2.1.4 Privatheit
Zur Zukunft des Datenschutzes

Nils Leopold

I Privatheit in Gefahr

Wie sehr Privatheit und Selbstbestimmung gefährdet sind, insbesondere was staatliches Handeln angeht, zeigte zuletzt die durch die *Snowden-Enthüllungen* bekannt gewordene, weltumspannende geheimdienstliche Massenüberwachung. Denn der Präventionsstaat als spezielle Form des Überwachungsstaates zielt auf die effiziente Überwachung des Verhaltens der Bürger*innen mit digitalen Mitteln.

Was das Handeln privater Akteure angeht gewinnt seit Jahren der Konflikt um Datenökonomie und Privatheit an Schärfe. Der moderne Datenkapitalismus hat persönliche Daten zum flüssigen Gold erklärt. Wie schief oder falsch auch immer diese Formel sein mag,[1] die Betonung liegt stets auf dem Grundsatz: »Die Daten müssen fließen.« Der Skandal um Facebook und seine millionenfache Weitergabe von Kundendaten an das mit Wahlmanipulationen durch sogenanntes Microtargeting befasste Unternehmen Cambridge Analytica war ein Weckruf. Im Mittelpunkt der Auseinandersetzung steht die gewachsene Datenmacht großer Unternehmen. Ihre datengestützten digitalen Geschäftsmodelle verschieben die gesellschaftlich akzeptierten Grenzen grundlegend: Insbesondere Big Data und künstliche Intelligenz (KI) erlauben eine bislang nicht dagewesene feingranulare Auswertung und Überwachung der Datenspuren ganzer Bevölkerungen. Sie schaffen ein spezifisches Prognosewissen zur Manipulation von Menschen zu meist kommerziellen Zwecken.

1 Zutreffender dürfte es sich bei Daten in vielen Kontexten um gemeinwohlrelevante Grundlagen für das Wissen der Gesellschaft insgesamt handeln. Dementsprechend bedürfte es eher der Verständigung über weitere staatliche Interventionen zur Sicherung solcher gemeinwohlbezogener Verwertungen (Stichwort: Open Data).

Die Bürger*innen haben es weitgehend nicht mehr selbst in der Hand, durch ihr eigenes Verhalten einer Erfassung und digitalen Bewertung zu entgehen, selbst wenn sie bestimmte Angebote und Plattformen nicht nutzen.

Zugleich verändern der soziale und technische Wandel die Ideen und Leitbilder von Privatheit. Die geradezu klassisch zu nennende Vorstellung von Privatheit als einer Art individueller Kontrolle, also der Möglichkeit, selbst entscheiden zu können, wer wann Zugang zu den eigenen Angelegenheiten hat, scheint überholt. Müssen wir daher das Ende der Privatheit konstatieren?

Die These dieses Beitrages lautet: Nein – denn in der liberalen Demokratie muss sich nicht der Mensch in digitale Geschäftsmodelle und staatliche Effizienzkonzepte einfügen, sondern vielmehr muss es weiterhin darum gehen, den Einsatz digitaler Technik menschengerecht zu gestalten. Das Private ist politisch – das gilt auch, wenn es um seine Formung durch die Digitalisierung geht.

Wenn etwa zukünftig anhand algorithmenbasierter Auswertungen des Verhaltens in sozialen Netzwerken Kredite vergeben und Arbeitsstellen besetzt werden, wenn dabei selbst Personen, die sich nie auf entsprechenden Plattformen bewegt haben, diesen maschinenbasierten Prognosen unterworfen werden oder wenn Videoüberwachung in öffentlichen Räumen mit biometrischer Gesichtserkennung aufgerüstet wird, dann stehen grundlegende Machtverteilungsfragen der Gesellschaft auf dem Spiel. Auch die Auseinandersetzungen um die Corona-Warn-App oder um die Einführung von digitalen Impfpässen belegen, wie sehr gesellschaftliche Konflikte um neue Technologien von Fragen nach den Folgen für die Privatheit der Einzelnen und der Gesellschaft insgesamt geprägt sind. Man kann fast sagen: Wertegeleitete Diskurse rund um die Digitalisierung sind aktuell vor allem Privatheitsdiskurse.

Funktionen von Privatheit

Bei all diesen Konflikten geht es um Privatheit als Sicherung der individuellen Zugänglichkeitsgrenzen von Menschen. Es geht um den Erhalt von persönlichen Freiräumen. Die Funktionen der Privatheit sind dabei vielfältig. Privatheit wird etwa als Bedingung von Identität und Individualität, physischer oder emotionaler Entspannung beschrieben, als Bedingung der Möglichkeit von Kreativität und des Lernens, der Verhaltensvielfalt, von vertraulichen Nähebeziehungen, der Ausbildung und Ausfüllung einer Pluralität von Rollen

oder der individuellen Autonomie. Damit trägt sie auch zu einer pluralistischen Gesellschaft bei.[2]

Datenschutz als Schutzkonzept der Privatheit

Privatheit bildet einen entscheidenden Wert in der Digitalisierung, gerade weil digitale Verfahren und Instrumente die Grenzen persönlicher Freiräume grundlegend verschieben. Sie steht daher mit Recht im Mittelpunkt der politischen Debatte darum, wie Datenmacht einzuhegen ist. Daneben steht die Selbstbestimmung als Paradigma liberaler Rechtsordnungen, die ihre Verankerung unter anderem im Würdegebot des Grundgesetzes findet. Als Grundrecht auf Datenschutz der Grundrechte-Charta der EU sowie als Menschenrecht auf Privatheit haben die Konzepte von Privatheit und Selbstbestimmung längst weltweite normative Verbreitung gefunden.

Privatheit und Selbstbestimmung[3] gelten deshalb als Bollwerk zum Schutz von Freiheit und Autonomie, weil sie nicht bloß eine moralische Idee oder partikulare Ethik der Vernunft repräsentieren, sondern als bindendes Recht entfaltet sind. Vor allem das Datenschutzrecht enthält wichtige Steuerungselemente zum Schutz vor Überwachungsstaat und Überwachungskapitalismus.

Doch muss der Datenschutz auf mehreren Ebenen entschlossen weiterentwickelt werden, um angesichts der enormen gesellschaftlichen Herausforderung durch die Digitalisierung seiner Funktion weiterhin gerecht zu werden. Dabei werden Konzepte von Privatheit und Selbstbestimmung weit über den Datenschutz hinaus zu einer Ausdifferenzierung der Instrumente und gesellschaftlichen Antworten zum Schutz der Rechte der Bürger*innen führen müssen. Ansatzpunkte für die nötigen Weiterentwicklungen liefert auch die Kritik an Privatheit und Selbstbestimmung, deren genauere Analyse daher lohnt.

