Dokument	**digma 2019 S. 206**
Autor	**Florent Thouvenin**
Titel	**Datenschutz auf der Intensivstation**
Seiten	**206-213**
Publikation	**Zeitschrift für Datenrecht und Informationssicherheit**
Herausgeber	**Bruno Baeriswyl, Beat Rudin, Bernhard M. Hämmerli, Rainer J. Schweizer, Günter Karjoth, David Vasella**
ISSN	**1424-9944**
Verlag	**Schulthess Juristische Medien AG**

Datenschutz auf der Intensivstation

Florent Thouvenin*, Prof. Dr. iur., Rechtsanwalt, ausserordentlicher Professor für Informations- und Kommunikationsrecht an der Universität Zürich, Vorsitzender des Leitungsausschusses des Center for Information Technology, Society, and Law (ITSL), und Direktor der Digital Society Initiative (DSI) der Universität Zürich, Zürich
florent.thouvenin@rwi.uzh.ch

Das Datenschutzrecht wurde und wird umfassend revidiert, es beruht aber noch immer auf Konzepten aus den 1960er- und 1970er-Jahren des letzten Jahrhunderts. Es erstaunt deshalb wenig, dass das geltende (und künftige) Recht nicht in der Lage ist, die heutigen Probleme überzeugend zu lösen. Dieser Beitrag legt den Finger auf die wunden Punkte und versucht, erste Schritte hin zu einem neuen Ansatz zu skizzieren. Er ist bewusst provokativ gehalten und hofft, eine (längst überfällige) Diskussion zu den Grundfragen des Datenschutzrechts anzuregen.

Die Arbeiten an der Datenschutzgrundverordnung der EU (DSGVO) und an der Konvention 108 des Europarats haben das Datenschutzrecht in Bewegung gesetzt, nicht nur in Europa, sondern auch in der Schweiz und zunehmend auf der ganzen Welt. Trotz einiger durchaus relevanter Neuerungen beruht das Datenschutzrecht nach europäischem Zuschnitt allerdings noch immer auf Konzepten aus den 60er- und 70er-Jahren des 20. Jahrhunderts. Der europäische Ansatz ist geprägt von der Idee der informationellen Selbstbestimmung und von der (impliziten) Überzeugung, dass die Bearbeitung von Personendaten grundsätzlich problematisch und deswegen umfassend zu regulieren ist. Dies hat zu einer Reihe von grundlegenden Problemen geführt, die sich mit der technischen Entwicklung der letzten Jahre noch

* Der vorliegende Beitrag ist die schriftliche Fassung eines Vortrags, den der Verfasser am 4. September 2019 am *24. Symposium on Privacy and Security* in Zürich gehalten hat. Die Vortragsform wurde weitgehend beibehalten, der Text wurde aber um einige Ausführungen und Nachweise in den Fussnoten ergänzt.

akzentuiert haben. Zu Recht wird deshalb zunehmend Fundamentalkritik laut[1]. Für immer mehr Experten wird immer deutlicher, dass der Ansatz des europäischen Datenschutzrechts mehr Probleme verursacht, als er zu lösen vermag.

Dieser Beitrag unternimmt den Versuch, die wichtigsten Probleme zu identifizieren, Gründe zu benennen und erste Schritte hin zu einem neuen Ansatz zu skizzieren. Er folgt dabei dem klassischen Dreischritt der Medizin von Befund, Diagnose und Therapie. Der Beitrag erhebt weder Anspruch auf Vollständigkeit noch auf langfristige Belastbarkeit. Er versteht sich vielmehr als bewusst provokativer Gedankenanstoss, der eine dringend erforderliche Diskussion über Aufgaben und Ausrichtung von Normen zum Schutz der Privatsphäre anregen will.

Natürlich hätte diese Diskussion geführt werden müssen, bevor der europäische Gesetzgeber mit der DSGVO Fakten geschaffen hat, an denen sich die Schweiz und viele andere Länder einstweilen orientieren müssen. Der Blick auf die wichtigsten Probleme des heutigen Datenschutzrechts macht aber deutlich, dass auch der europäische Gesetzgeber über kurz oder lang kaum darum herumkommen wird, die Büchse der Pandora wieder zu öffnen. Überzeugende gesetzliche Lösungen können dann nur geschaffen werden, wenn die konzeptionellen Grundlagen für einen neuen Ansatz gelegt worden sind. Mit dieser Arbeit sollten wir heute beginnen.

Befund 1: Rechtsunsicherheit

Das Datenschutzrecht operiert mit einer Vielzahl äusserst offener Begriffe, etwa «Erkennbarkeit», «Verhältnismässigkeit» oder «Treu und Glauben»[2]. Die Bedeutung dieser Begriffe für den Einzelfall ist meist unklar. Dem Gesetz selbst lassen sich jedenfalls keine hinreichend klaren Vorgaben entnehmen, was nach Massgabe dieser Grundsätze zulässig ist und wo die Grenzen verlaufen. Vielmehr öffnen diese Grundsätze einen äusserst weiten Interpretationsspielraum.

Dieser Raum ermöglicht, im konkreten Fall vernünftige Lösungen zu finden. Die Lösungen sind aber vom Gesetz kaum vorgezeichnet, was zu einem hohen Bedarf nach interner und externer Rechtsberatung führt. Die Offenheit des Datenschutzrechts kann man positiv sehen, gerade in einem Umfeld des raschen technologischen Wandels. Eigentlich ist der Anspruch an Rechtsnormen aber ungleich höher: Sie sollen hinreichend klar zwischen zulässigem und unzulässigem Verhalten trennen – und nicht einen nahezu beliebig weiten Argumentationsspielraum eröffnen.

Die Rechtsunsicherheit ist besonders bedenklich, wenn der Verstoss gegen Normen, wie namentlich in der DSGVO, mit scharfen Sanktionen bewehrt ist[3]. Die offenen Vorgaben des Datenschutzrechts genügen dem Bestimmtheitsgebot *(nulla poena sine lege)*

digma 2019 S. 206, 207

---

1 Bull Hans Peter, Sinn und Unsinn des Datenschutzes, Tübingen 2015; Schneider Jochen/Härting Niko, Datenschutz in Europa – Plädoyer für einen Neubeginn, CR 2014, 306–312 (zit.: Schneider/Härting, Datenschutz in Europa); dies., Das Ende des Datenschutzes – es lebe die Privatsphäre, CR 2015, 819–827(zit.: Schneider/Härting, Das Ende des Datenschutzes); Veil Winfried, Die Datenschutzgrundverordnung: des Kaisers neue Kleider, der gefährliche Irrweg des alten wie des neuen Datenschutzrechts, NVwZ 2018, 686–696; siehe auch: Bowden Caspar, Tweet vom 20.12.2014, abrufbar unter: <https://twitter.com/CasparBow den/status/546367811715870720> (letztmals kontrolliert: 23.10.2019); Krempl Stefan, Rechtsexperte: Datenschutz-Grundverordnung als «grösste Katastrophe des 21. Jahrhunderts» (Zitat von Thomas Hoeren), heise online, abrufbar unter: <https://www.heise.de/newsticker/meldung/Rechtsexperte-Da tenschutz-Grundverordnung-als-groesste-Katastrophe-des-21-Jahrhunderts-3190 299.html>.

2 Der Grundsatz von «Treu und Glauben» wird z.B. als eine Art «datenschutzrechtliche Generalklausel» verstanden, in der Praxis kommt ihm aber wenig Bedeutung zu; siehe dazu etwa: Rosenthal David, Handkommentar zum Datenschutzgesetz, sowie weitere, ausgewählte Bestimmungen, Zürich 2008, DSG 4 N 14; Maurer-Lambrou Urs/Steiner Andrea, in: Maurer-Lambrou/Blechta (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014, DSG 4 N 8; Weber Rolf H., E-Commerce und Recht, 2. Aufl., Zürich 2010, 448 f.

