Initiative D21

Kooperationspartner: Capgemini, digitales Denken

Arbeitsgruppe Innovativer Staat | Stand: 28. Mai 2019

DENKIMPULS INNOVATIVER STAAT:
Datensouveränität – Datenschutz neu verstehen

AUTOREN Dr. Nikolai Horn (Philosoph / Capgemini), Björn Stecher (Privacy-Experte / Digitales Denken)

MITWIRKENDE Marc Reinhardt (Initiative D21 / Capgemini)

- **Der Begriff „Datensouveränität" stellt die Autonomie des Datengebenden in den Mittelpunkt, welcher reflektiert und durch seine Fähigkeiten selbstständig in der Lage ist, sich informationell selbstbestimmt in der „Daten-Welt" zu bewegen. Die Folge daraus ist, dass es im Datenschutz neben der Einhaltung der Rechtsvorschriften auch darum geht, die NutzerInnen mit Kenntnissen und Instrumenten zur Reflexion ihres Handelns aktiv abzuholen und zu befähigen.**
- **Die Ermöglichung der Datensouveränität muss im Sinne der Befähigung der NutzerInnen als technologische, gesellschaftliche und staatliche Aufgabe begriffen werden. Dabei handelt es sich um den technologischen Datenschutz, den Ansatz der Corporate Digital Responsibility (CDR) und den Erwerb von Datenschutzkompetenzen.**
- **Als Vertrauensanker für die BürgerInnen kommt insbesondere der Staat als Garant der Einhaltung von Datenschutzbestimmungen, als Förderer und Anwender datenschutzfreundlicher Technologien und als Bürge für digitale Selbstbestimmungschancen in Frage. Die Gewährleistung der Datensouveränität muss also als ein Teil der öffentlichen Daseinsvorsorge aufgefasst werden.**

I. Dilemma des Datenschutzes

Kaum ein Begriff der Digitalisierung ist so widersprüchlich und paradox wie der des Datenschutzes – zumindest wenn es um den Zweck und um die gelebte praktische Umsetzung von diesem geht. Für NutzerInnen, Unternehmen, Politik, selbst Datenschutzbeauftragte in Unternehmen ist der Begriff so scharf und unscharf zugleich. JuristInnen, die sich mit dem Datenschutzrecht beschäftigen, haben einen klaren Bezug und auch eine Definition vom Datenschutz. So wichtig die juristische Perspektive ist, so unklar ist diese oft für die NutzerInnen. Für sie lässt sich daraus nicht einfach ableiten, wie sie sich in Bezug auf ihre Daten selbstbestimmt und vor allem informiert im Internet bewegen sollen.

In keinem Thema steckt mehr von dem „www"-Prinzip als im Datenschutz. „**W**unsch **w**iderspricht **W**irklichkeit" ist das Prinzip, das seit der immer stärker werdenden Digitalisierung die Debatte verfolgt.[1] Die NutzerInnen möchten Datenschutz, denn der Schutz ihrer Daten ist ihnen wichtig, aber ihr tatsächliches Handeln liegt zum Teil fern ab von

1 Vgl. Initiative D21 e.V. (2014): D21-Digital-Index 2014, Die Entwicklung der digitalen Gesellschaft in Deutschland; online verfügbar unter: https://initiatived21.de/app/uploads/2017/02/d21-digital-index-2014.pdf (letzter Abruf: 14.05.2019).

dem, was sich DatenschützerInnen unter einem verantwortungsvollen, selbstbestimmten Handeln vorstellen. Lediglich 19 Prozent lesen regelmäßig bis oft die Datenschutzbestimmungen im Internet.[2] Und die Nutzung von datenintensiven Diensten wie Google, Facebook, Alexa, Apple, WhatsApp, Gesundheitsapps und vielen weiteren datengetriebenen Anwendungen nehmen trotz der zum Teil mangelnden datenschutzrechtlichen Anforderungen zu.[3] Dem eigentlichen Ziel des Datenschutzes – das aufgeklärte selbstbestimmte Handeln auf der Grundlage von Transparenz und Verständnis – wird die Praxis nicht gerecht. Sowohl Politik als auch Zivilgesellschaft versuchen mit langsam wachsendem Erfolg für ein Mehr an Datenbewusstsein zu sensibilisieren. Auch die neue Datenschutz-Grundverordnung versucht auf viele praktische Umsetzungsdefizite einzugehen und sie juristisch zu regeln – Stichwort: privacy by design.

Der Begriff „Datenschutz" ist in den medialen und gesellschaftlichen Debatten kein Begriff, der Klarheit schafft, sondern auf vielen Ebenen eine Worthülse. Der Datenschutz in Unternehmen wird als notwendig, vielleicht als lästig, vor allem aber als sanktionierend wahrgenommen. Die erste Prämisse von Unternehmen ist vielmehr die Frage, wie kann ich mich vor möglichen Sanktionen schützen, und nicht, wie kann ich meine KundInnen oder MitarbeiterInnen zu mehr Datenbewusstsein befähigen und einen selbstbestimmten Umgang mit personenbezogenen Daten praktisch ermöglichen.

