Martin Kutscha

Informationelle Selbstbestimmung – ein Grundrecht ohne Zukunft?

„Ich weiß nicht, was soll es bedeuten,
daß ich so traurig bin,
ein Märchen aus alten Zeiten,
das kommt mir nicht aus dem Sinn.“[1]

Das „*Märchen aus alten Zeiten*“, von dem im Folgenden die Rede sein soll, ist nicht wie bei Heinrich Heine das schlimme Schicksal, das die *Loreley* den armen Rheinschiffern beschert haben soll, sondern das Recht auf informationelle Selbstbestimmung. Nicht nur Jurist_innen wissen, dass dieses Grundrecht durch das Volkszählungsurteil des Bundesverfassungsgerichts (BVerfG) im Jahre 1983 seine höchstrichterlichen Weihen empfangen hat. Es steht nicht explizit im Grundgesetz, sondern wurde aus dem allgemeinen Persönlichkeitsrecht, gestützt auf Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz, abgeleitet. Das neue Grundrecht gewährleiste, so damals das Gericht, „*die Befugnis des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“*[2] Flankiert wird diese positive Gewährleistung durch das richterliche Verdikt gegen eine bestimmte Zukunftsperspektive: „*Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.*“

Aber leben wir nicht schon seit einigen Jahren in einer Situation, in der wir infolge unserer tagtäglichen Internetkommunikation überhaupt keinen Überblick mehr haben, wie genau globale Player wie Google, Facebook und Amazon, aber auch die großen staatlichen Geheimdienste über unsere persönlichen Eigenarten, Neigungen, kulturelle und politische Präferenzen Bescheid wissen? „*Sie sind die Laborratte, die die Daten liefert, mit deren Hilfe Sie manipuliert werden*“, charakterisiert der Soziologe Harald Welzer sarkastisch die gewaltige Schar der unbedarften User_innen.[3] Wie steht es angesichts des massenhaften Web-Tracking und Profiling quasi hinter dem Rücken der Nutzer_innen mit dem Geltungsanspruch des Rechts auf informationelle Selbstbestimmung? Den verschiedenen Facetten dieser Frage widmet sich der aus einer Konferenz des „Forums Privatheit“ hervorgegangene Sammelband

Michael Friedewald/Jörg Lamla/Alexander Roßnagel (Hrsg.),
Informationelle Selbstbestimmung im digitalen Wandel.
Springer Vieweg Verlag Wiesbaden 2017, 332 S., ISBN 978-3-658-17661-7.
Preise: 74,99 € (Softcover) bzw. 59,99 € (eBook)

Der besondere Reiz des Werkes liegt in dessen Interdisziplinarität: Die Autor_ innen entstammen unterschiedlichen Fachdisziplinen, so dass die Problematik nicht nur in den Bahnen der herkömmlichen juristischen Dogmatik abgehandelt wird. Dies gilt bereits für den ersten Beitrag aus der Feder der Öffentlichrechtlerin *Marion Albers*. Auf der Grundlage des Volkszählungsurteils entfaltet die Autorin eine Konzeption des Rechts auf informationelle Selbstbestimmung als „*vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen*". In der Tat bedarf dieses Grundrecht zu seiner Verwirklichung eines Arsenals verschiedener Schutzmaßnahmen sowohl auf rechtlicher als auch auf technischer Ebene. Allerdings dürfte die Kritik von Albers fehlgehen, das BVerfG habe das Recht auf informationelle Selbstbestimmung zu „individualistisch-eingriffsabwehrrechtlich" zugeschnitten (S. 21). Das Volkzählungsurteil verweist nämlich durchaus auf die Notwendigkeit verfahrensrechtlicher Schutzvorkehrungen bei der Datenverarbeitung wie auch auf die Bedeutung der Beteiligung unabhängiger Datenschutzbeauftragter.[4] Darüber hinaus hat das Gericht auch herausgestellt, dass informationelle Selbstbestimmung nicht allein dem Schutz des Individuums dienen soll, sondern auch eine „kollektive" Seite hat, indem es die Funktionsbedingungen eines freien demokratischen Prozesses sichert.[5] Diese „demokratietheoretischen Implikationen" des genannten Grundrechts werden von dem Philosophen Max Winter überzeugend dargestellt. Seine Kritik an der gegenwärtigen Situation ist nur zu berechtigt: „*Eine Gesellschaft, in der einzelne private oder staatliche Akteure über persönliche Daten nahezu aller Bürger verfügen, beschränkt die Möglichkeiten der aktiven Mitgestaltung des Gemeinwesens und der öffentlichen Meinungsäußerung selbst dann, wenn kein aktiver Gebrauch von derartigem Herrschaftswissen gemacht wird.*" (S. 45) Dies kann sich freilich angesichts der gegenwärtigen Konjunktur autoritärer Regierungsmodelle rasch ändern.

