Datenschutz contra Wirtschaft und Big Data?

Eine politische Fehlentwicklung

Stand: 31.12.2015

Inhalt

Thilo Weichert
Waisenhofstr. 41, 24103 Kiel
0431 / 9719742,
weichert@netzwerk-datenschutzexpertise.de
Karin Schuler
Kronprinzenstraße 76, 53173 Bonn
0228 / 2420 733,
schuler@netzwerk-datenschutzexpertise.de
www.netzwerk-datenschutzexpertise.de

Der vorliegende Text des Netzwerks Datenschutzexpertise befasst sich mit aktuellen Angriffen durch Teile der Bundesregierung und der deutschen IKT-Wirtschaft auf den Datenschutz und macht Vorschläge für den Ausgleich wirtschaftsgesteuerter Big-Data-Anwendungen mit dem Grundrecht auf Datenschutz.

1 Agenda für Digitalisierung und Rechtsschutz

Wenn es um Fragen der Digitalisierung geht, so gibt es in Deutschland zwischen den Erwartungen, Wünschen und Befürchtungen der Bürgerinnen und Bürger einerseits und von Unternehmen andererseits erstaunlich große Übereinstimmungen: Nur ein Drittel der Bevölkerung gibt Daten gern heraus, um etwas über das Internet zu erhalten[1]. 70% der Bundesbürger lehnen eine Überwachung selbst dann ab, wenn dadurch Straftaten verhindert werden könnten. Über 70% halten es für „unausweichlich", dass von ihnen irgendwo im Internet angegebene Daten missbraucht werden[2] und fürchten finanzielle Schäden und Eingriffe in die Privatsphäre. Und auch bei den klassischen mittelständischen Industrieunternehmen sehen 91% die größten Risiken in der Sicherheit ihrer Daten[3].

Die deutliche Mehrheit der Bundesbevölkerung fordert den Schutz der Persönlichkeitsrechte ebenso ein wie Unternehmer den Schutz ihrer Geschäftsgeheimnisse. Sie vertrauen auf den Schutz von Grundrechten durch staatliche Institutionen und erwarten von staatlicher Seite, dass sie sich, wenn es darauf ankommt, auf den Schutz durch staatliche Stellen verlassen können. Die ausgeprägten Befürchtungen hinsichtlich des Missbrauchs privater und geschäftlicher Daten belegen, dass staatliche Stellen in der Wahrnehmung der Betroffenen den grundrechtlichen Schutz nicht hinreichend sichern und dass sie mit den Risiken sich selbst überlassen scheinen.

Während die Bevölkerung mehr Rechtsschutz erwartet, wird die aktuelle politische Diskussion davon beherrscht, den ohnehin defizitären staatlichen Schutz weiter aufzuweichen – und zwar zugunsten einer seit den 1970er Jahren mit Dienstleistungen und Wissensarbeit sich entwickelnden Datenökonomie, die als „Informationsgesellschaft" bezeichnet wurde und derzeit unter dem Begriff „Digitalisierung" neu erfunden wird. Zu deren Förderung soll der Datenschutz an entscheidenden Stellen abgebaut und die Grundsätze der Datensparsamkeit und Zweckbindung sollen geschleift werden. Für Big-Data-Anwendungen und darauf aufbauende Geschäftsmodelle sollen möglichst viele Daten aus möglichst vielen Erhebungsquellen ohne lästige Begrenzungen verknüpft werden können.

Der damit eröffnete Konflikt zwischen Datenschutz und wirtschaftlichen Begehrlichkeiten ist ein Beispiel für die in einem demokratischen Staatswesen hochproblematische Kluft zwischen Verfassungsanspruch und Rechtswirklichkeit. Das Fernmeldegeheimnis als ältestes Grundrecht der Informationsgesellschaft wird nach den Enthüllungen von Ed Snowden zur umfassenden Überwachung durch die Geheimdienste und der Auswertungsaktivitäten der Kommunikationsdienstleister

[1] So jüngst OFCOM: International Communications Market Report 2015, S. 86.
[2] GfK-Studie Daten & Schutz 2013"; http://www.gfk-verein.org/sites/default/files/medien/34/dokumente/pm_1_gfk_verein_daten_schutz_2013.pdf.
[3] Repräsentative Mittelstands-Umfrage der DZ Bank 2014: https://www.dzbank.de/content/dam/dzbank_de/de/library/presselibrary/pdf_dokumente/DZ_Bank_Digitalisierung_Grafiken.pdf.

mittlerweile als „Totalverlust“ abgeschrieben.[4] Das 2008 vom Bundesverfassungsgericht ausdrücklich gegen den Einsatz von Staatstrojanern formulierte Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[5] wurde bisher allenfalls andeutungsweise in staatliches Handeln übersetzt. Zwar werden die Grundrechte formal nicht aufgekündigt. Doch geben einige staatliche und gesellschaftliche Instanzen praktisch ihren Anspruch auf, diese Rechte zu schützen. Dies ist ein fatales Signal für die Zukunft unserer Informationsgesellschaft.

Eine solche Politik unterminiert die Aufgaben des Staates ebenso wie die Fortentwicklung der Informationsgesellschaft. In einer freiheitlichen Informationsgesellschaft gilt, in Abgrenzung zu autoritären Regimen: Grundlage für ein stabiles und entwicklungsfähiges System einer Datenökonomie ebenso wie für das politische System ist ein wirksamer Schutz der Rechte der Menschen. Wer die Datenökonomie weiterentwickeln und ihren Nutzen erschließbar machen will, darf nicht durch die Aufgabe von Grundrechten vor dieser Aufgabe kapitulieren, sondern muss sich seiner Verantwortung stellen, den miteinander im Wettstreit stehenden Rechten ausgewogen zur Geltung zu verhelfen.