3 Art. 83 f. DSGVO.

jedenfalls mit Bestimmtheit nicht[4]. Von der Rechtsunsicherheit besonders betroffen sind dabei Unternehmen, die nicht über interne Fachkompetenzen verfügen und sich eine externe Rechtsberatung nicht leisten können.

Die bisweilen informell geäusserten Beteuerungen gewisser Datenschutzbehörden, sich bei der Durchsetzung des Datenschutzrechts «auf die grossen Fische» zu konzentrieren, nützt da wenig. Vielmehr machen solche Aussagen die reichlich groteske Situation besonders deutlich: Die Vorgaben des Datenschutzrechts richten sich bewusst an alle Bearbeiter von Personendaten; diese haben alle die gesetzlichen Vorgaben einzuhalten und sie unterliegen alle den jeweiligen Sanktionsdrohungen. Dies mit der Beteuerung aufzuheben, dass man keine Sanktionen zu befürchten habe, läuft dem umfassenden Regelungsansatz des Datenschutzrechts diametral zuwider. Hinzu kommt, dass sich die Unternehmen auf solche «Zusicherungen» natürlich nicht verlassen können. Die Unsicherheit wird also nur vermeintlich geringer.

Befund 2: Missverhältnis von Kosten und Nutzen

Das Einhalten der Vorgaben von DSGVO und DSG verursacht bei den betroffenen Unternehmen enorme Kosten[5]. Erfahrene Praktiker betonen, dass es für Unternehmen gar nicht möglich sei, die Vorgaben des Datenschutzrechts vollständig einzuhalten[6]. Unabhängig von den Kosten der *compliance* wirft dies die ganz grundsätzliche Frage auf, ob es vertretbar und sinnvoll ist, ein Regelwerk aufzustellen, dessen Vorgaben niemand vollständig einhalten kann.

Wichtiger als die direkten Kosten der *compliance* sind die indirekten Kosten, die darin bestehen, dass bestimmte Geschäftsmodelle oder Forschungsprojekte nicht oder nur unter derart erschwerten Voraussetzungen durchgeführt werden können, dass sie unterbleiben[7]. Wie hoch die direkten Kosten für die *compliance* und die indirekten Kosten für *«lost opportunities»* sind, weiss heute niemand. Sicher ist aber, dass es um sehr grosse Beträge geht. Für die grossen US-amerikanischen Tech-Unternehmen dürften die Kosten für die *compliance* im dreistelligen Millionenbereich liegen. Die indirekten Kosten lassen sich nicht einmal schätzen. Sicher ist nur, dass es insgesamt um gigantische Kosten geht, welche die Volkswirtschaft zu tragen hat[8]. Besonders bedenklich ist dabei, dass grosse Unternehmen in der Lage sind, die Kosten für

---

4 Ungeachtet eines allfälligen strafrechtlichen Charakters müssen Bestimmungen, welche die Verhängung von Sanktionen durch die Verwaltung gestatten, den Grundsätzen der Bestimmtheit und Vorhersehbarkeit gerecht werden (EuGH vom 8.7.2008, Rs. T-99/04, Rn. 139; Frenzel Eike Michael, in: Paal Boris P./Pauly Daniel [Hrsg.], Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018, DSGVO 83 N 19); Bergt Matthias, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutzgrundverordnung/BDSG, Kommentar, 2. Aufl., München 2018, DSGVO 83 N 44 f.; ders., Sanktionierung von Verstößen gegen die Datenschutz-Grundverordnung, DuD 2017, 555–561, 560; Holländer Corinna, in: Brink Stefan/Wolff Heinrich Amadeus (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, München 2019 (Stand: 1.5.2019), DSGVO 83 N 6.

5 Konkrete und belastbare Zahlen sind bisher nicht verfügbar und die meisten Unternehmen werden sich hüten, solche zu veröffentlichen. Einigen öffentlich verfügbaren Aussagen lassen sich immerhin gewisse Anhaltspunkte entnehmen. So kostet das Einhalten der Vorgaben der DSGVO nach einer Einschätzung von Forbes rund 16 Millionen Dollar für Fortune-500-Unternehmen; siehe dazu: Smith Oliver, The GDPR Racket: Who's Making Money From This $ 9bn Business Shakedown, Forbes, 2.5.2018, abrufbar unter: <https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-busi ness-shakedown/#4727a86434a2>; ähnlich: Kahn Jeremy/Bodoni Stephanie/Nicola Stefan, It'll Cost Billions for Companies to Comply With Europe's New Data Law, Bloomberg Businessweek, Bloomberg, 22.3.2018, abrufbar unter: <https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law>; Heimes Rita/Pfeifle Sam, Study: GDPR's global reach to require at least 75 000 DPOs worldwide, iapp, 9.11.2016, abrufbar unter: <https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/#>.

6 Rosenthal David, Datenschutz-Compliance im Unternehmen: Eine etwas andere Anleitung …, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Datenschutz-Managementsysteme im Aufwind?, Zürich 2016, 7–29, 7; ders., Der Entwurf für ein neues Datenschutzgesetz, Was uns erwartet und was noch zu korrigieren ist, Jusletter vom 27.11.2017, Rn. 98 f.

7 Für Kritik an den negativen Auswirkungen der DSGVO auf innovative Tätigkeiten in der EU siehe: Chivot Eline/Castro Daniel, The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy, 13.5.2019, abrufbar unter: <https://www.datainnovation.org/2019/05/the-eu-needs-to-reform-the-gdpr-to-remain-competitive-in-the-algorithmic-economy>; Drexl Josef, Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy, Max Planck Institute for Innovation and Competition Research, Paper 2018/23, 11 f.

8 Die volkswirtschaftlichen Kosten der Einführung der DSGVO lassen sich nicht genau bestimmen. Nach einer jüngeren Analyse verzeichneten EU-Technologieunternehmen seit Inkrafttreten der DSGVO im Vergleich zu US-amerikanischen Technologieunternehmen allerdings einen Rückgang an Risikokapitalfinanzierung («venture funding») im zweistelligen Prozentbereich; siehe dazu: Jia Jian/Jin Ginger Zhe/Wagman Liad, The Short-Run Effects of GDPR on Technology Venture Investment, National Bureau of Economic Research, Working Paper 25248.

die *compliance* und die Risiken einer Sanktionierung zu tragen, kleine hingegen nicht[9]. Damit besteht die Gefahr, dass Markteintritte von *start-ups* verhindert werden und die grossen Unternehmen von den Vorgaben des Datenschutzrechts im Wettbewerb gar profitieren. So betrachtet führt das Datenschutzrecht im Ergebnis möglicherweise zu einer Stärkung der Starken und einer Schwächung der Schwachen.

Den enormen Kosten steht kein klarer Nutzen gegenüber: Ob unsere Privatsphäre seit Inkrafttreten der DSGVO wirklich besser geschützt ist und wir die Kontrolle über unsere Daten wiedererlangt haben, ist zumindest fraglich. Der Nutzen für die betroffenen Personen bleibt jedenfalls sehr diffus. Natürlich lässt sich dieser Nutzen noch schlechter quantifizieren als die Kosten. Man muss sich aber ganz ernsthaft fragen, ob der Nutzen des Datenschutzrechts für die betroffenen Personen und die Gesellschaft insgesamt dessen Kosten überwiegt.

Geradezu absurd ist der Umstand, dass viele Unternehmen offenbar erst bei der Umsetzung der Vorgaben der DSGVO realisiert haben, auf welchen Datenschätzen sie sitzen – und sich nun bemühen, diese Daten gewinnbringend zu nutzen. Auch wenn die Ziele des Datenschutzrechts weitgehend unklar sind – dies war (und ist) sicher nicht das Ziel.