II Kritik an der Privatheit

Die Auseinandersetzungen um Privatheit und Selbstbestimmung in der Digitalisierung erfolgen in Wellenbewegungen. Eher selten schlägt das Pendel

2 Vgl. Albers, Marion: Grundrechtsschutz der Privatheit, in: DVBL 2010, S. 1062 m.w.N.

3 Siehe auch den Beitrag von Christiane Woopen und Sebastian Müller in diesem Band.

dabei stärker zugunsten der Privatheit aus. Zuletzt allerdings konnte dies beobachtet werden, als in einem europäischen Kraftakt die Datenschutz-Grundverordnung (DSGVO) verabschiedet wurde. Vorherrschend scheint aber ein Grundsound der Vergeblichkeit. Die sozialwissenschaftliche Kritik behauptet unter anderem, die Konzepte seien der Komplexität der Herausforderung nicht (mehr) gewachsen, seien ohne Rückhalt im konkreten Handeln der Bevölkerung, die freiwillig auch noch die fragwürdigsten digitalen Angebote in Anspruch nehme (Privacy Paradox). Daher kommen die Konzepte stets zu spät oder seien sogar gleich denklogisch ausgeschlossen.

Systemtheorie und Big Data

Zum Teil wird vertreten, Privatheit und Selbstbestimmung seien am Ende, weil die Digitalisierung letztlich eine evolutionäre, quasi zwingenden Gesetzmäßigkeiten folgende Entwicklung darstelle. Die dabei innerhalb von Systemlogiken handelnden Wirtschaftsunternehmen oder staatlichen Stellen seien in ihrem Verhalten letztlich nicht determinierbar. Das Funktionieren digitaler Technik sichere vielmehr seine Akzeptanz. Privatheit und Selbstbestimmung werden verkürzend als Konzepte individueller Kontrolle dargestellt. Das Besondere digitaler Technik im Allgemeinen als auch von Big Data im Besonderen liege darin, dass sie Informationen bei Dritten erzeugten, die sich also der Kontrolle der Einzelnen entziehen.[4] Insbesondere das Konzept der Einwilligung (unter anderem als Cookie-Banner bekannt) laufe vor dem Hintergrund von Big Data leer, weil es letztlich nur eine kurzfristige Handlungshemmung in einer ansonsten überwiegend im Unbewussten ablaufenden Digitalnutzung setze.

Der Kritik ist darin zuzustimmen, dass sie einige der mit den überindividuellen Auswirkungen von Big Data verbundenen konzeptionellen Fragen für Selbstbestimmung und zunehmend fragwürdige Instrumente wie die Einwilligung aufgreift. Eine umfängliche Debatte im Datenschutz setzt sich seit langem mit der Frage auseinander, welche zusätzlichen Elemente die Relevanz dieses Instruments erhalten können. Nicht überzeugend ist die Suggestion

4 »Die Digitaltechnik mit ihren detektivischen Funktionen ist ein Mittler, der mich dazu bringt, etwas zu tun, was ich nicht selbst kontrollieren kann«, vgl.: Nassehi, Armin: Muster. Theorie der digitalen Gesellschaft, Bundeszentrale für politische Bildung, 2020, S. 315.

einer Alternativlosigkeit in der Gestaltung digitaler Anwendungen. Stets bestehen Handlungsoptionen, und der weitere gesellschaftliche Handlungsrahmen wird durch Politik und Recht mitbestimmt. Überholt ist jedoch das konzeptionelle Verständnis von Privatheit als individueller Kontrolle. Vielmehr wird Privatheit etwa im Datenschutz seit langem durch ein wesentlich breiteres präventives Konzept aus einer Vielzahl von Elementen geschützt, mit denen auf die die Informationen verarbeitende Organisation abgezielt wird (interne Datenschutzvorgaben, Rechtmäßigkeitskontrolle, Privacy by Design-Vorgaben usw.). Individuelle Kontrolle, etwa in Gestalt der Einwilligung, ist lediglich ein steuerndes Element, und unterliegt selbst weiteren zum Schutz der Betroffenen eingezogenen Beschränkungen.

Der Vorwurf der Fehlkonstruktion

Ein Kritikansatz betont konzeptionelle Mängel des Datenschutzrechts. Unterstellt wird ein allgemeines Verbot unterschiedslos allen personenbezogenen Datenverarbeitungen, egal ob es sich um Facebook oder den Bäcker an der Ecke handele. Stattdessen bedürfe es des Grundsatzes des freien Flusses von Daten, nur in besonderen Fällen müsse gesetzlich geregelt werden. Mit dem sogenannten »Verbotsvorbehalt« werde eine risikobezogene Unterscheidung von höchst unterschiedlichen digitalen Anwendungen unmöglich gemacht.

Diese Kritik überbetont einen letztlich rechtskonstruktiven Aspekt. In der Praxis bestehen für kleine und mittlere Unternehmen alle rechtlichen Freiheiten, die benötigten Daten zu verarbeiten. Richtig ist allerdings, dass viele kleine Unternehmen bedeutend geringere Risiken für die Privatheit von Kund*innen oder Beschäftigten darstellen. Erleichterungen von den zahlreichen Anforderungen der Datenschutzgesetze erscheinen daher ausbaufähig.

Datenschutz als Innovationsbremse und Bürokratieklotz

In diesem Gewand kommt politisch motivierte Kritik des Datenschutzes typischerweise daher. Zumeist fehlen Argumente, die den Vorwurf untermauern. Auch wird er häufig herangezogen, um von anderweitigen Missständen im Bereich unternehmerischer oder staatlicher Digitalisierungsvorhaben abzulenken. Der Datenschutz wird somit als Sündenbock genutzt. Oft scheint diese Kritik auch der parteipolitischen Profilierung zu dienen, weil sie als Ausweis der eigenen Fortschritts- und Wirtschaftsfreundlichkeit verstanden sein will.

Diese Kritik erschwert die Weiterentwicklung des Datenschutzes ungemein. Sie verstärkt bestehende Widerstände in Organisationen und erschwert sachbezogene Auseinandersetzungen. Die Unterstellung einer allgemeinen Innovationshemmung ist abwegig. Ob und in welchem Umfang etwa ein digitales Geschäftsmodell als innovativ bezeichnet werden kann, entscheidet sich auch nach seinen Gemeinwohlwirkungen. Letztlich stellen Datenschutzüberlegungen auch Faktoren der Akzeptanz von digitalen Anwendungen dar. Nachweisbare Datenschutzvorkehrungen schaffen Vertrauen bei Kund*innen und Bürger*innen.

