Die DSGVO – Ausgangspunkt für europäischen digitalen Grundrechtsschutz

Überlegungen anlässlich der Evaluation der DSGVO und des Beginns der deutschen Präsidentschaft im Europäischen Rat

Stand: 17.08.2020

Thilo Weichert
weichert@netzwerk-datenschutz-expertise.de
Waisenhofstraße 41, 24103 Kiel
www.netzwerk-datenschutzexpertise.de

Inhalt

Die inzwischen über 2 Jahre praktisch erprobte europäischen Datenschutz-Grundverordnung (DSGVO) stellt die Verwaltungspraxis, die Politik wie die Bürgerrechtsbewegung vor Herausforderungen. Sie verfolgt das Ziel, Grundrechte, demokratische Strukturen und Rechtsstaatlichkeit angesichts der Digitalisierung unserer Gesellschaft zu wahren. Diese sind durch Einflüsse bedroht, die aus den USA und in letzter Zeit verstärkt aus China kommen. Um sich diesen Entwicklungen entgegenzustellen kann und sollte die DSGVO als valide Grundlage genutzt werden für eine Weiterentwicklung des Grundrechtsschutzes in einer globalisierten Informationsgesellschaft, bei der es nicht mehr nur um die Verteidigung von Privatsphäre und von informationeller Selbstbestimmung geht, sondern um demokratische Teilhabe, Rechtsstaatlichkeit und Freiheitswahrung generell. Die seit Juli 2020 bestehende deutsche Präsidentschaft im Rat der Europäischen Union sollte die DSGVO zu einem zentralen Baustein ihrer umfassenderen Strategie zur Digitalisierung und zum Grundrechtsschutz nehmen.

1 In der Klemme zwischen den USA und China

Informationeller Grundrechtsschutz hat seine Wurzeln in den USA. Es waren die US-Juristen Samuel D. Warren und Louis D. Brandeis, die mit ihrem Aufsatz „The Right to Privacy“ im Jahr 1890 die rechtlichen Grundüberlegungen zu einem Immaterialgüter- und Privatheitsschutz legten.[1] Und es war Alan F. Westin, der 1966 mit „Privacy and Freedom“[2] die erste umfassende Analyse auf der Grundlage der inzwischen bestehenden Informationstechnik lieferte und hieraus verfassungsrechtliche Anforderungen ableitete. Seitdem ging es mit dem informationellen Grundrechtsschutz in den USA bergab und in Europa bergauf. Wichtige Wegmarken waren die Datenschutzgesetzgebung in Europa in den 70er Jahren, das Volkszählungsurteil des deutschen Bundesverfassungsgerichts (BVerfG) 1983[3], die europäische Datenschutz-Richtlinie aus dem Jahr 1995[4], die explizite Grundrechtsfixierung des Datenschutzes in Art. 8 der seit 2009 wirksamen europäischen Grundrechte-Charta (GRCh) und nun jüngst die seit dem 25.05.2018 in der Europäischen Union (EU) direkt anwendbare Datenschutz-Grundverordnung (DSGVO).[5]

Rechtlicher Grundrechtsschutz und faktische Grundrechtsdurchsetzung sind zwei Welten, die sich im Dauerkonflikt befinden. Alan F. Westin hat dies schon für die 60er Jahre beeindruckend und ernüchternd dargestellt. Spätestens seit dem Aufkommen des Internets entwickeln sich Rechtsanspruch und Realität schneller und weiter auseinander. US-Unternehmen wie Microsoft, Google, Apple, Facebook und Amazon begründeten ihre auf Informationstechnik basierenden Geschäftsmodelle ohne grundrechtliche Rücksichtnahmen. Es sind insbesondere Google und Facebook, die mit der Vermarktung ihres Wissens über ihre Digitalkunden vorrangig für Werbezwecke den globalen Markt dominieren. Während Google noch minimal Rücksicht auf rechtliche Vorgaben nimmt, basiert das Geschäftsmodell von Facebook von Anfang an und weiterhin auf Rechtsbruch.[6] In den USA wird dieser bisher rechtlich und politisch weitgehend billigend in Kauf genommen, nicht

[1] Warren/Brandeis, The Right to Privacy, Harvard Law Review, Vol. IV Dec.. 15, 1890 No. 5, übersetzt in DuD 2012, 755 ff. = FIfF-Ko 2/2012, 45 ff.; dazu Weichert DuD 2012, 753 f.
[2] Westin, Privacy and Freedom, 6th printing, 1970.
[3] BVerfG, U. v. 15.12.1983 – 2 BvR 209/83 u.a., NJW 1984, 419 ff.
[4] Richtlinie 95/46/EG v. 24.10.1995, ABl. v. 23.11.1995, L 281, 31.
[5] Verordnung (EU) 2016/679, ABl. v. 04.05.2016, L 119/1
[6] Weichert, DuD 2012, 716 ff.

zuletzt, weil damit erwünschte globale ökonomische und sicherheitspolitische, für das Land als positiv bewertete Effekte einhergehen: Es sprudeln nicht nur die Finanzquellen für die Unternehmen, sondern auch die Datenquellen, derer sich die US-Behörden nach Belieben bedienen.