Befund 3: Frontalkollision mit neueren Technologien

Die Konzepte und der Regelungsansatz des Datenschutzrechts stammen, wie erwähnt, aus den 60er- und 70er-Jahren des letzten Jahrhunderts. Es kann deshalb nicht erstaunen, dass diese Konzepte mit den neueren technischen Entwicklungen frontal kollidieren. Zu nennen

digma 2019 S. 206, 208

sind dabei v.a. *Big Data* und die Entwicklungen im Bereich der *Artificial Intelligence (AI),* insb. das *Machine Learning.*

Big Data beruht im Wesentlichen auf dem Gedanken, durch die Verknüpfung und Analyse sehr grosser Datenmengen neue Erkenntnisse zu gewinnen. Diese ergeben sich regelmässig daraus, dass Daten zu ganz anderen Zwecken analysiert werden, als die, für die sie ursprünglich gesammelt worden sind. *Big Data* kollidiert damit frontal mit dem Grundsatz der Zweckbindung[10]. Noch offensichtlicher ist die Kollision mit dem Grundsatz der Verhältnismässigkeit, insb., wenn man diesen im Sinn der Datenminimierung versteht[11]. Denn *Big Data* beruht auf dem Gedanken, dass die Ergebnisse der Analysen umso besser werden, je mehr Daten verwendet werden. Dies bedingt eine Datenmaximierung[12].

Grundlegende Probleme werfen auch Anwendungen im Bereich des *Machine Learning* auf. Im Vordergrund steht hier, dass *Deep Neural Networks* oft *«black boxes»*[13] darstellen, dass die Entwickler und Anwender dieser Systeme also gar nicht verstehen, wie ihre Modelle funktionieren. Transparenz über die Datenbearbeitung kann hier eigentlich nicht hergestellt werden – jedenfalls dann nicht, wenn man sich nicht damit begnügt, Input und Output zu verstehen, sondern auch einen Anspruch auf Transparenz des Prozesses *(logic involved)* erhebt[14].

---

9 Härting Niko, Warum das Datenschutzrecht kein Wettbewerbsinstrument ist, CR-online.de Blog, 15.10.2019, abrufbar unter: <https://www.cr-online.de/blog/2019/10/15/warum-das-daten schutzrecht-kein-wettbewerbsinstrument-ist>; Kostov Nick/Schechner Sam, GDPR Has Been a Boon for Google and Facebook, The Wall Street Journal, 17.7.2019, abrufbar unter <https://www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219> (letztmals kontrolliert: 23.10.2019).

10 Thouvenin Florent, Erkennbarkeit und Zweckbindung: Grundprinzipien des Datenschutzrechts auf dem Prüfstand von Big Data, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Big Data und Datenschutz – Gegenseitige Herausforderungen, Zürich 2014, 62–83, 68; ders., Privatversicherungen: Datenschutzrecht als Grenze der Individualisierung?, in: Epiney Astrid/Sangsue Déborah (Hrsg.), Datenschutz und Gesundheitsrecht, Zürich 2019, 15–42, 31; Paal Boris P./Hennemann Moritz, Big Data im Recht, Wettbewerbs- und daten(schutz)rechtliche Herausforderungen, NJW 2017, 1697–1701, 1700.

11 Thouvenin Florent, Forschung im Spannungsfeld von Big Data und Datenschutzrecht: eine Problemskizze, in: Gedächtnisschrift für Martin Usteri, Bern 2017, 27–53, 29, 35; Paal/Hennemann (Fn. 11), 1700.

12 Thouvenin (Fn. 11), 31; ders., (Fn. 12), 35 f.; Rubinstein Ira, Big Data: The End of Privacy or a New Beginning?, International Data Privacy Law 2013, 74–87, 74.

13 Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information, Cambridge 2015, 6 ff.

14 Burrell Jenna, How the machine «thinks»: Understanding opacity in machine learning algorithms, Big Data & Society 1/2016, 1–12, 1 ff.; Mittelstadt Bernt Daniel/Allo Patrick/Taddeo Mariarosaria/Wachter Sandra/Floridi Luciano, The ethics of algorithms: Mapping the debate, Big Data & Society 2/2016, 1–21, 1 ff.

Befund 4: Keine Lösung für zentrale Probleme

Man mag sich fragen, was die grössten Herausforderungen und Probleme sind, die sich aus der Bearbeitung von Personendaten ergeben können. Aus heutiger Sicht stehen meines Erachtens drei Bereiche im Vordergrund:

Erstens besteht die Gefahr, dass Menschen aufgrund ihrer Daten diskriminiert werden. In gewissen Konstellationen mag das sachlich gerechtfertigt und damit rechtlich unproblematisch sein (z.B., dass von risikogeneigten Fahrern höhere Prämien für eine Motorfahrzeughaftpflichtversicherung verlangt werden). In anderen Fällen wird es aber an einer Rechtfertigung fehlen. Mit seinem Fokus auf das Bearbeiten von Personendaten ist das Datenschutzrecht weitgehend blind für die Folgen der Bearbeitung, bspw. für Diskriminierung. Die negativen Folgen einer Datenbearbeitung für die betroffenen Personen können zwar allenfalls bei der Auslegung berücksichtigt werden, aber verhindern (oder wenigstens sanktionieren) lässt sich eine rechtlich problematische Diskriminierung mithilfe des Datenschutzrechts nicht.

Zweitens besteht die Gefahr, dass Menschen auf Grundlage der Bearbeitung ihrer Daten manipuliert werden. Auch hier wird nicht jeder Beeinflussungsversuch (z.B. durch *targeted advertising*) als rechtlich problematisch anzusehen sein. Bestimmte Ansätze sind es aber sicherlich, bspw. der (aus den USA bekannte) Versuch, Menschen vom Wählen abzuhalten[15]. Auch hier vermag das Datenschutzrecht keine Lösungen zu bieten.

Drittens wird immer klarer erkennbar, welche Macht gewissen Unternehmen aufgrund der gewaltigen Datenmengen zukommt, über die sie verfügen[16]. Bei Staaten ist das noch deutlicher und für die Gesellschaft wohl auch gefährlicher, weil Staaten in aller Regel weit umfassendere Ziele verfolgen als Unternehmen und vielfältige Zwangsmittel einsetzen können, um diese zu erreichen. Laufende Verwaltungs- und Gerichtsverfahren, etwa das Facebook-Verfahren des deutschen Bundeskartellamts, machen deutlich, wie das Kartellrecht bei der Einfassung und Begrenzung der Machtpositionen der grossen Tech-Unternehmen scheitert[17]. Auch das Datenschutzrecht kann hierzu nichts beitragen.

Zwischenfazit

Der Befund ist höchst bedauerlich, ja alarmierend: Das Datenschutzrecht kollidiert mit den neuen Technologien, es schafft Rechtsunsicherheit, verursacht gigantische Kosten und stiftet keinen klaren Nutzen – und es vermag zentrale Probleme, die sich aus der Bearbeitung von Personendaten ergeben, nicht zu lösen. Die Frage ist natürlich: weshalb?

Diagnose 1: Unklare Grundlagen

Bis heute ist unklar, auf welcher konzeptionellen Grundlage das Datenschutzrecht beruht: Geht es um den Schutz der persönlichen Freiheit (Art. 10 Abs. 2 BV), um den Schutz der Privatsphäre (Art. 13 Abs. 1 BV), um den Schutz vor Missbrauch der eigenen Daten (Art. 13 Abs. 2 BV), um den Schutz von Grundrechten (Art. 1 DSG), um den Schutz der Persönlichkeit (Art. 1 DSG i.V.m. Art. 27 ff. ZGB) oder beruht das

---

15 Cadwalladr Carole/Graham-Harrison Emma, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, 17.3.2018, abrufbar unter: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

16 Mantelero Alessandro, Masters of Big Data: Concentration of Power Over Digital Information, 15.2.2012, abrufbar unter: <http://dx.doi.org/10.2139/ssrn.2048236>; Rogoff Kenneth, Big tech has too much monopoly power – it's right to take it on, The Guardian, 2.4.2019, abrufbar unter: <https://www.theguar dian.com/technology/2019/apr/02/big-tech-monopoly-power-elizabeth-warren-technology>; Moore Martin, Tech Giants and Civic Power, London 2016, abrufbar unter: <https://www.kcl.ac.uk/policy-institute/assets/cmcp/tech-giants-and-civic-power.pdf>, 21 ff.