Bundesjustizminister Heiko Maas hat sich jüngst mit einem Vorschlag für eine „Charta der digitalen Grundrechte“ zu Wort gemeldet[6] und damit die Diskussion über ein digitales Grundrechtsregime bereichert. Dagegen stellen andere maßgebliche Akteure der Politik mit Unterstützung aus der Wirtschaft das Grundrecht auf Datenschutz als wirtschaftsfeindlich und unzeitgemäß dar und schaffen damit die Grundlage für dessen Erosion.

2 Die Rhetorik

Die prominenteste Vertreterin dieser Politik zum Abbau des Datenschutzes ist Bundeskanzlerin Angela Merkel. Sie forderte die deutsche Bevölkerung mehrfach auf, endlich ihre ständigen Datenschutz-Bedenken fallen zu lassen und den Schutz ihrer Privatsphäre der Weiterentwicklung der nationalen Wirtschaft unterzuordnen. Nur so könne man im digitalen Zeitalter international mithalten. Merkel begründet dies damit, dass die umfassende Sammlung und Auswertung von Nutzerdaten eine Grundlage des ökonomischen Erfolgsrezeptes von US-Firmen wie Google und Facebook ist. Deutsche Internet-Firmen beklagen immer wieder, dass die hiesigen Datenschutz-Regelungen sie daran hindern, ähnliche Entwicklungen vollziehen zu können. Laut Merkel müsse daher ein Umdenken beim Datenschutz stattfinden.

So erklärte Merkel z. B. schon im Sommer 2015: „Wer Daten als eine Bedrohung wahrnimmt, wer immer nur darüber nachdenkt, welchen Schaden jedes Stück Information anrichten kann, wird nicht in der Lage sein, die Möglichkeiten der Digitalisierung zu seinem Vorteil zu nutzen.“ Big Data sei keine Bedrohung, sondern „der Rohstoff der Zukunft“. Wertschöpfung entstehe künftig nicht mehr hauptsächlich über die maschinelle Herstellung eines Produkts, sondern vor allem über die Nutzung von Kundendaten. „Wenn wir aber die Verbindung zum Kunden dann nicht richtig aufbauen, dann wird uns ein wesentlicher Teil der Wertschöpfung verloren gehen.“ Die Wertschöpfung werde dann

[4] Prantl, http://www.sueddeutsche.de/politik/operation-eikonal-totalverlust-eines-grundrechts-1.2157335; so schon der ehem. Richter am BVerfG Kühling, Das Ende der Privatheit, Grundrechte-Report 2003, S. 15.
[5] BVerfG NJW 2008, 822.
[6] Heiko Maas, http://www.zeit.de/2015/50/internet-charta-grundrechte-datensicherheit/komplettansicht.

„irgendwo in Amerika oder Asien“ stattfinden. Der Wettlauf werde in fünf bis zehn Jahren entschieden sein.

Ein Hintergrund dieser Rhetorik waren die Trilog-Verhandlungen zwischen der Kommission, dem Parlament und dem Rat der Europäischen Union (EU) über die Europäische Datenschutz-Grundverordnung (EU-DSGVO), die am 15.12.2015 ihren Abschluss fanden. Die Argumentation geht aber deutlich darüber hinaus und wird insbesondere bei der Diskussion der Umsetzung des Art. 20 EU-DSGVO, bei dem es sich um eine normative Grundlage für Big-Data-Verfahren handelt, weiter vorangetrieben werden. Merkel fordert mit Blick auf die Wirtschaft, dass die EU-DSGVO kein Hindernis für Big-Data-Geschäftsmodelle werden dürfe: „Sie brauchen hinreichend Freiheiten, um neue Daten, um neue Möglichkeiten des Datenmanagements, des Big-Data-Minings oder auch für die Cloud für ihre Geschäftsmodelle zu nutzen“.[7]

Zur Eröffnung des 9. IT-Gipfels der Bundesregierung stieß Wirtschaftsminister und SPD-Vizekanzler Sigmar Gabriel am 19.11.2015 ins gleiche Horn: „Wir brauchen ein anderes Verständnis vom Datenschutz: Die Minimierung als oberstes Ziel ist das Gegenteil des Geschäftsmodells von Big Data.“ Wichtig sei „Datensouveränität“ mit einem „selbstbestimmten Umgang“.[8] Bundesverkehrsminister Alexander Dobrindt von der CSU sekundierte auf einem Empfang des IT-Branchenverbands „Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.“ (Bitkom) im Zusammenhang mit dem IT-Gipfel: „Der bisher gültige Grundsatz, dass Datensparsamkeit das Übermaß der Dinge ist, der hat sich überholt, der muss weg. Datenreichtum muss der Maßstab sein, nach dem wir unsere Politik ausrichten.“ Dafür wolle sich die Bundesregierung zusammen mit dem Bitkom einsetzen.[9]

Solche rhetorischen Figuren lassen die Antwort auf die sich aufdrängende Frage offen, wie sich aus dem Datenreichtum für das Geschäftsmodell Big Data ein „selbstbestimmter Umgang“ mit Daten für jene Betroffenen gestalten lässt, die die Souveränität über ihre Daten abgegeben haben.

3 Grundsatzpapiere

Diese politischen Statements werden von Grundsatzpapieren begleitet, mit denen versucht wird, die Rationalität des Angriffs auf digitale Grundrechte zu begründen. Aufschlussreiche aktuelle Beispiele sind Veröffentlichungen zum IT-Gipfel 2015 der Bundesregierung sowie das von der SPD auf ihrem Bundesparteitag am 11.12.2015 beschlossene digitale Grundsatzprogramm.