Seit Beginn des 21. Jahrhunderts drängen chinesische Firmen auf diesen globalen Markt. Gegenüber den US-Firmen stehen sie direkt unter der Aufsicht und der Fürsorge der chinesischen Regierung bzw. der diese leitenden kommunistischen Partei. Ihr informationstechnisches Handeln ist von menschenrechtlichen oder demokratischen Erwägungen vollständig befreit. Alibaba entwickelt sich auf den Märkten weltweit als ernsthafte Konkurrenz zu Amazon im Bereich der Online-Vermarktung. Huawei etablierte sich als globaler Marktführer bei der Netzausstattung. Mit TikTok schaffte es ein chinesischer Anbieter, in die Dominanz der US-Firmen im Social-Media-Bereich einzubrechen. Die auch in Europa eingesetzten Geschäftsmodelle chinesischer Anbieter sind aus europäischer Sicht nicht besser als die Praktiken der US-amerikanischen Konkurrenz.

In Europa wird mit diesem Geschäftsgebaren das Grundrecht auf Datenschutz verletzt, ohne dass es Politik, Verwaltung und Gerichten bisher gelungen ist, diese Verstöße gegen die die europäische Grundrechte-Charta und die DSGVO nachhaltig zu beenden. Von der europäischen und allen voran die deutsche Politik wurde diese Entwicklung über viele Jahre hinweg zunächst mit ungläubigem, dann begeistertem Staunen verfolgt. Erst in jüngster Zeit weicht dies dem Erschrecken. Unternehmen aus Nordamerika und Südostasien besetzen sukzessive die informationstechnischen Märkte und überlassen den europäischen Unternehmen allenfalls Zubringer- oder Hilfsdienste. Gestützt wurde und wird dieses Machtverhältnis durch das in Europa geltende Recht, das zersplittert und nationalen Egoismen folgend keine gemeinsame Antwort auf die Herausforderungen der neuen Digitalmärkte fand: Während die ausländischen Unternehmen ihre illegalen Geschäftsmodelle weiterentwickeln konnten, sahen und sehen sich die inländischen Unternehmen weiterhin einem hohen regulativen Druck, auch im Bereich des Datenschutzes, ausgesetzt. Dies brachte und bringt die europäischen Unternehmen weiter ins technische und wirtschaftliche Hintertreffen.

2 Die europäische Antwort

Die europäische Politik in Brüssel entwickelte für diese schleichende digitale Entmündigung, früher und klarer als die nationale Politik, ein zunehmendes Bewusstsein. Eine Antwort auf die digitale, ökonomische und letztlich sicherheitspolitische Bedrohung ist die DSGVO: Nur durch einen Zusammenschluss in der Union und eine rechtliche Harmonisierung besteht die Chance, den globalen Herausforderungen durch US- und anderen ausländischen Unternehmen entgegenzutreten und dabei zugleich die bestehenden rechtlichen Werte zu bewahren. Der Fokus der DSGVO liegt auf dem Schutz personenbezogener Daten, also letztlich dem Schutz der Privatsphäre sowie des allgemeinen Persönlichkeitsrechts. Diese sind durch die zunehmende Digitalisierung aller Lebensbereiche immer stärker bedroht.

Die Herausforderungen durch außereuropäische Unternehmen gehen aber darüber hinaus: Diese monopolisieren die Digitalmärkte in Europa, gefährden mit ihrer unbeschränkten Verbreitung von Hassrede und Falschnachrichten den demokratischen Diskurs, machen Profit ohne Steuern zu zahlen oder auch nur für die gesellschaftlich verursachten Schäden aufzukommen und betreiben eine Kommunikationsinfrastruktur, die nicht nach demokratischen Regeln funktioniert und deren Sicherheit

vom Wohlwollen der Unternehmen abhängt. Sie usurpieren die europäischen Märkte, beeinflussen dadurch den Meinungsaustausch und die Meinungsbildung und verhindern das Sichentwickeln von grundrechtsorientierten, demokratisch und rechtsstaatlich kontrollierten Alternativen. Beeinträchtigt ist damit nicht nur die informationelle Selbstbestimmung der Nutzenden, sondern generell die gesellschaftliche und staatliche Souveränität im Bereich der Digitalisierung.

Die Antworten der DSGVO auf die geschilderten Herausforderungen in Sachen Persönlichkeitsschutz scheinen dem ersten Anschein nach angemessen zu sein: Mit einem einheitlichen materiell-rechtlichen und prozeduralen Rahmen wird ein gemeinsamer Rechtsraum geschaffen, in dem eine wirksame Rechtsverfolgung und Sanktionierung angestrebt wird unter Stärkung der Betroffenenrechte und der Möglichkeiten der staatlichen Aufsicht. Anknüpfend an bestehende Strukturen wird durch Kooperations- und Kohärenzmechanismen eine dezentral agierende und zugleich zentral wirksame Exekutive angestrebt. Mit dem Europäischen Gerichtshof (EuGH) besteht eine Instanz zur verbindlichen Klärung europaweit bestehender Anwendungskonflikte.