17 Siehe dazu: Bundeskartellamt, Beschluss vom 6.2.2019, B6-22/16, in dem Facebook gestützt auf das Gesetz gegen Wettbewerbsbeschränkungen (GWB) unter anderem untersagt wurde, Konditionen zu verwenden, die die Nutzung des gleichnamigen sozialen Netzwerks davon abhängig machen, dass Facebook Daten, die bei der Benutzung konzerneigener Dienste, wie etwa WhatsApp, erhoben werden, ohne Einwilligung der Nutzer mit den für Facebook geführten Nutzerkonten verknüpfen und verwenden kann. Mit Beschluss vom 26.8.2019, VI-Kart 1/19 (V), liess nun aber das Oberlandesgericht Düsseldorf die Beschwerde gegen den Beschluss des Bundeskartellamts zu und erteilte der Beschwerde aufschiebende Wirkung mit der Begründung, dass «[s]chon nach summarischer Pru fung […] die Annahme eines Ausbeutungsmissbrauchs in Gestalt eines Konditionenmissbrauchs zum Nachteil der Nutzer des sozialen Netzwerks von Facebook durchgreifenden rechtlichen Bedenken [begegnet]».

Datenschutzrecht auf dem Konzept der «informationellen Selbstbestimmung», wie es die überwiegende Lehre[18] vertritt?

Die EU hat es sich recht einfach gemacht, indem sie schlicht ein «Grundrecht auf Datenschutz» (Art. 8 EU-Charta) geschaffen hat. Dieses vermag die konzeptionellen Fragen allerdings auch nicht zu beantworten, weil es lediglich ein nicht näher umrissenes Recht jeder Person auf den Schutz der sie betreffenden Daten statuiert (Art. 8 Abs. 1 EU-Charta) und im Übrigen

digma 2019 S. 206, 209

bloss einige der Kernkonzepte des Datenschutzrechts wiedergibt (Art. 8 Abs. 2 EU-Charta). Statt Klärung bietet das Grundrecht auf Datenschutz damit nur einen Verweis – ein Zirkelschluss, der keine Antworten auf die drängenden Grundfragen zu geben vermag.

Sollte die Grundlage des Datenschutzrechts ein (in der Schweiz ungeschriebenes) «Grundrecht auf Datenschutz» sein, stellen sich weitere Fragen, etwa: Was ist dessen Aufgabe? Handelt es sich um eine Art «Supergrundrecht» oder um ein Grundrecht mit «Vorfeldcharakter», dem eine dienende Funktion beim Schutz anderer Grundrechte zukommt[19]? Wenn ja: Macht es Sinn, ein allein dienendes und damit für sich allein weitgehend inhaltsleeres Grundrecht zu anerkennen?

Wie auch immer die Antworten auf diese Fragen ausfallen: Klar ist, dass die konzeptionellen Grundlagen des Datenschutzrechts der Klärung bedürfen. Gerade für die zahlreichen Wertungen, die bei der Anwendung des geltenden Rechts vorgenommen werden müssen, braucht es zwingend einen Orientierungspunkt, der sich nur aus Sinn und Zweck des Datenschutzrechts ergeben kann. Ohne diese Klarstellung scheint eine Begrenzung des entgrenzten Datenschutzrechts ebenso unmöglich wie die dringend erforderliche Erhöhung der Rechtssicherheit.

Diagnose 2: Entgrenzung des Datenschutzrechts

Ein zentrales Problem des Datenschutzrechts ist seine Entgrenzung: Die Kernbegriffe, die den Anwendungsbereich von DSGVO und DSG definieren – die Begriffe «Personendaten» und «Bearbeitung» –, sind schon nach dem Wortlaut der jeweiligen Bestimmungen äusserst weit[20]. Mit an sich guten Gründen wurde der Begriff der Personendaten in Lehre und Rechtsprechung immer weiter ausgedehnt[21]. Dies hat aber zur Folge, dass dem Anwendungsbereich des Datenschutzrechts kaum noch Grenzen gezogen sind und jedes Unternehmen sowie alle staatlichen Behörden erfasst. Denn kein Unternehmen und keine Behörde kommt ohne Bearbeitung von Personendaten aus – und seien es nur die Daten über die eigenen Mitarbeitenden. In der Informationsgesellschaft beruhen zudem immer mehr Geschäftsmodelle auf der Bearbeitung von Daten, die wegen des äusserst weiten Begriffs meist als Personendaten zu qualifizieren sind.

---

18 Statt vieler: BGE 145 IV 42 E. 4.2; BGE 143 I 253 E. 4.8 f.; BGE 128 II 259 E. 3.2 ff.; Belser Eva Maria, in: Belser Eva Maria/Epiney Astrid/Waldmann Bernhard, Datenschutzrecht, Grundlagen und öffentliches Recht, Bern 2011, § 6 Rz. 115; Biaggini Giovanni, Bundesverfassung der Schweizerischen Eidgenossenschaft, Kommentar, 2. Aufl., Zürich 2017, BV 13 N 11; Frey Marco, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Handkommentar Datenschutzgesetz (DSG), Bern 2015, DSG 1 N 13; Maurer-Lambrou Urs/Kunz Simon, in: Maurer-Lambrou Urs/Blechta Gaborc (Hrsg.), Basler Kommentar Datenschutzgesetz/Öffentlichkeitsgesetz, 3. Aufl., Basel 2014, DSG 1 N 18 f.; Rosenthal (Fn. 3), DSG 1 N 4; Schweizer Rainer J., in: Ehrenzeller Bernhard/Mastronardi Philippe/Schweizer Rainer J./Vallender Klaus (Hrsg.), Die schweizerische Bundesverfassung, St. Galler Kommentar, 3. Aufl., Zürich/St. Gallen 2014, BV 13 N 72; Flückiger Alexandre, L'autodétermination en matière de données personnelles: un droit (plus si) fondamental à l'ère digitale ou un nouveau droit de propriété?, AJP 2013, 837–864, 847 f.;

19 Siehe dazu etwa: Marsch Nikolaus, Das europäische Datenschutzgrundrecht, Grundlagen, Dimensionen, Verflechtungen, Tübingen 2018, 87 ff., insb. 87, wonach das Datenschutzgrundrecht «nicht selbstzweckhaft auf den Schutz von Daten abzielt, sondern dem Schutz einer Vielzahl anderer Rechte und Interessen dient».

20 Art. 3 Bst. a und c DSG; Art. 4 Nr. 1 und 2 DSGVO. Zum Begriff der Personendaten: Für das Schweizer Recht siehe: Rosenthal (Fn. 3), DSG 3 N 2; Rudin Beat, in: Baeriswyl Bruno/Pärli Kurt (Hrsg.), Handkommentar Datenschutzgesetz (DSG), Bern 2015, DSG 3 N 4. Für das europäische Recht siehe: Ziebarth Wolfgang, in: Sydow Gernot (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. Aufl., Baden-Baden 2018, DSGVO 4 N 8.

21 Für die Rechtsprechung: BGE 136 II 508 E. 3; EuGH vom 19.10.2016, Rs. C-582/14, Rn. 23 ff. Für die Lehre statt vieler: Probst Thomas, Die unbestimmte «Bestimmbarkeit» der von Daten betroffenen Personen im Datenschutzrecht, AJP 2013, 1423–1436, 1431 ff.; Meyerdierks Per, Sind IP-Adressen personenbezogene Daten?, MMR 2009, 8–13, 10.

In einer Welt, in der alle möglichen Arten von Tätigkeiten (zumindest auch) das Sammeln und Bearbeiten von Personendaten mit sich bringen, wird die fehlende Begrenzung des Datenschutzrechts zu einem zentralen Problem. Denn ein Recht, das den Umgang mit Personendaten umfassend regeln will, wird damit zunehmend zum *«law of everything»*[22]. Und dieses *«law of everything»* will *«everything»* mit einer Handvoll allgemeiner Regeln erfassen.