Privatheitspraktiken

Nachdem im 1. Teil des Buches die normativen Grundlagen der informationellen Selbstbestimmung erörtert wurden, widmet sich der 2. Teil der Empirie, nämlich den „Privatheitspraktiken und Datenökonomien". Der Medienwissenschaftler *Ramón Reichert* beschreibt die Selbstvermessung von Individuen anhand von „Fitness-Trackern" und „Wearables", die ihren Träger_innen, aber eben nicht nur diesen, detaillierte Informationen über die eigenen Körperfunktionen vermitteln. Es wäre lohnenswert, schreibt der Autor am Schluss seines Beitrags, „*die Perspektive auf Biomedialität als Markt aufzunehmen und der Frage nachzugehen, welches Interesse unterschiedliche Anbieter mit ihrem finanziellen Engagement verbinden, um Praktiken der digitalen Selbstvermessung zu fördern und sicht- und sagbar zu machen.*" (S. 104) Gerade an diesem Punkt hätten die ökonomischen Interessen z. B. von Versicherungen an den Gesundheitsdaten ihrer (potentiellen) Kund_innen freilich deutlicher herausgearbeitet werden können. Auch wäre es interessant gewesen, das Self-Tracking als ein Aspekt der Totalisierung des Wettbewerbs der Individuen und als Teil neoliberaler Ökonomie und Herrschaft kritisch in den Blick zu nehmen.[6]

Aus der Sicht der Medienpädagogik untersuchen *Niels Brüggen* und *Ulrike Wagner* die Bedingungen bei der alltäglichen Nutzung der „sozialen" Netzwerke durch Ju-

gendliche. Diese würden, so ihr empirischer Befund, die Angebote „*trotz starker Bedenken*“ wahrnehmen, „*da die digitalen Dienste eng mit ihrer Lebensführung verknüpft sind.*“ Sie würden mit Recht davon ausgehen, dass sie über keinerlei Verhandlungsmöglichkeiten mit den globalen Internetfirmen wie Facebook und Google verfügten und deshalb deren Bedingungen akzeptieren müssten. Es würde indessen zu kurz greifen, „*lediglich auf der Subjektseite ein Privacy Paradox zu konstatieren und daraus ggf. eine schwindende Bedeutung des Wertes von Privatheit abzuleiten. Vielmehr gilt es, Realisierungsbedingungen zu schaffen, die Selbstbestimmung überhaupt ermöglichen.*“ (S. 142) Hierfür sehen Brüggen und Wagner Ansatzpunkte auf zwei Ebenen, und zwar präventive Maßnahmen auf der individuellen Ebene sowie regulative Elemente auf der kollektiven Ebene. Das ist grundsätzlich überzeugend, angesichts der ökonomischen Machtposition des Oligopols der großen Internetfirmen und der begrenzten Bereitschaft von Regierungen, sich international für ein striktes Datenschutzregime zu engagieren, aber auch schwer durchzusetzen.

Wie wenig die reale Machtposition der Internetgiganten mit den Vorstellungen der klassischen Ökonomie zu vereinbaren ist, verdeutlichen zwei Beiträge aus der Feder von Wirtschaftswissenschaftlern. *Arnold Picot*, *Dominik van Aaken* und *Andreas Ostermaier* erinnern zunächst an das zentrale Paradigma der dominanten Volkswirtschaftslehre: „F*reiheit bildet gerade in marktwirtschaftlichen, privatwirtschaftlichen Wirtschaftssystemen einen zentralen Eckpfeiler, weil sich die Idee der Überlegenheit dezentraler Entscheidungen nur auf Basis von Freiheiten im jeweiligen institutionellen Rahmen verwirklichen und entfalten lässt: Souveränität und Freiheit des Konsumenten bei der Verwendung seiner Lebenszeit und seiner verfügbaren Mittel, Freiheit des handelnden Unternehmers bei der Wahl seiner Geschäftsmodelle und Geschäftspartner, Freiheit des Investors bei der Auswahl der Projekte, in denen er seine Mittel bindet, Freiheit von Wissenschaft, Forschung und Entwicklung bei der Verfolgung von neuen Ideen.... Wird nun die Wahlfreiheit jedes Einzelnen beschnitten oder gar beseitigt*“, so die Autoren weiter, „*muss die Legitimität des marktwirtschaftlichen und auch demokratischen Systems grundlegenden Schaden nehmen.*“ (S. 170) Privatsphäre sei eine besondere Form von Freiheit, Eingriffe in die Privatsphäre müssten deshalb reversibel sein. Anhand einer Untersuchung der Geschäftsbedingungen bzw. der „Privacy Notes“ von Amazon, Facebook und Google wird gezeigt, dass die aus dem Freiheitspostulat abgeleiteten Voraussetzungen bei diesen Internetfirmen nicht gegeben sind.