Die DSGVO blieb nicht das einzige Instrument zur Abwehr der mit der Digitalisierung entstandenen Gefahren. Europäische Initiativen für mehr Informationssicherheit[7], für eine Digitalsteuer[8], gegen die digitalen Marktmonopole oder durch Absprachen bei Ausschreibungen für den neue 5G-Mobilfunkstandard zur Verhinderung einer technischen Abhängigkeit von nichteuropäischen Einflüssen sind weitere Schauplätze, mit denen die Politik der EU versucht, die Dominanz der außereuropäischen Unternehmen zurückzudrängen und die eigenen zu stärken. Am 19.02.2020 stellten Margret Vestager (Digitales) und Thierry Breton (Binnenmarkt) dazu eine Digitalstrategie der EU-Kommission vor.[9]

3 Evaluation der DSGVO

Vor diesem Hintergrund ist eine Evaluation der DSGVO zwei Jahre nach ihrem Wirksamwerden von großer Relevanz. Die EU-Kommission stellte sich dieser Herausforderung und legte am 24.06.2020 einen Bericht[10] sowie einen diesen erläuternden Arbeitsbericht[11] vor. Auch die Nichtregierungsorganisationen (NGOs) in Europa werteten die bisher gesammelten Erfahrungen aus. Während die EU-Kommission ein grundsätzlich positives Resümee zieht, den Grundansatz der DSGVO als valide bewertet und einige spezifische Korrekturen vorschlägt, äußerten die im Dachverband der europäischen Datenschutzorganisationen EDRi (European Digital Rights) zusammengeschlossenen 44 NGOs aus 19 EU-Mitgliedstaaten eher Fundamentalkritik. EDRi teilt zwar die Grundanliegen der DSGVO, stellt aber infrage, dass diese tatsächlich erreicht werden:[12] Die Umsetzung der Verordnung in vielen Mitgliedstaaten sei ungenügend und systematische Verstöße blieben ungeahndet. Staaten wie

[7] European Network and Information Security Agency (ENIS), Richtlinie (EU) 2016/1148 v. 06.07.2016 (NIS-RL); Ruhmann/Bernhardt, IT-Sicherheit und Telekommunikationsrecht, 15.11.2017, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_tkg-neufassung2017.pdf.
[8] Gammelin, Am Ball – Paris und Berlin betonen Einigkeit bei Digitalsteuer, Süddeutsche Zeitung (SZ) 23.06.2020, 5.
[9] Beisel, Gesichtsverlust, SZ 20.02.2020, 18.
[10] European Commission, Data protection rules as a pilar of citizen´s empowerment and EU´s approach to digital transition – two years of application of the General Data Potection Regulation, COM(2020) 264.
[11] European Commission, Commission Staff Working Document, SWD(2020) 115.
12 EDRi, 25.05.2020, https://edri.org/open-letter-edri-urges-enforcement-and-actions-for-the-2-year-anniversary-of-the-gdpr/.

Ungarn, die Slowakei oder Rumänien würden die Datenschutzbehörden politisch instrumentalisieren, um gegen die freie Presseberichterstattung vorzugehen. In Polen werde die DSGVO zur Durchsetzung von undemokratischen Regierungszielen missbraucht.

Die noyb-Initiative des Aktivisten Max Schrems (none of your business) stellte gar fest, dass die irische Datenschutzbehörde (DPC) mit dem globalen Platzhirsch im Bereich der sozialen Medien – Facebook – zwecks Umgehung der geltenden Regelungen regelrecht konspiriert. Schrems wirft der DPC vor, in zehn gemeinsamen Sitzungen mit dem Unternehmen einen Plan ausgearbeitet zu haben, mit dem die strengen Anforderungen der DSGVO an eine wirksame Datenschutzeinwilligung umgangen werden können, indem stattdessen ein „Datennutzungsvertrag" fingiert wird.[13] Ein solches Vorgehen trifft einen Nerv der in der DSGVO vorgesehenen Mechanismen zur Durchsetzung des Datenschutzes, da die irische Aufsichtsbehörde wegen des europäischen Hauptsitzes von Facebook in Irland für die Kooperation und Durchsetzung federführend ist. Ihren Hauptsitz in Irland haben außerdem u.a. Google und Apple. Ein ähnliches Problem tut sich in Luxemburg auf, wo weitere wichtige Digitalunternehmen, z.B. Amazon, ihren Hauptsitz haben. Hintergrund dieser Standortpolitik, zu der auch eine nachsichtige Datenschutzaufsicht gehört, sind massive Steuervergünstigungen in diesen eher marginalen EU-Mitgliedstaaten. So wird der Datenschutz als digitaler Grundrechtsschutz zum steuer- und wirtschaftspolitischen Faktor.

Die Defizite bzgl. der Umsetzung der DSGVO sind aber nicht nur ökonomisch bedingt. Sie beruhen auch auf bürokratischen Beharrungskräften und einer Bürgerrechtsverweigerung durch viele Regierungen. Slowenien sah es bis heute nicht für nötig an, die Vorgaben der DSGVO normativ umzusetzen.[14] In Österreich ist die nationale gesetzliche Umsetzung, so z.B. Max Schrems, zur „Pfuschaktion" missraten. Die Umsetzung in Deutschland ist ähnlich kritikwürdig: Sachsen-Anhalt hat eine Anpassung an die DSGVO bisher vollständig verweigert. Niedersachsens Regierung missachtet bewusst zentrale DSGVO-Vorgaben.[15] Und auch auf nationaler Ebene wurde die DSGVO-Umsetzung weitgehend nur nominell umgesetzt und in einigen Bereichen dazu genutzt, den Datenschutz zurückzuschrauben. Die im EDRi-Dachverband organisierten Mitgliedsorganisationen haben Beispiele aufgelistet, bei denen die DSGVO nicht umgesetzt wurde, diese bewusst ignoriert oder deren Intention gar konterkariert wird.