Diagnose 3: One size does not fit all

Zur fehlenden Begrenzung des Anwendungsbereichs kommt hinzu, dass das Datenschutzrecht alle Arten von Datenbearbeitungen und Verantwortlichen mit einem einzigen Satz von Regeln erfassen will[23]. Nicht einmal zwischen der Bearbeitung durch Unternehmen und durch den Staat wird (vollständig) unterschieden. Vielmehr finden im DSG die materiell wichtigsten Regeln – die Grundsätze der Datenbearbeitung – auf den Staat ebenso Anwendung wie auf Private. Und in der DSGVO fehlt eine solche Differenzierung gleich ganz[24].

Differenzierungen wären aber dringend erforderlich. Ganz sicher zwischen Bearbeitungen durch den Staat und die Unternehmen. Zu unterscheiden wäre aber wohl auch nach Art und Menge der bearbeiteten Daten, nach dem Sektor und nach den Folgen für die betroffenen Personen. Es macht keinen Sinn, den Bäcker und die Fahrradvermietung um die Ecke denselben Regeln zu unterstellen wie Google und Facebook – obwohl die Geschäftstätigkeit und das Gefährdungspotenzial unterschiedlicher nicht sein könnten[25]. Besonders problematisch ist für Bäcker, Fahrradvermieter und die meisten KMU, dass man sich beim Festlegen der Regeln an den grossen US-amerikanischen Tech-Unternehmen orientiert hat[26]. Dass damit kein Regelwerk entstehen kann, das für KMU Sinn macht, liegt auf der Hand. Daran vermögen auch die wenigen Erleichterungen nichts zu ändern, die für KMU in der DSGVO vorgesehen sind[27].

Diagnose 4: Versagen von Kernkonzepten

Eine weitere Problematik des Datenschutzrechts liegt im Versagen seiner Kernkonzepte. Nicht wenige dieser Konzepte vermögen die ihnen zugedachte Aufgabe nicht (oder zumindest nicht hinreichend) zu erfüllen. Das gilt in erster Linie für den Grundsatz der Transparenz und für das Konzept der Einwilligung, teilweise auch für den Grundsatz der Zweckbindung.

Auch wenn der Grundsatz der Transparenz als solcher nicht infrage zu stellen ist, muss man doch eingestehen, dass wir in der Realität vom Bestehen von Transparenz weit entfernt sind. Wir wissen es aus dem eigenen Alltag und

---

22 Purtova Nadezha, The law of everything, Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology 2018, 40–81, 40 ff.

23 Veil (Fn. 2), 692 f.; Härting/Schneider (Fn. 2), Das Ende des Datenschutzes, 819.

24 Verantwortlicher i.S.v. Art. 4 Nr. 7 DSGVO können Private oder Behörden sein (Petri Thomas, in: Simitis Spiros/Hornung Gerrit/Spiecker genannt Döhmann Indra [Hrsg.], NomosKommentar Datenschutzrecht, Baden-Baden 2019, DSGVO 4 Nr. 7 N 13). Bei der Systematik und den materiellen Regelungen der DSGVO gibt es grundsätzlich keine Unterscheidung zwischen öffentlichen und privaten Stellen (siehe dazu auch Kühling Jürgen/Klar Manuel/Sackmann Florian, Datenschutzrecht, 4. Aufl., Heidelberg 2018, Rz. 310).

25 Veil (Fn. 2), 692 f.; Härting/Schneider (Fn. 2), Das Ende des Datenschutzes, 819.

26 Siehe dazu: Houser Kimberly/Voss Gregory, GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?, Richmond Journal of Law & Technology 2018, 1–109; Härting (Fn. 10), passim.

27 Siehe dazu: Erwägungsgrund 13 DSGVO; Art. 30 Abs. 5 DSGVO (Ausnahme von der Pflicht zur Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten); Art. 40 Abs. 1 DSGVO (Berücksichtigung der Besonderheiten von Kleinstunternehmen sowie KMU bei der Ausarbeitung von Verhaltensregeln).

28 Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policy Makers, FTC Report, march 2012, 61; Solove Daniel J., Introduction: Privacy Self-Management and the Consent Dilemma, Harvard Law Review 2013, 1880–1903, 1884 ff.; Hull Gordon, Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data, Ethics and Information Technology 2015, 89–101, 90 ff.; McDonald Aleecia M./Faith Cranor Lorrie, The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society 2008, 543–568, 545 ff.

die Forschung hat es vielfach bestätigt: Datenschutzerklärungen werden von (praktisch) niemandem gelesen, der dafür nicht bezahlt wird – die Transparenz ist damit nur theoretisch hergestellt[28]. Wenig hilfreich ist der Ansatz, der fehlenden Transparenz durch weitgehende Informationspflichten zu begegnen[29]. Mehr Information wird einfach weniger wahrgenommen *(information overload)*[30]. Viel spricht dafür, dass die umfassenden Informationspflichten der DSGVO die Transparenz im Ergebnis nicht erhöhen, sondern weiter untergraben werden. Immerhin: Das Problem ist erkannt und mögliche Lösungsansätze werden seit einiger Zeit diskutiert[31].

Auch das Konzept der Einwilligung hat sich in der Praxis als zunehmend inhaltsleer erwiesen. Zu Recht ist eine Einwilligung nur gültig, wenn sie informiert erteilt wird[32]. Wenn aber niemand Datenschutzerklärungen liest und die Einwilligung in alle möglichen Arten von Datenbearbeitungen durch einen Klick beiläufig erteilt wird, kann von einer informierten Einwilligung nicht die Rede sein[33]. Der Vorgang der Einwilligung verkommt damit zunehmend zur Farce[34].

Ähnliches zeigt sich bei der Zweckbindung. Unternehmen definieren den Zweck meist so weit, dass dieser kaum noch eine Begrenzung bildet[35]. Hinzu kommt, dass die betroffenen Personen bei einer derart weiten Zweckumschreibung kaum einschätzen können, was Unternehmen mit den Daten effektiv tun.

Diagnose 5: Fokus auf Vorgang statt Folgen

Das Datenschutzrecht erfasst jede Bearbeitung von Personendaten und unterstellt diese einer Reihe von Regeln. Es fokussiert dabei ganz auf den Vorgang des Bearbeitens und lässt die Folgen weitgehend unberücksichtigt. Man mag die Folgen zwar bei der Auslegung gewisser Normen (z.B. bei der Interessenabwägung) bedenken, eine zentrale Rolle kommt ihnen aber nicht zu[36]. Das Datenschutzrecht ist damit weitgehend blind für die Folgen von Datenbearbeitungen – dabei käme es gerade auf diese an. Aufgrund dieses Ansatzes erstaunt denn auch nicht, dass das Datenschutzrecht negative Folgen von Datenbearbeitungen – bspw. Diskriminierung oder Manipulation – nicht adäquat erfassen oder gar verhindern kann. Vielmehr führt der Fokus auf die Bearbeitung dazu, dass negative Folgen ebenso verhindert werden wie positive. Nur eine Konzentration auf konkrete, nachteilige Folgen würde ermöglichen, eine adäquate Trennung zwischen positiven und negativen Effekten der Bearbeitung von Personendaten vorzunehmen – und damit die Kosten/Nutzen-Analyse des Datenschutzrechts massgeblich zu verbessern.

Zwischenfazit

Eine erste Diagnose macht zwei Dinge deutlich: Zum einen sieht das Datenschutzrecht die Bearbeitung von Personendaten als solche als problematisch an, was den Bedarf nach einer umfassenden Regulierung erst begründet. Das DSG geht zwar (auch hier) weniger weit als die DSGVO, weil es nicht für jede Bearbeitung

---

29 Ebenso: Rosenthal David/Vasella David, Erste Erfahrungen mit der DSGVO, digma 2018, 166–171, 167.

30 Zum information overload siehe etwa: Beaudoin Christopher, Explaining the Relationship between Internet Use and Interpersonal Trust: Taking into Account Motivation and Information Overload, Journal of Computer-Mediated Communication 2008, 550–568.