---

[7] Nicht zu viel Datenschutz, SZ 14.09.2015, Kahle, Merkel: Deutsche sollen Datenschutz für die Wirtschaft aufgeben, www.winfuture.de, 10.06.2015; http://www.bundesregierung.de/Content/DE/Rede/2015/11/2015-11-03-merkel-publisher-summit.html; https://www.bundesregierung.de/Content/DE/Rede/2015/11/2015-11-03-bkin-bdi.html.

[8] Gabriel, http://www.bmwi.de/DE/Mediathek/videos,did=739022.html, vgl. Krempl, Gabriel plädiert für Datensouveränität statt Datenschutz, www.heise.de 19.11.2015.

[9] Alexander Dobrindt: Grundsatz der Datensparsamkeit „muss weg“, www.golem.de 19.11.2015.

3.1 „Leitplanken Digitaler Souveränität“

Noch dem auf Altbundeskanzler Kohl zurückgehenden analogen Bild der „Datenautobahn“ verbunden, veröffentlichte anlässlich des IT-Gipfels das Bundesministerium für Wirtschaft und Energie „Leitplanken Digitaler Souveränität“. Diese „Leitplanken“ fassen, so deren ausdrückliches Selbstverständnis „einige konkrete Maßnahmen und Handlungsempfehlungen zur Stärkung der digitalen Souveränität in Deutschland und Europa zusammen“. Daraus soll folgend zitiert werden:[10]

„Daten sind Ware und Währung zugleich und bilden den Kern einer entstehenden globalen Datenökonomie“. Es gehe um „digitale Souveränität“, also „zunächst allgemein die Fähigkeit zu Selbstbestimmung, die sich durch Eigenständigkeit und Unabhängigkeit ausdrückt. (…) Auf der Seite der Nutzer sind Vertrauen in einen starken Datenschutz und ein rechtlicher Gestaltungsrahmen nötig, der die wirtschaftliche Datennutzung mit dem Schutzinteresse des Einzelnen in Einklang bringt. Es muss gelingen, dass ganze Datenwertschöpfungsketten gebildet werden. (…) Deshalb dürfen datenbasierte digitale Geschäftsmodelle nicht durch ein unzeitgemäßes Datensparsamkeitsdiktat verhindert werden. Eine wettbewerbsfähige Datenwirtschaft mit Plattformen und intelligenten Diensten braucht vielmehr ein internationales Level-Playing-Field. (…) Um im globalen Standortwettbewerb zu bestehen, brauchen digital souveräne Systeme eine `Ermöglichungskultur´ (…) Bisherige Grundprinzipien des Datenschutzes wie Datensparsamkeit und Zweckbindung müssen überprüft und durch Prinzipien der Datenvielfalt und des Datenreichtums ergänzt und ersetzt werden.“

Weiter heißt es in den „Leitplanken“:

„Erforderlich ist ein echter digitaler Binnenmarkt mit EU-weiten einheitlichen Bedingungen vom Daten- und Verbraucherschutz bis zur Besteuerung, der Europa sehr viel näher an große homogene Märkte wie die USA und China heranbringen würde. (…) Eine rasche Verabschiedung der EU-Datenschutzgrundverordnung zwecks Harmonisierung der sehr unterschiedlichen nationalen Bestimmungen ist zwingend erforderlich. Dabei sollten im Entwurf gleichzeitig die Bestimmungen z. B. für die Pseudonymisierung oder Anonymisierung von Daten überarbeitet werden, um administrative Hemmnisse abzuschaffen. (…) Die Wettbewerber, die sich in diesen Märkten etabliert haben und sich zunehmend etablieren, basieren ihr Geschäftsmodell ganz wesentlich auf die Verfügbarkeit großer Datenmengen und deren intelligente Verwertung. Wir müssen aus Europa heraus in der Lage sein, Industriedaten, die einen Verbraucherbezug aufweisen können, auch zukünftig ohne komplizierte bzw. unrealistische Einwilligungsmechanismen nutzen zu können.“

Damit wird der Begriff der „digitalen Souveränität“ zerteilt in vage Glaubensdinge und harte ökonomische Anforderungen. So wird den Nutzern „Vertrauen in einen starken Datenschutz“ abverlangt, während die Wirtschaft Daten „ohne unrealistische Einwilligungsmechanismen nutzen“ soll. „Digitale Souveränität“ wird reduziert auf die Souveränität von Unternehmen, mit Daten tun zu können, was ihnen wirtschaftlich nutzt. Dass „digitale Souveränität“ eine individuelle und eine gesamtgesellschaftliche, demokratische Dimension hat, wird in den „Leitplanken“ nicht erwähnt. Dass selbst die unternehmerische Souveränität in Europa durch eine weitgehende Abhängigkeit von

[10] Veröffentlicht unter https://www.bmwi.de/BMWi/Redaktion/PDF/IT-Gipfel/it-gipfel-2015-plattform-innovative-digitalisierung-wirtschaft-leitplanken-digitaler-souveraenitaet.

unregulierten, vor allem US-amerikanischen IT-Dienstleistern aufgegeben wurde und wird, ist keine Erwähnung wert, ebenso wenig, dass eine verstärkte Regulierung dieser Dienstleister in Europa den hiesigen Wettbewerbern einen gleichberechtigteren Marktzugang eröffnen würde. Nicht einmal die Forderung nach mehr Angebotstransparenz taucht in den eng beschriebenen neun Seiten auf – als habe Transparenz mit Selbstbestimmung und Souveränität nichts zu tun.