Liest man dagegen die Evaluation der EU-Kommission, so erscheint die DSGVO in einem erheblich positiveren Licht. Unternehmen mit Hauptsitz in den USA oder China werden mit keinem Wort erwähnt. Doch hinter der diplomatischen Darstellung und zwischen den Zeilen tauchen die gleichen Defizite auf: Das ungenügende Funktionieren der Kooperations- und Kohärenzmechanismen wird konstatiert[16], ebenso wie die ungenügende Ausstattung der Datenschutzaufsicht durch die nationale Politik[17] oder der misslungene Ausgleich zwischen Meinungsfreiheit und Datenschutz.[18]

[13] Moechel, Datenschutz-NGOs frontal gegen Datenschutzbehörden, 31.05.2020, fm4.orf.at/stories/3003167/.
[14] Commission (Fn. 10), S. 6; Commission Staff Working Document (Fn. 11), S. 26.
[15] Deutsche Vereinigung für Datenschutz (DVD), DANA 2/2019, 79.
[16] Commission (Fn. 10), S. 5.
[17] Commission (Fn. 10), S. 6.
[18] Commission (Fn. 10), S. 7.

4 Positive Effekte

Das Glas der DSGVO ist zwar halb leer, es ist aber auch halb gefüllt. Für die Bewertung der DSGVO ist relevant, dass Datenschutz zuvor noch weniger ernst genommen wurde, etwa wegen der minimalen drohenden Sanktionen bei Verstößen. Die maximale Bußgeldhöhe betrug z.B. in Deutschland 300.000 Euro, gemäß der DSGVO sind es nun 4% des globalen Jahresumsatzes eines Unternehmens (Art. 83 Abs. 4, 5 DSGVO). Es ist leider kein Paradoxon, dass Liberalität – digitaler Freiheitsschutz – in der DSGVO nur mit massiven Sanktionsandrohungen realisiert werden kann. Datenverarbeitung ist weitgehend ökonomisch motiviert. Solange sich Rechtsverstöße wirtschaftlich lohnen, gibt es keinen Grund, diese einzustellen. Tatsächlich hatten die Sanktionsdrohungen der DSGVO insbesondere in der deutschen Wirtschaft und im gesellschaftlichen Leben die Wirkung, dass die eklatanten Vollzugsdefizite beim Datenschutz reduziert wurden. Datenschutz wird erstmals von vielen Akteuren wahr- und ernstgenommen und in der Praxis umgesetzt und nicht, wie bisher oft, ignoriert oder eingepreist.

Nach den ersten zwei Jahren der DSGVO-Anwendung muss man aber den Eindruck haben, dass die Kleinen gehängt werden, während man die Großen laufen lässt. Und diese Großen haben ihren Hauptsitz regelmäßig in den USA. Darüber kann das Datenschutzgesäusel der Großkonzerne[19] oder mancher staatlichen Einrichtung nicht hinwegtäuschen. Medial verbreitete Lippenübungen haben oft ausschließlich die Funktion, von den tatsächlichen Rechtsverstößen abzulenken. Geht es um eine effektive Umsetzung der DSGVO, stößt man immer noch auf heftige Gegenwehr. Wie wenig Einsicht oft besteht, demonstriert wohl an anschaulichsten Facebook, das trotz vollmundigem Propagieren individueller Selbstbestimmung kein Jota ihres Selbstbestimmung leugnenden Geschäftsmodells aufgibt, wenn das Unternehmen nicht durch Aufsicht und Gerichte hierzu gezwungen wird.

Die DSGVO – bestärkt durch den EuGH mit seiner Rechtsprechung z.B. zu Safe Harbor[20], zu Google[21] oder Facebook[22] – erweist sich aber trotz aller Ernüchterung durch die Praxis als ein Gegenkonzept zur Überwachungsstaatlichkeit und Überwachungskapitalismus,[23] Sie könnte ein Rezept gegen die US-amerikanische und chinesische Gefährdung digitaler Grundrechte sein. Sie verbietet die digitale Gleichschaltung von Menschen und Gesellschaft nach dem Willen eines dominanten Partei- und Staatsapparats, so wie dies in China praktiziert wird. Sie steht auch der US-amerikanischen Variante entgegen, wo der Staat den Konzernen weitgehend freien Lauf lässt bei ihrem Bestreben, die auf Konsumenten reduzierten Menschen informationell auszubeuten, und wo sich die Geheimdienste der informationellen Möglichkeiten der Konzerne nach Belieben bedienen, auch um daraus politisches Kapital zu schlagen. Für die Bürgerrechtsorganisationen und selbst für Teile des politischen Establishments in den USA ist die DSGVO Vorbild für eine nationale Regulierung von „Privacy“. Im Bundesstaat Kalifornien wurde ein Datenschutzgesetz verabschiedet, dem die DSGVO Pate stand.[24]

[19] Z.B. Graff, Brunftiges Einhorn - Der Facebook-Konzern will sich neu erfinden, SZ 06.11.2019, 11.
[20] EuGH 06.10.2015 – C-362/14.
[21] EuGH 13.05.2014 – C-131/12.
[22] EuGH 05.06.2018 – C-210/16.
[23] Vgl. z.B. Zuboff, Das Zeitalter des Überwachungskapitalismus, 2018.
[24] Kalifornien verabschiedet Internet-Datenschutzgesetz, DANA 3/2018, 154.