31 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017, 7050; Article 29 Data Protection Working Party (Fn. 30), 6 ff.; siehe auch: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), 24. Tätigkeitsbericht 2016/2017, Bern 2017, 18.

32 Art. 4 Abs. 5 DSG; Art. 7 DSGVO i.V.m. Erwägungsgrund 32 DSGVO.

33 Veil (Fn. 2), 688.

34 Edwards Lilian/Veale Michael, Slave to the Algorithm? Why a «Right to an Explanation» is probably not the Remedy you are looking for, Duke Law & Technology Review 2017, 19–84, 33, 66, m.w.H.

35 Siehe dazu bspw. die Privacy Policy von Facebook, in der zahlreiche, jeweils breit gefasste Verwendungszwecke aufgezählt werden, so etwa «Bereitstellung, Personalisierung und Verbesserung unserer Produkte», «Bereitstellung von Messungen, Analysen und sonstigen Unternehmens-Services», «Förderung von Schutz, Integrität und Sicherheit», «Kommunikation mit dir», «Forschung und Innovation für soziale Zwecke» (abrufbar unter: <https://www.facebook.com/policy.php>); ähnlich die Privacy Notice von Nestlé, in der Zwecke aufgeführt werden, wie die Nutzung der Daten für «Kundendienst/Verbraucherservice», «Wettbewerb, Marketing und andere Werbung», «Soziale Netzwerke Dritter», «Andere allgemeine Zwecke (z.B. interne oder Marktforschung, Analytik, Sicherheit)», «Durchführung von Geschäftsbeziehungen», aber auch «Rechtliche Gründe oder Zusammenschluss/Akquisition» (abrufbar unter: <https://www.nestle.de/info/rechtshinweise#Datenschutz>).

36 Für die Berücksichtigung bei der Interessenabwägung siehe: EuGH vom 13.5.2014, Rs. C-131/12, Rn. 86; Veil Winfried, Einwilligung oder berechtigtes Interesse?, Datenverarbeitung zwischen Skylla und Charybdis, NJW 2018, 3337–3344, 3341.

eine Rechtsgrundlage verlangt[37]. Die (implizite) Grundannahme ist aber dieselbe. Diese wäre allerdings erst einmal zu begründen und zu belegen. Das Verhalten der meisten Menschen und die zahlreichen Arbeiten zum *privacy paradox*[38] legen vielmehr nahe, dass die überwiegende Mehrheit der Personen die Bearbeitung ihrer Daten nicht *per se* als problematisch ansieht.

Zum andern steht das Datenschutzrecht mit der umfassenden Regelung jeder Datenbearbeitung im Widerspruch zum gesamten (restlichen) Privatrecht. Dieses beruht auf dem Grundsatz, dass erlaubt ist, was nicht verboten ist. Und verboten ist in aller Regel nur, was anderen Schaden oder andere massgebliche Nachteile zufügt. Das Datenschutzrecht geht aber vom gegenteiligen Ansatz aus, indem es jede Bearbeitung von Personendaten der Regulierung unterstellt – und dies ebenso unterschieds- wie anlasslos. Im Minimum sind dabei die Grundsätze der Datenbearbeitung einzuhalten; nach der DSGVO braucht es gar für jede Bearbeitung eine Rechtsgrundlage. Zumindest nach dieser Regelung sind wir damit beim Gegenteil des Grundsatzes des Privatrechts angelangt – eine überzeugende Begründung hierfür gibt es nicht.

Hinzu kommt, dass die Bearbeitung von Personendaten nach DSG und DSGVO im Prinzip einer umfassenden Kontrolle durch die Datenschutzbehörden untersteht[39]. In einer Welt, die zunehmend auf der Bearbeitung von Personendaten beruht, sind wir damit an einem Punkt angelangt, an dem ein Teil jeder unternehmerischen Tätigkeit – für immer mehr Unternehmen der zentrale Teil – der staatlichen Kontrolle untersteht. Eine Begrenzung dieser Kontrolle ergibt sich in der Schweiz zwar aus dem Konzept des «Systemfehlers»[40] und aus den beschränkten Kapazitäten des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Das ist allerdings eine konzeptionell ungenügende und möglicherweise auch nur vorübergehende Sicherheitslinie. Mit einer umfassen-

digma 2019 S. 206, 211

den staatlichen Kontrolle (fast) jeder unternehmerischen Tätigkeit gestützt auf das Datenschutzrecht ist hierzulande zwar nicht zu rechnen – sie wäre aber zumindest theoretisch möglich. Dies gilt erst recht für Europa, zumal die DSGVO keine mit dem DSG vergleichbare Begrenzung der Kontrollbefugnisse von Datenschutzbehörden kennt[41].

Therapie 1: Differenzierung der Regelung

Kein Zweifel kann an der Notwendigkeit bestehen, die Regeln für den Staat von den Regeln für die Privaten zu trennen. Diese Forderung ist nicht neu und sie wird auch von vielen geteilt[42]. In der Schweiz wäre dies auch «nur» eine Rückführung auf die historischen Grundlagen, zumal diese Trennung ursprünglich vorgesehen war. In den 80er-Jahren des 20. Jahrhunderts gab es bekanntlich zwei Entwürfe für ein DSG: einen für Bearbeitungen von Personendaten durch den Staat und einen für die Bearbeitung durch Private[43]. Aus Gründen der politischen Pragmatik hat man diese Entwürfe dann aber zusammengeführt und die heutige Struktur geschaffen, die für alle Bearbeiter geltende «allgemeine Datenschutzbestimmungen» und

---

37 Während unter dem DSG nur bei einer Persönlichkeitsverletzung, etwa bei einem Verstoss gegen die Bearbeitungsgrundsätze, eine Rechtfertigung erforderlich ist (Art. 12 Abs. 2 Bst. a i.V.m. Art. 13 Abs. 1 DSG), beruht die DSGVO auf dem Konzept des Verbots mit Erlaubnisvorbehalt, weshalb jede Bearbeitung von Personendaten auf eine Rechtsgrundlage gestützt werden muss (Art. 6 DSGVO).

38 Siehe dazu statt vieler: Kirsten Martin/Nissenbaum Helen, Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables, Columbia Science & Technology Law Review 2016, 176–218, 178 ff.; Hull (Fn. 29), 90 ff.; Acquisti Alessandro/Grossklags Jens, What Can Behavioral Economics Teach Us about Privacy?, in: Acquisti et al. (Hrsg.), Digital Privacy – Theory, Technologies, and Practices, New York/London 2008, 363–377, 368 ff.; Barnes Susan B., A privacy paradox: Social networking in the United States, First Monday vom 4.9.2006.

39 Art. 27 und 29 DSG; Art. 51 DSGVO.

40 Art. 29 Abs. 1 Bst. a DSG.

41 Vielmehr sieht die DSGVO eine grundsätzlich umfassende Überwachung und Durchsetzung der Vorgaben durch die nationalen Aufsichtsbehörden vor (Art. 57 Abs. 1 Bst. a DSGVO); siehe dazu statt vieler: Selmayr Martin, in: Ehmann Eugen/Selmayr Martin (Hrsg.), Beck'sche Kurz-Kommentare, Datenschutz-Grundverordnung, 2. Aufl., München 2018, DSGVO 57 N 6 ff.

42 Veil Winfried, 21 Thesen zum Irrweg der DS-GVO, CR-online.de Blog, 23.5.2018, abrufbar unter: <https://www.cr-online.de/blog/2018/05/23/21-thesen-zum-irrweg-der-ds-gvo/#anker19>, These 19; siehe auch: Rudin Beat/Baeriswyl Bruno/Mund Claudia, Das revidierte Datenschutzgesetz ist keine souveräne Lösung, Neue Zürcher Zeitung, 31.10.2017, abrufbar unter: <https://www.nzz.ch/meinung/das-revidierte-datenschutzgesetz-ist-keine-souveraene-loesung-ld.1325078>.

