MERKUR

Deutsche Zeitschrift für europäisches Denken

69. Jahrgang, Mai 2015 12 €
Klett-Cotta

792

Datenschutzversagen

Von Max-Otto Baumann

Jüngst veröffentlichte Analysen der Online-Plattform Lobbyplag zeigen, dass Deutschland in den Verhandlungen über die neue EU-Datenschutz-Grundverordnung eine »unrühmliche Rolle« spielt:[1] Die deutsche Regierung, vertreten durch das Innenministerium, unterlaufe systematisch die europäischen Bemühungen für einen starken Daten- und Privatsphärenschutz. Dabei hatte Bundeskanzlerin Merkel nach den Snowden-Enthüllungen öffentlich erklärt, dass sich Deutschland nun erst recht in Brüssel für die Verabschiedung einer starken Datenschutz-Grundverordnung einsetzen werde.

Man kann sich über diesen Wortbruch empören. Aber die zurückhaltende, bisweilen regelrecht obstruktive Rolle der Politik beim Datenschutz war für kritische Beobachter schon länger erkennbar. Sie zeigt sich paradoxerweise nicht nur im – mehr oder weniger offenen – Widerstand gegen eine Stärkung des Datenschutzes, sondern sie kommt auch darin zum Ausdruck, welche inhaltlichen Strategien die Politik zur Stärkung des Datenschutzes zumindest in ihren öffentlichen Stellungnahmen verfolgt.

1 Vgl. Katharina Blaß, *Europäischer Datenschutz: So groß ist der Einfluss von Lobbyisten*. *Spiegel Online* vom 10. März 2015 (www.spiegel.de/netzwelt/netzpolitik/europaeischer-datenschutz-lobbyplag-beweist-lobbyeinfluss-a-1022721.html).

Seit Jahren vertritt die Politik die Ansicht, dass eine Hebung des Datenschutzniveaus sich am besten über eine Stärkung der Medienkompetenz im Rahmen des »Rechts auf informationelle Selbstbestimmung« verwirklichen lasse. Die Strategie »Datenschutz durch Medienkompetenz« wird von allen Parteien propagiert – von CDU/CSU und FDP (in der letzten Koalition) als tragendes Element ihrer Datenschutzpolitik; von SPD, Grünen und Linken eher als eine komplementierende Herangehensweise zu einer rechtlichen Regulierung.

CDU/CSU-Abgeordnete haben im Parlament immer wieder die »Vorstellung vom mündigen Bürger« und dessen »Eigenverantwortung« aufgegriffen und auf dieser Grundlage einen Ausbau der Medienkompetenz gefordert. Im aktuellen Koalitionsvertrag heißt es: »Wir sehen … Medien- und Informationskompetenz als zentrale Maßnahme für den Datenschutz.« Die Digitale Agenda von 2014 möchte Medienkompetenz stärken, um »die Souveränität der Verbraucherinnen und Verbraucher auf den digitalen Märkten« zu sichern. Weitere Belege ließen sich nennen, so hat etwa die Kultusministerkonferenz 2012 den Ausbau von Medienkompetenz in der Schule als Mittel zum Datenschutz gefordert. Darüber hinaus findet die Forderung nach Medienkompetenz auch im gesellschaftlichen Diskurs viel Resonanz; Fachtagungen zum Thema Privatsphäre enden gerne mit einem Bekenntnis zur Medienkompetenz.

Medienkompetenz hat in Bezug auf den Datenschutz zwei Komponenten: nämlich erstens »Selbstdatenschutz«, und dies, zweitens, auf der Grundlage (teilweise auch darüber hinausgehend) des

existierenden Rechts auf informationelle Selbstbestimmung. Mit ihrer Kombination aus gefälliger liberaler Rhetorik und Grundrechtsbegrifflichkeit erzielt die Rede von der Medienkompetenz jedoch vor allem eine Blendwirkung. Das Ganze erweist sich so als Strategie der Entpolitisierung eines zutiefst politischen Themas. Medienkompetenz ist praktisch kaum umsetzbar, und vor allem ist sie, insofern sie die Verantwortung für den Schutz der Privatsphäre dem Individuum zuweist, ein Arrangement, das eines modernen Rechtsstaats unwürdig ist.

Praktische Probleme der Medienkompetenz

Es beginnt schon damit, dass die Bundespolitik eine Forderung erhebt, die sie gar nicht einlösen kann, denn Medienkompetenz ist Bildungs- und damit Ländersache. Der Verdacht der Wählertäuschung drängte sich weniger auf, gäbe es in Deutschland eine finanziell entsprechend ausgestattete, inhaltlich auf den Datenschutz bezogene und bei der richtigen Personengruppe ansetzende Medienkompetenzförderung. Das ist leider nicht der Fall.

