen Datenschutzrechts in erster Linie nach dem Territorialitätsprinzip.[1574] Dabei genügt es, dass die Erhebung der Personendaten oder eine Persönlichkeitsverletzung in der Schweiz erfolgen, damit die hiesige Datenschutzgesetzgebung einschlägig ist.[1575] Es ist daher grundsätzlich davon auszugehen, dass, sofern Daten über eine Person aus der Schweiz auf einer Blockchain bearbeitet werden, die schweizerische Datenschutzgesetzgebung anwendbar ist.[1576] Je nachdem, ob die Bearbeitung dabei in erster Linie durch eine kantonale Behörde oder ein Bundesorgan stattfindet, ist die jeweilige kantonale Datenschutzgesetzgebung oder das eidgenössische Datenschutzgesetz einschlägig.[1577] Für die mit dem Einsatz verbundenen privaten Datenbearbeitungen ist stets das DSG zu beachten. 679

1573 ISLER, Jusletter, 4. Dezember 2017, N. 16 ff.

1574 BÜHLMANN/REINLE, digma, 2017, S. 12; PASSADELIS, in: Datenschutzrecht. N. 23.

1575 Vgl. dazu etwa BGE 138 II 346, E. 3.2 m.w.H.

1576 Vgl. auch ISLER, Jusletter, 4. Dezember 2017, N. 18 f.

1577 Denkbar ist bei Blockchain auch, dass die DSGVO gestützt auf Art. 3 DSGVO extraterritoriale Anwendung erlangen könnte, da Personendaten im Zusammenhang mit Vertragsangeboten oder der Beobachtung von Personen bearbeitet werden; vgl. ISLER, Jusletter, 4. Dezember 2017, N. 20. Dies ist indes im Bereich der öffentlichen Verwaltung i.d.R. nicht anzunehmen, siehe dazu oben Rz. 62.

B. Folgen

1. Gesetzliche Grundlagen

680 Die soeben etablierte Anwendbarkeit der Datenschutzgesetzgebung bedeutet in erster Linie, dass gemäss Art. 17 DSG Personendaten nur bearbeitet werden dürfen, sofern eine gesetzliche Grundlage dies vorsieht. Der Terminus des Bearbeitens ist dabei – wie an anderer Stelle ausgeführt – weit zu verstehen und umfasst etwa bereits die Speicherung der Daten.[1578] Sofern die Aufgabe, welche neu gestützt auf die Blockchain oder die «Distributed Ledger»-Technologie erfolgen soll, bereits zuvor vom öffentlichen Organ erfüllt wurde, ist davon auszugehen, dass schon gesetzliche Grundlagen bestehen, welche eine Datenbearbeitung durch das öffentliche Organ rechtfertigen. So gibt es etwa im Bereich der Registerführung bereits etliche Rechtsgrundlagen, welche oftmals detailliert in Verordnungen oder Weisungen konkretisiert werden. Inwiefern diese gesetzlichen Grundlagen hinsichtlich der Datenbearbeitungen anzupassen sind, wird im konkreten Einzelfall zu beurteilen sein.[1579] Sollten Blockchain-Anwendungen in Bereichen verwendet werden, in welchen bisher noch keine gesetzlichen Grundlagen für die Datenbearbeitung bestehen, sind solche zwingend neu zu schaffen.

681 Zusätzliche Probleme hinsichtlich der Datenverarbeitung können sich je nach Ausgestaltung der jeweiligen Blockchain-Lösung daraus ergeben, dass die Daten jeweils nicht zentral gespeichert, sondern auf verschiedenen Servern oder Knoten eines Netzwerks verteilt sind.[1580] Weniger problematisch ist dies bei privaten Blockchains (im Unterschied zu öffentlichen [public] Blockchains) und insbesondere bei sogenannten «permissioned Blockchains», da diese in ihrer Funktionsweise herkömmlichen Datenbanken ähneln und es klare Verantwortlichkeiten sowie vorgängig bekannte Teilnehmende gibt.[1581] Basiert eine von der öffentlichen Verwaltung benutzte Anwendung indes auf einer öffentlichen, weit verbreiteten Blockchain, wie diejenige der bekanntesten Kryptowährung Bitcoin, so sind diese Daten auf Rechnern überall auf der Welt gespeichert.[1582]

682 Wie zuvor ausgeführt, sind die Daten auf einer Blockchain zwar in der Regel verschlüsselt gespeichert, es kann jedoch nicht ausgeschlossen werden, dass dadurch eine Person bestimmt oder bestimmbar ist, womit sie als

1578 Siehe dazu oben Rz. 76.

1579 Vgl. zum Ganzen Bericht DLT, S. 84.

1580 WELZEL/ECKERT/KIRSTEIN/JACUMEIT, S. 17, s. weiter oben Rz. 47 ff.

1581 ISLER, Jusletter, 4. Dezember 2017, N. 13.

1582 ISLER, Jusletter, 4. Dezember 2017, N. 7.

Personendaten im Sinne der Datenschutzgesetzgebung zu gelten haben.[1583] Somit besteht also je nach Ausgestaltung des jeweiligen Blockchain-Projekts die Gefahr, dass entsprechende Daten nicht nur im Besitz des jeweiligen öffentlichen Organs sind, sondern auch Dritten zugänglich gemacht werden. Diesem zusätzlichen Risiko ist Rechnung zu tragen. Es ist davon auszugehen, dass die aktuellen gesetzlichen Grundlagen – etwa im Bereich der Registerführung – nicht derart weit ausgelegt werden können, dass der Betroffene mit der Speicherung seiner Daten auf einer Vielzahl anderer, mithin privater Computer rechnen muss. Daher wird vertreten, dass die betreffenden Gesetzesgrundlagen entsprechend anzupassen seien.[1584] In der Praxis scheint eine gesetzliche Grundlage, welche vorsieht, dass Personendaten im Rahmen einer Blockchain-Lösung unter Umständen auch an Private ausserhalb der öffentlichen Behörde bekanntgegeben werden können, wohl aufgrund ihrer weitreichenden Natur wenig realistisch.

683 Allenfalls könnte es sich bei der Speicherung der Blockchain auf den dezentralen Rechnern um eine Datenbearbeitung durch Dritte im Sinne von Art. 10a DSG handeln, wie diese etwa bei der Speicherung von Daten auf Cloud-Diensten wie «Google Drive» oder «Dropbox» durch öffentliche Verwaltungsstellen vorliegt.[1585] Da die einzelnen «Nodes» einer Blockchain die entsprechenden Daten ebenfalls nur speichern, womit nach dem oben Ausgeführten allerdings bereits eine Bearbeitung vorliegt, ist dies durchaus vergleichbar.[1586] Gemäss Art. 10a DSG darf die Bearbeitung von Personendaten durch Vereinbarung oder Gesetz auf Dritte übertragen werden, wenn die Daten nur so bearbeitet werden, wie der Auftraggeber dies selbst dürfte, und falls keine gesetzlichen oder vertraglichen Bestimmungen die Bearbeitung durch Dritte verbieten. Eine entsprechende gesetzliche Grundlage ist nach dem bereits oben Ausgeführten eher unwahrscheinlich. Auch eine Übertragung durch vertragliche Regelung ist aufgrund der potenziellen Vielzahl an Personen, welche in einem entsprechenden Netzwerk verbunden sind, praktisch eher schwierig zu realisieren.[1587]

684 Bei der Benutzung entsprechender Blockchain-Systeme wird allenfalls versucht, die jeweiligen Datenbearbeitungen und -bekanntgaben über die Eigenverantwortung der Betroffenen zu legitimieren, oder es wird auf die

1583 Siehe dazu oben Rz. 672 ff.

1584 Bericht DLT, S. 84.

1585 Vgl. zum «Outsourcing» bzw. «Cloud Computing» im Detail weiter oben Rz. 98 ff.

1586 ROSENTHAL, Jusletter, 17. Juni 2019, S. 58.

1587 ROSENTHAL, Jusletter, 17. Juni 2019, S. 59.

Einwilligung als Rechtfertigungsgrund hingewiesen.[1588] Eine entsprechende Einwilligung hat nach gemäss den Vorgaben von Art. 4 Abs. 5 DSG nach angemessener Information freiwillig zu erfolgen. Die Angemessenheit der Information bestimmt sich nach den konkreten Umständen der jeweiligen Datenbearbeitung, speziell in Bezug auf den Umstand, mit welchen Risiken bzw. Folgen diese für die betroffenen Personen verknüpft ist.[1589] Problematisch kann dabei insbesondere sein, dass bei auf Blockchain basierenden Systemen unter Umständen nicht bekannt ist, wer im Rahmen der Blockchain Zugriff auf diese Daten hat und diese allenfalls gar weiterverarbeiten kann.[1590] Gerade bei öffentlichen Blockchains (public Blockchains) fehlt zudem in aller Regel ein zentraler Verantwortlicher, so dass es den betreffenden öffentlichen Organen regelmässig bereits aus diesem Grund schwerfallen (wenn nicht gar unmöglich sein) dürfte, über die damit verbundene Risiken in genügender Weise zu informieren.[1591] Es ist m.E. ebenso und insbesondere im Kontext der Verwendung durch öffentliche Organe fraglich, ob ein grundsätzlicher Hinweis auf die mit der Bearbeitung über die Blockchain verbundenen Gefahren der Datenbearbeitung durch Dritte bereits ausreicht, um eine rechtsgültige Einwilligung nach angemessener Information annehmen zu können.