Im Zeitalter der Digitalisierung befindet sich der Datenschutz vor einem Dilemma: Auf der einen Seite steht individuell greifbarer und leicht nachvollziehbarer Mehrwert der Nutzung personenbezogener Daten durch staatliche und privatwirtschaftliche Einrichtungen. Sei es bei der Gesundheitsvorsorge, bei der Erlangung günstiger Versicherungstarife, bei der Individualisierung von Angeboten, der Verbesserung von Services oder auch bei der Nutzung einer scheinbar kostenfreien digitalen Anwendung. Auf der anderen Seite steht der weitgehend abstrakte Wert „informationelle Selbstbestimmung", dessen praktische Bedeutung für den Einzelnen erst in mittel- bis langfristigen (aber nicht unrealistischen) Zukunftsszenarien vermittelbar wird. Hinzu kommt die von einem Laien kaum überschaubare Komplexität der Datenschutzthematik selbst. Da die Bedeutung des Datenschutzes sehr abstrakt und die Materie komplex ist, wird in der Praxis die Verantwortung für die Datennutzung auf die in die Datenverarbeitung einwilligenden NutzerInnen verschoben, ohne mit einem reflektierten und faktisch selbstbestimmten Umgang der Einzelnen mit den eigenen personenbezogenen Daten zu rechnen. Frei nach dem Prinzip: Wenn die NutzerInnen einwilligen, dann bin ich als Unternehmen fein raus.

Das Resultat der Debatten rund um den Datenschutz liegt dann zwischen Weltuntergangsszenarien und Verschwörungstheorien[4], „Bedenken second" oder Klingelschildern[5] und Datenkraken – kurz: Sie sind negativ konnotiert, aber selten reflektierend und befähigend. Am deutlichsten zeigt sich das Dilemma an der Forderung nach Datensparsamkeit bzw. Datenminimierung. Für Nicht-JuristInnen ist die Forderung nach weniger Daten in Zeiten von Facebook, Google, Big Data und „Daten sind das neue Öl" meist ein Zirkelbezug, der kommunikativ nicht zu erklären ist.

Einer der zentralen Aspekte der nächsten Jahre sollte es daher sein, dem Datenschutz ein neues Verständnis zu geben. Der Datenschutz braucht ein neues Branding, bei dem Wirkung und Assoziation mit dem tatsächlichen Handeln übereinstimmt, ohne dass das Ziel der informellen Selbstbestimmung weichen muss. Es ist vielleicht gerade deshalb geboten, über ein neues Verständnis von Datenschutz zu diskutieren, weil sich das eigentliche Ziel des Datenschutzes nur schwer entfalten kann und praktisch schwer vermittelbar ist.

Es geht daher beim Datenschutz auch um eine soziokulturelle Komponente. Die rechtlichen Regulierungen schaffen zwar Rahmenbedingungen für die informationelle Selbstbestimmung der BürgerInnen. Um im digitalen Raum dieselben

2 Statista (2019): Lesen Sie die Datenschutzbestimmungen im Internet?; online verfügbar unter: https://de.statista.com/statistik/daten/studie/189794/umfrage/lesen-der-datenschutzbestimmungen-im-internet/ (letzter Abruf: 12.05.2019).

3 Der D21-Digital-Index 2018/2019 (S. 24-25) zeigt eine steigende Nutzung sozialer Medien. Vgl.: Initiative D21 e.V. D21-Digital-Index 2018/2019, Jährliches Lagebild zur Digitalen Gesellschaft; online verfügbar unter: https://initiatived21.de/app/uploads/2019/01/d21_index2018_2019.pdf (letzter Abruf: 12.05.2019).

4 Berkemeyer, Kim (2017): Amazon Echo: CIA-Frage bringt Alexa in Bedrängnis; online verfügbar unter: https://www.chip.de/news/Amazon-Echo-CIA-Frage-bringt-Alexa-in-Bedraengnis_110368207.html (letzter Abruf: 12.05.2019).

5 Verstoßen Klingelschilder gegen die DSGVO – mediale Debatte 2018. Z.B.: Remsky, Sarah (2018): Wenn der Mieter es will, soll Name auf dem Klingelschild weg; online verfügbar unter: https://www.zeit.de/gesellschaft/zeitgeschehen/2018-10/dsgvo-name-klingelschild-haus-und-grund-datenschutz (letzter Abruf: 12.05.2019).

Freiheitschancen wie im analogen zu bieten, braucht die Gesellschaft allerdings zusätzlich eine gelebte Hochachtung digitaler Grundechte als Wertefundament. Damit ist eine, und zwar nicht erst durch Sanktionsandrohung erzeugte, Haltung gegenüber der (digitalen) Freiheit des Anderen und um die Respektierung der legitimen Ansprüche der Menschen auf Achtung ihrer Privatsphäre gemeint.

Man stelle sich vor, Datenschutz hat die Aufgabe, nicht sanktionierend für die informelle Selbstbestimmung zu kämpfen, sondern Sinn und Zweck des Datenschutzes ist die Befähigung, souverän mit eigenen Daten umzugehen.