Die wesentlichen Befunde zur Medienkompetenzförderung in Deutschland lassen sich wie folgt zusammenfassen:[2] Die Landesmedienanstalten, die für die staatliche Medienkompetenzförderung zuständig sind, geben zusammen geschätzt 2,4 Millionen Euro jährlich für die *internetbezogene* Medienkompetenzförderung aus – eine Lappalie. Sie beschäftigen sich mit dem Thema Internet, wenn überhaupt, aus eigener Initiative, denn einen politischen Auftrag dafür gibt es nicht, die entsprechenden Gesetze (primär die Landesmediengesetze) wurden nie unter diesem Aspekt novelliert.

Schon der Begriff »Medienkompetenz« ist in Bezug auf Datenschutz völlig ungeeignet, denn er kommt aus der Pädagogik, deren Thema die gesellschaftliche Sozialisation und Teilhabe Heranwachsender ist; die Begriffe »Privatsphäre« und »Datenschutz« findet man in der einschlägigen Literatur nicht. Die von der Politik (als Auftraggeber) hergestellte Verknüpfung von Medienkompetenz mit Datenschutz muss also in der Wissenschaft und bei den Medienkompetenzpraktikern auf Kopfschütteln treffen: Sie haben dieses Produkt nicht im Programm.

So kommen bizarre Kategorienfehler zustande wie jener in einer Broschüre des IT-Planungsrates der Bundesregierung, die Medienkompetenz als Datenschutzstrategie empfiehlt, während sie zugleich das Schreiben von E-Mails und die Nutzung von sozialen Online-Netzwerken als Ziel von Medienkompetenz nennt – damit fängt aber das Problem des Datenschutzes überhaupt erst an. Die Ziele Teilhabe und Datenschutz widersprechen sich also förmlich.

Alle Theorien und Initiativen der Medienkompetenzförderung sind fast ausschließlich auf Heranwachsende eingestellt, auch dies ein Grund, weshalb sie das Thema Datenschutz verfehlen müssen. Heranwachsende sind keine vollwertigen Bürger und auch nur sehr eingeschränkt Kunden (sie sind nicht

2 Vgl. Max-Otto Baumann, *Datenschutz durch Medienkompetenz?* In: Ulrike Ackermann (Hrsg.), *Freiheitsindex 2014*. Frankfurt: Humanities online 2014.

wahlberechtigt, nicht strafbar, gehen keine Verträge ein, haben keine Versicherungen etc.), weshalb sie von der Problematik des Datenschutzes und der informationellen Selbstbestimmung nur peripher betroffen sind. Last but not least bedeutet die Fokussierung auf Heranwachsende, dass die Medienkompetenzförderung die breite Gesellschaft, deren Datenschutzniveau gehoben werden soll, nur im Schneckentempo des Generationenwechsels erreicht. Die digitale Revolution aber rast.

Praktische Probleme der informationellen Selbstbestimmung

Schon angesichts dieser Unstimmigkeiten ist fraglich, ob es überhaupt lohnt, die Medienkompetenzförderung unter Einsatz enormer finanzieller Mittel völlig neu aufzustellen, um den Selbstdatenschutz und das Recht auf informationelle Selbstbestimmung ausüben zu können. Viel wichtiger ist die Frage, was Medienkompetenz im hypothetisch besten Falle für den Datenschutz leisten kann, ob sie auch das richtige Mittel zum Zweck ist. Auch da liegen prinzipielle Einwände auf der Hand.

Zunächst einmal sind Selbstdatenschutz und informationelle Selbstbestimmung zwei unterschiedliche Dinge, wobei über Selbstdatenschutz wohl nicht allzu viel zu sagen ist: Ob man seine Daten effektiv gegen die NSA schützen kann, ist sehr fraglich. Besonders medienkompetente Menschen mögen hier Teilerfolge durch Anonymisierung und Verschlüsselung erzielen, bewirken aber zugleich, dass sie überhaupt erst ins Visier staatlicher Überwachung geraten. Die anonyme Kommunikation hilft außerdem wenig, wenn man an vielen anderen Stellen im Netz auftaucht, und sei es durch die Kontaktlisten der Freunde – die NSA investiert enorme Mittel, um diese Datenschnipsel wieder zu einem Persönlichkeitsbild zusammenzufügen. Gegen die privatwirtschaftliche Datensammlung bietet das Blockieren von Tracking und Werbung einen gewissen Schutz, darüber hinaus versagt der Selbstdatenschutz aber, wenn man Dienste nutzen möchte, für die personenbezogene Daten preisgegeben werden müssen, über die man dann keine angemessene Kontrolle mehr hat. Es bleibt da nur die Vermeidung, was aber umso »teurer« wird, je mehr das Internet zum Medium fast aller Lebensaktivitäten wird.