Die DSGVO hat auch Vorbildwirkung in Staaten, die mit Europa Handel betreiben und durch eine entsprechende Gesetzgebung Erleichterungen bei informationellen Wirtschaftsaktivitäten erhoffen. So wurde nach gesetzlichen Änderungen der Datenschutz in Japan von der EU-Kommission als angemessen anerkannt.[25] Brasilien hat sich ein Gesetz gegeben, das sich an der DSGVO orientiert.[26] Auch in Chile, Südkorea, Kenia und Indien steht die DSGVO Pate für entsprechende Regulierungen.[27]

5 Digitaler Grundrechtsschutz

Bei der DSGVO steht zwar der Grundrechtsschutz nach Art. 8 GRCh, also der Datenschutz, im Mittelpunkt. Zugleich verfolgt sie aber darüber hinausgehend das Ziel, generell die Grundrechte und Grundfreiheiten natürlicher Personen bei der Digitalisierung zu schützen (Art. 1 Abs. 2 DSGVO). Adressiert werden damit der Schutz des Telekommunikationsgeheimnisses in Art. 7 GRCh, der in Art. 21 GRCh garantierte Schutz vor (digitaler) Diskriminierung sowie anderweitiger Schutz, etwa von Kindern und Familien, von Verbrauchern und Beschäftigten, der demokratischen Meinungsbildung. Mit einer weitgehenden Privilegierung wissenschaftlicher Forschung (Art. 13 GRCh) liefert sie die Grundlagen für einen evidenzbasierten Fortschritt.[28] Die DSGVO verfolgt damit umfassend das Ziel der Wahrung von Demokratie und Rechtsstaatlichkeit in einer freiheitlichen Informationsgesellschaft.[29]

Die DSGVO kann insofern nur ein wichtiger Zwischenschritt sein. Um eine demokratische und freiheitliche Informationsgesellschaft zu wahren bzw. zu entwickeln, bedarf es eines umfassenderen Rechtsrahmens. Grundlage hierfür sollte ein neuer verfassungsrechtlicher Rahmen sein, wozu es mit den Entwürfen für eine „Charta der digitalen Grundrechte der Europäischen Union“ erste Vorschläge gibt.[30] Dabei geht es um die rechtliche Einhegung von selbstlernenden maschinellen Systemen, der sog. „künstlichen Intelligenz“ und von „Big Data“ bzw. generell um Algorithmenkontrolle, um die Verwirklichung von Informationsfreiheit in Staat und Wirtschaft sowie um eine Grundversorgung mit digitalen Diensten und Netzen.[31]

6 Nachbesserungsbedarf

Zwei Jahre Praxiserfahrung mit der DSGVO haben offengelegt, dass deren Grundansatz richtig ist, dass es aber schon innerhalb dieses Regelwerks Nachbesserungsbedarf gibt. So ist es offensichtlich, dass die bisherigen Kooperations- und Kohäsionsmechanismen bei der Datenschutzaufsicht zu schwerfällig und zeitaufwändig sind. Diese Mechanismen sind auf deutscher Seite dadurch verkompliziert, dass die Datenschutzaufsicht nicht zentral, sondern durch die Behörden der Länder erfolgt. Die Forderung nach einer nationalen Zentralisierung im Interesse der Rechtssicherheit der Unternehmen steht schon seit längerem zur Diskussion und wurde jüngst von der Wirtschaftsministerkonferenz und in einem

[25] Geminn/Laubach ZD 2019, 403; Fujiwara/Geminn/Roßnagel ZD 2019, 204.
[26] Commission (Fn. 10), S. 4 Datenschutzgesetz nach DSGVO-Vorbild verabschiedet, DANA 4/2018, 214 f.
[27] Pelz, Afrika: Weiße Flecken beim Datenschutz, www.dw.com 18.12.2019.
[28] Weichert, ZD 2020, 18 ff.
[29] Weichert in Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 1 Rn. 19-25.
[30] Überarbeitete Fassung 2018: https://digitalcharta.eu/wp-content/uploads/Digital_Charta_deutsch.pdf.
[31] Balser, Anschluss gesucht – die Grünen wollen schnelles Internet zum Grundrecht machen, SZ 30.06.2020, 22.

Gutachten der Datenethikkommission vorgetragen.[32] Das Durchsetzungsproblem beim Datenschutz liegt aber nicht auf der nationalen, sondern auf der europäischen Ebene: Die notorischen Gesetzesverstöße erfolgen europaweit durch internationale Konzerne. Dass lokale Egoismen und Standortinteressen bei der Durchsetzung des Datenschutzes hinderlich sind, ist weniger ein deutsches als ein europäisches Problem. Es ist deshalb naheliegend, auf europäischer Ebene eine einheitliche Instanz zu schaffen, die bei EU-weiten Verarbeitungen die Aufgabe der Datenschutzaufsicht wahrnimmt. Um dessen Unabhängigkeit zu wahren ist es denkbar, dass eine solche Instanz als operativer Arm des Europäischen Datenschutzausschusses (Art. 68 ff. DSGVO) installiert wird.

Die in der DSGVO vorgesehenen Verhaltensregeln (Art. 40, 41), mit denen sich die Wirtschaft im vorgegebenen gesetzlichen Rahmen spezifische Regeln schaffen kann, haben ein hohes Potenzial, das noch nicht ansatzweise ausgeschöpft wird. Die Bereitschaft zur Selbstregulierung nimmt in dem Maße zu, in dem sie als angenehmere Alternative zur staatlichen Regulierung erscheint. Angesichts des weiterhin bestehenden Vollzugsdefizits im Datenschutz wegen Überforderung der Aufsichtsbehörden fehlt dieser Druck derzeit. Dies kann und muss sich dadurch ändern, dass die Kontrolldichte in den einzelnen Wirtschaftssektoren erhöht wird. Auch Klageaktivitäten der Verbraucherschutzorganisationen können den Druck bewirken, der Unternehmensbranchen zur kontrollierten Selbstregulierung motiviert. Staatlicher regulatorischer Druck kann auch dazu beitragen, dass der derzeit hohe Einfluss von US-Unternehmen in den nationalen und europäischen Wirtschaftsverbänden zurückgedrängt wird und dadurch die originär europäischen Wirtschaftsinteressen bestimmend werden.