Was bedeutet das für Unternehmen und Staat, wenn sie nicht nur die Gesetze einhalten sollen, sondern die NutzerInnen proaktiv in diesem Sinne abholen müssen? Was, wenn Datenschutzbehörden und Datenschutzbeauftragte ein neues Rollenverständnis entwickeln und mehr als BeraterInnen wahrgenommen werden anstatt als „ökonomische Blockierer"? Was, wenn die Aufgabe des Staates bei seinen behördlichen Leistungen ist, BürgerInnen nicht nur rechtlich zu schützen, sondern sie hinsichtlich ihrer Selbstbestimmungschancen individuell abzuholen und zu befähigen? Dafür sind andere Definitionen und Assoziationen mit dem Begriff des Datenschutzes nötig.

II. Vom Datenschutz zu Datensouveränität

In der Digitalisierungsdebatte wird kaum ein anderer Begriff so oft verwendet und unterschiedlich interpretiert wie „Datensouveränität": Ob als „Lobbybegriff der Dateninindustrie"[6], als Datenschutz-Synonym oder als Oberbegriff für „Meine Daten gehören mir" – je nach Kontext wird er unterschiedlich verwendet und dabei oft entweder positiv oder auch negativ aufgeladen. Der Begriffsgehalt bleibt jedoch meist unscharf. Bereits vor rund einem Jahr plädierte der ehemalige Bundesdatenschutzbeauftragte Peter Schaar gegenüber der IT-Zeitschrift „heise online" dafür, „die dargebotene Worthülse aufzugreifen und im Sinne der Kontrollbehörden positiv zu besetzen"[7].

Die Präzisierung des Bedeutungsgehalts von „Datensouveränität" ist in der Tat wichtig. Wird die Bedeutung von Datensouveränität präzisiert, so könnte dies das Verständnis von informationeller Selbstbestimmung erweitern. Diese Präzisierung geht über die rein rechtliche Dimension des Datenschutzes hinaus, ohne diese jedoch zu relativieren. Eine Präzisierung des Begriffs „Datensouveränität" kann dabei helfen, eine selbstbestimmte Entfaltung von BürgerInnen, NutzerInnen sowie Unternehmen auch in einer datengetriebenen Gesellschaft sicherzustellen.

Das Wort „Datenschutz" impliziert ein Schutzerfordernis derjenigen Person, die ihre Daten Dritten zur Verfügung stellt. Es impliziert zugleich ein Machtverhältnis, welches zu Lasten desjenigen geht, der seine Daten zur Verfügung stellt, um diese Asymmetrie mittels Sanktionen auszugleichen. Durch den Einsatz von Sanktionen soll das Machtverhältnis zwischen Datengebenden und Datenverwendenden ausbalanciert werden. Allerdings ist dem Begriff nicht implizit abzunehmen, dass er den Datengebenden in seinem Handeln befähigt, selbstbestimmt und informiert entscheiden zu können. Dem Schutzansatz im Begriff „Datenschutz" kommt eine passive Rolle gleich. Der Souveränitätsbegriff beschreibt hingegen eine proaktive, reflektierende und damit befähigendere Perspektive. Aus dem mittellateinischen *superanus*, „darüber befindlich" bzw. „überlegen", wird von einer Fähigkeit einer Person zur ausschließlichen rechtlichen Selbstbestimmung gesprochen. Sie zeichnet sich durch Eigenständigkeit und Unabhängigkeit aus und grenzt sich vom Zustand der Fremdbestimmung ab. Demnach auch von der passiven Dimension im Begriff „Datenschutz".

Bei dem Autonomieprinzip, das dem Souveränitätsbegriff innewohnt, geht es also um die Souveränität des Individuums, sich und seine Umwelt nach eigener Vorstellung immer wieder neu zu „entwerfen". Die Souveränität bedeutet, jederzeit die Hoheit und Verantwortung über den eigenen Lebensentwurf zu haben. Von dieser normativen Grundlage ausgehend kann die „Datensouveränität" daher nichts anderes bedeuten, als Selbstbestimmung über das Daten-Abbild seines Selbst und Freiheit, in seinem Lebensentwurf nicht durch eigene Datenspuren

6 Vgl. Krempl, Stefan (2018): Datensouveränität: Die Säge am informationellen Selbstbestimmungsrecht; online verfügbar unter: https://www.heise.de/newsticker/meldung/Datensouveraenitaet-Die-Saege-am-informationellen-Selbstbestimmungsrecht-3953776.html (letzter Abruf: 12.05.2019).
7 Ebd.

aus der Vergangenheit „prädeterminiert“ zu sein. Hierauf zielt letztlich das Konzept der „informationellen Selbstbestimmung“. Denn es geht hierbei um mehr als nur die Schonung der Privatsphäre als ein Rückzugsraum des Individuums. Es geht um die Möglichkeit einer aktiven, selbstbestimmten Gestaltung der Lebenswelt unter der Nutzung digitaler Technologien.