685 Zu guter Letzt bleibt zu beachten, dass die «Nodes» von Blockchain-Netzwerken generell global verteilt sein können. Unter Umständen ist es nicht ersichtlich, in welchen Ländern die entsprechenden Bearbeiter ihren Rechner haben.[1592] Dies ist insbesondere problematisch, da gemäss Art. 6 DSG die grenzüberschreitende Datenbekanntgabe nicht zulässig ist, wenn dadurch die Persönlichkeit der betroffenen Person schwerwiegend gefährdet wird, namentlich weil eine Gesetzgebung fehlt, welche einen angemessenen Schutz gewährleistet. In diesem Fall wäre der angemessene Schutz gemäss Art. 6 Abs. 2 DSG anderweitig – etwa mithilfe von vertraglichen Garantien – sicherzustellen oder die Einwilligung der jeweiligen Person einzuholen. Auch dies dürfte aufgrund der oftmals unbekannten Teilnehmer in einem entsprechenden Netzwerk kaum praktikabel sein.[1593]

686 Zusammenfassend lässt sich festhalten, dass die Ausgestaltung der gesetzlichen Grundlagen zur Datenbearbeitung und -bekanntgabe wesentlich

1588 Vgl. Bericht DLT, S. 84; STENGEL/AU, sic!, 2018, S. 449.

1589 MAURER-LAMBROU/STEINER, BSK DSG/BGÖ, Art. 4 DSG, N. 16i.

1590 RAINER BÖHME / PAULINA PESCH, DuD, 2017, S. 479.

1591 SCHREY/THALHOFER, NJW, 2017, S. 1433. Zum Problem der Verantwortlichkeit siehe sogleich Rz. 688.

1592 BITKOM E. V., Blockchain-Studie, S. 33.

1593 ISLER, Jusletter, 4. Dezember 2017, N. 37; BITKOM E. V., Blockchain-Studie, S. 33.

von der Ausgestaltung des jeweiligen Systems abhängig ist. Unter Umständen können die bestehenden gesetzlichen Grundlagen reichen, wenn ein Register neu auf einer «permissioned Blockchain» mit geschlossenem Benutzerkreis (private Blockchain) geführt werden soll, da sich deren Funktionsweise oft nicht wesentlich von der Funktionsweise bestehender Datenbanken unterscheidet. Gerade bei der Verwendung öffentlicher Blockchains ist indes der Ausgestaltung besondere Beachtung zu schenken. Eine schrankenlose Bekanntgabe liesse sich wohl weder mit einer gesetzlichen Grundlage noch über das Institut der Datenbearbeitung durch Dritte oder mit der Einwilligung zufriedenstellend rechtfertigen. Indes wird davon ausgegangen, dass auch bei öffentlichen Blockchains eine datenschutzkonforme Ausgestaltung, etwa durch technische Massnahmen, nicht grundsätzlich ausgeschlossen ist.[1594]

2. Betroffenenrechte

Aus der Anwendbarkeit des Datenschutzrechtes ergibt sich einerseits, dass 687
für die jeweiligen Bearbeiter die Grundsätze der Datenbearbeitung zu beachten sind, welche insbesondere in den Artikeln 4, 5 und 7 des Datenschutzgesetzes zu finden sind.[1595] Zudem gesteht das Datenschutzgesetz betroffenen Personen gewisse Betroffenenrechte zu, wobei insbesondere das Auskunftsrecht (gemäss Art. 8 DSG) sowie die Ansprüche zur Durchsetzung einer gesetzesmässigen Datenbearbeitung gemäss Art. 25 DSG zu nennen sind. Im Folgenden soll aufgezeigt werden, dass die dezentrale und grundsätzlich unabänderliche Natur der Blockchain teilweise Schwierigkeiten hinsichtlich der Erfüllung dieser Vorgaben mit sich bringt.

a) Verantwortlichkeit

Aufgrund der Tatsache, dass unter Umständen eine Vielzahl an Personen als 688
Datenbearbeiter auf der Blockchain in Frage kommt, ist in erster Linie zu beantworten, wer für die jeweilige Datenbearbeitung verantwortlich ist und an wen somit die entsprechenden Ansprüche gerichtet werden können. Gemäss Art. 8 DSG richtet sich der Auskunftsanspruch in der Regel an den Inhaber der jeweiligen Datensammlung. Als Inhaber der Datensammlung ist gemäss Art. 3 lit. i DSG diejenige Person oder dasjenige Bundesorgan zu betrachten, welche bzw. welches über den Zweck und den Inhalt der Datensammlung entscheidet. Bei der Datenbearbeitung durch Bundesorgane sieht Art. 25 DSG vor, dass die obengenannten Ansprüche gegen das verantwortliche Bundesorgan geltend gemacht werden können. Die Verantwortlichkeit bestimmt

1594 Bericht DLT, S. 84.

1595 Vgl. ISLER, Jusletter, 4. Dezember 2017, N. 30 und 36 ff.

sich wiederum nach Art. 16 DSG, welcher festschreibt, dass für den Datenschutz dasjenige Bundesorgan verantwortlich ist, welches Personendaten in Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt. Im Weiteren ist relevant, dass Rechtsansprüche zum Schutz der Persönlichkeit sich aufgrund von Art. 15 DSG grundsätzlich nach den Artikeln 28, 28a sowie 28l des Zivilgesetzbuchs richten, womit eine Klage gegen jeden möglich ist, der an einer Verletzung mitgewirkt hat.[1596]

689 Aufgrund der – bereits beschriebenen – klaren Regelungen von Inhabern und Berechtigten sind geschlossene (private) und insbesondere «permissioned Blockchain»-Systeme hier grundsätzlich unproblematisch, zumal es regelmässig eine Instanz gibt, welche die relevanten Verantwortlichkeiten übernehmen kann.[1597] Im Zusammenhang mit öffentlichen Registern kann etwa das registerführende öffentliche Organ über Zweck und Inhalt der jeweiligen Datensammlung bestimmen und hat somit als Inhaber der Datensammlung zu gelten. In der Regel bearbeitet es auch die jeweiligen Personendaten oder lässt diese zumindest bearbeiten und kann als verantwortlich im Sinne von Art. 16 DSG angesehen werden.

690 Mit Schwierigkeiten verbunden ist die Zuordnung der Verantwortlichkeit indes insbesondere bei öffentlichen (public) Blockchains. Im Schweizer Recht lässt sich in diesen Fällen die Frage nach dem Inhaber einer Datensammlung nicht einfach beantworten. Da jedoch – wie weiter oben ausgeführt wurde – im Schweizer Recht alle Bearbeitenden gestützt auf Art. 28 ZGB ins Recht gefasst werden können und somit Adressaten sind, scheint unser Recht in diesem Punkt einigermassen auf die speziellen Eigenheiten der Blockchain vorbereitet. Zu betrachten ist jedoch, dass auch hier die zentralen Pflichten dem Inhaber einer Datensammlung (bzw. de lege ferenda dem Verantwortlichen) auferlegt werden, welcher teilweise schwer zu bestimmen ist.[1598]

691 Rechtsvergleichend stellen sich ähnliche Probleme hinsichtlich der Verantwortlichkeit für die Blockchain übrigens auch im Anwendungsbereich der DSGVO. Hier können die entsprechenden Rechte gegenüber dem Verantwortlichen geltend gemacht werden.[1599] Als Verantwortlicher wird in Art. 4 Ziff. 7 DSGVO definiert, wer als «natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle [„,] allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet». In der Regel wird davon ausgegangen, dass es sich dabei um eine

1596 Vgl. STENGEL/AU, sic!, 2018, S. 446; MEILI, BSK ZGB I, Art. 28, N. 37.

1597 ISLER, Jusletter, 4. Dezember 2017, N. 13; STENGEL/AU, sic!, 2018, S. 446.

1598 Vgl. zum Ganzen: STENGEL/AU, sic!, 2018, S. 446.

1599 Vgl. etwa BECHTOLF/VOGT, ZD, 2018, S. 69; vgl. etwa Art. 5 Abs. 2 DSGVO, Art. 15 DSGVO oder Art. 16 DSGVO, welche sich jeweils an den Verantwortlichen richten.

konkrete Person oder Institution handelt, welche die Verarbeitung vornimmt und somit für die Einhaltung des Datenschutzes verantwortlich ist.[1600] In der dezentralen Struktur einer – insbesondere öffentlichen – Blockchain nehmen indes alle Systeme Transaktionen vor und bearbeiten somit Daten im Sinne des Gesetzes.[1601] Da es keine einzelne Person gibt, welche über den Zweck und die Mittel der Verarbeitung der Daten entscheidet, wird häufig vertreten, dass alle Personen als Verantwortliche im Sinne der DSGVO zu gelten hätten.[1602]