Entsprechende Defizite werden auch in dem folgenden Beitrag von *Malte Dold* und *Tim Krieger* aus dem Blickwinkel der Ordnungsökonomie konstatiert: Eine rechtlich abgesicherte Souveränität der Informationsemittenten, also der Nutzer_innen, im Hinblick auf ihre privaten Informationen sei derzeit nicht gewährleistet. Die Netzwerkeffekte wirkten in Richtung einer Art natürlichen Monopols für die jeweiligen Marktplattformen, denn ein Ausweichen auf konkurrierende kleinere Plattformen sei aus individueller Sicht wenig attraktiv. Deshalb bestehe die „*Gefahr der Bildung eines Machtmonopols, bei dem die Nutzer ausgebeutet werden.*“ (S. 188) Die Autoren setzen dagegen auf eine Stärkung des Wettbewerbs z. B. durch eine verbesserte Bereitstellung von Informationen. Statt „*immer höhere Abwehrmauern um das ‚private Individuum’*“ zu bauen, sollte den Verbrauchern gezeigt werden, „*dass sie über enorme Assets in Form ihrer persönlichen Daten verfügen, welche sie auf abgesicherten Informationsmärkten selbstbewusst, offensiv und vor allem gewinnbringend veräußern können.*“ (S. 195) – Wie dieses

marktwirtschaftliche Modell eines „selbstbewussten“ und „offensiven“ Verkaufs der eigenen Daten angesichts des beschriebenen Machtungleichgewichts funktionieren soll, bleibt allerdings ein Rätsel.

Perspektiven

Die Beiträge im 3. Teil des Sammelbandes sollen Zukunftsperspektiven aufzeigen, beschäftigen sich aber zunächst mit dem unbefriedigenden Ist-Zustand. Die Informatiker *Sven Türpe*, *Jürgen Geuter* und *Andreas Poller* legen dar, dass die Annahmen des herkömmlichen Datenschutzes der heutigen Realität von Big Data nicht mehr gerecht werden. „*Ein scheinbar einfacher Vorgang wie der Besuch einer Website umfasst in Wirklichkeit komplizierte Interaktionen mit einer Vielzahl von Akteuren und ihren technischen Artefakten, die größtenteils verborgen bleiben.*“ Die klassische Kombination aus Betroffenenrechten und Aufsichtsbehörden stehe vor dem Problem, „d*ass Betroffene die Vielfalt der Datenempfänger und Nutzungen nicht mehr überblicken können.*“ (S. 245) In der heutigen Welt vielfältig vernetzter Anwendungen, fortwährender Datenproduktion und lernender Maschinen führten die alten Rezepte des Datenschutzes nicht zum Erfolg. Als Schritt auf dem Weg zu wirksameren Mitteln präsentieren die Autoren die Metapher der Datenemission: Ähnlich einer Lichtquelle sende jeder Einzelne fortlaufend und in alle Richtungen Daten aus, über die er dann keine Kontrolle mehr habe (S. 239). – Als Beschreibung ist diese Metapher plausibel. Welche Ansatzpunkte sich daraus für einen Datenschutz der Zukunft ergeben, lassen die Autoren allerdings offen.