Das vom Bundeswirtschaftsministerium in Kooperation mit Bitkom erarbeitete Papier entstand ohne erkennbare Beteiligung von Datenschützern, Verbraucherschützern und Beschäftigtenvertretern, deren „digitale Souveränität" darin folgerichtig auch keine Rolle spielt. Die „digitale Souveränität" ist allerdings auch innerhalb des Bitkom äußerst umstritten, da dort US-amerikanische Unternehmen einen prägenden Einfluss haben. Zu den mehr als 2.300 Unternehmen der digitalen Wirtschaft, die bei Bitkom Mitglied sind, gehören nahezu alle sogenannten Global Player mit Hauptsitz in den USA.[11] Mit Mühe konnten sich diese auf eine höchst fragile Argumentationskette zur „digitalen Souveränität" einigen, die auch die Position der US-Unternehmen wiedergibt.[12]

In den „Leitplanken" finden sich nicht nur die widersprüchlichen Argumente der IT-Wirtschaft wieder, sie greifen auch die zuvor formulierte Positionen der IT-Wirtschaft auf, die nicht müde wird, den Nutzen von Big Data undifferenziert anzupreisen.[13] Dabei wird auf die Notwendigkeit der Beachtung gesetzlicher Regelungen zum Datenschutz hingewiesen, die aber aufgeweicht werden müssten. So heißt es etwa in „Leitlinien für den Big-Data-Einsatz" des Bitkom, im Hinblick auf die damit verbundenen „nennenswerten Investitionen": „Ein Mindestmaß an Rechtssicherheit bezüglich der datenschutzrechtlichen Bewertung ist deshalb unverzichtbar." Bisher sei Big Data „nur unter Schutzaspekten gesetzlich erfasst"; künftig müssten Regelungen „der zentralen Bedeutung von Daten in einer Data Driven Economy gerecht werden. (…) Letztlich erstrebenswert wäre ein globaler Datenschutz, ähnlich einem Weltinformationsethos, wie er bereits auf dem ersten UNESCO-Kongress über ethische und rechtliche Aspekte der digitalen Information im März 2015 in Monaco niedergeschrieben wurde. Die freiwillige Selbstkontrolle ist insbesondere dann geeignet, wenn Rechtsgüter von Verbrauchern betroffen sind, da sich die Verbraucher über eine zentrale Stelle informieren und gegebenenfalls Beschwerde einlegen können."[14] Bitkom veröffentlichte zwölf „Leitlinien für den Big-Data-Einsatz", die in der 12. Leitlinie zusammengefasst werden: „Politische Rahmenbedingungen vervollkommnen – Datenschutz und Datennutzen neu abwägen". Es müssten „Rechte der Betroffenen angemessen geschützt und ungerechtfertigte regulatorische Hindernisse abgebaut werden". „Deutsche Unternehmen dürfen hierbei keinen Wettbewerbsnachteil gegenüber anderen Unternehmen aus anderen EU-Staaten oder anderen Staaten der Welt ausgesetzt werden".[15]

.

[12] Siehe die aufschlussreiche Zusammenstellung unter https://www.bitkom.org/Themen/Standort-Deutschland/Digitale-Souveraenitaet/index.jsp

[13] Eine Zusammenstellung der Bitkom-Äußerungen finden sich unter https://www.bitkom.org/Themen/Hard-und-Software-Services-Loesungen/Big-Data/index.jsp.

[14] Bitkom, Leitlinien für den Big-Data-Einsatz, Positionspapier 15.09.2015, S. 90 f.

[15] Bitkom, Leitlinien für den Big-Data-Einsatz, Positionspapier 15.09.2015, S. 89.

Der frühere Bitkom-Präsident Dieter Kempf gab in einer Rede am 04.03.2015 die neue Richtschnur der Wirtschaft an: „Eine moderne Datenpolitik muss das überkommene Prinzip der Datensparsamkeit, so wenig wie möglich zu sammeln, umkehren. Sie muss dafür sorgen, dass vorhandene Daten auch genutzt werden können: zur Verkehrslenkung, zur Steuerung unseres Energieverbrauchs, zur Überwachung von Körperfunktionen oder für individualisierte Krebstherapien“.[16] Und Sabine Bendiek vom Bitkom ergänzte in einem Blogbeitrag vom 17.06.2015: „Daten sind ein viel zu kostbares Gut, um sie ungenutzt liegen zu lassen.“[17]

Mit den USA kann es jedoch in Sachen Datenschutz keinen einheitlichen Markt geben, solange sich dort nicht das Verständnis für Grundrechte in der digitalen Gesellschaft ändert. Das Datenschutzrecht ist in den USA föderal unter den 50 Bundesstaaten aufgeteilt und oft branchenspezifisch geregelt. Es gibt keine Anerkennung des Datenschutzes als Grundrecht. In den informationstechnisch besonders relevanten Sektoren, etwa im Bereich der Internetwirtschaft, gibt es derzeit allenfalls Regelungen zu Einzelfragen.[18]

Deutschland würde keinen Nutzen daraus ziehen, den niedrigen Rechtsstandard der USA zu übernehmen. Und doch zeigte der IT-Gipfel des Jahres die folgsame Übernahme der Forderungen der internationalen IT-Wirtschaft durch die deutsche Politik.