692 Die gemeinsame Verantwortlichkeit mehrerer Stellen wird in Art. 26 DSGVO geregelt. Die Rechte der Betroffenen können dabei gemäss Art. 26 Abs. 3 DSGVO gegenüber jedem Verantwortlichen geltend gemacht werden. Die gemeinsam verantwortlichen Stellen müssen grundsätzlich in einer Vereinbarung festlegen, wer die sich aus der DSGVO ergebenden Verpflichtungen erfüllt, wobei eine entsprechende Vereinbarung nicht zwingende Voraussetzung für die gemeinsame Verantwortlichkeit ist.[1603] Es ist indes fraglich, ob die datenschutzrechtliche Verantwortlichkeit jedes Teilnehmers überhaupt zielführend ist, zumal der einzelne «Node» in der Regel derart geringen Einfluss auf die Bearbeitungen hat, dass es kaum möglich sein dürfte, die entsprechenden Rechte ihm gegenüber überhaupt durchsetzen zu können.[1604] Andere Konzepte versuchen etwa, die Entwickler einer Blockchain[1605] oder die Miner[1606] als Verantwortliche im Sinne der DSGVO herbeizuziehen, was jedoch aufgrund von deren mangelnden Einflussmöglichkeiten auf die Blockchain ebenfalls keine wirkliche Verbesserung der Durchsetzbarkeit der Betroffenenrechte mit sich bringt.[1607] Es bleibt somit festzuhalten, dass insbesondere bei öffentlichen (public) Blockchains die DSGVO bei der Frage des Verantwortlichen, bei welchem die Datenschutzrechte durchgesetzt werden können, an ihre Grenzen stösst.[1608]

1600 Vgl. Erwägungsgrund 79 DS-GVO; PETRI, Nomos Komm. DSGVO, Art. 4 Abs. 7, N. 13.

1601 SCHREY/THALHOFER, NJW, 2017, S. 1433. CMS Law-Now, Petrányi/Domokos, Hungary: Data Protection Aspects of Blockchain.

1602 Vgl. STENGEL/AU, sic!, 2018, S. 446; SCHREY/THALHOFER, NJW, 2017, S. 1433;.

1603 SCHREY/THALHOFER, NJW, 2017, S. 1434.

1604 RAINER BÖHME / PAULINA PESCH, DuD, 2017, S. 473 ff.; datenschutzrechtlich problematisch können in dieser Hinsicht auch die Nutzer sein, welche selbst nicht am System teilnehmen, z.B. «Wallet»-Provider, vgl. BECHTOLF/VOGT, ZD, 2018, S. 69.

1605 FASCHING, S. 20.

1606 CZARNECKI, Blockchains and Personal Data Protection Regulations Explained, CoinDesk, 26. April 2017.

1607 ISLER, Jusletter, 4. Dezember 2017, N. 39 ff.

1608 ISLER, Jusletter, 4. Dezember 2017, N. 39 ff; im Ergebnis wohl ebenso RAINER BÖHME / PAULINA PESCH, DuD, 2017, S. 479.

b) Auskunftsrecht

693 Die Datenschutzgesetzgebung sieht in Art. 8 DSG vor, dass jede Person Auskunft darüber verlangen kann, welche Daten über sie bearbeitet werden, wobei diese Auskunft auch umfasst, zu welchem Zweck und gestützt auf welche Rechtsgrundlagen diese Daten bearbeitet werden. Adressat dieses Anspruchs ist der «Inhaber der Datensammlung».[1609] Der Inhalt der Auskunftsbegehren umfasst alle in der Datensammlung vorhandenen Informationen über die Person, über den Bearbeitungszweck der Daten und gegebenenfalls die Rechtsgrundlagen des Bearbeitens sowie über die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger.[1610]

694 Werden Blockchain-Systeme im Bereich der öffentlichen Verwaltung eingesetzt, so existiert – wie bereits ausgeführt wurde – in der Regel ein klar definierter Verantwortlicher für die Datenbearbeitung. Dieser Verantwortliche ist primärer Adressat der jeweiligen Auskunftsansprüche. Dabei kann es sich beispielsweise um diejenige Behörde handeln, welche ein auf Blockchain basiertes Register betreibt. Insbesondere bei öffentlichen Blockchain-Systemen (public Blockchain) können sich mangels klarer Verantwortlichkeiten Schwierigkeiten bei der Durchsetzung ergeben. Allenfalls kann damit argumentiert werden, dass die eigenen Daten aufgrund der Transparenz der Blockchain zumindest für die Teilnehmenden an einem entsprechenden Netzwerk durchaus einsehbar sind und das Auskunftsrecht auf diese Weise bereits erfüllt ist.[1611] Nicht zulässig ist ein vorgängiger Verzicht auf das Auskunftsrecht durch die Betroffenen etwa mittels rechtlicher Abrede.[1612]

695 Die meisten dieser Punkte, über welche Auskunft erteilt werden muss, bringen im Zusammenhang mit Distributed-Ledger-Technologien keine zusätzlichen Schwierigkeiten mit sich, da gerade beim Einsatz durch die öffentliche Verwaltung oftmals klar sein dürfte, welche Daten bearbeitet werden und zu welchem Zweck. Problematisch ist allenfalls, dass Auskunft über allfällige an der Sammlung Beteiligte und Datenempfänger erteilt werden muss. Gemäss herrschender Lehre reicht es dabei aus, wenn nicht über die Identität, sondern lediglich über die Kategorie der beteiligten Personen Angaben gemacht werden, wozu aber auch Angaben zur Branche und zum Land zählen.[1613]

1609 In der DSGVO sieht Art. 15 ein analoges Recht vor, wobei hier der Verantwortliche der Datenbearbeitung der Adressat des Anspruchs ist.

1610 RUDIN, SHK-DSG, Art. 8, N. 40 f.

1611 SCHREY/THALHOFER, NJW, 2017, S. 1434.

1612 GRAMIGNA/MAURER-LAMBROU, BSK DSG/BGÖ, Art. 8, N. 60; vgl. für Deutschland: SCHREY/THALHOFER, NJW, 2017, S. 1435.

1613 RUDIN, SHK-DSG, Art. 8, N. 18.

Auch dies könnte indes bei offenen Systemen problematisch werden, da unter Umständen nicht ersichtlich ist, bei wem weitere «Nodes» der jeweiligen Blockchain vorhanden sind oder welche Intermediäre (z.B. «Wallet»-Betreiber) ebenfalls Zugriff auf die Daten haben.

c) Berichtigungs- und Löschungsrechte

Aus Art. 25 DSG ergeben sich zudem gegenüber Bundesorganen weitere Ansprüche der Betroffenen bei widerrechtlicher Bearbeitung. Dazu zählt insbesondere ein Recht auf die Berichtigung oder die Vernichtung oder Sperrung von widerrechtlich bearbeiteten Personendaten (Art. 25 Abs. 3 lit. a DSG). Insbesondere wenn Daten – etwa mangels gesetzlicher Grundlage – gar nicht bearbeitet werden dürfen, besteht ein Recht auf deren Vernichtung.[1614] Wie beim Auskunftsrecht beschrieben, kann insbesondere bei öffentlichen Blockchain-Systemen mangels klar definierter Verantwortlichkeiten bereits problematisch sein, an wen die entsprechenden Ansprüche zu richten sind. 696

Ein weiteres Problem ergibt sich daraus, dass sich die Blockchain gerade durch ihre Unveränderlichkeit auszeichnet und es somit eben gerade nicht möglich sein sollte, die gespeicherten Daten nachträglich zu verändern. Diesbezügliche Ansprüche können daher auf der Blockchain technisch nicht oder nur eingeschränkt durchgesetzt werden.[1615] In der Lehre werden verschiedene alternative Möglichkeiten thematisiert, mit denen allenfalls eine Durchsetzung dieser Ansprüche auch auf der Blockchain möglich ist. Hinsichtlich des Berichtigungsanspruchs sieht das Schweizer Recht in Art. 25 Abs. 2 DSG vor, dass bei Daten ein Bestreitungsvermerk angebracht werden kann, wenn sich weder die Richtigkeit noch die Unrichtigkeit bewiesen lässt.[1616] Sofern ein Bestreitungsvermerk technisch nicht möglich ist, dürfen grundsätzlich nur erwiesenermassen richtige Daten bearbeitet werden.[1617] Die DSGVO sieht dagegen etwa in Artikel 16 explizit vor, dass eine Berichtigung auch mittels ergänzender Erklärung erfolgen kann. Auf diese Weise könnte allenfalls die Richtigkeit der Daten durch die Aufnahme der richtigen Daten in einem anderen Block der Berichtigungspflicht genügen, auch wenn der ursprüngliche Block dabei nicht gelöscht oder bearbeitet wird.[1618] 697

1614 STURNY, SHK-DSG, Art. 25, N. 24 und 29. Im E-DSG wird dieses Recht auf Löschung in Artikel 28 Abs. 2 erstmals auch explizit anerkannt; vgl. Botschaft Rev. DSG 2017, S. 7077. Die DSGVO sieht in Artikel 17 ein entsprechendes Recht bereits vor.