Die Wahrnehmung von Privatheit wird auch durch Bewertungen des digitalen Wandels in seiner Gesamtheit beeinflusst. So wird in der Debatte um Künstliche Intelligenz fundamentaler Zweifel am menschlichen Selbstverständnis freier Selbstbestimmung laut. Die Vorstellung von Menschen als individuelle autonome Entscheidungsträger sei aufgrund der Überlegenheit KI-gestützter, durchdigitalisierter Umgebungen nicht mehr aufrecht zu erhalten.[5] Richtig ist vielmehr, dass Konzeptionen von Privatheit und Selbstbestimmung schon heute ein differenziertes Verständnis menschlicher Autonomie zugrunde legen. Ob und in welchem Umfang ein Schutz gewährleistet werden kann, bleibt letztlich eine Frage der politischen Verständigung.

Die allermeisten Klagegesänge haben der Privatheit letztlich nichts anhaben können. Im Gegenteil zeigt sich: Privatheit ist mehr denn je tragende Säule der Digitalisierung, weil sie ein diverses, sich ständig wandelndes Konzept und Denkmuster ist: Als privat kann bezeichnet – und muss geschützt – werden, was jeweils die Funktionen von Privatheit erfüllt.[6]

Zudem ist sie im Recht – den Grundrechten des Grundgesetzes ebenso wie dem europäischen Recht und den internationalen Menschenrechtsregimen – tief verankert. Daran kommt auch die sozialwissenschaftliche und politisch motivierte Kritik nicht vorbei. Allerdings verweisen einige der hier angeführten Kritikbeispiele auf Modernisierungsbedarf insbesondere beim Datenschutzrecht.

5 Vgl. u.a. Harari, Yuval, Harari: Homo Deus, München: C.H. Beck 2018.
6 Vgl. Albers, a.a.O., S. 1063.

III Datenschutz: Plötzlich im Mittelpunkt

Der Datenschutz hat weltweit Konjunktur. Nach neuen Datenschutzgesetzen in Ländern wie Japan, Brasilien und Thailand ist am 1. Januar 2020 sogar in Kalifornien, am Ursprungsort des Überwachungskapitalismus, der California Consumer Privacy Act (CCPA) in Kraft getreten. Er orientiert sich in vielem an deutschen und europäischen Datenschutzregelungen für die Wirtschaft und öffentliche Institutionen.[7] Insbesondere die Datenschutz-Grundverordnung (DSGVO) der EU gilt als globaler Goldstandard der Gesetzgebung.[8]

Allerdings sollte man die bloße Schaffung von Gesetzen nicht überbewerten. Schließlich entscheidet über deren tatsächliche Bedeutung und Wirkung erst der gesellschaftliche und kulturelle Zusammenhang, in dem sie zur Anwendung kommen. So boten etwa das ausgefeilte Bundesdatenschutzgesetz über Jahrzehnte einen eher geringen Schutz der Rechte der Bürger*innen, weil es kaum durchgesetzt wurde. Private Akteure jedenfalls ignorierten über Jahre dessen Vorgaben größtenteils und betrachteten es als bloßen Papiertiger.

Die 2018 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) hat diese Lage wesentlich verändert. Die EU beendete damit ihre gut 20 Jahre andauernde eigene Laissez-faire-Haltung in Sachen Digitalisierung und Privatheit. Denn die effektive Umsetzung stellt einen der Schwerpunkte des Gesetzes dar.

Möglich war das politisch wohl nur aufgrund einiger besonderer Umstände. In der EU war über Jahre der Eindruck gewachsen, man habe vor allem den großen US-Unternehmen der Digitalwirtschaft wirtschaftlich nichts entgegenzusetzen. Aufwändige Kartellverfahren gegen Google oder Microsoft zogen sich lange hin, selbst Strafen in Milliardenhöhe schienen keine Wirkung zu haben. Angebote und Plattformen dieser Unternehmen dominieren nach wie vor die verschiedenen Märkte in einer Weise, die zu massiven Abhängigkeiten europäischer Unternehmen führt. Echten Handlungsdruck erzeugten schließlich die Bedrohungen für so etablierte europäische Wirtschaftszweige

7 Er ist zwar nicht auf EU-Bürger anwendbar, deren Daten im Silicon Valley verarbeitet werden. Seine Existenz hat allerdings Auswirkungen auf die lange geführte US-Debatte um die Schaffung einer möglichen bundesstaatlichen Regelung. Zum Teil geht der CCPA sogar darüber hinaus.

8 Vgl. Bradford, Anu: The Brussels Effect. How the European Union Rules the World, Oxford: Oxford University Press 2020.

wie das Automobilgeschäft. Vor diesem Hintergrund waren womöglich wettbewerbsförderliche Korrekturen von Geschäftsmodellen zumindest in Teilen auch über die Datenschutzgesetzgebung erreichbar und daher auch für europäische Wirtschaftskreise akzeptabel. Und die großen US-Digitalkonzerne konnten so immerhin auf mehr Rechtssicherheit und ein *level playing field* (gleiche Wettbewerbsbedingungen) in Europa setzen.

Stets spielt dabei auch das Ziel der Datensouveränität eine gewisse Rolle. Es fasst im Wesentlichen die Bereitschaft Europas zusammen, eine gegenüber den dominanten Digitalmächten USA und China eigenständige Datenpolitik zu verfolgen, um die heimische Wirtschaft vor Abhängigkeiten zu schützen.

Doch auch und insbesondere der bundesdeutsche und europäische Datenschutzdiskurs haben die DSGVO ermöglicht. Der Unmut über das Geschäftsgebaren von Unternehmen wie Facebook, Google und Co. und deren offenkundiger Unwille zu mehr Transparenz und Mitbestimmung über die kommerzielle Verwertung der kundenbeziehbaren Informationen und Daten war und ist groß. Mitten in die Umsetzungsphase des Gesetzes fielen im Sommer 2013 dann die Veröffentlichungen des Whistleblowers Edward Snowden. Sie gaben der DSGVO Rückenwind. Schwere Irritationen löste die mit den Snowden-Leaks verursachte Erkenntnis aus, wie sehr Europa in ein weltumspannendes Netzwerk von Massendatenabgriffen westlicher Geheimdienste verstrickt ist. Das totalitäre Potenzial der modernen Datenverarbeitung wurde sichtbar. Zumindest lag es nicht fern, Privatheit als eine vor dem Untergang zu bewahrende kulturelle Leistung moderner demokratischer Gesellschaften wahrzunehmen. Immerhin hatte der Geheimdienstskandal damit seinen Anteil daran, dass der schillernde Begriff der digitalen Souveränität seinen Eingang in die Datendebatten fand.[9]

Heute steht die EU mit der DSGVO im Wettbewerb mit den streng marktliberal ausgerichteten, datenschutzarmen USA und dem autoritären, auf Überwachung der Gesamtbevölkerung abzielenden China als Leuchtturm grundrechtlicher und rechtsstaatlicher Bürgerorientierung da.