3.2 Der Entwurf eines „SPD Grundsatzprogramms für die digitale Gesellschaft“

Die Hoffnung, dass die SPD in der Bundesregierung ihren Koalitionspartnern CDU und CSU grundrechtsfreundliche Positionen entgegensetzen würde, kann sich als trügerisch erweisen. Die SPD verabschiedete auf ihrem Parteitag am 10.12.2015 das „erste digitale Grundsatzprogramm einer politischen Partei in der Bundesrepublik Deutschland“. Darin finden sich widersprüchliche Aussagen zum datenschutzrechtlichen Grundsatz der Datensparsamkeit. Die oben dargestellte Argumentation spiegelt nicht nur die Sicht einiger Regierungsmitglieder sowie der Industrie wieder, sondern hat zumindest teilweise in den programmatischen Prozess der SPD Eingang gefunden, die in den kommenden fünf bis zehn Jahren die Grundlage der Digitalpolitik der Partei bilden soll.[19]

Das „Grundsatzprogramm“ enthält viele richtige Darstellungen und Aussagen und mehrere, teilweise redundante Bekenntnisse zum Schutz des Grundrechts auf informationelle Selbstbestimmung. Anders als die zuvor zitierten Statements betont es auch die Relevanz der Transparenz der Datenverarbeitung für die Realisierung informationeller Selbstbestimmung. Die personenbezogene Datenverarbeitung wird jedoch nicht als Grundrechtseingriff verstanden und die konkrete Ausgestaltung des Datenschutzes orientiert sich, ganz wie die zuvor zitierten politischen Statements, hauptsächlich an deren ökonomischer Verwertung:

---

[16] Kempf, https://www.bitkom.org/Presse/Blog/Sind-Daten-die-Waehrung-von-morgen.html.

[17] Bendiek, https://www.bitkom.org/Presse/Blog/Big-Data-braucht-eine-moderne-Datenpolitik.html.

[18] EuGH, U. v. 06.10.2015, C-362/14 – Safe Harbor, vgl. Weichert, Privatheit und Datenschutz im Konflikt zwischen den USA und Europa, RDV 2012, 113.

[19] Bohsem, Lockerer machen, SZ 24.11.2015, 26.

„Der Datenpolitik kommt daher in Zeiten von Big Data eine Schlüsselfunktion zu. (…) Datenpolitik steht in der Verantwortung, die Chancen und Risiken, die sich aus den Möglichkeiten von Big Data ergeben, gegeneinander abzuwägen und für einen Ausgleich der Interessen zu sorgen. (…) Eine Politik, die einseitig auf Vermeidung von Daten und Datensparsamkeit setzt, würde diese Chancen gefährden. Es muss uns daher gelingen, das gesellschaftliche und wirtschaftliche Potential von Daten als Rohstoff des 21. Jahrhunderts nutzbar zu machen und gleichzeitig unsere gesellschaftlichen Werte, wie das Grundrecht auf informationelle Selbstbestimmung und das Recht auf Privatsphäre zu gewährleisten. (…) Auf dieser Grundlage (…) ist es dann das Ziel, möglichst viele Daten für Big-Data-Analysen verfügbar zu machen."[20]

Diese vom SPD-Parteivorstand vorgeschlagene Formulierung im Entwurf war offensichtlich in der parteiinternen Diskussion umstritten. Sie blieb im Beschluss unverändert. Doch wurde an einer völlig anderen Stelle unter der Überschrift „Datenschutz und Innovation" eine Textpassage aufgenommen, die zugunsten des Individuums transparente Anwendungsgestaltung erreichen soll und zu der zitierten Formulierung in einem Spannungsverhältnis steht: „Unverzichtbare Grundlage hierfür sind die Prinzipien der Datensparsamkeit, der Zweckbindung der Datenverarbeitung und der Freiwilligkeit, Daten anzugeben".[21]

SPD-Bundesjustizminister Heiko Maas setzte tendenziell einen Kontrapunkt zu der Positionierung des SPD-Vorsitzenden und Wirtschaftsministers mit seinem Vorschlag für eine „Charta der digitalen Grundrechte". Darin tauchen zwar die Prinzipien der Datensparsamkeit und der Zweckbindung nicht explizit auf, was als Defizit anzusehen ist, doch enthält Art. 2 und seine Begründung folgenden Wortlaut: „Jeder Mensch hat das Recht, über seine persönlichen Daten selbst zu bestimmen. Daten sind angeblich das Öl des 21. Jahrhunderts. Wenn das stimmt, betreiben all diejenigen, die behaupten, Datenschutz sei im digitalen Zeitalter obsolet, unsere Enteignung."[22] Offen bleibt, welche Schlüsse aus dieser richtigen Beobachtung für die Betroffenen und deren Rechte gezogen werden müssen.

4 „Primat des Rechts" statt „Primat der Wirtschaft"

Die Bundesregierung verfolgt derzeit eine Digitalisierungspolitik, die vom Vorrang wirtschaftlicher Erwägungen geleitet wird. Nachdem das Bundesverfassungsgericht in vielen Entscheidungen die Behauptung „Datenschutz ist Täterschutz" widerlegt und im Sicherheitsbereich differenzierte Abwägungen eingefordert hat, wird nun die Wirtschaft gegen den Datenschutz in Stellung gebracht.

[20] SPD Grundsatzprogramm für die digitale Gesellschaft, Entwurf 30.09.2015, Zeilen 1702-1735; Beschluss Nr. 23 v. 11.12.2015, S. 37.

[21] SPD Grundsatzprogramm für die digitale Gesellschaft, Beschluss (Fn. 19), S. 13.

[22] Maas, Internet-Charta: Unsere digitalen Grundrechte, www.zeit.de 10.12.2015.

Ähnliche verwendete Argumentationsmuster sind „Datenschutz verhindert Forschung“[23] oder „Datenschutz kostet Leben“[24].

Diese Denkmuster sind im besten Fall spekulativ und in ihren Grundannahmen falsch. Datenschutz ist weder für die wirtschaftliche Entwicklung noch für Forschung oder Gesundheitsschutz hinderlich. Das Gegenteil kann der Fall sein: So stärkt z. B. die datenschutzrechtlich begründete Feststellung des Europäischen Gerichtshofes, dass die Safe-Harbor-Entscheidung der EU-Kommission aus dem Jahr 2000 rechtswidrig ist, die europäische Wirtschaft, weil sie Unternehmen veranlasst, in Europa zu investieren und die Daten in Europa zu verarbeiten. Datenmassen allein bringen weder Erkenntnisse, noch Fortschritt oder Profit. Auf den intelligenten, innovativen und grundrechtskonformen Gebrauch kommt es an.