Noch mehr Potenzial als in den Verhaltensregeln liegt in den in der DSGVO vorgesehenen Möglichkeiten zur Zertifizierung von Datenverarbeitungsverfahren. Insofern waren nach außen hin in den ersten zwei Jahren keine Fortschritte erkennbar. Der Eindruck drängt sich auf, dass die Aufsichtsbehörden, anders als etwa die EU-Kommission[33], kein Interesse an solchen Marktmechanismen haben. Es wäre eine vertane Chance, wenn die Regelungen der Art. 42, 43 DSGVO weiterhin fleischlose normative Skelette blieben. Es bietet sich an, das dort vorgesehene freiwillige Zertifizierungsverfahren nicht nur auf Verarbeitungssysteme zu beschränken, sondern auch IT-Produkte einzubeziehen, die die Hersteller einer unabhängigen Datenschutzüberprüfung unterziehen lassen können.[34] Zudem sollten Zertifizierungen in hochsensiblen Bereichen, etwa im Gesundheitssektor, im Bereich der Telekommunikation oder bei anderen kritischen Infrastrukturen obligatorisch gemacht werden, um dort einen höheren Grad an Rechtskonformität zu bewirken.

Entwicklungsbedürftig ist die Regelung automatisierter Entscheidungen – einschließlich Profiling (Art. 22 DSGVO), die darauf abzielt, die Kontrolle über die Menschen kontrollierende Computer zu wahren. Die Tatbestandsvoraussetzungen sind so vage, dass weder ein mehr an Transparenz noch ein Mehr an individueller Selbstbestimmung erreicht wird. Schuld hieran ist zweifellos auch eine rückständige nationale Rechtsprechung, die invasive Algorithmen als Betriebs- und Geschäftsgeheimnisse im Dunkeln lässt.[35] Der verwendete Begriff der „Entscheidung“ erleichtert die Ausblendung manipulativer

[32] Schulzki-Haddouti, Landesdatenschützer sollen Kontrolle über Firmen verlieren, www.golem.de 03.06.2020.
[33] Commission (Fn. 10), S. 9.
[34] Weichert, DuD 2020, 295.
[35] Weichert DANA 3/2018, 133 f.

Werbemaßnahmen und Informationsangebote.[36] Diskriminierung durch Algorithmen, ein inzwischen in Bezug auf sog. Künstliche Intelligenz intensiv diskutierter Topos[37], wird in Art. 22 DSGVO nicht direkt adressiert. Algorithmen treffen nicht nur die von der DSGVO geschützten natürlichen, sondern auch juristische Personen. Dessen ungeachtet enthält Art. 22 DSGVO einen ausfüllungsfähigen Rahmen, der von der Politik zum Ausgangspunkt für eine umfassendere Algorithmenkontrolle genommen werden kann.[38]

7 Spezifizierungsbedarf

Der EuGH hat mit seinen Entscheidungen zur gemeinsamen Verantwortlichkeit, die in Art. 26 DSGVO geregelt ist, einen gewaltigen Klärungsbedarf verursacht, da sie in der Vergangenheit bisher nur selten angenommen wurde, in der Praxis aber von umfassender Relevanz ist.[39] Er hat damit zugleich klargestellt, dass bei kooperativen digitalen Geschäftsmodellen zwischen US-Konzernen und europäischen Unternehmen die Letztgenannten eine Mitverantwortung tragen für unzulässige Praktiken der Erstgenannten. Zwar ist durch den EuGH weitgehend geklärt, wann Verarbeitung gemeinsam zu verantworten ist. Rechtsunsicherheit besteht aber, wie die Rechtsbeziehung zwischen den Verantwortlichen konkret zu gestalten ist und welche Ansprüche sich hieraus ergeben, etwa auf Information oder auf Vertragsabschluss.[40] Hier sind legislatorische Klarstellungen, wie sie für die einfacher gestaltete Auftragsverarbeitung in Art. 28 DSGVO bestehen, dringend nötig.

Dem Ausgleich zwischen Meinungsfreiheit und Datenschutz kommt eine zentrale Bedeutung für die Wahrung einer freien Meinungsbildung in unserer digitalisierten Gesellschaft zu. Die Erfahrungen mit der Beeinflussung politischer Prozesse über Internetdienste, etwa anlässlich des US-Präsidentschaftswahlkampfs 2017 oder der Brexit-Kampagne in Großbritannien 2016 zeigen, dass es eines rechtlichen Instrumentariums bedarf, um den Medienmissbrauch zu begrenzen. Zwar hat die DSGVO diesen Bereich noch den nationalen Gesetzgebern überlassen (Art. 85). Bisherige nationale Regelungsansätze, wie z.B. das deutsche Netzdurchsetzungsgesetz, bauen vor allem auf eine Selbstkontrolle der Internetkonzerne, was letztlich auf einen weitgehend hilflosen Appell hinausläuft, diese mögen doch bitte ihr eigenes Geschäftsmodell in Frage stellen. Es besteht jedoch die Option, hier auf Unionsebene verstärkt vereinheitlichend und zugleich grundrechtsoptimierend tätig zu werden und dabei einer hoheitlichen Aufsicht einen stärkeren Einfluss zuzusprechen. Beschränkt sich dieser auf die Bekämpfung von Falschinformation und Hassbotschaften, so muss dies keine staatliche Zensur zur Folge haben. Vielmehr kann dies, von unabhängigen Einrichtungen ausgeübt, zu einer rechtsstaatlich kontrollierten Zivilisierung des digitalen Dialogs beitragen. Die Datenschutzbehörden in Europa zeigen, dass staatliche Aufsicht und Regierungsferne zugleich möglich sind.