Deutlich pessimistischer fällt die Bestandsaufnahme des an der Uni Rostock lehrenden Informatikers *Clemens H. Cap* zur „*Verpflichtung der Hersteller zur Mitwirkung bei informationeller Selbstbestimmung*“ aus. Die Entwicklung einzelner Anwendungen und ganzer Infrastrukturen folge, so der Autor, „*den ökonomischen Interessen der Hersteller so weitgehend, dass der gläserne Kunde Normalfall und informationelle Selbstbestimmung praktisch unmöglich geworden ist.*“ (S. 249) Als Beispiel nennt er die Hersteller der Hardware von Smartphones, die den Normalanwendern keine Möglichkeit ließen, alternative Betriebssysteme zu verwenden. Auch werde die anonyme oder pseudonyme Nutzung der Smartphones unmöglich gemacht oder massiv erschwert (S. 250). Anhand des Vergleichs mit dem Verbraucherschutzstandard im nichtdigitalen Bereich weist Cap nach, dass der Schutz der Anwender digitaler Technologien erhebliche Defizite aufweist. „*Im Vergleich mit anderen Branchen ist im Digitalen die Ausbeutung des Bürgers und seiner Privatsphäre weitgehend legalisiert.*“ (S. 253) – Es bleibt abzuwarten, so wäre hinzuzufügen, ob sich dies mit der Verabschiedung der EU-ePrivacy-Verordnung ändern wird.

Ausgangspunkt des folgenden Beitrags der Informatiker *Max R. Ulbricht* und *Karsten Weber* ist die Feststellung, dass die klassischen datenschutzrechtlichen Konzepte der „informierten Einwilligung“ und der Zweckbindung sich der Herausforderung durch die heutige Praxis von Big Data stellen müssen. Sie entwickeln Vorschläge, wie durch neue technische Mechanismen die Einhaltung dieser Prinzipien erzwungen werden könnte. Es ist allerdings fraglich, ob sich angesichts des erheblichen ökonomischen

Interesses an der Gewinnung möglichst zahlreicher personenbezogener Daten solche ehrgeizigen Schutzkonzepte durchsetzen lassen.

„*Wege aus einer Krise des Rechts und der Demokratie*" – dieser anspruchsvolle Untertitel des Beitrags des Juristen *Christian L. Geminn* und der Juristin *Maxi Nebel*, die beide in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Uni Kassel tätig sind, bringt den elementaren Charakter der aktuellen Herausforderungen durchaus treffend auf den Punkt. Angesichts dieser Herausforderungen, so schreiben sie, sei das Recht in einer schwierigen Lage, weil es tief im Nationalstaat verwurzelt und an ihn gebunden sei, der Datenverkehr und -handel jedoch keine Staatsgrenzen kenne. „*Befinden sich der Nationalstaat und sein Recht durch Verlust der Kontrollfähigkeit, Legitimationsdefizite und Unfähigkeit zu legitimationswirksamen Steuerungsleistungen in einer Krise, führt das zu Defiziten im demokratischen Entscheidungsprozess, da der Nationalstaat die Rechte seiner Bürger bei grenzüberschreitenden Sachverhalten nicht ausreichend zu schützen vermag.*" (S. 293) Untersucht werden verschiedene Möglichkeiten zur „*Rückgewinnung der Rechtshoheit*" wie z. B. die Installation von „nationalem Routing" bzw. die Abschottung von Datennetzen, wie sie insbesondere von autoritär regierten Staaten praktiziert wird. Verwiesen wird auch auf die Möglichkeit, über das Setzen technischer Standards den Geltungsbereich nationalen Rechts zumindest indirekt über die eigenen Staatsgrenzen hinweg auszuweiten. Geminn und Nebel skizzieren sodann die Ansatzpunkte auf der internationalen Ebene, also die inzwischen geschaffenen Datenschutzbestimmungen der EU sowie den noch schwach entwickelten Menschenrechtsschutz im Völkerrecht. Sie plädieren darüber hinaus für einen Grundrechtsschutz durch Technik, etwa in Gestalt datenschutzfreundlicher Voreinstellungen bei der Internetnutzung. Der Nationalstaat, so das Fazit, habe seine Regelungskraft jedenfalls noch nicht verloren. „*Letztlich geht es sowohl bei nationalen als auch internationalen Ansätzen darum, die Hoheit des Rechts über einen vermeintlich ‚rechtlosen' Raum zu gewinnen.*" (S. 311)

Ein wenn auch begrenzter Optimismus spricht auch aus dem abschließenden Beitrag von *Tobias Matzner* und *Philipp Richter* (letzterer ist Geschäftsführer von provet) mit dem Titel „Ausblick", der als eine geraffte Zusammenfassung des ganzen Bandes gelesen werden kann. Die Autoren skizzieren noch einmal die zentrale Problematik bei der Internetnutzung: Es bestehe ein immenser wirtschaftlicher und sozialer Druck, seine persönlichen Daten z. B. in den „sozialen" Netzwerken preiszugeben. „*Wer an den neuen Diensten nicht teilnimmt, wer nicht mitkommuniziert, wer nicht bereit ist, nach den Regeln der Diensteanbieter zu spielen und hierfür seine Daten preisgibt, der isoliert sich…Von einer bewussten, selbstbestimmten ‚Preisgabe' der Daten kann also in vielen Fällen nicht gesprochen werden.*" (S. 319f.)