Die DSGVO kommt in den EU-Mitgliedstaaten unmittelbar zur Anwendung, was die Möglichkeiten, ihre Vorgaben zu umgehen, entscheidend verringert. Massive Sanktionsandrohungen und gerichtliche Klagen von Betroffenen verschafften dem Datenschutz erstmalig die volle Aufmerksamkeit auch in den Chefetagen. Der Anwendungsbereich wurde auf alle

9 Siehe hierzu auch den Beitrag von Julia Pohle und Thorsten Thiel in diesem Band.

Unternehmen ausgeweitet, die mit ihren Produkten und Dienstleistungen den europäischen Markt erreichen (Marktortprinzip). Das zwang sogar die sogenannten GAFA plus M[10], sich mit der DSGVO auseinanderzusetzen. Erst kürzlich erklärte der Europäische Gerichtshof dann in der spektakulären Schrems-II-Entscheidung auf Grundlage der DSGVO das EU-Abkommen mit den USA über Datenübermittlungen in die USA für unwirksam. Damit wurden auf einen Schlag sämtliche Datenflüsse in die USA von Unternehmen mit Kunden in Europa rechtlich unsicher. Denn das Urteil lässt offen, in welchem Umfang bestehende rechtliche Instrumente diesen Datenflüssen weiter als Grundlage dienen können. Das Urteil war eine Reaktion auf den umfassenden Zugriff von US-Geheimdiensten auf die Daten der Digitalunternehmen, und auf den nicht mit Europa vergleichbaren Schutzstandard für Daten in den USA. Zwar bleibt damit die Rechtsunsicherheit der vielen betroffenen Unternehmen hoch und eine tragfähige Rechtsgrundlage für die Datenflüsse fehlt weiterhin. Doch der Datenschutz ist zu einer rechtlichen Größe gewachsen, mit der gerechnet werden muss.

Auf den zweiten Blick sieht es für den Datenschutz kurz- bis mittelfristig weniger rosig aus. Zumindest die EU-Kommission und die Datenschutzaufsichtsbehörden stehen unter Druck, viele Bestimmungen der DSGVO erst noch tatsächlich umzusetzen. Es hakt unter anderem bei der Abstimmung zwischen den Aufsichtsbehörden, ausgerechnet die Quasi-Monopolisten wie Facebook und Co. konnten bislang nicht belangt werden. Ungemach droht dem Datenschutz auch und gerade aus der Politik. Dort steigt der Druck, endlich Erfolge bei der Digitalisierung der Verwaltung, dem sogenannten E-Government, vorzuweisen. Der Datenschutz wird oft als störend wahrgenommen, übergangen oder als Sündenbock für gescheiterte Digitalprojekte missbraucht. Die immer wieder aufflammende Debatte um den Datenschutz als vorgebliches Hindernis bei der Corona-Bekämpfung steht stellvertretend für diesen Umgang. Die etablierte EU-Wirtschaft schließlich sieht sich durch die Digital-Konkurrenz aus China und den USA bedroht und fordert deshalb massive Unterstützung beim Aufbau datengetriebener Märkte. Die Politik gibt diesem Druck zunehmend nach, zugleich sträubt sie sich dagegen, nach

10 Google, Amazon, Facebook, Apple und Microsoft

der Verabschiedung der DSGVO noch eine weitere rote Linie zum Schutz der Bürger*innenrechte zu ziehen.[11]

Auch die Corona-Pandemie spitzt viele liegen gebliebene oder verdrängte Probleme der Digitalisierung weiter zu. Der Druck zur sofortigen Digitalisierung, etwa im Bereich der Schulen, erzwingt pragmatische Entscheidungen und legt gnadenlos die Überforderung der zuständigen Behörden offen. Diese sind beispielsweise weder rechtlich noch faktisch in der Lage, Videokonferenzsoftware auf Datenschutzkonformität zu prüfen und Empfehlungen auszusprechen, ohne mit dem Risiko längerer Gerichtsverfahren gegen ihre Bewertungen rechnen zu müssen. Derweil sind fast die einzigen Profiteure der Pandemie die Quasi-Monopolisten der Digitalwirtschaft, deren Einfluss auch in der EU beständig zunimmt und die weiterhin als Quasi-Gesetzgeber Standards in ihrem Einflussbereich setzen. Hier bleibt der Gesetzgeber gefordert, im Rahmen der Plattformregulierung seinen grundrechtlichen Schutzpflichten nachzukommen und gegebenenfalls bis hin zu Entflechtungen der betreffenden Konzerne die Grundrechte der Bürger*innen durchzusetzen.

Was schützt der Datenschutz?

Was genau aber schützt der Datenschutz? Die Antwort weist den Weg, wie der Datenschutz weiterzuentwickeln ist.

Lange Jahre dümpelte der Datenschutz als Steckenpferd früher Informatiker*innen und Nischenjurist*innen in einem eher akademischen Abseits. Vieles änderte sich mit dem Volkszählungsurteil von 1983. Vorausgegangen waren breite Proteste in der Bevölkerung gegen Art und Umfang dieser Datenerhebung. Das Bundesverfassungsgericht schuf aus unterschiedlichen anerkannten Strängen des Grundrechts auf Achtung der freien Entfaltung der Persönlichkeit ein auf die Datenwelt zugeschnittenes, eher weit angelegtes Recht auf informationelle Selbstbestimmung.[12]

Vor dem Urteil galten Inhalte und Daten allerdings nur dann als schützenswert, wenn sie der *Privatsphäre* entstammten, also die Privatheit ihres Entstehungskontextes teilten.[13] Digitalisierung aber verselbstständigt gera-

11 Insoweit beispielhaft erscheinen die Verzögerungen um die sogenannte E-Privacy-Verordnung, die ursprünglich mit der DSGVO verabschiedet werden sollte und Regelungen zum Schutz der Onlinekommunikation vorsieht.