1615 ISLER, Jusletter, 4. Dezember 2017, N. 39; STENGEL/AU, sic!, 2018, S. 448; Bericht DLT, S. 83.

1616 Vgl. zu diesem Instrument, STURNY, SHK-DSG, Art. 25, N. 34 f.

1617 Vgl. STURNY, SHK-DSG, Art. 25, N. 43.

1618 STENGEL/AU, sic!, 2018, S. 448; zweifelnd: FINCK, EDPL, 2018, S. 22.

698 Es gibt technisch weitere Möglichkeiten, eine Blockchain nachträglich zu bearbeiten, etwa mittels «Forking» (also einer gewollten oder ungewollten Zweiteilung der Blockchain) oder durch einen Hacker-Angriff, bei dem die Hacker 51 % der Hälfte des Mining-Netzwerks unter Kontrolle bringen, um auf diese Weise den Konsensmechanismus zu beeinflussen. Da jedoch diese Vorgehensweisen mit einem grossen Aufwand verbunden sind und keine Garantie dafür bieten, dass die gewollte Version sich durchsetzt, liegt es auf der Hand, dass sie nicht als taugliches und verlässliches Mittel zur Durchsetzung der datenschutzrechtlichen Ansprüche betrachtet werden können.[1619] Denkbar wäre je nach Art der Blockchain auch eine Durchführung von Reverse Transactions, wobei solange fiktive Transaktionen durchgeführt würden, bis der korrekte Zustand wiederhergestellt ist. Auch dieses Vorgehen ist jedoch aufgrund des damit verbundenen Aufwands als nicht zielführend zu beurteilen.[1620]

699 Inzwischen scheint es indes möglich, Blockchains auf eine Weise zu programmieren, dass eine nachträgliche Änderung auch ohne derart komplexe Vorgänge unter gewissen Umständen möglich bleibt.[1621] So kann etwa eine «permissioned Blockchain» derart ausgestaltet werden, dass ein vertrauenswürdiger Administrator auch nachträglich Änderungen vornehmen kann (basierend auf einem kryptografischen Schlüsselpaar).[1622] Um einen Missbrauch dieser Rechte zu verhindern, soll jeder veränderte Block ein unabänderliches Kennzeichen (quasi eine Narbe) der Veränderung tragen.[1623] Auch diese Lösung wird indes kritisiert, da auf diese Weise wieder ein vertrauensvermittelnder Intermediär eingesetzt werden muss, was die Blockchain ihrem Wesen nach eben gerade verhindern bzw. entbehrlich machen soll. Zudem ist aktuell noch unklar, ob diese Vorgehensweise technisch skalierbar ist.[1624]

700 Auch wenn die eigentlichen Daten «off-chain» gespeichert werden und auf der Blockchain nur referenziert werden, können sie allenfalls berichtigt oder gelöscht werden.[1625] Dem Recht auf Löschung könnte zudem je nach Ausgestaltung durch eine Verschlüsselung oder Pseudonymisierung der Daten und die anschliessende Vernichtung des Schlüssels nachgekommen werden.[1626]

1619 Vgl. zum Ganzen: BECHTOLF/VOGT, ZD, 2018, S. 70 f.

1620 SCHREY/THALHOFER, NJW, 2017, S. 1435.

1621 BECHTOLF/VOGT, ZD, 2018, S. 70; vgl. ein entsprechendes Patent von Accenture: LUMB/TREAT/JELF, S. 1 ff.

1622 Vgl. STENGEL/AU, sic!, 2018, S. 450.

1623 LUMB/TREAT/JELF, S. 7.

1624 STENGEL/AU, sic!, 2018, S. 450.

1625 Vgl. STENGEL/AU, sic!, 2018, S. 451.

1626 STENGEL/AU, sic!, 2018, S. 448.

Als Alternative zur Löschung wird teilweise auch die Sperrung von Daten angeführt, wobei dadurch der eigentliche Sinn der Blockchain, durch die dauerhafte Speicherung von Daten Vertrauen zu bilden, in gewisser Weise unterlaufen würde.[1627]

d) Fazit

Die Durchsetzung der Betroffenenrechte ist bei Blockchain-Systemen mit Schwierigkeiten bzw. Paradoxien verbunden. So stellt sich insbesondere bei öffentlichen Blockchain-Systemen (public Blockchains) bereits die Frage nach dem Adressaten der jeweiligen Ansprüche. Die Vielzahl möglicher Bearbeiter kann zudem auch hinsichtlich der Auskunftsgewährung zusätzliche Probleme bereiten. Am schwersten wiegt indes, dass die Grundkonzeption der Blockchain eine nachträgliche Berichtigung oder Vernichtung nicht vorsieht. Es gibt indes verschiedene technische Möglichkeiten, eine Blockchain nachträglich zu bearbeiten, wobei einige – wie das Forking – aufgrund des damit verbundenen Aufwands und unklarer Auswirkungen nicht als Mittel zur Durchsetzung datenschutzrechtlicher Ansprüche in Betracht kommen. Dennoch ist eine nachträgliche Berichtigung je nach Ausgestaltung denkbar, etwa wenn ein vertrauenswürdiger Administrator ernannt wird, welcher nachträgliche Änderungen vornehmen kann. Gerade bei der Verwendung der Blockchain-Technologie durch öffentliche Organe dürften diese die entsprechende Rolle wohl einnehmen können. Ist die nachträgliche Bearbeitung allerdings im jeweiligen Anwendungsfall technisch nicht möglich oder vorgesehen, so kann ein Blockchain-System nach dem heutigen Stand der Technik und des Wissens nicht datenschutzkonform ausgestaltet werden. 701

C. Anwendungsbereiche

Wie weiter oben dargestellt, gibt es auch für die öffentliche Verwaltung eine Vielzahl an möglichen Anwendungsfeldern für Distributed-Ledger-Technologien. Bei diesen können sich wiederum spezifische Probleme in rechtlicher oder tatsächlicher Hinsicht ergeben, welche im Folgenden betrachtet werden sollen. 702

1. Registerführung

Distributed-Ledger-Technologien decken bereits aufgrund ihrer technologischen Bauweise wichtige Attribute wie Integrität oder Nachvollziehbarkeit besser ab als etwa Datenbanken und werden darum oftmals als neue 703

1627 SCHREY/THALHOFER, NJW, 2017, S. 1435.

Möglichkeit der Registerführung betrachtet.[1628] Hinsichtlich der Eignung der Blockchain-Technologie zur Registerführung sind allerdings einige gewichtige Einschränkungen zu beachten. Gewisse Register wie das Handelsregister (vgl. Art. 933 OR) oder das Grundbuch (vgl. Art. 973 ff. ZGB) erfüllen durch ihre Publizität wichtige Funktionen hinsichtlich des Gutglaubensschutzes. Aus diesem Grund sind an die Gewährleistung ihrer Richtigkeit hohe Anforderungen zu stellen, und der Staat muss in dieser Konstellation eine Überwachungs- und Gewährleistungsfunktion wahrnehmen.[1629] Da Blockchains technisch so ausgestaltet werden können, dass staatliche Stellen als Verantwortliche definiert werden und als einzige Änderungen vornehmen können (im Rahmen einer «permissioned Blockchain»), können sie diese Funktionen grundsätzlich erfüllen.[1630]

704 Es eignen sich jedoch nicht alle Register für eine Umstellung auf die Blockchain. Gerade Register wie das Grundbuch unterliegen einem steten Wandel, welcher sich mit der grundsätzlichen Unveränderbarkeit der Blockchain auf den ersten Blick nicht vereinbaren lässt. Zwar gibt es wie soeben beschrieben technische Möglichkeiten, eine Blockchain nachträglich zu verändern. Indes lassen sich insbesondere komplexe Register auf der Blockchain nur begrenzt abbilden. So muss etwa das Grundbuch sämtliche dinglichen Rechte, welche sich auf einem Grundstück befinden, abbilden können und nicht bloss eine Aneinanderreihung verschiedener Transaktionen auflisten, welche von den Benutzenden weitere Nachforschungen über den Bestand der jeweiligen dinglichen Verhältnisse erfordern.[1631] Generell würde eine Umstellung von Registern auf Blockchain aufgrund derart weitreichender Konsequenzen wohl auch verschiedene Gesetzesänderungen notwendig machen. Aufgrund des Umstands, dass das schweizerische Registerwesen gut funktioniert, wird daher auf Bundesebene bis anhin kein direkter Handlungsbedarf gesehen.[1632]

705 In verschiedenen Kantonen und Städten bestehen indes – wie weiter oben beschrieben – bereits einzelne Lösungen im Zusammenhang mit Registern, welche von deren Vorteilen Gebrauch machen. Bei diesen Lösungen werden allerdings nicht die Registerdaten auf der Blockchain eingetragen, sondern diese dient lediglich zur Verifikation der entsprechenden Daten (z.B. Ausweise) oder der Vereinfachung von Prozessen (z.B. Gründung von Unternehmen via «Smart Contract»).[1633]