Die angemessene Antwort auf diese Situation muss nach Auffassung der beiden Autoren die Kombination zweier Ebenen sein: Notwendig sei ein Zusammenspiel aus Eigenverantwortung und kollektivem, demokratisch legitimiertem Schutz. „*Die politische Entscheidung über den Umgang mit personenbezogenen Daten in der Welt von Big Data und Ubiquitous Computing ist keine Entscheidung, die Großkonzernen überlassen werden darf, die sie an die Menschen nur in der transformierten Form von Konsumentscheidungen weiterleiten.*" (S. 322) Der politische Rahmen informationeller Selbstbestimmung müsse daher auch die Regulierung großer, transnationaler Unternehmen beinhalten.

So überzeugend diese Postulate angesichts der dargestellten Herausforderungen auch sind, es bleibt doch die Frage nach den Durchsetzungschancen angesichts der gegenwärtigen ökonomischen und politischen Machtverhältnisse offen. Das massive ökonomische Interesse der *Global Player* im Netz an möglichst vielen persönlichen Daten trifft sich mit der mangelnden Bereitschaft vieler verantwortlicher Politiker_innen zu effektiver Regulierung und Begrenzung. Repräsentativ hierfür dürfte die Äußerung von Bundeskanzlerin *Merkel* sein, Datensparsamkeit sei überholt und gehöre „ins vergangene Jahrhundert“[7]. So ist es nur folgerichtig, dass Finanzmittel und Energien statt in einen effektiveren Datenschutz vor allem in die Verbesserung der Internetzugänge (an Schulen, auf dem flachen Land etc.) investiert werden.

Am notwendigen politischen Druck auf die Verantwortlichen mangelt es nicht zuletzt auch wegen der Sorglosigkeit zahlreicher Nutzer_innen beim Umgang mit ihren elektronischen Geräten. Die fortwährend auf ihr Smartphone starrenden und tippenden Zombies („*Smombies*“), die auf Gehwegen und selbst gefährlichen Straßenkreuzungen herumstolpern, geben einen Eindruck vom Maß ihrer Abhängigkeit von dem faszinierenden kleinen Ding in ihrer Hand. Auch die Werbung für vernetzte Haushaltsgeräte („*Internet der Dinge*“) dürfte auf fruchtbaren Boden fallen – die Bedienung ist ja so easy, und was dabei im Hintergrund passiert, wollen viele vielleicht gar nicht so genau wissen. Dass die moderne Loreley aus dem Silicon Valley unzählige unsichtbare Krakenarme hat, wird angesichts ihres betörenden Gesangs gerne verdrängt. Wenn es uns nicht gelingt, entschieden gegenzusteuern, wird der Kahn unseres Privatsphäreschutzes schließlich versinken und das Postulat der informationellen Selbstbestimmung nur noch wie ein „*Märchen aus alten Zeiten*“ klingen.

PROF. DR. MARTIN KUTSCHA Professor i. R. für Staats- und Verwaltungsrecht an der Hochschule für Wirtschaft und Recht Berlin, Mitglied des Bundesvorstands der Humanistischen Union und des Forschungsinstituts für öffentliche und private Sicherheit.

Anmerkungen:

1 Heinrich Heine (1823), Buch der Lieder - „Die Heimkehr“.
2 Vgl. BVerfGE 65, 1ff.
3 Welzer, Die höchste Stufe der Zensur: Das Leben in der Ich-Blase, in: Blätter f. dt. u. intern. Politik 7/2016, S. 61 (66).
4 BVerfGE 65, 1 (46).
5 Vgl. BVerfGE 65, 1 (43).
6 Vgl. dazu z. B. Selke, Lifelogging oder: Der fehlerhafte Mensch, in: Blätter f. dt. u. intern. Politik 5/2015, S. 79 ff.
7 Merkel auf dem CDU- Parteitag am 6. 12. 2016, zit. n. Roßnagel u. a., Datensparsamkeit oder Datenreichtum? Policy Paper des Forums Privatheit, 2017, S. 3.