12 Siehe hierzu auch den Beitrag von Ulf Buermeyer und Malte Spitz in diesem Band.

13 Vgl. dazu die maßgebliche Untersuchung von Albers, Marion: Informationelle Selbstbestimmung, Baden-Baden: Nomos 2001.

de Informationen gegenüber ihrem Entstehungszusammenhang. Wer etwa seine private Kommunikation über das auf Vernetzung und Werbung ausgelegte Unternehmen Facebook führt, bewegt sich angesichts der entstehenden und nicht steuerbaren zusätzlichen Datenerfassungen nicht mehr in einem als privat zu bezeichnenden Raum. Kontextverlust ist Kennzeichen und insoweit Ziel der Datenverarbeitung, als gerade eine multifunktionale Verwendung von Daten angestrebt wird. Besonders deutlich wird das im heutigen Paradigma der Kombination aus Big Data und Techniken der KI, mit denen beliebige Korrelationen von Datenbeständen für statistische Prognosen ermöglicht werden. Am prominentesten wird die breite Nutzung von Gesundheitsdaten diskutiert. Der Datenschutz bietet hier ein weit angelegtes Schutzkonzept mit verschiedenen Schutzelementen, wie der Zweckbindung von Datenverarbeitungen, der Notwendigkeit von Rechtsgrundlagen, von Transparenz, Beteiligungsrechten und effektiver Aufsicht. Das Bundesverfassungsgericht bestätigte mit dem Volkszählungsurteil dieses Konzept im Wesentlichen innerhalb des Rechts auf informationelle Selbstbestimmung, das damit weit über technischen Datenschutz hinausreicht.

Der Umgang des Staates mit persönlichen Informationen und Daten wurde danach vom Bundesverfassungsgericht zielgenauer bearbeitet: Spezielle weitere Rechte wie das Recht am eigenen Wort, am eigenen Bild, das allgemeine Persönlichkeitsrecht oder auch das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (das sogenannte IT-Grundrecht) wurden geschaffen. Mit dieser Auffächerung setzte das Bundesverfassungsgericht eine Dimension des Volkszählungsurteils um, wonach erst der konkrete Verwendungskontext von Daten über den Schutzbedarf entscheidet.

It's the infomation, stupid

Im Volkszählungsurteil schlummert eine weitere Grundentscheidung. Anders als die bis dahin bestehenden Datenschutzgesetze, die sich eng auf die Verarbeitung personenbezogener Daten konzentrieren, wurde das Recht auf informationelle Selbstbestimmung eben gerade nicht allein als Recht am eigenen Datum, sondern gleich eine ganze Dimension höher angelegt.[14] Statt eines eigentumsanalogen Verständnisses, wonach Daten natürlichen Personen

14 So zutreffend Forgó, Rn. 33, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, München: C.H. Beck, 3. Auflage 2019.

praktisch *gehören*, wurden übergreifend *Selbstbestimmungsrechte* für diejenigen geschaffen, die von Datenverarbeitungsprozessen betroffen sind. Die Bürger*innen bestimmen zum Teil darüber mit, ob und in welchem Umfang die sie betreffenden Informationen und Daten verarbeitet werden dürfen. Dementsprechend steht heute die Einwilligung als Rechtsgrundlage für Verarbeitungen im Mittelpunkt, aber auch etwa Auskunftsrechte, Widerspruchs- und Löschungsrechte.

Auf Grundlage dieses Urteils zeigte sich in der Rechtswissenschaft[15] schon bald: Eigentlich geht es nicht um Datenschutzrecht, sondern um ein Recht des Umgangs mit personenbezogenen Informationen und Daten.[16] Man kommt ohne die Unterscheidung von Informationen und Daten nicht mehr aus: Informationen sind die eigentliche Leitkategorie, nicht Daten. Daten sind die auf einem Datenträger sehr selektiv festgehaltenen Zeichen, die als Informationsgrundlagen dienen. Als bloße Zeichen weisen sie für sich allein auch keinen Personenbezug auf.

Informationen hingegen betreffen den Sinn, der aus Beobachtungen, Mitteilungen oder Daten erst erzeugt werden kann und muss. Informationsinhalte knüpfen also an Daten an, doch sie setzen auch eine aktive Interpretationsleistung des sinnhaften Verstehens der empfangenden Stelle oder Institution voraus. Damit rücken die Behörden oder Unternehmen und deren Prozesse in den Vordergrund. Deren interne Prozesse bilden einen Wissens- und Interpretationskontext, der auch ihr Handeln bestimmt. Deutlich wird: Wer den Umgang mit diesen personenbeziehbaren Daten effektiv schützen will, muss auf dieser empfangenden und verarbeitenden Seite durch präventive Vorgaben regulieren. Letztlich wird damit erst klar, wo die Risiken liegen, und wie weitgehend die Vorgaben des Rechts sein müssen, um die Betroffenen wirksam zu schützen. Der Schutz vor Staat und Wirtschaft hat inzwischen vergleichbaren Umfang, auch wenn er juristisch anders hergeleitet wird. Die Risiken für die Privatheit mögen im Einzelnen anders gelagert sein, erscheinen aber im Bereich der Wirtschaft heute vielfach tiefgreifender. Zudem behalten sich staatliche Stellen auch hier den Zugriff vor.

15 Grundlegend: Albers, Marion: Informationelle Selbstbestimmung, Baden-Baden: Nomos 2005.

16 Mit dem Telekommunikationsgeheimnis in Artikel 10 des Grundgesetzes gibt es eine spezifische Schutzausprägung von Kommunikationen und allen dabei anfallenden Daten.

Die neuen (und alten) Herausforderungen der Digitalisierung

Der Datenschutz musste sich in Reaktion auf neue Entwicklungen der IT-Industrie beständig fortentwickeln, um den durch die informationelle Selbstbestimmung gebotenen Schutzstandard zu gewährleisten. Bedeutende Weiterentwicklungen lagen in Konzepten von Zertifizierungen und Audits, dem Privacy by Design, dem Selbstdatenschutz oder der Transparenz von Technik.[17] Den Aufsichtsbehörden wird viel Konkretisierungsarbeit bei der Auslegung von Gesetzen überlassen. Doch für einzelne Entwicklungen wird dieser bestehende allgemeine Rahmen kaum mehr genügen.

Bereits während der Verhandlungen zur DSGVO wurde die vielgestaltige Nutzbarkeit von Big Data in Verbindung mit KI als offenkundig grundlegende Veränderung in Wirtschaft und Verwaltung erkannt. Dabei geht es um technische Systeme, die so konzipiert sind, dass sie Probleme eigenständig bearbeiten und sich selbst auf veränderliche Bedingungen einstellen können. Systeme künstlicher Intelligenz basieren auf der Analyse von Massen von Daten (Big Data), die zum ständigen Trainieren der Algorithmen gebraucht werden. Noch geht es um die auf bestimmte Ziele beschränkte, schwache KI und um überwiegend unterstützende Aufgaben. Doch zukünftig werden mit der sogenannten starken KI Systeme entstehen, die in der Lage sind, die Vorgaben der Programmierung zu verlassen und eigenständige kognitive Fähigkeiten aufzubauen. Sie sind mehr als je zuvor bei digitaler Technologie eine Black Box. Sie sind insbesondere mit der Auswertung großer Datenmengen (Big Data) befasst, um Prognosen zu erstellen und komplexe Prozesse zu steuern. Als ein Beispiel gilt das selbstfahrende Auto. Sensorgestützte Umwelten der Datenerfassung, die wiederum digitale Zwillinge analoger Umgebungen zu erstellen suchen, bilden die Grundlage. Deren Daten werden den sogenannten Big-Data-Reservoirs (z.B. in Gestalt von Cloud-Datenspeichern) zur Verfügung gestellt, die als Datenpools für das Trainieren der Algorithmen dienen. Es handelt sich um eine übergreifende, alle Wirtschafts- und Gesellschaftsbereiche erfassende IT-Entwicklung: Von der Krebsbekämpfung über Predictive Policing (vorhersagende Polizeiarbeit) bis zum autonomen Fahren soll KI die technische Grundlage für Innovationen und neue Geschäftsmodelle bilden