Es ist irritierend, dass verantwortliche Politiker und Wirtschaftsvertreter Verfassungsverstöße propagieren, ohne dass hierzu öffentlich Kritik geäußert wird.[25] Der Zweckbindungsgrundsatz, der laut „Leitlinien“ abgeschafft werden soll, hat gemäß Art. 8 Abs. 2 Europäische Grundrechte Charta (EuGRCh) explizit Verfassungsrang. Er ist in Deutschland seit der Entscheidung des Bundesverfassungsgerichts (BVerfG) vom 15.12.1983 zum damaligen Volkszählungsgesetz im deutschen Verfassungsrecht anerkannt.[26] Die Begründung dieses Grundrechts mit dem Menschenwürdegrundsatz der Verfassung lässt eine Abkehr nicht zu; das Datenschutz-Grundrecht unterliegt der Ewigkeitsgarantie des Grundgesetzes. Auch bei heutiger Lektüre haben die Ausführungen des BVerfG zur freien Selbstbestimmung durch die Digitalisierung an ihrer Gültigkeit nichts verloren, sondern eher noch gewonnen:

> „Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen (...) heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. § 2 Abs. 1 BDSG]) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus - vor allem beim Aufbau integrierter Informationssysteme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsichtnahme und Einflussnahme erweitert, welche

[23] So z. B. Riphahn am 08.12.2015, http://www.tagesspiegel.de/wissen/position-der-wissenschaft-droht-blockade-durch-datenschutz/12690960.html.

[24] So Bäuml, 10.12.2015, http://www.zeit.de/2015/48/datenschutz-krankenhaus-opfer-patienten-daten.

[25] Eine Ausnahme ist insofern Marit Hansen, Leiterin des ULD, Die Zukunft der informationellen Selbstbestimmung – mit Datensparsamkeit UND digitaler Souveränität, PE 27.11.2015.

[26] BVerfG NJW 1984, 419.

> auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.
>
> Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.
>
> Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein “belangloses„ Datum mehr.
>
> Wieweit Informationen sensibel sind, kann hiernach nicht allein davon abhängen, ob sie intime Vorgänge betreffen. Vielmehr bedarf es zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs: Erst wenn Klarheit darüber besteht, zu welchem Zweck Angaben verlangt werden und welche Verknüpfungsmöglichkeiten und Verwendungsmöglichkeiten bestehen, lässt sich die Frage einer zulässigen Beschränkung des Rechts auf informationelle Selbstbestimmung beantworten.“[27]

Dies gilt auch in Bezug auf Big Data, wenn wir in der folgenden, dem Volkszählungsurteil des BVerfG entnommenen Textpassage die Begriffe „Statistik“ und „Volkszählung“ durch den Begriff „Big Data“ ersetzen und anstelle der „Auskunftspflicht“ die generelle informationelle Betroffenheit der Menschen setzen:

> Gerade weil es von vornherein an zweckorientierten Schranken fehlt, die den Datensatz eingrenzen, bringt *Big Data* tendenziell die Gefahr einer persönlichkeitsfeindlichen Registrierung und Katalogisierung des Einzelnen mit sich. Deshalb sind an die Datenerhebung und Datenverarbeitung für Zwecke des *Big Data* besondere Anforderungen zum Schutz des Persönlichkeitsrechts der betroffenen Bürger zu stellen.
>
> Dieses Ziel kann nur erreicht werden, wenn bei dem betroffenen Bürger das notwendige Vertrauen in die Abschottung seiner für *Big-Data*-Zwecke genutzten Daten geschaffen wird, ohne welche seine Bereitschaft, wahrheitsgemäße Angaben zu machen, nicht herzustellen ist. Eine Praxis, die sich nicht um die Bildung eines solchen Vertrauens durch Offenlegung des Datenverarbeitungsprozesses und strikte Abschottung bemühte, würde auf längere Sicht zu schwindender Kooperationsbereitschaft führen, weil Misstrauen entstünde.
>
> Kann damit nur durch eine Abschottung von *Big Data* dessen Zielsetzung erreicht werden, ist das Prinzip der Geheimhaltung und möglichst frühzeitigen Anonymisierung der Daten nicht nur zum

[27] BVerfG NJW 1984, 421 f.

> Schutz des Rechts auf informationelle Selbstbestimmung des Einzelnen vom Grundgesetz gefordert, sondern auch für *Big Data* selbst konstitutiv.[28]

Diese Feststellungen werden von den wirtschaftlichen Erwägungen zu Big Data konterkariert. Der Abgesang auf die Grundsätze der Datensparsamkeit und der Zweckbindung durch Teile der Politik und der Wirtschaft greift nicht eine konkrete Ausgestaltung bzw. Umsetzung des Datenschutzes an, sondern stellt de facto die Existenz des Grundrechts auf informationelle Selbstbestimmung in Frage: Eingriffe in Grundrechte bedürfen einer Rechtfertigung, setzen also einen legitimen Zweck voraus. Eine Verarbeitung persönlicher Daten ist nur zulässig, wenn sie erforderlich ist. Folgt man den dargestellten Positionen, werden informationelle Grundrechtseingriffe ohne rechtlichen Grund legitimiert. Daten werden zum ökonomischen Selbstzweck erklärt.

Trifft es zu, dass personenbezogene Daten Ware und Währung in der globalisierten Informationsgesellschaft sind, was schwerlich zu bestreiten ist, dann ist die Forderung nach dem Verzicht auf eine Rechtfertigung und eine Erforderlichkeitsprüfung nicht nur ein unzulässiger Eingriff in das Recht auf informationelle Selbstbestimmung, sondern zugleich auch – und da hat Heiko Maas Recht – eine ungerechtfertigte und willkürliche informationelle Enteignung, also ein Verstoß gegen Art. 14 GG.