1628 Bericht Zukunft, S. 148.

1629 Bericht Zukunft, S. 148 f.

1630 Siehe dazu oben Rz. 699.

1631 WILSCH, DNotZ, 2017, S. 762; SPICHIGER, Die Volkswirtschaft, 2019 S. 25.

1632 Bericht DLT, S. 84.

1633 SPICHIGER, Die Volkswirtschaft, 2019, S. 25.

2. Smart Contracts

Denkbar ist die Ausgestaltung verwaltungsrechtlicher Vertrags- oder Auszahlungsverhältnisse als «Smart Contract». So könnte etwa die Auszahlung staatlicher Beträge (z.B. Subventionen) aufgrund eines entsprechend programmierten «Smart Contract» nur erfolgen, wenn durch den Antragssteller spezifische Unterlagen eingereicht und diese durch einen Algorithmus überprüft werden, der sodann die Zahlung freigeben kann. Somit würde eine derartige Entscheidung automatisiert und ohne menschlichen Einfluss gefällt.[1634] Hierbei stellen sich weitere datenschutzrechtliche Fragen. Art. 22 DSGVO und de lege ferenda auch Art. 19 DSG sehen vor, dass in solchen Fällen grundsätzlich das Recht auf eine Überprüfung der automatisierten Entscheidung durch einen Menschen bestehen muss (sog. «menschliches Gehör»).[1635] Ein entsprechendes Überprüfungsrecht scheitert unter Umständen bereits an der Abwesenheit eines zentralen Verantwortlichen. Auch wenn dieser vorhanden ist, ergeben sich Probleme mit der Unabänderlichkeit und der vermuteten Richtigkeit der Daten als Grundprinzipien der Blockchain-Technologie.[1636] Aufgrund der grundsätzlichen Unabänderlichkeit von «Smart Contracts» stellen sich zudem auch privatrechtliche Fragen, etwa betreffend den Umgang mit der nachträglichen Änderung der Verhältnisse oder der Rückabwicklung. Darauf soll indes im vorliegenden Kontext nicht vertieft eingegangen werden.[1637] Aufgrund dieser Einschränkungen eignen sich wohl nach dem jetzigen Stand der Technik «Smart Contracts» noch nicht für einen gross angelegten Einsatz im Bereich der öffentlichen Verwaltung. Wo dieser dennoch erfolgt, ist das Recht auf menschliches Gehör zu beachten und sind Mechanismen für die Anpassung an geänderte Verhältnisse und zur Streitbeilegung vorzusehen.[1638] 706

3. Blockchain als Chance für den Datenschutz

Die bisherigen Ausführungen haben gezeigt, dass es aus datenschutzrechtlicher Warte durchaus Vorbehalte gegenüber dem Einsatz von Blockchain geben kann. Es ist jedoch zu beachten, dass je nach technischer Ausgestaltung die Blockchain trotz oder gerade wegen ihrer grundsätzlichen Transparenz auch eine Chance für den Datenschutz und dessen wirksame Durchsetzung 707

1634 Vgl.n EGGEN, AJP, 2017, S. 6; MEYER/SCHUPPLI, recht, 2017, S. 207 f.

1635 Vgl. dazu weiter oben Rz. 628 ff.

1636 Vgl. zum Ganzen: ISLER, Jusletter, 4. Dezember 2017, N. 41 ff.

1637 Vgl. etwa Bericht DLT, S. 84.

1638 WEBER, Jusletter, 4. Dezember 2017, N. 37 ff.

bedeuten kann.[1639] Gewisse Datenschutz-Prinzipien können durch den Einsatz von auf Blockchain basierten Systemen auf den ersten Blick gut umgesetzt werden, wie etwa das Transparenzprinzip, da zumindest auf öffentlichen Blockchains die Bearbeitungen öffentlich einsehbar sind.[1640] Auch das Prinzip der Datenintegrität kann dadurch gewährleistet werden, dass aufgrund der verteilten Struktur eine bessere Risikoverteilung und eine kleinere Abhängigkeit von Einzelkomponenten besteht.[1641] Verschiedene Autoren sehen auch das Potenzial, dass die Blockchain je nach Ausgestaltung den in Art. 25 DSGVO und de lege ferenda in Art. 6 E-DSG verankerten Grundsatz des Datenschutzes durch Technik (Privacy by Design) erfüllen kann.[1642] Dabei geht es in erster Linie darum, dass die Verantwortlichen durch geeignete technische Massnahmen die Datenschutzgrundsätze wirksam umsetzen können.[1643] Zu verweisen ist hier auf verschiedene Ansätze, die auf eine datensparsame Entwicklung der Technologie hinzielen.[1644] Angedacht ist etwa ein auf Blockchain basierter Ansatz eines Identitätsmanagements, bei dem der Nutzer seine Identitätsdaten auf der Blockchain speichert und selber entscheiden kann, welchen Dritten er Zugang gewährt.[1645]

D. Fazit

708 Es bestehen zahlreiche Einsatzmöglichkeiten für die Blockchain- oder «Distributed Ledger»-Technologie in der öffentlichen Verwaltung. Dabei stellen sich in erster Linie datenschutzrechtliche Fragen, welche unter Umständen auch eine gesetzliche Regelung notwendig machen. Auch wenn Daten auf der Blockchain unter Umständen verschlüsselt gespeichert werden, kann es sich dabei um Personendaten handeln, wenn eine Re-Identifizierung möglich ist. Gerade bei einer Verwendung durch öffentliche Stellen ist es unter Umständen notwendig, dass diese die teilnehmenden Personen identifizieren können. Insbesondere bei öffentlichen Blockchain-Systemen stellen sich aufgrund des dezentralen und grundsätzlich unveränderbaren Wesens der Technologie zudem Fragen nach der Verantwortlichkeit sowie der Durchsetzung der

1639 GUGGENBERGER, ZD, 2017, S. 49 f.

1640 STENGEL/AU, sic!, 2018; RAINER BÖHME / PAULINA PESCH, DuD, 2017, S. 480.

1641 ISLER, Jusletter, 4. Dezember 2017, N. 48 ff.; RAINER BÖHME / PAULINA PESCH, DuD, 2017, S. 473.

1642 GUGGENBERGER, ZD, 2017, S. 49; BECHTOLF/VOGT, ZD, 2018, S. 71.

1643 BECHTOLF/VOGT, ZD, 2018, S. 71.

1644 GUGGENBERGER, ZD, 2017, S. 50 f.; RAINER BÖHME / PAULINA PESCH, DuD, 2017, S. 473 ff

1645 ZYSKIND/NATHAN/PENTLAND, IEEE security and privacy workshops, 2015, S. 2 ff. Zum Konzept der «Self Sovereign Identity» vgl. etwa STENGEL/AU, sic!, 2018, S. 443; ZANOL/CZADILEK/LEBLOCH, Jusletter IT, 22. Februar 2018.

Betroffenenrechte. Es existieren indes technische Möglichkeiten, welche eine datenschutzkonforme Ausgestaltung zulassen, auch wenn auf diese Weise einige der Spezifika und Vorteile der Blockchain-Technologie wieder verloren zu gehen drohen. Die entsprechenden Fragen sind je nach Ausgestaltung der Blockchain unterschiedlich zu beantworten, so dass eine konkrete Einschätzung nur im jeweiligen Einzelfall vorgenommen werden kann. Zu beachten bleibt, dass die Blockchain je nach Ausgestaltung durchaus auch wesentliche Vorteile für den Datenschutz bringen kann.

IV. Zusammenfassung

Die Blockchain und Anwendungen der «Distributed Ledger»-Technologie sind bisher in der Verwaltung noch nicht stark präsent. Da indes interessante Einsatzmöglichkeiten bestehen, stellen sich Fragen insbesondere datenschutzrechtlicher Natur, sofern im Rahmen der jeweiligen Lösungen Daten bearbeitet werden, welche eine Person bestimmbar machen. Dies ist trotz der Verschlüsselung von Daten auf der Blockchain vor allem auch beim Einsatz durch die öffentliche Verwaltung, welche die Beteiligten unter Umständen identifizieren können muss, durchaus denkbar. Sofern die Datenschutzgesetzgebung anwendbar ist, stellen sich gerade bei öffentlichen Blockchain-Systemen Fragen nach der Verantwortlichkeit und dazu, inwiefern eine Gewährung der datenschutzrechtlichen Betroffenenrechte möglich bleibt. Problematisch kann aufgrund des dezentralen Wesens der Blockchain und der Schwierigkeit der Zuordnung eines Verantwortlichen etwa die Gewährung der Betroffenenrechte werden. Das Recht auf Berichtigung oder Löschung von Daten steht zudem im Konflikt mit der Unveränderbarkeit der Blockchain. Indes existieren technologische Möglichkeiten, um die Einträge zu verändern, welche jedoch teilweise die charakteristischen Vorteile der Blockchain wieder abschwächen, da z.B. ein zentraler Verantwortlicher notwendig wird. Je nach Ausgestaltung des Systems kann jedoch auch dies datenschutzkonform bewerkstelligt werden oder gar datenschutzrechtliche Vorteile gegenüber herkömmlichen Systemen bringen, so dass eine konkrete Einschätzung zur Rechtsmässigkeit des jeweiligen Einsatzes der Blockchain oder der «Distributed Ledger»-Technologie im Einzelfall vorzunehmen ist. 709

Teil 4: Zusammenfassung der Ergebnisse und Würdigung

§12 Zusammenfassung der Ergebnisse

• *Erster Teil*

Der erste Teil der Arbeit diente dazu, für die Untersuchung relevante Begriffe 710
zu definieren und technisch zu erklären. Zudem wurde der Rechtsrahmen, in welchem sich das Thema der Arbeit bewegt, grob skizziert. Dabei sind einerseits internationale Rechtsquellen zu beachten. Neben grundrechtlichen Ansprüchen existieren indes aufgrund der Neuheit des Themas und des oftmals fehlenden Konsenses in der Staatengemeinschaft nur wenig verbindliche internationale Regeln. Hervorzuheben ist indes, dass es in verschiedenen Teilbereichen supranationale Anstrengungen gibt, wobei insbesondere der Bereich des Datenschutzes hervorzuheben ist. Auf nationaler Ebene gilt es zu beachten, dass der Bund keine generelle Kompetenz zur Regelung der Digitalisierung des Verwaltungsverfahrens hat und somit keine entsprechende Querschnittgesetzgebung erlassen kann. Daher sind im Untersuchungsgegenstand auch kantonale und interkantonale Regelungen von Relevanz.