17 Zu den vielfältigen Ambivalenzen dieser Ansätze vgl. z.B.: Richter, Philipp: Big Data, Statistik und die Datenschutz-Grundverordnung, in: Datenschutz und Datensicherheit 2016, S. 91.

und Entscheidungsprozesse steuern. Die beschriebenen Herausforderungen lassen sich unter anderem durch die folgenden Ansätze angehen.

(1) Anonymisierung und Personenbezug

Gerade bei Big-Data-Analysen ist vorab unklar, wofür Daten verarbeitet werden. Zusätzlich ist es für Aufsichtsbehörden kaum möglich, die Transparenz der Funktionsweise und Nachvollziehbarkeit (Revisibilität) zu sichern. Und Anwender*innen versuchen durch vollständige Anonymisierung den Anwendungsbereich des Datenschutzes gänzlich zu meiden. Doch gelingt eine vollständige Anonymisierung im heutigen Umfeld der Datenverarbeitung faktisch kaum noch oder nicht dauerhaft zuverlässig. Dynamische Veränderungen der Datensätze und auch wachsendes Zusatzwissen wie etwa durch Open-Data-Datenbanken erlauben die De-Anonymisierung.

Dieser Befund stellt daher die bislang auch vom Gesetzgeber vehement vorgenommene Trennung personenbezogener und nicht-personenbezogener Daten infrage. Wenn heute scheinbar anonyme Datenbestände durch die erwartbare Art und Weise ihrer Verarbeitung zu irgendeinem Zeitpunkt doch wieder personenbeziehbar werden, liegt es nahe, auch die bisherige völlige Befreiung nicht-personenbezogener Daten vom rechtlichen Regime des Datenschutzes anzuzweifeln. Damit gerät auch der Glauben an die schützenden Wirkungen der Anonymisierung, an den sich auch der Gesetzgeber klammert, ins Wanken.

(2) Daten als kommerzielle Güter und Innovationsressource

Die neuen Technologien entwickeln sich im internationalen Wettbewerb der Datenökonomien.[18] Aus ökonomischer Sicht werden personenbezogene Daten längst als kommerzielle Güter bewertet und auch gehandelt. Beispielhaft stehen hierfür die gigantischen Werttaxierungen der großen IT-Unternehmen sowie die in der Praxis von Unternehmenskäufen entscheidende Due-Diligence-Prüfung (sorgfältige Prüfung) auch der personenbezogenen Datenbestände zur Werterhebung und Kaufpreisbildung. Politisch erfahren derzeit Datenstrategien und KI-Entwicklungen allerhöchste Priorität und Förderung. Im Kern geht es darum, Datennutzung, Datentausch und Datenhandel zu ermöglichen und zu fördern, um die für die digitale und insbesondere die KI-Wirtschaft erforderlichen massenhaften Datenbestände zu erschließen. Neben der Öffnung von (zunächst) nicht-

18 Lesenswert: Datenökonomie, APuZ, 60. Jahrgang, 2019.

personenbezogenen Daten sollen dabei stets auch personenbezogene Datenbestände mobilisiert und besser handelbar werden. Beispielsweise werden vermehrt sogenannte Datentreuhänder und datenaltruistische Organisationen in Stellung gebracht.[19] Unabhängig von diesen gesetzgeberischen Anstrengungen besteht ein weltweit organisierter, sehr weitgehender grauer Handel mit personenbezogenen Daten.

(3) Einwilligungsfragen und kollektive Wirkungen durch Datenverarbeitung
Das bestehende Datenschutzregime bleibt individualistisch ausgerichtet. Der Schutz der oder des Einzelnen steht im Mittelpunkt. Konsequenterweise steht im privaten Sektor die individuelle Einwilligung zur Datenverarbeitung im Mittelpunkt. Diese ist im Kontext des Internets und komplexer Datenverarbeitungen schon lange als problembehaftet erkannt, wenn nicht dysfunktional geworden. Die Allgemeinen Geschäftsbedingungen der Anbieter sind unlesbar, überfordern und fallen damit als Informationsquelle für die Betroffenen aus.[20] Die allermeisten Menschen klicken sich ritualisiert durch. Das beste Beispiel bieten die mit Inkrafttreten der DSGVO noch penetranteren sogenannten Cookie-Banner. Hier blockiert die Werbeindustrie weiterhin nutzerfreundliche technische Lösungen etwa durch sogenannte Do-not track-Browser-Voreinstellungen.

IV Die Weiterentwicklung des Datenschutzes

Recht bietet stets hochselektive, notwendig unvollkommene Antworten auf komplexe gesellschaftliche Problemlagen. Aber es ist ein wichtiger Teil einer Immunantwort rechtsstaatlich gefasster Gesellschaften auf die Folgen des digitalen Wandels.

Der Datenschutz und das bestehende Datenschutzrecht werden in den kommenden Jahren im Wesentlichen fortbestehen. Dafür hat schon die umfassende Aufnahme des Konzepts in die DSGVO gesorgt. Um den Erfolg der DSGVO zu bewahren, bedarf es in den kommenden Jahren großer Anstrengungen der EU-Kommission, der Aufsichtsbehörden der Mitgliedstaaten, des

19 Vgl. etwa den Entwurf des Data Governance Act vom 25.11.2020, COM (2020) 767 final. Mit dem sog. Data Act wird für Herbst 2021 gerechnet.

20 Fallen die Begleittexte zu schlicht aus, bergen sie allerdings das Risiko des Überlesens wichtiger Konsequenzen, ebenfalls ein Dilemma.

Europäischen Datenschutzausschusses als ihr Koordinierungsgremium und der Regierungen der EU-Mitgliedstaaten. Der Nachweis der Vollziehbarkeit dieses Rechts steht im Mittelpunkt. Wo irgend möglich, muss die Aufsicht effizienter konstruiert und auf die wirklich wesentlichen Aufgaben der Rechtsdurchsetzung gegenüber besonders risikoreichen Verfahren und Anwendungen ausgerichtet werden.