Aus diesem Grund kann auch die Verwendung des Begriffes „Datensouveränität“ als Schlagwort im Sinne einer eigentumsähnlichen Position leicht zu Missverständnissen führen. Einerseits gehört es sehr wohl zum Verständnis der informationellen Selbstbestimmung, dass die personenbezogenen Daten mit Dritten geteilt werden können. Andererseits kann aber die Hoheit über personenbezogene Daten genauso wenig „erworben“, „gehortet“ noch „veräußert“ oder „umverteilt“ werden, wie die Hoheit über den eigenen Körper. Die Datensouveränität kommt vielmehr dadurch zum Tragen, dass das Individuum über die Verwendung seiner Daten jederzeit selbstbestimmt entscheiden kann. Im Zusammenhang mit der kommerziellen Datenverarbeitung personenbezogener Daten stellt sich dabei weniger die Frage nach „Dateneigentum“, sondern vielmehr danach, wie die unternehmerische Freiheit von Diensteanbietenden mit der Freiheit verträglich sein kann, sich durch Zurverfügungstellung von personenbezogenen Informationen am digitalen Wertschöpfungsprozess selbstbestimmt zu beteiligen und daraus Vorteile zu erzielen.[8]

Kurz gefasst charakterisiert der Begriff „Datenschutz“ einen passiven Ansatz, der aufgrund fehlender Kompetenz und Entscheidungsoptionen der NutzerInnen die informationelle Selbstbestimmung durch Sanktionen schützt. Hingegen stellt der Begriff „Datensouveränität“ die Autonomie des Datengebenden in den Mittelpunkt, welcher reflektiert und durch seine Fähigkeiten selbstständig in der Lage ist, sich informationell selbstbestimmt in der „Daten-Welt“ zu bewegen. Die Folge daraus ist, dass es im Datenschutz auch darum geht, die NutzerInnen mit Kenntnissen und Instrumenten zur Reflexion ihres Handelns aktiv abzuholen und zu befähigen. Vergleichbar mit dem nutzerzentrierten oder kundenzentrierten Ansatz im Marketing bzw. digitalen Geschäftsmodellen.

III. Elemente der Datensouveränität

Für die Befähigung im Umgang mit den eigenen Daten braucht es neben dem normativen Ansatz weitere Elemente, die sowohl die NutzerInnen als datengebende Komponente, als auch die datenverwendende Seite – sprich die Unternehmen – und den Staat einbeziehen.

Grundlage für die Datensouveränität ist die normative bzw. rechtliche Komponente. Die Datenschutzgrundverordnung (DSGVO) ist das Fundament bzw. das Sicherheitsnetz bei Verstößen gegen das informationelle Selbstbestimmungsrecht. Auf diesem Fundament bauen drei Kernbestandteile auf, die insbesondere den Befähigungsansatz der NutzerInnen zum Kern haben. Dabei handelt es sich um den technologischen Datenschutz, die Selbstverpflichtung von Unternehmen bzw. den Ansatz der Corporate Digital Responsibility (CDR) und den Erwerb von Datenschutzkompetenzen.

Technologischer Datenschutz

Der technologische Datenschutz ist in seinem Verständnis vom Begriff der Datensicherheit klar abzugrenzen. Unter dem Begriff des technologischen Datenschutzes ist vielmehr die Usability zu verstehen, wie NutzerInnen technisch in die Lage versetzt werden können, intuitiv über die Verwendung ihrer Daten zu entscheiden. Denn die Vorschriften der Datenschutz-Grundverordnung führen nicht automatisch zur Ermöglichung der Datensouveränität der NutzerInnen im digitalen Alltag. Ihre Transparenz- und Interventionsrechte werden in der Praxis nach wie vor nur von wenigen Menschen in Anspruch genommen. Auch das datenschutzrechtliche Ideal einer „informierten Einwilligung“ in die Datenverarbeitung bleibt meist Wunschdenken.

8 Horn, Nikolai & Reinhardt, Marc (2018): Datenhoheit – Gerechtigkeitsfrage in einer Digitalen Gesellschaft; online verfügbar unter: https://initiatived21.de/app/uploads/2018/10/denkimpuls_datenhoheit.pdf (letzter Abruf: 12.05.2019).

Vermutlich nimmt sich nur selten jemand Zeit, um die Datenschutzerklärungen sowie die sogenannten „One-Pager“ zu lesen. Wenn diese gelesen werden, können sie nur von Wenigen in allen Konsequenzen durchdrungen werden. Doch sogar wenn sie gelesen und verstanden werden, können die NutzerInnen ohnehin wenig ändern – also lässt man es von vorn herein sein. Wer zweifelt schon an seiner persönlichen Selbstbestimmtheit, wenn er die Cookie-Bedingungen einer Webseite nicht gelesen hat? Zumal lässt sich das Lesen von Datenschutzbestimmungen mit technologischen Veränderungen immer schwerer gewährleisten. Seitenlange Bestimmungen vor der Nutzung des eigenen smarten Autos zu lesen, entspricht nicht dem Verhalten der NutzerInnen. Viele Geräte, die Daten sammeln, verfügen heute zum Teil über keine Displays mehr oder sind schlicht zu klein, um umfassend Datenschutzbestimmungen abbilden zu können. Zurzeit bedient man sich noch Behelfslösungen, um den NutzerInnen zumindest rechtlich die Gelegenheit zu geben, sich über die Verwendung ihrer Daten zu informieren. Ist das Display der smarten Uhr zu klein, wird auf die Datenschutzbestimmungen der Webseite verwiesen. Sprachassistenten führen die NutzerInnen freundlich bestimmt auf die Webseite oder den Button auf der dazugehörigen App. Ein nutzerfreundlicher Zugang zu den eigenen Rechten sieht gewiss anders aus, wenn die NutzerInnen sich über mehrere Geräte zu den Informationen durchkämpfen müssen.