43 Konzeption und Durchführung der Datenschutzgesetzgebung, Protokoll der Besprechung der HH. Dir. J. Voyame, Dr. W. Wern, Prof. H. Hausheer, H. Münst und Dr. R. Schweizer vom 26. April 1977, abrufbar unter: <https://cutt.ly/UegV36U>; Botschaft zum Bundesgesetz über den Datenschutz (DSG), BBl II 1988, 426.

jeweils eine Reihe von «besonderen Bestimmungen» für Datenbearbeitungen durch private Personen und Bundesorgane enthält. Bemerkenswert ist dabei, dass die allgemeinen Grundsätze der Datenbearbeitung alle aus dem Entwurf des Gesetzes über die Datenbearbeitung durch Bundesorgane stammen[44]. Es kann also nicht überraschen, dass diese Grundsätze – etwa die Verhältnismässigkeit – für die Datenbearbeitung durch Private nicht passen.

Nimmt man eine vollständige Trennung vor, spricht einiges dafür, die Bearbeitung von Personendaten durch Bundesorgane (und kantonale Organe) auch weiterhin umfassend zu regeln und sich dabei im Wesentlichen an den heutigen Konzepten zu orientieren. Dies schon deshalb, weil der Staat (in seiner Gesamtheit) über sehr viele, teilweise besonders heikle Daten verfügt und diese auch gegen den Willen der betroffenen Personen erheben und bearbeiten kann. Zentral ist zudem, dass der Staat über vielfältige Zwangsmittel verfügt, die Unternehmen gänzlich fehlen. Hinzu kommt, dass der Staat – anders als die Angebote der meisten Unternehmen – alternativlos ist. Schon allein aus diesen Gründen erscheinen umfassende Regeln und eine angemessene Kontrolle staatlicher Datenbearbeitungen zwingend.

Für Datenbearbeitungen durch Private ist hingegen ein grundsätzlich neuer Ansatz erforderlich. Hier sollte der Fokus auf der Verhinderung nachteiliger Folgen von Datenbearbeitungen liegen, wie dies auch im übrigen Privatrecht der Fall ist. Sinnvoll dürfte zudem sein, gewisse Unternehmen stärker in die Pflicht zu nehmen. Ausgangspunkt ist dabei die Erkenntnis, dass Unternehmen aufgrund der Menge oder Art der ihnen verfügbaren Daten bedeutende Macht erlangen können. Trifft dies zu, geht es nicht nur um nachteilige Folgen für die betroffenen Personen, sondern um systemische Risiken für die Gesellschaft. Das Problem ist offensichtlich, die Lösungen sind es aber nicht. Denkbar wäre, solche «datenmächtigen» Unternehmen besonderen Re-geln und einer gewissen Kontrolle zu unterstellen. Wünschenswert erschiene zudem, als alternativlos erscheinende Diensteanbieter zu verpflichten, ihren Kunden auch Produkte anzubieten, die *«privacy friendly»* sind, für deren Nutzung aber allenfalls ein Entgelt zu leisten ist[45]. Voraussetzung wäre natürlich, dass man «normale» von «datenmächtigen» Unternehmen unterscheiden kann, etwa nach Art und Menge der Daten, nach der Zahl der betroffenen Personen, nach dem Geschäftsmodell, nach dem Tätigkeitsfeld (bspw. Suchmaschinen, Social Media, Empfehlungsdienste etc.) sowie nach der Marktsituation.

Therapie 2: Klärung der Grundlagen

Die Frage nach Sinn und Zweck des Datenschutzrechts bedarf dringend der Klärung[46]. Anders als im angelsächsischen Raum, in welchem der (allerdings äusserst weite und diffuse) Begriff der *«privacy»* konzeptionell diskutiert wird[47], fehlt in Europa eine vergleichbare Debatte.

Denkbar und naheliegend wäre eine Rückbesinnung auf den Schutz der Persönlichkeit. Dieser könnte mit Blick auf die fundamentale Bedeutung von Autonomie und Menschenwürde einen Schutz gegen Manipulation und Diskriminierung ebenso umfassen wie einen Schutz der Privatsphäre. Dieser Schutz sollte den betroffenen Personen im Grundsatz ermöglichen selbst zu bestimmen, wer Daten über sie erheben und nutzen darf. Im Gegensatz zum heutigen Datenschutzrecht würde dieser Ansatz erlauben, dass Personendaten, welche die Privatsphäre mit Zustimmung der beteiligten Person verlassen haben, ohne Einschränkungen bearbeitet werden dürfen – solange die Bearbeitung keine nachteiligen Folgen für die Betroffenen hat.

Damit löst sich die Regelung von der Idee der informationellen Selbstbestimmung, die – wenn man sie beim Wort

---

44 Siehe dazu: Botschaft zum Bundesgesetz über den Datenschutz (DSG), BBl II 1988, 431; siehe auch: 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, Freiburger Schriften zum Europarecht Nr. 10, Freiburg i.Ü. 2009, 18.

45 Siehe dazu im Zusammenhang mit Diensten, die nicht gegen eine Geldleistung, sondern im Austausch für das Recht zur Nutzung von Personendaten erbracht werden: Traung Peter, The Proposed New EU General Data Protection Regulation, Further Opportunities, CRi 2012, 33–49, 42; Schneider Jens-Peter, in: Brink/Wolff (Fn. 4), Völker- und unionsrechtliche Grundlagen N 91.1.

46 Veil (Fn. 2), 693 f.

47 Siehe dazu statt vieler: Solove Daniel, Understanding Privacy, Cambridge 2008; Nissenbaum Helen, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford 2010; Waldman Ari Ezra, Privacy as Trust, Cambridge 2018.

nimmt – offensichtlich nicht haltbar ist, weil jeder soziale Kontakt und jede Kommunikation auf der Bearbeitung von Personendaten über das Gegenüber beruht, eine Interaktion mit der Umwelt also stets einen Verzicht auf die Kontrolle über die eigenen Daten erfordert. Zumindest für das Verhältnis unter Privaten ist der Gedanke der informationellen Selbstbestimmung schon deshalb verfehlt. Dies erstaunt insofern nicht, als dieses Konzept in Europa bekanntlich im sog. Volkszählungsurteil vom deutschen Bundesverfassungsgericht etabliert worden ist, in dem aber nur das Verhältnis von Privaten und Staat infrage stand[48]. Auf dieses Verhältnis sollte das Konzept auch zurückgeführt werden.

Das Datenschutzrecht vermag das Konzept der informationellen Selbstbestimmung auch gar nicht umzusetzen. Denn den Interessen der betroffenen Personen an einer Kontrolle der Bearbeitung ihrer Daten stehen die regelmässig nicht minder wichtigen Interessen Dritter an der Bearbeitung dieser Daten gegenüber. In der Praxis kommt der Interessenabwägung als Rechtsgrundlage (DSGVO) oder Rechtfertigung (DSG) denn auch eine ungleich grössere Bedeutung zu als der Einwilligung[49]. Im Gegensatz zur Einwilligung, die sich unmittelbar auf die informationelle Selbstbestimmung abstützen lässt, steht die Interessenabwägung dieser Idee diametral entgegen. Allein dies macht deutlich, dass das Datenschutzrecht nicht als solches auf den Gedanken der informationellen Selbstbestimmung gestützt werden kann.