Doch daneben zeichnen sich notwendige gesetzliche und konzeptionelle Weiterentwicklungen ab.

Zum einen gilt dies für die DSGVO selbst. Viele ihrer Bestimmungen sind notwendig abstrakt und unpräzise. Oft wird die Konkretisierung der Bestimmungen insoweit durch den Europäischen Datenschutzausschuss der Aufsichtsbehörden und die Gerichte erfolgen müssen. Doch teilweise wird das nicht ausreichen. Ein Beispiel bietet die Regelung von automatisierten Entscheidungen beziehungsweise des Profilings. Die entsprechende Norm des Artikels 22 DSGVO regelt ausgerechnet die vielfältigen Risiken, die mit Profilbildungen einhergehen, äußerst unzureichend. Für zahlreiche andere Bestimmungen erscheinen Präzisierungen der Normen im Sinne der Rechte der Verbraucher*innen diskussionswürdig.[21]

Von grundlegenderer Bedeutung ist die durchgängige bessere Differenzierung von Datenverarbeitungen nach ihren tatsächlichen Risiken. Während wegen des Grundsatzes der Technikneutralität bestimmte Formen der Datenverarbeitung wie Big Data, Cloud Computing oder KI in ihren Funktionen nicht gezielt geregelt werden, gelten viele der Grundsätze des Datenschutzes in praktisch gleichem Umfang auch für kleine Unternehmen, die im Schwerpunkt gar nicht mit der Verarbeitung von Daten befasst sind. Hier muss letztlich, auch im Sinne der Fokussierung und der Akzeptanz des Datenschutzes, zukünftig besser abgeschichtet werden.

Besonders hervorzuheben sind notwendige Verbesserungen zum Schutz von unbeteiligten Dritten. Big-Data-Analysen und selbstlernende algorithmenbasierte Entscheidungsverfahren liefern umfassende statistische Prognosegrundlagen. So werden auch Personen und Personengruppen bewertet und womöglich diskriminierend schlechter gestellt, die selbst gar nicht notwendigerweise durch ihre Daten an der Herstellung der Bewertungsgrundlagen mitgewirkt haben. Ehepartner*innen und Familienangehörige etwa erhalten aufgrund ihrer Nähe zur betroffenen Person

21 Umfangreiche Vorschläge für mögliche Änderungen finden sich bei Roßnagel/Geminn: Datenschutz-Grundverordnung verbessern, Baden-Baden: Nomos 2020.

vergleichbare Kreditbewertungen. Ähnliches geschieht beim Geoscoring, bei dem alle Bewohner*innen einer Straße oder eines Stadtviertels aufgrund der statistisch errechneten Dichte von Kreditrisiken einsortiert werden. Bei der Verarbeitung genetischer Daten einer Person sind automatisch alle näher Verwandten mit betroffen. Diese womöglich auch gänzlich anonymen Verfahren bewirken eine kollektive Vergemeinschaftung bestimmter Merkmalsträger[22] und können das Handeln Betroffener weitreichend bestimmen, wenn sie sich entsprechend anpassen, um bestimmten Mustern statistischer Normalität zu entsprechen. Die damit verbundenen Fragen weisen über das Datenschutzrecht teilweise deutlich hinaus und adäquate Schutzvorkehrungen müssen gefunden werden. Ein grundlegendes, bislang nicht gelöstes Problem stellt schließlich auch die Reproduktion von Diskriminierungen in den Algorithmen dar. So kam es vor, dass biometrische Gesichtserkennung Menschen mit dunkler Hautfarbe überhaupt nicht erkannte.[23]

Grundsätzlich bietet der Datenschutz zwar ein überaus breites Anwendungsfeld mit je nach Kontext seines Einsatzes ganz unterschiedlichen Schutzgegenständen. So können beispielsweise Maßnahmen zum Schutz vor Diskriminierungen bereits im Rahmen von bestehenden gesetzlichen Vorgaben für soziale Netzwerke zur Anwendung kommen. Sogenannte Dark Patterns von Plattformangeboten, also Designs von Oberflächen mit dem Ziel, zu bestimmten Handlungen zu verleiten, können die Freiwilligkeit von Einwilligungen berühren und verdienen nähere Beachtung. Gerade für den Bereich von Big Data und KI bedarf es aber der Weiterentwicklung und problemgerechten Erweiterung der Normen. Eine nach Risiken der Anwendungen abgestufte Regelung, wie etwa von der Datenethikkommission der Bundesregierung vorgeschlagen, sichert eine differenzierte gesetzliche Bewertung.

Auf einer grundlegenden konzeptionellen Ebene wird der Datenschutz nicht um die Klärung einiger Grundlagen herumkommen: Die für seine Anwendbarkeit maßgebliche Grenze des Personenbezuges wirkt einerseits zu eng, andererseits zu unspezifisch. So basiert Big Data häufig auf *mixed data sets*, es werden also personenbezogene und nicht-personenbezogene Daten miteinander vermengt. Wie oben beschrieben, werden so vormals nicht-personenbezogene Daten personenbeziehbar und müssen daher – je nach ge-

22 Vgl. zum Ganzen Roßnagel, a.a.O, S. 162ff.

23 Siehe hierzu auch die Beiträge von Eric Hilgendorf, von Lorena Jaume-Palasí und von Francesca Schmidt und Nicole Shephard in diesem Band.

planter Verarbeitung – womöglich schon vor einem feststellbaren Personenbezug gewissen Schutzregelungen unterworfen werden.

Zentrale Herausforderungen für den künftigen Datenschutz zeichnen sich ebenso in einzelnen Regelungsfeldern ab, etwa die im Gesundheitsdatenschutz augenfällige überkomplexe Regelungsvielfalt, die Reform der Datenschutzaufsicht mit dem Ziel größerer Einheitlichkeit und Augenhöhe gegenüber großen Unternehmen sowie die effektivere Durchsetzung des Datenschutzes bei der Abstimmung der Behörden im Mehrebenensystem der EU.

Das Gesetzgebungverfahren zur DSGVO selbst hat die Idee von bereichsspezifischen Datenschutzregelungen aufgegriffen. So sollte neben der Datenschutz-Grundverordnung eine E-Privacy-Verordnung der EU unter anderem für einen ausgeprägten Schutz der besonders gefährdeten Online-Kommunikation sorgen. Dies erscheint angesichts der Schutzvorgaben des Grundgesetzes etwa für das Telekommunikationsgeheimnis auch dringend geboten.

Den Mitgliedstaaten werden in der DSGVO zudem eigene gesetzliche Regelungen nahegelegt, etwa für den Bereich des Beschäftigtendatenschutzes oder zum Ausgleich von Pressefreiheit und Datenschutz. In beiden Bereichen gibt es vielfältige offene und komplexe Regelungsfragen, deren Lösung auf gesetzlicher Ebene für alle Seiten mehr Rechtssicherheit bieten könnte.