Bemerkenswert ist, dass die politischen Statements zum Wirtschaftspotenzial von Big Data – so auch das digitale Grundsatzprogramm der SPD – nicht die mit Big Data verbundenen Gefahren für Freiheitsrechte und Demokratie thematisieren. Welches Potenzial in Big Data steckt, zeigen die Überwachung der Weltbevölkerung durch die Geheimdienste; nicht nur der USA und Großbritanniens, und die informationelle Totalkontrolle der chinesischen Bevölkerung durch die dortigen Zensur- und Sicherheitsbehörden und auch der Marktmachtmissbrauch privater Unternehmen wie Google und Facebook.

Datenschutz ist nicht digitalisierungsfeindlich. Es mag sein, dass manche Menschen schwer nachvollziehbare oder unbegründete Ängste vor der Digitalisierung der Gesellschaft haben. Der Datenschutz schürt diese Ängste nicht, sondern trägt zu deren Abbau bei, indem er effektive Instrumente gegen die tatsächlichen Bedrohungen wie informationelle Ausforschung, Manipulation, Diskriminierung, Fremdbestimmung oder informationelle Ausbeutung bietet. Wer eine Datenökonomie will, darf nicht Vertrauen in Datenschutz bei den Bürgern einfordern und gleichzeitig Schutzrechte abbauen. Vertrauen lässt sich nur erreichen, wenn der geforderte Schutz auch faktisch gewährleistet wird.

5 Big Data und digitalen Grundrechtsschutz zusammen verwirklichen

Die Kampagne gegen das Prinzip der Datensparsamkeit in der Europäischen Datenschutz-Grundverordnung (EU-DSGVO) war erfreulicherweise nicht erfolgreich.[29] Das Prinzip und dessen

[28] Originalzitat BVerfG NJW 1984, 423.

[29] EU-DSGVO-Vorschlag, abrufbar unter https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPD_consolidated_LIBE-vote-2015-12-17.pdf.

praktische Umsetzung durch „Privacy by Default“ sind in Art. 23 ausdrücklich festgeschrieben. Dies wird aber die bisherigen Gegner nicht daran hindern, diesen Grundsatz weiterhin anzugreifen.

Die EU-DSGVO ist zu Big Data in Art. 20, der Regelung zu „automatisierten Einzelentscheidungen, einschließlich Profiling“, wenig konkret. Darin wird ein Anspruch für jede Person bestätigt, „nicht einer allein auf einer automatisierten Entscheidung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie erheblich beeinträchtigt“. Materielle Voraussetzungen für solche Entscheidungen sind ein Vertrag mit der betroffenen Person, eine konkretisierende Rechtsvorschrift oder die „ausdrückliche Einwilligung der betroffenen Person“. Ergänzend fordert Art. 20 „geeignete Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf persönliches Eingreifen des für die Verarbeitung Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung gehört“.

Damit wird ein normativer Rahmen für eine Optimierung von Persönlichkeitsschutz und ökonomischer Datenverwertung gesetzt. Es darf nicht darum gehen, Silicon Valley zu kopieren; es muss das Ziel europäischer Politik und Praxis der Datenverarbeitung sein, es anders und besser zu machen als die wirtschaftsgläubigen und technikfixierten Vorreiter.

Die mit dem Ziel der Wirtschaftsförderung formulierten Angriffe auf den Datenschutz mögen ein Indiz dafür sein, dass die Kenntnisse über die Möglichkeiten, Big-Data-Analysen und Datenschutz in Einklang zu bringen, noch wenig verbreitet sind. Tatsächlich lassen sich mit Anonymisierungs- und Pseudonymisierungsmechanismen die persönlichkeitsrechtlichen Risiken der Ansammlung und Auswertung großer Datenmengen reduzieren. Das wusste 1983 schon das Bundesverfassungsgericht. Deshalb sind Pseudonymisierung und Anonymisierung zentrale Strategien zur Realisierung von Datensparsamkeit und Datenminimierung (vgl. § 3a S. 2 BDSG). Die Vorstellung, diese technisch-organisatorischen Mechanismen genügten, um einen effektiven Persönlichkeitsschutz realisieren zu können, ist jedoch naiv. Vielmehr bedarf es – wie schon die obige Referenz auf das BVerfG zeigt – eines umfassenden Instrumentensets, um Persönlichkeitsschutz und Erkenntnis durch Datenauswertung, also z. B. die Schaffung wirtschaftlich nutzbaren Wissens, in Einklang zu bringen bzw. diese Ziele zu optimieren.

Wie eine Konkretisierung eines solchen Instrumentensets aussehen kann, wird derzeit im Auftrag des Bundesministeriums für Wirtschaft erforscht, hat aber offensichtlich bisher noch wenig Eingang in die politische Meinungsbildung des Ministeriums gefunden. Unter der Überschrift „Smart Data – Smart Privacy“ werden „Impulse für eine interdisziplinär rechtlich-technische Evaluation“ von Big Data gesucht.[30] Ziele sind dabei nicht einseitig eine neue pseudo-objektive Erkenntnishöhe und ein damit verbundenes Wirtschaftspotenzial, sondern konkrete Handlungsmöglichkeiten zur Förderung individuell wirkender und zugleich gesellschaftlich erwünschter Innovation. Angeknüpft wird dabei bewusst an den Ausführungen des Volkszählungsurteils des BVerfG mit dem Anliegen eines

[30] Smart-Data-Begleitforschung, FZI Forschungszentrum Informatik Smart Data Smart Privacy? November 2015, http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/SmartData_Thesenpapier_smart_Privacy.html; im Folgenden wird auf diesen Report Bezug genommen.

normativen und technologischen Ausgleichs widerstreitender Positionen. Dieser Ansatz der „Wissenskontrolle“ zielt nicht auf Deregulierung, sondern auf staatliche Regulierung, ohne das Potenzial von Selbstregulierungsmöglichkeiten auszuschließen.