• *Zweiter Teil*

Im zweiten Teil wurde untersucht, inwiefern die geltenden Rechtsgrundla- 711
gen einen geeigneten Rahmen für die Digitalisierung des Verwaltungshandelns darstellen und in welchen Bereichen allenfalls Bedarf nach zusätzlichen Regelungen besteht. Die Untersuchung unterschiedet dabei zwischen dem rechtlichen Verwaltungshandeln (innerhalb von Verfahren) und dem tatsächlichen Verwaltungshandeln (insbesondere Information und Kommunikationshandeln).

Im Bereich des tatsächlichen Verwaltungshandelns kann der Staat auf- 712
grund der weitgefassten Gesetzesgrundlagen seine Informations- und Kommunikationspflicht auch über Internet oder gar soziale Medien erfüllen. Solange es sich dabei nur um einen zusätzlichen Kanal handelt, stellt dies auch gegenüber Gruppen, welche etwa die entsprechenden Mittel nicht bedienen oder verstehen können, keine Diskriminierung dar. Die Bekanntgabe von

Personendaten über Internet bringt zusätzliche Gefahren mit sich. Diesen wird im Rahmen des Datenschutzgesetzes wirkungsvoll dadurch begegnet, dass entsprechende Veröffentlichungen nur zulässig sind, solange und sofern daran ein überwiegendes öffentliches Interesse besteht. Rechtsunsicherheit besteht dagegen bei der Erhebung von Personendaten im Rahmen der Behördeninformation, etwa über Tracker auf Websites. Diese Programme erfassen IP-Adressen, aus welchen sich unter Umständen auch die Person dahinter bestimmen lässt. Wenn dies der Fall ist, so wird eine gesetzliche Grundlage benötigt, welche aktuell ebenfalls umstritten ist. Auch Social-Media-Plattformen wie Facebook bieten Dienste an, in denen sie Personendaten für ihre Verwender aufbereiten. Nach der geltenden Rechtsprechung ist davon auszugehen, dass das öffentliche Organ für diese Bearbeitungen eine Mitverantwortung trägt. Auf sozialen Medien stellt sich zudem das Problem, dass Personen blockiert und ihre Beiträge gelöscht werden können, was einen Eingriff in die Meinungsfreiheit darstellt. Während gewisse Beiträge, etwa aufgrund der offensichtlichen Erfüllung von Straftatbeständen, gelöscht werden dürfen, fehlt bei anderen (z.B. Fake News) eine entsprechende gesetzliche Grundlage zur Löschung. Weitergehende Löschungen sind daher den privaten Plattformbetreibern zu überlassen.

713 Der Rechtsschutz gegenüber behördlichen Informationshandlungen ist grundsätzlich auch dann sichergestellt, wenn diese im Internet stattfinden. Es bestehen allerdings aktuell noch offene Fragen zur Haftung für staatliche Internetinhalte, insbesondere betreffend den Vertrauensschutz hinsichtlich der im Internet durch eine Behörde getätigten Aussagen. Behörden haben dabei nach der hier vertretenen Auffassung zu beachten, dass ihre Aussagen im Internet bezüglich Konkretheit und Verbindlichkeit durchaus Vertrauen bilden können. Auf der Website verborgene Haftungsausschlüsse (Disclaimer) dürften hier kaum ausreichen, um eine aus fehlerhaften Informationen resultierende Haftung auszuschliessen.

714 Hinsichtlich des rechtlichen Verwaltungshandelns gilt es zu beachten, dass auf Bundesebene und in zahlreichen Kantonen Rechtsgrundlagen für den elektronischen Rechtsverkehr geschaffen wurden und es somit möglich und zulässig ist, Verfahrenshandlungen online vorzunehmen. Richtigerweise ist beim elektronischen Rechtsverkehr ein Nachweis über die Identität der Parteien zu erbringen, wobei dies mittels elektronischer Unterschrift oder auf andere Weise geschehen kann. In dieser Hinsicht besteht gerade im Bereich des Verwaltungsverfahrens eine erhebliche Rechtszersplitterung, da je nach Bereich und Gemeinwesen der elektronische Rechtsverkehr noch nicht zugelassen wird. Auch bei der Bearbeitung des Sachverhalts bestehen neue Möglichkeiten, indem etwa Internetquellen oder Erkenntnisse aus sozialen

Medien beigezogen werden können. Insbesondere die Recherche auf sozialen Medien ist dabei entgegen der Rechtsprechung des Bundesgerichts aus Gründen des Privatsphärenschutzes und der informationellen Selbstbestimmung als kritisch zu betrachten. Zudem ist zu beachten, dass nicht alles, was im Internet steht, korrekt sein muss. Daher ist es umso wichtiger, dass den Betroffenen hinsichtlich von Erkenntnissen aus Internetquellen, welche die Behörden einer Entscheidung zugrunde legen, das rechtliche Gehör gewährt werden muss.

Technologischer Fortschritt kann auch für neue Mitwirkungspflichten 715
oder für verstärkten Datenverkehr unter den Behörden sorgen. Sofern hier neue Pflichten geschaffen werden, ist insbesondere der Verhältnismässigkeit ein besonderes Gewicht beizumessen. Auch die informationelle Selbstbestimmung und das Datenschutzrecht nehmen bei der Begrenzung entsprechender Vorhaben eine wichtige Rolle ein.

In Verwaltungsverfahren werden Algorithmen als Entscheidungshilfen 716
eingesetzt. Dieser Verwendung steht die Rechtsordnung grundsätzlich nicht entgegen, zumal gewisse Einsatzbereiche (etwa komplexe Berechnungen oder die Durchsuchung von grossen Datenmengen) nicht per se mit grösseren Risiken für die Betroffenen verbunden sind. Je komplexer jedoch die zugrundeliegenden Regeln werden, desto problematischer kann der Einsatz sein. Hier stösst etwa das Datenschutzrecht an seine Grenzen, zumal weder im aktuellen noch im revidierten Datenschutzrecht eine explizite Regelung von Algorithmen als Entscheidungshilfe stattfindet, womit es den Betroffenen erschwert wird, ihre Rechte durchsetzen zu können. Ein erster Schritt wäre es hier, den Anwendungsbereich von Art. 19 E-DSG, welcher eine Informationspflicht für automatisierte Entscheidungen enthält, entsprechend zu ergänzen. Weitere in der Rechtsordnung vorgesehene Korrektive, wie das rechtliche Gehör und der Diskriminierungsschutz, können beim Einsatz von Algorithmen ebenfalls relevant sein. Sie finden ihre Grenzen insbesondere bei komplexen Entscheiden, welche für die Betroffenen und allenfalls gar die Behörde selber nicht mehr im Detail nachvollziehbar sind. Daher ist der Einsatz entsprechender Systeme durch die öffentliche Verwaltung gerade in sensiblen Bereichen kritisch zu betrachten.

- *Dritter Teil*

Der dritte Teil befasst sich mit aktuell absehbaren Entwicklungen im Bereich 717
der Digitalisierung des Verwaltungshandelns und deren verfassungsmässigem Kontext. Da festgestellt wurde, dass der elektronische Rechtsverkehr aus verschiedenen Gründen in der Schweiz nicht so verbreitet ist wie in anderen Ländern, bestehen verschiedene Vorhaben, um diesen weiter zu fördern. Diese

Herangehensweisen bringen indes jeweils eigene rechtliche Probleme mit sich. Zentrale Behördenportale können etwa dazu dienen, Behördendienstleistungen einfacher erreichbar zu machen. Aus rechtlicher Sicht kritisch zu betrachten ist, dass dadurch zumindest in der erzeugten Wahrnehmung Kompetenzen verwischt werden können. Digitale Identitäten sollen die elektronische Identifizierung auch im Behördenverkehr erleichtern. Der Gesetzgeber hat sich dabei entschieden, dass privaten Betreibern die Entwicklung entsprechender Lösungen überlassen wird, während der Staat lediglich die Identifizierung der Personen übernimmt. Diese Herangehensweise wurde aufgrund der Meinung, dass es sich bei der Ausstellung digitaler Identitäten um eine Staatsaufgabe handeln müsse, und damit verbundenen datenschutzrechtlichen Bedenken zumindest teilweise berechtigt kritisiert. Auch aufgrund der starken Kritik ist es fraglich, ob die entsprechende Lösung sich durchsetzen wird, zumal neben der Nutzungsmöglichkeit und -sicherheit auch das Vertrauen der Bevölkerung für den Erfolg von digitalen Identitäten relevant ist. Ein umfassender Nutzungszwang für den elektronischen Rechtsverkehr könnte zudem gegen das Diskriminierungsverbot verstossen, da gewisse Gruppen vom Rechtssystem ausgeschlossen würden. Für die Betroffenen wären diesfalls Übergangsregelungen und Ausweichmöglichkeiten vorzusehen.