Über alternative konzeptionelle Grundlagen eines neuen Datenschutzrechts (oder eines anderen Regelungskonzeptes) wird man nachdenken müssen. Ein Ansatzpunkt für ein Neudenken für das Verhältnis unter Privaten könnte auf zwei Säulen beruhen: dem Schutz der Privatsphäre und dem Schutz gegen nachteilige Folgen von Datenbearbeitungen. Die erste Grundannahme eines solchen Ansatzes wäre, dass die Bearbeitung von Personendaten nicht *per se* problematisch ist und deshalb auch nicht *per se* umfassend geregelt werden muss. Bedarf nach einer Regelung besteht vielmehr nur, wenn die Bearbeitung von Daten die Privatsphäre verletzt oder nachteilige Folgen für die Betroffenen hat. Die zweite Grundannahme bestünde darin, dass nicht nur die physische, sondern auch die informationelle Privatsphäre geschützt sein muss, dass also alle Menschen in der Lage sein müssen, selbst darüber zu entscheiden, welche zur informationellen Privatsphäre gehörenden Daten an welche Dritten gelangen. Sind Daten aber rechtmässig an Dritte gelangt und haben sie damit die informationelle Privatsphäre verlassen, ist die weitere Bearbeitung der Daten durch diese Dritten frei. Erneut berührt wäre die informationelle Privatsphäre nur durch eine allfällige Weitergabe der Daten an Dritte.

Therapie 3: Fokus auf nachteilige Folgen

Der Fokus auf die Verhinderung nachteiliger Folgen von Datenbearbeitungen wird schon durch die Formulierung der Bundesverfassung nahegelegt, wonach jede Person Anspruch auf Schutz gegen den Missbrauch ihrer persönlichen Daten hat (Art. 13 Abs. 2 BV). Es drängt sich geradezu auf, diesen Missbrauch mit den nachteiligen Folgen gleichzusetzen, die sich für die betroffenen Personen aus der Bearbeitung ihrer Personendaten ergeben können, und das Vorliegen eines Missbrauchs zu verneinen, wenn es an solchen Folgen fehlt. Der hier vorgeschlagene Regelungsansatz lässt sich damit unmittelbar auf die verfassungsmässige Grundlage des Datenschutzrechts stützen und muss nicht, wie die Idee der informationellen Selbstbestimmung, kunstvoll in diese hineininterpretiert werden[50].

Bei den negativen Folgen stehen zwei Bereiche im Vordergrund: die Diskriminierung und die Manipulation[51]: Zum einen dürfen Menschen – auch durch Unternehmen – nicht aufgrund ihrer Daten diskriminiert werden, wenn keine sachlichen Gründe vorliegen. Ein solches privatrechtliches Diskriminierungsverbot ist zwar (noch) nicht allgemein anerkannt, wird aber in der Lehre vereinzelt schon heute aus dem allgemeinen Persönlichkeitsrecht abgeleitet[52]. Dieser Ansatz ist weiter zu verfolgen und zu vertiefen.

Zum andern dürfen Menschen nicht durch die Bearbeitung ihrer Daten manipuliert werden. Auch wenn dieses Problem in jüngerer Zeit breit diskutiert wird, stehen wir bei der Suche nach Lösungen noch ganz am Anfang. Gewisse Ansätze für die rechtliche Erfassung von Manipulation lassen sich immerhin im

---

48 Bundesverfassungsgerichtshof vom 15.12.1983, BVerfGE 65, 1.

49 Siehe dazu: Albers Marion/Veit Raoul-Darius, in: Brink/Wolff (Fn. 4), DSGVO 6 N 45; Future of Privacy Forum/NYMITY innovating compliance, Processing Personal Data on the Basis of Legitimate Interests under the GDPR: Practical Cases, abrufbar unter: <https://bit.ly/2rxQfjW>, 2; Veil (Fn. 37), 3343.

50 Siehe dazu: Belser (Fn. 19), § 6 Rz. 115 ff.; Flückiger (Fn. 19), 847; Maurer-Lambrou/Kunz (Fn. 19), DSG 1 N 18 f.; Rosenthal (Fn. 3), DSG 1 N 4.

51 Ebenso: Härting/Schneider (Fn. 2), Datenschutz in Europa, 308; dies. (Fn. 2), Das Ende des Datenschutzes, 820.

52 Arnet Ruth, Freiheit und Zwang beim Vertragsschluss, Zürich 2008, Rz. 356; Gauch Peter/Schluep Walter R./Schmid Jörg, OR AT, Band 1, 10. Aufl., Zürich 2014, Rz. 1111; Göksu Tarkan, Rassendiskriminierung beim Vertragsabschluss als Persönlichkeitsverletzung, Freiburg i.Ü. 2003, Rz. 214 ff.

Wettbewerbsrecht (UWG) finden, welches die Ausübung von Zwang gegenüber Konsumenten[53] und die Irreführung erfasst[54].

Beide Aspekte, der Schutz gegen Diskriminierung und gegen Manipulation, lassen sich im allgemeinen Persönlichkeitsrecht verorten. Das bedeutet freilich nicht, dass sich diese Probleme durch blosses Richterrecht in Anwendung von Art. 28 ZGB lösen liessen und keine neuen Normen erforderlich wären. Auch soll damit nichts über die systematische Einordnung einer allfälligen

digma 2019 S. 206, 213

neuen Regelung gesagt sein. Die Grundlage im Persönlichkeitsrecht legt aber nahe, dass nicht jede marginale Diskriminierung oder Manipulation zu erfassen wäre, sondern diese nachteiligen Folgen, wie im allgemeinen Persönlichkeitsrecht, eine «gewisse Intensität» erreichen müssten[55].

Schluss

Mit dem hier vorgeschlagenen Ansatz wäre man gedanklich schon weit weg vom umfassenden Ansatz des heutigen Datenschutzrechts, das unterschieds- und anlasslos jede Bearbeitung von Personendaten erfassen und – nach der DSGVO – nur beim Vorliegen einer Grundlage für die Rechtmässigkeit zulassen will. Dies bedeutet allerdings nicht, dass gewisse Grundkonzepte des heutigen Datenschutzrechts nicht auch in einem neuen Ansatz erhalten bleiben sollten. Das gilt namentlich für den Grundsatz der Transparenz, mitsamt dem Auskunftsrecht, und für den Grundsatz der Datensicherheit, dem künftig noch eine viel grössere Rolle zukommen wird.

Wesentliche Fortschritte auf dem Weg zur Genesung des Datenschutzrechts sind aber nur möglich, wenn wir den Finger auf die wunden Punkte der heutigen Regelung legen und bereit sind, den Datenschutz in seiner Gesamtheit noch einmal von Grund auf neu zu denken: Rethink Privacy!

---

53 Siehe dazu statt vieler: Jung Peter, in: Jung Peter/Spitz Philippe (Hrsg.), Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Kommentar, 2. Aufl., Bern 2016, UWG 2 N 35 ff.; Pichonnaz Pascal, in: Martenet Vincent/Pichonnaz Pascal (Hrsg.), Commentaire Romand, Loi contre la concurrence déloyale, Basel 2017, UWG 2 N 79, N 84; Ferrari Hofer Lorenza, in: Heizmann Reto/Loacker Leander D. (Hrsg.), UWG, Bundesgesetz gegen den unlauteren Wettbewerb, Kommentar, Zürich/St. Gallen 2018, UWG 2 N 78 ff.; Baudenbacher Carl, Lauterkeitsrecht, Kommentar zum Gesetz gegen den unlauteren Wettbewerb (UWG), Basel/Genf/München 2001, UWG 2 N 41 ff.; im Ansatz auch Hilty Reto M., in: Hilty Reto M./Arpagaus Reto (Hrsg.), Basler Kommentar Bundesgesetz gegen den unlauteren Wettbewerb (UWG), Kommentar, Basel 2013, UWG 2 N 89 f.

54 Art. 3 Abs. 1 Bst. b UWG.

55 Siehe dazu für das allgemeine Persönlichkeitsrecht: BGE 125 III 70; BGE 129 III 715; Büchler Andrea, in: Kren Kostkiewicz Jolanta/Wolf Stephan/Amstutz Marc/Fanmkhauser Roland (Hrsg.), Kommentar ZGB, 3. Aufl., Zürich 2016, ZGB 28 N 14; Meili Andreas, in: Geiser Thomas/Fountoulakis Christiana (Hrsg.), Basler Kommentar ZGB I, 6. Aufl., Basel 2018, ZGB 28 N 38.
(Alle URL letztmals kontrolliert am 23.10.2019.)