(1) Verbraucher(-daten-)schutzrecht

Die nun seit über zwanzig Jahren diskutierte Kommerzialisierung personenbezogener Daten und das stetig wachsende Feld des Verbraucherdatenschutzrechts legen eine aktive gesetzgeberische Weiterentwicklung nahe. Einen Anfang hat die EU mit der Digitale-Güter- und Dienstleistungen-Richtlinie[24] gemacht. Auch der Datenschutzdiskurs darf sich dieser Diskussion nicht verschließen. Zu sehr sind Daten in ihrem kommerziellen Wert längst Gegenstand und Ziel der Geschäftsmodelle der Wirtschaft.

Verbessert werden muss die Stärkung der Stellung der Verbraucher*innen im Verhältnis zu übermächtigen Anbietern. Verbraucher*innen verdienen Unterstützung etwa durch gezielte Qualitätsprüfungen von riskanten Verfahren wie etwa KI-Anwendungen durch unabhängige Prüfstellen. Verbraucherschutzverbände könnten mit eigenständigen Beschwerderechten ausgestattet werden. Und Verfahren der treuhänderischen Wahrnehmung

24 Vgl. https ://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX :32019L0770

von Datenschutzrechten durch spezialisierte Anbieter verdienen zur Entlastung der Verbraucher*innen eine nähere Prüfung. Im Umgang mit Big Data, aber auch zur Unterstützung der Bürger*innen bei der Nutzung der vielen privaten digitalen Angebote können zukünftig sogenannte PIM-Software (Product Information Management) und Datentreuhandangebote womöglich entscheidend zum Schutz der Bürger*innen beitragen.

Der Überforderung der Verbraucher*innen mit der Art und Weise, wie Transparenzpflichten wahrgenommen und Entscheidungsverfahren ausgestaltet werden, muss mit weiteren Vorgaben vorgebeugt werden. Das Ziel der Verständlichkeit und der *Verdaubarkeit* von Informationen kann mit abgestuften Verfahren, den sogenannten *layered notices*, verbessert werden. Auch für Lösungen durch bildhafte Darstellungen liegen längst zahlreiche Vorschläge auf dem Tisch.

Naheliegend wären etwa gezielt den IT-Bereich aufgreifende zivilrechtliche Regelungen zur Kontrolle von Allgemeinen Geschäftsbedingungen (AGB). Die den Verbraucher*innen aufgezwungenen, skandalös intransparenten AGB der Internetunternehmen bieten hier genug Anhaltspunkte. Vorgeschlagen werden etwa inhaltliche Restriktionen des zulässig zu Vereinbarenden und Zertifizierungspflichten für besonders bedeutsame AGB.[25]

(2) Informationelle Selbstbestimmung für das digitale Zeitalter verankern

Gerade die jüngsten Reformvorschläge der EU zur Plattformregulierung zeigen eine gesteigerte Bereitschaft, auch Allgemeininteressen und weitere gesetzgeberische Ziele auf die Digitalwirtschaft auszudehnen. Dazu zählt etwa der Schutz vor Monopolbildung. Im Kern basiert das sich erweiternde Eingriffs-Instrumentarium der Kartellbehörden allerdings auf dem besonderen Schutzbedarf der von Plattformen monopolisierend und zweckwidrig verarbeiteten personenbezogenen Daten. Deutlich wird, dass daten- und informationsbezogene Regelungskomponenten in bislang davon unberührte Rechtsmaterien integriert werden.

Auch die Regelungen zur Bekämpfung von Hassbotschaften, Hassrede und Verhetzungen könnten in diesem Zusammenhang genannt werden, soweit diese Pflichten zur Herausgabe und Übermittlung personenbezogener Daten von Kund*innen an Sicherheitsbehörden betreffen, aber auch die hoch

25 So etwa Hoffmann-Riem, Wolfgang: Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht, in: Archiv des öffentlichen Rechts 2017, S. 39.

problematische Filterung der persönlichen, zur Veröffentlichung bestimmten Inhalte von Kund*innen. Deutlich wird jedenfalls, dass der Datenschutz hier nur noch einen beschränkten Teil der informationellen Konflikte bearbeitet, zunehmend von weiteren Schutzzielen begleitet wird und Einbettung in übergreifendere Informationszusammenhänge erfährt.

(3) Rote Linien gegen ausufernde Datenerfassung

Viele Elemente des Datenschutzes zielen auf wohlabgewogene Anwendungen im Einzelfall und lassen den Betroffenen Handlungsspielräume im Sinne ihrer Selbstbestimmung. Damit wird einer vielfältigen Lebenswirklichkeit Rechnung getragen. Doch es muss auch klare und eindeutige rote Linien geben. Wo gravierende und multiple Risiken nicht nur für einzelne Betroffene und deren Rechte, sondern auch für die Kommunikation und die Privatheit der Gesellschaft insgesamt drohen, braucht es klare, absolute Grenzen. Hierzu zählen beispielsweise die unterschiedslos alle Bürger*innen betreffende anlasslose Vorratsdatenspeicherung von Kommunikationsverkehrsdaten, die biometrische Gesichtserkennung in öffentlichen Räumen sowie das umfassende Verhaltenstracking von sozialen Netzwerken zur Erstellung von Persönlichkeitsprofilen oder die verdeckte gezielte Beeinflussung von politischen Wahlen im Wege des sog. Microtargeting. Diese Beispiele belegen je für sich die enorme Dimension der Bedrohung für die Grundrechte, die die Digitalisierung angenommen hat.

Anpassung und Durchsetzung von Privatheit als Daueraufgabe

Die Zukunft der Privatheit hängt wesentlich vom politischen Willen ab. Letztlich zählt sie zwar dank der vielfältigen grundrechtlichen Verankerung zum Recht, dass notfalls dem Staat auch Schutzpflichten zu dessen Erhalt auferlegt. Deutlich sollte aber geworden sein, dass die Durchsetzung des bestehenden Rechts als auch dessen notwendige Weiterentwicklung eine anspruchsvolle Daueraufgabe darstellen. Angesichts der raschen Veränderungen durch die Digitalisierung muss das Datenschutzrecht selbst vielfältige und auch innovative Wege einschlagen, um weiter mithalten zu können. Abgesänge kommen, das zeigen gerade die intensiven Auseinandersetzungen um Privatheit in der jüngsten Zeit, jedenfalls zu früh. Die Selbstbehauptung menschlicher Freiheit und Privatheit in der sich beschleunigenden Digitalisierung erscheint vielmehr lebendiger denn je.