[36] Weichert in Reiffenstein/Blascheck, Konsumentenpolitisches Jahrbuch 2017, S. 248 ff.
[37] Z.B. Kreye, Das neue Plutonium, SZ 22.01.2020, S. 4.
[38] Weichert, Stellungnahme zum Draft Ethics Guidelines for Trustworthy Artificial Intelligence, 21.02.2019, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2019_eu_ki_ethik.pdf; Commission Staff Working Document (Fn. 11), S. 28.
[39] EuGH 05.06.2018 – C-210/16 (Facebook-Fanpage/Wirtschaftsakademie), NJW 2018, 2537 = DuD 2018, 518; zur Prozessgeschichte Weichert DANA 2019, 4 ff.; EuGH 10.07.2018 – C-25/17 (Zeugen Jehovas), NJW 2019, 285; EuGH 29.7.2019 – C-40/17 (Fashion ID), NJW 2019, 2755.
[40] Weichert DANA 2019, 8; Specht-Riemenschneider/Schneider MMR 2019, 506 ff.

Die DSGVO macht als Grundverordnung nur grundlegende Vorgaben für den Datenschutz. Dies wird gerade in Deutschland oft beklagt, wo wir teilweise hoch differenzierte spezielle Konkretisierungen des Datenschutzes kennen. Die DSGVO steht einer solchen Spezifizierung nicht entgegen, sondern ist die Voraussetzung hierfür. Leider kommt die – überfällige – bereichsspezifische Präzisierung im Bereich der Telekommunikation durch die ePrivacy-Verordnung nicht voran. Auch in anderen Bereichen sollten Präzisierungen nicht durch die Mitgliedstaaten, sondern durch die Union selbst erfolgen. Im Bereich des Verbraucherschutzes haben sich EU-Parlament und Mitgliedstaaten auf ein Regelwerk für kollektiven Rechtsschutz in Form von Sammelklagen geeinigt, der in Art. 80 DSGVO angelegt ist und über die nationalen Instrumente der Verbands- und der Musterfeststellungsklage hinausgeht.[41] Angesichts der Jahrzehnte dauernden Zurückhaltung der nationalen Gesetzgeber beim Beschäftigtendatenschutz ist nun im Rahmen des Art. 88 DSGVO die Union gefordert.[42] Auch die Digitalisierung der Gesundheitsversorgung[43] und die informationelle Stärkung der Forschung[44] lassen sich auf Unionsebene wirksamer realisieren als national.

8 Über den Datenschutz hinaus

Die DSGVO verknüpft bisher getrennte Rechtsbereiche. Dies gilt nicht nur für den Verbraucherschutz (Art. 80 DSGVO)[45] und das Arbeitsrecht (Art. 88 DSGVO). Dies kann und sollte auch für die Informationssicherheit gelten (Art 25, 32 DSGVO), wobei einheitliche Zertifizierungen (vgl. Art. 42, 43 DSGVO) als verbindendes Element geschaffen werden können. Rudimentär blieben bisher die Verbindungen zwischen Datenschutz und Marktregulierung. Die Orientierung der DSGVO-Sanktionen am Kartellrecht war ein erster Anfang einer Annäherung der beiden Rechtsgebiete. Inzwischen verbreitet sich die Erkenntnis im Kartellrecht, dass Datenschutzverstöße unlauterer Wettbewerb und eine Beeinträchtigung eines freien Marktes sein können.[46] Die Durchsetzung von Datenschutz gegenüber marktdominierenden Unternehmen sind Voraussetzung und teilweise sogar Garant für das Funktionieren digitaler Märkte.

Das nächste Digitalthema lauert schon vor der Tür: Anfang 2019 verkündete Facebook-Chef Mark Zuckerberg die Schaffung einer privaten Weltwährung, die er „Libra“ nennt. Facebook sucht für die „Libra Association“ weltweit Mitstreiter. Schon bisher ist digitales Zahlen ein Vorgang, dem sich allenfalls Finanzaufsichtsbehörden, aber kaum Bürgerrechtler und Datenschützer widmen. Digitales Zahlen hinterlässt Spuren der Nutzer, deren Sekundärnutzung von höchster Sensitivität ist. Durch die Zurückdrängung des anonymen Bargeldes werden diese Spuren immer mehr und aussagekräftiger. Zum Zweck der Geldwäschebekämpfung haben die EU-Staaten schon erste Strukturen aufgebaut, um diese Spuren gezielt auszuwerten.[47] Schon bisher haben die Internet-Plattformanbieter ihre eigenen

[41] New rules allow EU consumers to defend their rights collectively, www.europal.europa.eu 22.06.2020, Beisel, Schadenersatz für alle, SZ 24.06.2020, 7.
[42] Weichert/Schuler, Die EU-DSGVO und die Zukunft des Beschäftigtendatenschutzes, 08.04.2016, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_dsgvo_beschds.pdf.
[43] Weichert, Big Data im Gesundheitsbereich, 2018, Kap. 11, https://www.abida.de/sites/default/files/ABIDA%20Gutachten-Gesundheitsbereich.pdf.
[44] Weichert ZD 2020, 18 ff.
[45] Weichert in Däubler u.a. (Fn. 29), Kommentierung des Art. 80 und des UKlaG.
[46] Buchner WRP 2019, 1243 ff.; BGH 23.06.2020 – KVR 69/19.
[47] Weichert, Das Recht auf Anonymität finanzieller Transaktionen, 27.12.2016, https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2016_5gwrl271216.pdf.