718 Das tatsächliche Verwaltungshandeln kann durch die Digitalisierung etwa dadurch weiter verändert werden, dass Informations- und Kommunikationshandlungen künftig ausschliesslich über das Internet erfolgen sollen. Hierbei ist im Sinne des Diskriminierungsverbots aufzupassen, dass sensible Gruppen (ältere Menschen, Menschen mit Behinderung) nicht ausgeschlossen werden. Gerade wichtige Informationen oder Informationen, die mit der Ausübung von Rechten verbunden sind, müssen für alle zugänglich sein. Es ist indes denkbar, dass Informationen bereichsspezifisch grundsätzlich nur noch online abrufbar sind, sofern hinsichtlich der Ausübung von Rechten keine Schlechterstellung stattfindet. Auch in diesem Fall sind aufgrund des Diskriminierungsverbots Übergangsregeln oder Ausnahmebestimmungen vorzusehen. Ein ungelöstes Problem stellt der staatliche Ausschluss von Social-Media-Nutzenden dar. Die in anderen Ländern vorgesehenen gesetzlichen Grundlagen überzeugen kaum, insbesondere unter dem Aspekt der Meinungsfreiheit.

719 Weiter wurde die Möglichkeit betrachtet, dass «Maschinen» eigenständig vollautomatisierte Entscheide fällen können. Zu beachten ist, dass aktuell wohl nur Entscheide ohne Ermessensspielraum für eine vollständige Automatisierung geeignet sind. Da entsprechende Entscheide für die Betroffenen Rechte und Pflichten begründen können, ohne dass ein Mensch dies überprüft, werden gewisse zusätzliche Schutzvorkehrungen notwendig. Das E-DSG

sieht hier insbesondere gewisse Informationspflichten, Einsichtsrechte und einen Anspruch auf menschliches Gehör vor. Indes stossen auch diese neuen Möglichkeiten bei komplexen Entscheiden, etwa hinsichtlich der Nachvollziehbarkeit, an ihre Grenzen. Gerade im Bereich von selbstlernenden Algorithmen sollten daher zusätzliche Korrektivmethoden geprüft werden (etwa die Einrichtung einer Kontrollstelle für Algorithmen).

Schliesslich wurde die Blockchain-Technologie betrachtet, welche in der 720
öffentlichen Verwaltung verschiedene Anwendungsmöglichkeiten findet, aber aktuell noch kaum rechtlich geregelt ist. Rechtliche Vorbehalte, welche gegen einen Einsatz sprechen, sind hier je nach Ausgestaltung der entsprechenden Lösungen vor allem im Datenschutz zu finden. Diskutiert werden muss dabei bereits, ob es sich bei den oft verschlüsselten Daten um Personendaten handelt. Gerade in staatlichen Einsatzbereichen (z.B. Registerlösungen) müssen die betroffenen Personen für den Staat unter Umständen bestimmbar bleiben. Sofern das Datenschutzrecht anwendbar ist, bringt dies Probleme hinsichtlich der Gewährung der Betroffenenrechte einerseits aufgrund der Zuständigkeit und anderseits aufgrund der grundsätzlichen Unveränderbarkeit der Blockchain mit sich. Indes existieren durchaus technische Möglichkeiten, um eine Blockchain auch in diesem Sinne datenschutzkonform auszugestalten.

§13 Würdigung

Zusammenfassend gilt es festzuhalten, dass die Rechtsordnung sich in vie- 721
lerlei Hinsicht mit den Themen und Risiken der Digitalisierung auseinandergesetzt hat. So sehen etwa das Datenschutzrecht und die Verfahrensgesetze gewisse Regelungen vor, welche sich mit wichtigen Aspekten der Digitalisierung befassen. Die Grundrechte spielen auch im digitalen Raum eine überaus wichtige begrenzende Rolle. Es ist jedoch festzustellen, dass der Gesetzgeber nicht auf alle Probleme, welche sich im Zusammenhang mit der Digitalisierung der Verwaltung stellen, bereits eine zufriedenstellende Lösung gefunden hat. Während in gewissen Einsatzbereichen das Für und Wider der Benutzung abgewogen wurde, ehe der Einsatz reglementiert und erlaubt wurde, werden in anderen Bereichen die Vorzüge des Internets und der Informationstechnologien scheinbar ohne grosse vorgängige Diskussion oder rechtliche Auseinandersetzung genutzt. Zu denken ist hier etwa an die Recherche via soziale Medien.

Zu diversen (durchaus gewichtigen) Fragestellungen liefert das Schweizer 722
Recht im jetzigen Zeitpunkt noch keine befriedigende Antwort. Im Folgenden

sollen daher die meines Erachtens dringlichsten unbeantworteten Fragestellungen aufgezeigt werden, und es soll vorgeschlagen werden, wie diese beantwortet werden können. Zu beachten ist, dass der schnelle technologische Wandel und das gerade in dieser Thematik evidente Hinterherhinken des Rechts dafür sorgen, dass eine rein rechtliche Lösung nicht immer die beste bzw. effektivste Variante darstellt. Daher sollen auch andere, allenfalls zielführendere Herangehensweisen (etwa technischer Natur) präsentiert werden.

723 1. Kritisch zu beachten ist die sorglose Verwendung von Daten aus sozialen Medien in Verfahren ohne genügende gesetzliche Grundlage. Um Rechtssicherheit zu schaffen, ist hier analog zur Observation eine Gesetzesgrundlage zu schaffen, welche wichtige Punkte zum Umgang mit diesen Daten regelt. Sofern der Gesetzgeber hierzu keine Notwendigkeit sieht, sind immerhin die Verwaltungsbehörden zwingend gefordert, den Betroffenen das rechtliche Gehör hinsichtlich der getroffenen Feststellungen zu gewähren.

724 2. Beim Einsatz von Trackingtools auf Websites kann Art. 45c FMG als gesetzliche Grundlage beigezogen werden, welcher indes die Einwilligung des Betroffenen verlangt. Die Verwaltung hat sich in erster Linie die Frage zu stellen, inwiefern das Tracking zur Erfüllung ihrer Aufgaben wirklich notwendig ist. Kommt man zum Schluss, dass dies der Fall ist, sind entsprechende Lösungen technisch möglichst datenschutzfreundlich auszugestalten (Kürzung der IP-Adressen, Verzicht auf Bearbeitung durch Dritte).

725 3. Für entsprechende Trackingtools, welche Social-Media-Anbieter auf ihren Plattformen unabdingbar einsetzen, wird es kaum möglich sein, eine gesetzliche Grundlage zu schaffen. Daher ist vorderhand auf deren Nutzung zu verzichten oder auf die Anbieter dahingehend einzuwirken, dass eine entsprechende Nutzung fakultativ wird.

726 4. Wollen staatliche Stellen Private von der Nutzung ihrer Social-Media-Präsenz ausschliessen, besteht nur in gewissen Fällen eine gesetzliche Grundlage dafür (z.B. bei strafrechtlich relevanten Kommentaren). Die Löschung gewisser unerwünschter Wortmeldungen (etwa «Fake News») wird von den entsprechenden Regelungen indes nicht erfasst und ist daher bis zur Schaffung einer gesetzlichen Grundlage durch den Staat zu unterlassen und Privaten vorzubehalten. Dabei ist die Schaffung einer gesetzlichen Regelung, welche die Meinungsfreiheit vollständig respektiert, mit erheblichen Schwierigkeiten verbunden. Daher ist es wohl zielführender, Löschungen und Sperrungen von Nutzern in erster Linie den Plattformbetreibern zu überlassen und gleichzeitig auf deren Transparenz hinzuwirken.

5. Beim Einsatz von Algorithmen als Entscheidungshilfen ist als heikel zu beurteilen, wenn die Betroffenen unter Umständen nicht wissen, dass ihre Daten durch eine Maschine beurteilt wurden. Hier würde es helfen, die in Art. 19 E-DSG vorhandene Informationspflicht auch auf den Einsatz von Algorithmen als Entscheidungshilfe auszudehnen. Aus technischer Sicht ist wichtig, dass insbesondere bei komplexen Entscheidungen die Nachvollziehbarkeit für Behörde und Betroffene gewahrt bleibt. Aufgrund von Diskriminierungsrisiken sind entsprechende Programme durch die Verwaltung in sensitiven Bereichen vorderhand zurückhaltend einzusetzen. 727
6. Bei automatisierten Einzelfallentscheidungen stossen die bisherigen Instrumente noch in vermehrtem Masse an ihre Grenzen. Neben dem soeben Ausgeführten ist deren Einsatz daher in erster Linie auf Entscheide zu begrenzen, bei welchen der Behörde kein Ermessensspielraum bleibt. Bei komplexen selbstlernenden Algorithmen ist zudem ernsthaft über weitere Kontrollmechanismen (z.B. im Sinne einer Algorithmen-Kontrollstelle) nachzudenken. 728
7. Blockchain-Anwendungen lassen sich in vielen Ausgestaltungen nicht mit dem geltenden Datenschutzrecht vereinen. Indes bestehen nach dem Ausgeführten technische Möglichkeiten zur datenschutzkonformen Ausgestaltung dieser Technologie, welche daher beachtet und unbedingt bevorzugt werden sollen. 729
8. Überall dort, wo eine Behördendienstleistung ausschliesslich online erbracht werden soll, ist auch an diejenigen zu denken, welche diese Kanäle nicht (oder nicht mehr) bedienen oder verstehen können. Den Betroffenen kann etwa mittels Übergangsregelungen oder Ausweichmöglichkeiten eine Lösung angeboten werden. 730