Für die Ermöglichung der Datensouveränität müssen daher die rechtlichen Rahmenbedingungen des Datenschutzes mit Leben gefüllt werden. Datenschutzfreundliche Technologien können dabei den NutzerInnen praktische Instrumente an die Hand geben, um ihre digitalen Freiheitsrechte auszuüben und Machtasymmetrien zwischen NutzerInnen und datenverarbeitenden Unternehmen entgegenzuwirken. Sie sollen ermöglichen, individuelle Privacy-Einstellungen vorzunehmen, die Datenzugriffe durch andere Institutionen nachzuvollziehen und Betroffenenrechte (Änderung, Löschung, Portierung etc.) unkompliziert auszuüben.

Solche Ansätze nehmen insbesondere durch die sogenannten „Privacy Information Management Systems“ (PIMS) eine immer prominentere Rolle ein.[9] Auf der technologischen Seite sollen die BürgerInnen ex ante mit Hilfe eines Einwilligungsassistenten gemäß ihren individuellen Privacy-Präferenzen Einstellungen zu Kategorien der Datenempfangenden und Verarbeitungszwecken vornehmen können. Ex post sollen die BürgerInnen in einer Art „Privacy-Cockpit“ einsehen können, welche Institutionen in der Vergangenheit auf ihre Daten zugegriffen haben (Logging der Zugriffe und Austausche), ihre Privacy-Einstellungen dynamisch anpassen und ihre Betroffenenrechte (Löschung, Auskunft etc.) unkompliziert ausüben können. Die Datensouveränität soll damit durch nutzerzentrierte Schnittstellen zur Datenverarbeitung, Einstellungsmöglichkeiten für individuelle Privacy-Präferenzen sowie durch Visualisierungen von Datenverarbeitungsvorgängen gestärkt werden. Insbesondere muss einfach, intuitiv und ohne Medienbrüche gewährleistet werden, dass Betroffene ihre Ansprüche managen und erfüllen können.

Corporate Digital Responsibility (CDR)

Aufgrund der Komplexität und einer gewissen Unüberschaubarkeit der Funktionsweise digitaler Technologien für die NormalnutzerInnen einerseits und einer ebenso undurchsichtigen rechtlichen Regulierungslage andererseits, entstehen Bruchstellen zwischen dem Anspruch auf die Achtung der Datensouveränität und der in Wirklichkeit erfahrenen Ohnmacht der Einzelnen gegenüber den Datenhaltenden. Für ein „datensouveränes Leben“ der BürgerInnen in einer Digitalen Gesellschaft müssen solche Bruchstellen überwunden werden. Dafür benötigt es Vertrauensanker, welche einen fairen Umgang mit personenbezogenen Daten garantieren und auf die sich die NutzerInnen verlassen können.

Unternehmen kommt dabei eine besondere Verantwortung zu Teil. Sie müssen weg von dem Verständnis des Datenschutzes als eine Art der ökonomischen Risikominimierung. Datenschutz ist als Teil der gesellschaftlichen Verantwortung eines jeden Unternehmens zu sehen. Das Konzept einer Corporate Digital Responsibility (CDR) kann dabei ein wichtiges Instrument sein. CDR steht für verantwortungsvolles unternehmerisches Handeln nach innen und außen bei der Ausübung digitaler Geschäftsprozesse, der Gestaltung von digitalen Services und Produkten sowie den damit verbundenen (Daten-)Austauschbeziehungen gegenüber MitarbeiterInnen, allen Marktpartnern und der Gesellschaft.[10] Sie kann sehr unterschiedlich ausgeprägt

9 Stiftung Datenschutz (2017): Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen; online verfügbar unter: https://stiftungdatenschutz.org/themen/pims-studie/ (letzter Abruf: 12.05.2019).
10 Jänig, Jens-Rainer (2018): Kurzeinführung | Corporate Digital Responsibility. Vortrag, 21.06.2018. Berlin, Arbeitsgruppe Ethik der Initiative D21.

und gelebt werden. So könnten bspw. die Unternehmen im Rahmen des Jahresabschlussberichts einen verpflichtenden Datenreport offenlegen, in dem beschrieben wird, welche Investitionen und Maßnahmen das Unternehmen im Geschäftsjahr in Sachen Datenschutz und Datensicherheit geleistet hat. Darauf aufbauend könnte ein Unternehmen, welches sich selbstverpflichtend zu einer CDR-Strategie bereit erklärt, vom Staat mittels Steueranreizen unterstützt werden.