Datensparsamkeit ist dabei nicht ein „Weniger“ als Gegensatz zum platten „Mehr“ an Daten, sondern ein Konzept zur „Minimierung der Eingriffsintensität“, bei dem Anonymisierung und Pseudonymisierung wichtige, aber nicht allheilende Instrumente sind. Vielmehr müssen vor Auswahl technisch-organisatorischer Maßnahmen Risikobewertungen nach einem sachgerechten Verfahren vorgenommen werden, um ihren sinnvollen Einsatz überhaupt erst zu ermöglichen. Besonders schützenswert ist die „Wissensgenerierung über die Privatsphäre des Einzelnen“ sowie über rechtlich als sensibel eingestufte Daten. Während offene Systeme regelmäßig sowohl aus Grundrechtssicht wie auch aus Erkenntnissicht als problematisch eingestuft werden müssen, sind anwendungsspezifische und kontextbezogene Analyseverfahren positiver zu bewerten. Big oder Smart Data produzieren nicht automatisch Mehrwert sondern sind von einem umfangreichen Bedingungsgefüge abhängig, in dem eine Risiko- und eine Erkenntnisabschätzung zueinander in Beziehung gesetzt werden müssen und bei dem folgende Aspekte relevant sind:

- demokratische Legitimation des Analyseverfahrens (einschließlich parlamentarischer, administrativer oder gerichtlicher Zulassungs- und Kontrollprozesse),
- öffentliche Transparenz von Input, Verfahren und Output,
- Options- und Rechtsschutzmöglichkeit für Betroffene (Opt-in, Opt-out, Auskunft, nachträgliche individuelle Intervention),
- Einsatz technisch-organisatorischer Maßnahmen gemäß dem Standard-Datenschutzmodell (unter Berücksichtigung der Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit und Nichtverkettbarkeit),
- Verwendung von Standards und zertifizierten Vorgehensweisen zur Risikobewertung und Folgenabschätzung.

6 Umdenken gefordert

Die Digitalisierung aller gesellschaftlichen Bereiche und das Internet von heute werden in Deutschland von gesetzlichem Denken zu Anfang der 1990er Jahre bestimmt. Deutschland ist in der Entwicklung technologischer Grundlagen nicht schlechter aufgestellt als die USA oder China. Mit dem deutschen Schlagwort „Industrie 4.0“ verbinden sich fortschrittliche technische Innovationen, mit denen sowohl gesellschaftliche Erkenntnisse wie auch wirtschaftlicher Fortschritt erreicht werden können. Geht es bei „digitaler Souveränität“ um die Kompetenz zur technischen Gestaltung, so ist Deutschland durchaus souverän.

Ist aber auch die Politik „digital souverän“? Daten- und IKT-Politik in Deutschland erschöpft sich bisher darin, Grundrechte und politische Gestaltungsmöglichkeiten in der Informationsgesellschaft zum Widerspruch zu erklären und wertfrei und ideenlos quantitatives Wachstum zu predigen. Die Debatte um den Datenschutz ist Beleg für die bisherige Unfähigkeit, möglicherweise aber auch die Unwilligkeit politischer Meinungsführer, die Werte unserer demokratischen und freiheitlichen Verfassung mit moderner Technik und einer innovativen Gesellschaft zusammenzuführen.

Digitale Fremdbestimmung und Ausbeutung mit Big-Data-Instrumenten sind keine Spezialität ausländischer IKT-Unternehmen, sondern werden auch – wenn dem staatlicherseits nicht entgegengesetzt wird – von deutschen Unternehmen praktiziert. Ein beredtes Beispiel hierfür ist die Zusammenführung und Auswertung von medizinischen Verschreibungsdaten und deren Bereitstellung für die Pharmaindustrie.[31]

Während in Deutschland das höchste Gericht zukunftsweisende Maßstäbe setzt, gelingt es der Politik seit mehr als 30 Jahren nicht, eine Datenpolitik zu formulieren und zu gestalten, bei der die digitalen Grundrechte wie auch die im Interesse der Öffentlichkeit liegenden Erkenntnisse bei Auswertung vorhandener Daten zur Geltung gebracht werden. Sie hat wenig für die Umsetzung der weitsichtigen richterlichen Vorgaben getan und nichts für die Ausgestaltung der zukünftigen Entwicklung. Trotz entsprechender einhelliger Forderungen – etwa aus dem Bereich der Forschung oder der Gesundheitswirtschaft – sahen sich Bundesregierung und Bundestag nicht veranlasst, die rechtlichen Voraussetzungen für wissenschaftlichen Fortschritt, ökonomischen Erfolg und digitalen Grundrechtsschutz zu schaffen. Die nationalen Öffnungsklauseln in der EU-DSGVO geben dem deutschen Gesetzgeber aktuell eine neue Chance. Die Ideen liegen auf dem Tisch. Woran es fehlt, ist der politische Gestaltungswille in Sachen Daten(schutz)politik und Informationsgesellschaft. Politisches Handeln erschöpft sich bisher darin, Rolle und Gestaltung der IKT in den USA kopieren zu wollen und damit bei der Umsetzung schon per definitionem der abgeschlagene Zweite zu bleiben. Nötig wäre jedoch die Vorstellung einer deutschen und europäischen Zukunft, verbunden mit dem Willen, diese grundrechtskonform zu gestalten.

[31] Millionen deutsche Patienten und Ärzte werden ausgespäht, www.spiegel.de 18.08.2013.