Über diese Fragestellungen hinaus bleiben bei jedem Umgang mit kommenden technologischen Neuerungen selbstverständlich die Grundprinzipien der Verfassung zu beachten. Insbesondere sind entsprechende Regelungen verhältnismässig auszugestalten. Da inskünftig noch in vermehrtem Masse die staatliche Aufgabenerfüllung mit der Bearbeitung von Personendaten einhergehen wird, spielt die Einhaltung des Datenschutzes und seiner Grundsätze eine wichtige Rolle, wobei gerade auch Aspekten wie der Datensicherheit verstärktes Gewicht zukommt. Auch in einer zunehmend digitalisierten Welt ist es wichtig, dass der Bürger ein gewisses Grundvertrauen in den Staat haben und erhalten kann. 731

Trotz all dieser Vorbehalte bleibt es wichtig, dass sich die Verwaltung mit offenem Visier den Herausforderungen der Digitalisierung stellt, um einen 732

für alle Seiten nutzenstiftenden Einsatz digitaler Technologien im Verwaltungshandeln zu ermöglichen. Denn, um mit dem einleitenden Sprichwort zu schliessen, es ist nichts so beständig wie der Wandel. Allerdings können wir selber bestimmen, wie wir diesem Wandel gegenübertreten, getreu dem chinesischen Sprichwort:

«Wenn der Wind der Veränderung weht, bauen die einen Mauern und die anderen Windmühlen.» Iditatur, et es del iderfernam faceprest, sum numque con pra di dictoriatem cus moluptatio. Ut vellit, sume sunt la vellic to tem eum, totatem inctest, te velecte remoloreped quaest omnim eum in reperum re, is consecturem. Ut volo mollaboribus dolupis maximusa ea ium harupta dolupta tiisque nimagnim rero dolorro testia andit occus evelibus et omnist hiciusam, omnisquam ad most, volorent latum dessi delit, utem quiae. Is maio elique premporiam incta intur, odis ad que et occaepratur, utectem dis ut as eum laborerchit velibusci ullaccus, unt porroribus, ides modistrum aruntium quamus recae. Ita dolupti busdand andelitas venit, ut amus enis que nonsequi cupic te pratest, nonse que cus.
Vidi occus sitio incto et vitatum sit, qui recti ut aut que dolorem voluptatur am quod molupta dendic tem vel modi te perchit accum voluptatusam nis et odi officipsam iuscidus anitatur aut fugia perrovit, ipsuntis sae. Et aut ommosto bla et que nam fuga. Faceatiiscia enimusant arias quam explab ide nis et unde dolupta tiunt, omnim inum unturitia conet apiene moluptasped que simusam, volut maxim nonsed utem ut endenimin provitis experescia consenectum, con reperferum rehenis dem et plibus am harum aut lant quo voluptas aria aute nimaxim usapersperum quasperferia nos ratempo rrovit, ut pore, sitio dolore esciet laborio explias dolupta ectati te nulliquibea qui vendes et occabora que provid quam comnis sed evelescient excepe odit, num iliqui quo quiberum nonem ex et volendae pari verum fugiatem et untur? Quiatem ea sundebis dis veni is magnis repe sus eos doluptati si ilianditia dolorro blabore volendipsus eicium faceaqu isquos exeris et fugiatius nonecum, nonsequo omnis et apictor estiasitis doluptur, volessin cumquassimi, voluptat voluptiorum et dolupit minciendae quam vent molorum rerio volut andam eatibus volorio. Itatect ureperuptio es remoluptaque cum abo. Borestis exceri optiis minciam vent. Dandus voluptatur sequia sania illest aut esequassus et volorep tatur? Qui coneste plitiissum voluptatus et facearu nditatis doluptati te quam velic tota nonsequo quatem la de dolor apit ut quibus mossime exeratur alitium unt. Idemporiatur assequa menimagnis aut eum dolenis eum ipicae qui blam laccum restia dolore comnis sit ut vel mollupt aecabo. Eptatquam, autemperio erum illupta ssequod ignatqui tempedis magnim nat est que volecepra et elluptur sunt doluptiissit es exeratiosam quam dolupta doluptate nis vel ipsum co-

Über den Autor:
Roger Plattner studierte Rechtswissenschaft an den Universitäten Basel und Neuchâtel. An der Universität Zürich arbeitete er im Team der SNF-Förderungsprofessur Altwicker.

Die Rechtswissenschaftliche Fakultät der Universität Zürich hat vorliegende Arbeit am 30. September 2020 auf Antrag von Prof. Dr. Tilmann Altwicker und Prof. Dr. Andreas Glaser als Dissertation angenommen und mit dem Prädikat *magna cum laude* versehen.

sui generis ist ein Verein, der sich der Förderung des freien Zugangs zu juristischer Literatur, Gerichtsurteilen, Behördenentscheidungen und Gesetzesmaterialien verschrieben hat. Unter dem Label *sui generis* erscheint seit 2014 eine juristische Open-Access-Fachzeitschrift. 2019 erfolgte die Gründung des *sui generis* Verlags.

sui generis Buchreihe
herausgegeben von Daniel Hürlimann und Marc Thommen

In dieser Reihe werden juristische Dissertationen und Habilitationen sowie Lehrbücher und Fachpublikationen einem breiten Publikum zugänglich gemacht. Die Bücher dieser Reihe erscheinen als gedruckte Werke und online. Die digitale Version ist weltweit kostenlos zugänglich (Open Access). Die Urheberrechte verbleiben bei den AutorInnen; die Werke werden unter einer Creative-Commons-Lizenz veröffentlicht.

Bisher in der *sui generis* Reihe erschienen:
001 – Monika Simmler: Normstabilisierung und Schuldvorwurf
002 – Marc Thommen: Introduction to Swiss Law
003 – Silvio Hänsenberger: Die zivilrechtliche Haftung für autonome Drohnen unter Einbezug von Zulassungs- und Betriebsvorschriften
004 – Mais A.M. Qandeel: Enforcing Human Rights of Palestinians in the Occupied Territory
005 – Moritz Oehen: Der Strafkläger im Strafbefehls- und im abgekürzten Verfahren
006 – Jens Lehne: Crisis at the WTO: Is the Blocking of Appointments to the WTO Appellate Body by the United States Legally Justified?
007 – Lorenz Garland: Waffengleichheit im Vorverfahren
008 – Christoph Urwyler: Die Praxis der bedingten Entlassung aus dem Strafvollzug
009 – Dominik Elser: Die privatisierte Erfüllung staatlicher Aufgaben
010 – David Henseler: Datenschutz bei drohnengestützter Datenbearbeitung durch Private
011 – Lorenz Raess: Court Assistance in the Taking of Evidence in International Arbitration
012 – Christoph Hurni / Christian Josi / Lorenz Sieber: Das Verfahren vor dem Berner Kindes- und Erwachsenenschutzgericht
013 – Emanuel Bittel: Die Rechnungsstellung im schweizerischen Obligationenrecht

014 – Stephan Bernard: Was ist Strafverteidigung?
015 – Frédéric Erard: Le secret médical
016 – Valentin Botteron: Le contrôle des concentrations d'entreprises
017 – Monika Pfyffer von Altishofen: Ablehnungs- und Umsetzungsraten von Organtransplantationen
018 – Kristin Hoffmann: Kooperative Raumplanung: Handlungsformen und Verfahren
019 – APARIUZ XXII: Unter Gleichen
020 – Raphaël Marlétaz: L'harmonisation des lois cantonales d'aide sociale
021 – Roger Plattner: Digitales Verwaltungshandeln
022 – Nicole Roth: Miteigentum an Grundstücken und einfache Gesellschaft

Dieses Werk ist erschienen in der Reihe sui generis, herausgegeben von Daniel Hürlimann und Marc Thommen.

1. Auflage 30. August 2021

Abdruck der von der Rechtswissenschaflichen Fakultät der Universität Zürich genehmigten Dissertation.

Die Druckvorstufe dieser Publikation wurde vom Schweizerischen Nationalfonds zur Förderung der wissenschaftlichen Forschung unterstützt.

ISBN: 978-3-907297-21-6
DOI: 10.38107/021
Korrektorat: Christoph Meyer
Gestaltung: Müller+Hess, Basel
Druck: Ebner & Spiegel, Ulm

www.suigeneris-verlag.ch

021

DIGITALES VERWALTUN

In einer Zeit, in der die meisten Aufgaben des Alltagslebens online erledigt werden können, werden auch an die öffentliche Verwaltung steigende Ansprüche bezüglich Erreichbarkeit, Verfügbarkeit und Vereinfachung ihrer Dienstleistungen gestellt. Daher wurden in den letzten Jahren unter dem Begriff des «E-Government» zahlreiche Verwaltungsdienstleistungen digitalisiert. Neben allen positiven Aspekten ist diese Digitalisierung auch mit Herausforderungen sowie Gefahren für die Rechtstellung Privater verbunden.

Die vorliegende Monographie soll einen Beitrag zur Beantwortung der Frage leisten, wie die mit der Digitalisierung einhergehenden Veränderungen im Bereich des Verwaltungshandelns rechtlich zu beurteilen sind. Dabei werden einerseits Technologien und Phänomene, welche im Handeln der öffentlichen Verwaltung bereits zum Einsatz gelangen, auf ihre Vereinbarkeit mit dem bestehenden Rechtsrahmen beleuchtet. Anderseits werden sich abzeichnende, künftigen Entwicklungen aufgezeigt und mit kritischem Blick auf mögliche rechtliche Probleme untersucht.

sui generis
ISBN 978-3-907297-21-6
DOI 10.38107/021