Ebenso könnten CDR-Konzepte ähnlich wie Umweltreports verpflichtender Bestandteil in der Vergabe öffentlicher Ausschreibungen sein. Eine weitere Möglichkeit besteht darin, den Aufsichtsrat von Aktiengesellschaften hinsichtlich seiner Kontrollbefugnisse zu stärken sowie die vom Vorstand gesetzten CDR-Ziele zu kontrollieren und auf deren Umsetzung zu achten. So bekäme das Thema „Privacy" verstärkte Aufmerksamkeit und wird zu einer faktischen und nicht nur rein formellen ChefInnensache.

Branchenspezifische selbstverpflichtende Maßnahmen im Bereich der Digitalisierung und des Datenmanagement sind weitere Möglichkeiten, den Wirkungskreis der CDR zu erweitern. Auch Berufsgruppen wie Data Analysten oder Data Scientists könnten mit einem „Code of Conduct" dafür sorgen, dass Selbstverpflichtungen zu gesellschaftlichen Vertrauensanker werden, an die sich Unternehmen, die solche Berufsgruppen beschäftigen oder beauftragen, halten müssen.

Die CDR könnte damit das Ziel erfüllen, fehlende Datenschutzkompetenz oder auch fehlendes technisches Wissen von NutzerInnen durch Vertrauen in eine Organisation oder eine Marke teilweise zu kompensieren. Damit CDR nicht in der Freiwilligkeit untergeht, bedarf es bestimmter Anreiz- und Verbindlichkeitsmechanismen für Unternehmen, um Maßnahmen und Konzepte für CDR zu etablieren.

Datenkompetenz

Um die bestehende Komplexität des Themas in der Praxis zu reduzieren, ist neben technologischen Maßnahmen und CDR vor allem der Erwerb von Kompetenzen im Bereich Datenschutz erforderlich. Hierfür kommen verschiedene Institutionen für die Vermittlung von Kompetenzen ins Spiel. Zu aller erst müssen Bildungseinrichtungen wie Schulen und Hochschulen Datenschutz als integralen Bestandteil ihrer Pädagogik verstehen. Hierbei geht es aber nicht um die Vermittlung von datenschutzrechtlichen Fakten, sondern um das Verstehen von Logiken der Digitalisierung. Ziel sollte es sein, dass junge NutzerInnen ein intuitives Gefühl dafür bekommen, was mit ihren Daten passiert und was sie wert sind. Sie sollten die Daten in ihrem „Daten-Portemonnaie" erfassen können und befähigt werden, einzuschätzen, welche Datenkategorien wie zu behandeln sind. Die E-Mail-Adresse als personenbezogenes Datum ist anders einzuschätzen als Fotos aus dem privaten Umfeld oder die sexuelle Orientierung.[11] Es gilt, Datenschutz individueller und differenzierter zu vermitteln. Schließlich sollte das Ziel der Kompetenzvermittlung sein, ein Bewusstsein für den Wert personenbezogener Daten sowie für die Verletzlichkeit der Freiheit zur digitalen Selbstentfaltung zu erzeugen.

Um dem Prinzip der Befähigung zu folgen, sind ebenso Unternehmen gefordert, ihre Datenschutzmaßnahmen so zu kommunizieren, dass die NutzerInnen in der Lage sind, Kompetenz in diesem Bereich zu erwerben. Dazu muss erstens Technik vor allem im B2C Bereich verständlich und einfach erklärt werden (Recht auf Einfachheit) und zweitens ist Kommunikation von datenschutzrelevanten Sachverhalten auf die jeweilige Zielgruppe auszurichten. Die DSGVO hat dafür einen ersten Ansatz für die Datenerhebung bei Minderjährigen vorgenommen.[12] Wobei hier nicht das Augenmerk auf den Grad der Komplexität der Technik, sondern auf die Kenntnis und Wissensstand der Zielgruppe gelegt werden sollte.

11 Ergebnisse des D21-Digital-Index 2018/2019 (S. 53) zeigen deutliche Unterschiede, wie differenziert die Befragten das Sicherheitsniveau bei persönlichen Daten einschätzen. Vgl.: Initiative D21 e.V. D21-Digital-Index 2018/2019, Jährliches Lagebild zur Digitalen Gesellschaft; online verfügbar unter: https://initiatived21.de/app/uploads/2019/01/d21_index2018_2019.pdf (letzter Abruf: 12.05.2019).
12 Siehe Erwägungsgrund 58 DSGVO – Grundsatz der Transparenz.

IV. Die Rolle des Staates

Versteht man die Datensouveränität als eine aktive Befähigung der NutzerInnen zum selbstbestimmten Umgang mit ihren Daten, muss auch die Rolle des Staates neu gedacht werden. Denn als Vertrauensanker für die BürgerInnen kommen nicht nur CDR-Ansätze von Unternehmen in Frage, sondern auch der Staat als Garant der Einhaltung von Datenschutzbestimmungen und als Förderer digitaler Selbstbestimmungschancen.