Zahlungsverfahren. Hierüber gelangen sie an ökonomisch wertvolle personenbezogene Daten, die sie zur Stärkung ihrer Marktmacht nutzen. Mit einer übergreifenden globalen privaten digitalen Währung könnten sich die Digitalunternehmen als Betreiber noch stärker nationaler Kontrolle entziehen und ökonomischen Einfluss wahrnehmen. Es ist daher an der Zeit, dass sich Finanz- und Grundrechtsaufseher austauschen.[48]

Bisher tut sich die EU-Kommission noch schwer, einen Ansatz für eine umfassende Regulierung für Internet-Plattformen zu finden.[49] Ein Grund dafür liegt wohl darin, dass auch in der Kommission noch sektorspezifische Sichtweisen dominieren. In der Praxis haben sich aber die Bedrohungen für Datenschutz und Verbraucherschutz, durch Hass- und Falschnachrichten, durch Markkonzentration und Wettbewerbsverzerrung schon längst vereint. Es ist daher nötig, auch die Bekämpfung dieser Gefahren zusammenzuführen. Dies kann durch Aufgabenkonzentration erfolgen, in vieler Hinsicht wäre aber wohl schon eine engere institutionalisierte Kooperation der zuständigen Stellen ausreichend.

Die DSGVO eignet sich schließlich als ein zentraler Ausgangspunkt für die Sicherung „digitaler Souveränität“.[50] Angesichts der globalen informationellen Vernetzung und der damit einhergehenden Abhängigkeiten dringt immer mehr ins Bewusstsein, dass informationelle Selbstbestimmung die technische Unabhängigkeit von Fremdbestimmung voraussetzt. Und dies gilt nicht nur für natürliche Personen, sondern ebenso für juristische Personen als Wirtschaftsunternehmen und Behörden und letztlich für Nationalstaaten und die Europäische Union als einheitliches Rechtsgebiet. Diese Fremdbestimmung erfolgt derzeit insbesondere durch große US-Unternehmen. Chinesische Unternehmen sind dabei, diese zumindest in einzelnen Marktsegmenten zu verdrängen. In keinem Fall geht es dabei darum, die in Europa gewährleisteten Grundrechte und die hier praktizierte Demokratie voranzubringen, sondern darum, wirtschaftlich zu expandieren und dadurch zugleich politische Einflusssphären zu erweitern. Seit den Enthüllungen Edward Snowdens über die geheimdienstliche Durchdringung unseres informationellen Lebens durch Geheimdienste wie die NSA oder den GCHQ im Jahr 2013 sollte klar sein, dass Selbstbestimmung die Kontrolle über die selbst genutzte Informationsinfrastruktur bedingt.[51]

9 Fazit

Die DSGVO ist trotz vieler Defizite eine Erfolgsgeschichte, die erst am Anfang steht und die weitergeschrieben werden muss. Mit ihr kann auf der Grundlage gemeinsamer europäischer Werte ein Markt geschaffen werden, der diese Werte – auch vor äußeren Bedrohungen – sichert. Die DSGVO lässt genügend Raum und schafft den Raum für die freie Entfaltung lokaler und regionaler digitaler Initiativen. Dass diese noch zart entwickelte Erfolgsgeschichte nachhaltig wird und bleibt, ist keine Selbstverständlichkeit. Nötig sind vor allem mehr politische Unterstützung und mehr Druck aus der Zivilgesellschaft. Die DSGVO schafft ein Fundament für einen notwendigen und viel umfangreicheren

[48] Spiekermann, Moment des Aussterbens, SZ 15.07.2019, 10.
[49] Beisel, Regulieren, aber richtig, SZ 27.05.2020, 16.
[50] Bizer in Lühr/Jabkowski/Smentek, Handbuch digitale Verwaltung, 2019, 23 ff.
[51] Snowden, Permanent Record, 2019; Greenwald, Die globale Überwachung, 2014; Harding, Edward Snowden, 2014; Rosenbach/Stark, Der NSA Komplex, 2014.

digitalen Grundrechtsschutz in Europa, bei dem der Datenschutz mit weiteren Rechtsgebieten verzahnt werden muss. In der Politik wurde lange Zeit relativ unreflektiert „mehr Digitalisierung“ gefordert. Inzwischen zeigt sich, dass es nicht einfach um „mehr“ geht, sondern um eine hochdifferenzierte Gestaltung. Die DSGVO gibt hierfür wichtige Impulse. Diese dürfen nicht verpuffen. Anderenfalls besteht die realistische Gefahr, dass sich die freiheitsnegierenden Angebote aus den USA und China in Europa weiter verbreiten und etablieren. Die deutsche Präsidentschaft in Europäischen Rat während der zweiten Hälfte des Jahres 2020 hat die politische Möglichkeit, Initiativen zu starten und fortzuentwickeln, mit denen der digitale Grundrechtsschutz der DSGVO ausgebaut und dabei zugleich die digitale Souveränität Europas gestärkt wird. Sie sollte diese Chance nutzen.