Die Gewährleistung der Datensouveränität muss also als ein Teil der öffentlichen Daseinsvorsorge aufgefasst werden. Denn die Digitalisierung des öffentlichen Raums im Sinne des Ausbaus öffentlicher Infrastruktur, digitaler Kultur-, Bildungs- und Verwaltungsangebote kann nur dann im Sinne von BürgerInnen sein, wenn ihre informationelle Selbstbestimmungschancen dadurch nicht verengt, sondern gestärkt und eventuell sogar ausgeweitet werden. Damit ist nicht nur die (selbstverständliche) Einhaltung von Datenschutz- und Datensicherheitsstandards im Zuge der Digitalisierung gemeint, sondern auch die Ausarbeitung von Konzepten und die Implementierung von Anwendungen, welche die Hoheit der Menschen über die Verwendung ihrer personenbezogenen Daten – z. B. in urbanen Datenräumen – ermöglichen und mit nutzerfreundlichen Tools fördern.

Das gilt beispielsweise auch für die Umsetzung des sog. Once-Only-Prinzips. Mit dem Once-Only-Prinzip soll erreicht werden, dass BürgerInnen und Unternehmen bestimmte Standardinformationen den Verwaltungsbehörden nur einmal mitteilen müssen und diese die Informationen untereinander im Bedarfsfall austauschen (Once-Only 1.0). Die Idee des Once-Only 2.0 geht dabei noch weiter und zielt auf die Einbeziehung der bereits vorliegenden Daten aus der Wirtschaft in die Verwaltungsprozesse. Die Verwaltung könnte damit künftig zur zentralen Drehscheibe für den Datenfluss zwischen BürgerInnen und staatlichen Stellen sowie Unternehmen werden – mit Vorteilen für alle Seiten. Wenn der Staat bei der lebenslagenbezogenen Digitalisierung seiner Leistungen konsequente Datenweitergabe zwischen Öffentlichen und Privaten ermöglichen soll, muss er gleichzeitig eine neue Qualität bei Transparenz und Nutzungskontrolle ermöglichen – nicht zuletzt auch für die Stärkung der Akzeptanz dieses Angebotes durch BürgerInnen. Es bedarf Kontroll- und Steuerungselementen, über die zu jeder Zeit Anpassungen individueller Privacy-Einstellungen vorgenommen werden können. Darüber ließen sich etwa Datenempfangende und Verarbeitungszwecke kategorisieren und die sogenannten Betroffenenrechte wie Änderung, Löschung oder Portierung unkompliziert ausüben.[13]

Bei der Befähigung der NutzerInnen soll der Staat gegenüber den Privaten mit gutem Beispiel vorangehen und bei der Datenerhebung von vornherein transparent sein sowie nutzerfreundliche Steuerungsmöglichkeiten für die Datenverwendung ermöglichen. Um das Konzept „Datensouveränität" über alle Bereiche hinweg durchgehend zu gewährleisten, sollten staatliche Stellen nicht nur reaktiv, wie z. B. bei konkreten Auskunftsanfragen, agieren. Vielmehr sollten sie bereits von vornherein intuitiv nachvollziehbar zeigen, wie und zu welchen Zwecken die jeweiligen personenbezogenen Daten verarbeitet werden. Damit würde der Staat als ein Vertrauensanker fungieren. Der Staat ist sowohl Teil einer Lösung als auch Teil des Problems und steht im Konflikt (Vorratsdatenspeicherung, Fluggastdatenspeicherung etc.) mit dem Konzept der Datensouveränität, wenn es beispielsweise um die Überwachung und die Sicherheit des öffentlichen Raums geht.

Zusammenfassend lässt sich feststellen, dass die Datensouveränität durch den Staat konkret dadurch ermöglicht werden kann, indem die Einhaltung von Datenschutzregeln sichergestellt, technologische Instrumente für ein selbstbestimmtes Handeln im Netz bereitgestellt und digitale Kompetenzen vermittelt werden. So kann die Gewährleistung von Datensouveränität analog zu Sicherheit, Bildung oder Gesundheit als staatliche Daseinsvorsorge aufgefasst werden.

13 Reinhardt, Marc & Horn, Nikolai (2018): Datensouveränität als Bestandteil des Once-Only-2.0-Prinzips, begleitende Publikation zur Plattform 6, Digitale Verwaltung und öffentliche IT des Digital-Gipfels 2018; online verfügbar unter: https://www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p6-datensouveraenitaet-once-only-2-0-prinzip.pdf?__blob=publicationFile&v=2 (letzter Abruf: 12.05.2019).

Ein Blick in die Zukunft – Privacy-Utopie 2040

In einer Welt voller Daten und florierenden Smart Cities der Zukunft ist der Einsatz von datenschutzfreundlichen Technologien genauso selbstverständlich wie der Einsatz von energieeffizienter und umweltfreundlicher Technik. Standards der DSGVO wurden schon vor einigen Jahren über den EU-Rechtsrahmen hinaus übernommen und ein einheitliches, weltweit gültiges Datenschutz-Zertifikat eingeführt, das die Einhaltung dieser Standards garantiert. Sicherheitsstandards wurden vereinheitlicht und zu einem „Security-Data-Reporting" für NutzerInnen vereinfacht, um zu erkennen, ob ein Dienst sicher und datenschutzfreundlich ist oder nicht. Die BürgerInnen verfügen über ein eigenes individuelles „Privacy-Data-Profile", das ihnen ihre Einstellungen zum Datenschutz einfach visualisiert, und das außerdem mit anzuwendenden Diensten und dem dahinterliegenden „Security-Data-Reporting" verglichen werden kann. Für die BürgerInnen ist es zudem möglich, in ihrem Privacy-Cockpit mit wenigen Klicks die weltweite Nutzung ihrer Daten durch Dritte nachzuvollziehen und ihr ggf. zu widersprechen. Mit einem „Reset"-Knopf ist es den NutzerInnen auch möglich, ihre „digitalen Zwillinge" jederzeit auf null zu setzen und das digitale Dasein immer wieder neu zu beginnen. Durch die Selbstverpflichtung von Unternehmen, dem „Digital-Newborn" in einem schonenden Ausgleich gleichwertige Produkte anzubieten, haben datenschutzfreundliche Technologien eine Nachfrage erfahren, die einen globalen Wettbewerb um „besseren Service mit weniger Personendaten" auslösten. Da die Datenschutzverstöße massiv zurückgegangen sind, konzentrieren sich die Aufsichtsbehörden primär auf die Beratung von NeugründerInnen beim Aufbau privatsphärenfreundlicher Geschäftsmodelle. Im „Digitalunterricht" wird neben den Grundlagen der Data Analytics ebenso Digitale Ethik unterrichtet und die Sozialwissenschaften behandeln den „Überwachungstotalitarismus" als Gegenteil einer offenen Digitalgesellschaft.

V. Fazit

Um dem Ziel einer gelebten informationellen Selbstbestimmung als „Datensouveränität" in den nächsten Jahren näher zu kommen, müssen folgende Schritte bereits heute unternommen werden:

- Die Ermöglichung der Datensouveränität muss im Sinne der Befähigung der NutzerInnen als technologische, gesellschaftliche und staatliche Aufgabe begriffen werden, die über die selbstverständliche Sicherstellung der Einhaltung von Datenschutzvorschriften hinausgeht.

- Der Einsatz von nutzerfreundlichen Transparenz- und Kontrollmechanismen muss sowohl beim Ausbau von digitalen Verwaltungsangeboten als auch bei der Entwicklung neuer datengestützter Geschäftsmodelle gefördert werden.

- Vertrauensanker für den Umgang mit personenbezogenen Daten der BürgerInnen müssen ausgebaut und implementiert werden: Von unternehmerischer Seite durch den Ausbau von CDR-Strategien, die das Handeln von Unternehmen an der informationellen Selbstbestimmung ausrichten. Von staatlicher Seite durch die Förderung datenschutzfreundlicher Technologien und durch proaktive Implementierung dieser Technologien im Zuge des Ausbaus des digitalen Staates.

- Die Vermittlung von Datenkompetenzen muss mehr sein als die Vermittlung von technologischem Wissen. Sie muss sich mit den gesellschaftlichen, wirtschaftlichen und sozialen Logiken hinter den Prozessen auseinandersetzen und NutzerInnen in der Rolle als Datengebende mit dem Ziel befähigen, souverän am digitalen Leben teilzunehmen.

- Stärkere personelle und finanzielle Ausstattung von Datenschutzbehörden, damit sie nicht nur ihre Kontrollfunktionen erfüllen, sondern auch BürgerInnen und Unternehmen in einer beratenden Funktion zur Verfügung stehen können.

Initiative D21

Kooperationspartner:

Capgemini

digitales Denken

Die Arbeitsgruppe Innovativer Staat

- Die Arbeitsgruppe Innovativer Staat der Initiative D21 bietet Akteuren aus Politik, Verwaltung, Wirtschaft, Wissenschaft und Zivilgesellschaft eine neutrale Austausch- und Aktionsplattform, um Themen rund um den innovativen Staat in Deutschland voranzubringen. In der Arbeitsgruppe werden Ideen, Positionen, Erfahrungen und Meinungen auf Augenhöhe ausgetauscht, Kontakte geknüpft, Barrieren und Missverständnisse zwischen Akteuren abgebaut und Themen zielorientiert nach vorne gedacht.
- Die Arbeitsgruppe leistet einen aktiven Beitrag im Sinne einer Handlungsaufforderung für den Bereich „Moderner Staat, lebendige Demokratie und Bürgerbeteiligung“ und steht als Expertengremium mit Rat und Tat zur Seite, damit zukünftig die Potenziale der Digitalisierung zur Stärkung der Demokratie und des Standortes Deutschland noch stärker genutzt werden.

Impressum

Initiative D21 e.V.
Reinhardtstraße 38
10117 Berlin
www.InitiativeD21.de

Telefon: 030 5268722-50
kontakt@initiatived21.de

Download
initiatived21.de/publikationen/denkimpulse-zum-innovativen-staat