Dagegen führt der Schritt vom Selbstdatenschutz zur Ausübung eines Rechts auf eine ganz andere Ebene. Rechte sind Fremdverpflichtungsbefugnisse, das heißt das Recht auf Privatsphäre erfüllt sich in der korrespondierenden Pflicht von anderen (Unternehmen, Staat), dieses Recht zu respektieren. Das Recht auf informationelle Selbstbestimmung ermöglicht es also, wirtschaftliche Beziehungen einzugehen und trotzdem noch Kontrolle über die eigenen Daten zu behalten, wenngleich in bestimmten rechtlichen Grenzen. Moralisch betrachtet, ist die gesetzlich vorgesehene Einwilligungsregelung eine starke Legitimation: Lade ich einen Fremden in mein Haus ein, verletzt dies meine Privatsphäre nicht; verschafft er sich unerlaubt Zutritt, dagegen schon.[3] Einwilli-

3 Vgl. Bart W. Schermer / Bart Custers / Simone van der Hof, *The crisis of consent: how stronger legal protection may lead to weaker consent in data protection*. In: *Ethics and Information Technology*, Nr. 2, 2014.

gung wirkt also moralisch transformativ, sie wahrt die individuelle Autonomie.

In Deutschland hat das Recht auf informationelle Selbstbestimmung, das auf dem Prinzip der Einwilligung beruht, Grundrechtsrang; es liegt auch dem Entwurf einer neuen EU-Datenschutz-Grundverordnung zugrunde und hat im amerikanischen Rechtssystem ein, wenngleich etwas schwächeres, Pendant im »notice and consent«-Prinzip. Allerdings bestehen schon seit längerem Zweifel, ob das Rechtsparadigma der informationellen Selbstbestimmung nicht längst von der Realität überholt wurde. Damit würde auch das letzte Argument für Medienkompetenz stürzen, sofern diese nämlich zur Ausübung dieses Rechts befähigen soll.

Studien und Umfragen belegen immer wieder, dass kaum jemand von seinem Recht auf informationelle Selbstbestimmung Gebrauch macht: AGBs werden nicht gelesen, man legt keine Einsprüche ein, fordert keine Auskunft über seine Daten ein, beantragt keine Löschung. Zwar könnte man dies als ein Problem betrachten, das gerade durch Medienkompetenz zu beheben wäre. Allerdings argumentieren die Studien, dass es schlicht nicht mehr realistisch ist, alle AGBs zu lesen, geschweige denn zu verstehen und dann in eine zwanglose Abwägung zu treten, ob man einen Dienst nutzen möchte oder nicht. Massenhaftes Versagen bei der Ausübung eines Grundrechts deutet auf strukturelle Probleme hin.

Die Gründe, weshalb die Internetnutzer bei der informationellen Selbstbestimmung versagen, sind offenkundig: Viele Menschen sind sich der enormen Datenmengen, die sie freisetzen, nicht bewusst. Sie wissen zum Beispiel nicht, wie ein Cookie funktioniert, welche Daten es sammelt und welche Informationen sich daraus ableiten lassen. Damit ist eine Prämisse der informationellen Selbstbestimmung verletzt, nämlich das *Bewusstsein* über die eigenen Datentransaktionen und die möglichen Folgen. Die Datensammlung- und verarbeitung ist technisch und ökonomisch derart komplex geworden, dass der durchschnittliche Nutzer auch gar nicht mehr die *Fähigkeit* haben kann, zu kontrollieren, wie andere seine Daten verwenden.

Wir kennen solche Situationen aus anderen Bereichen: Wenn sich im Straßenverkehr die schweren Autounfälle an einer bestimmten Kurve signifikant häufen, geht die moralische Verantwortung dafür vom Fahrer auf die Verkehrsbehörde über, ungeachtet gesetzlicher Regelungen, die den Fahrer haftbar machen. Viktor Mayer-Schönberger, der Vordenker des 2014 vom Europäischen Gerichtshof geschaffenen »Rechts auf Vergessenwerden«, hat deshalb das Ende des Paradigmas der informationellen Selbstbestimmung ausgerufen: »The naked truth is that informational self determination has turned into a formality devoid of meaning and import … Protection for the consumer should not depend on the ability to comprehend what's going on with her data and ability to take action.«[4]

Angriff auf die Selbstbestimmung

Im Grunde ist die absichtliche Verletzung der Selbstbestimmung schon Teil des Systems. Noch immer hört man häu-

4 Vgl. www.privacyassociation.org/news/a/keynote-forget-notice-and-choice-lets-regulateuse

fig den Satz: »Der Nutzer zahlt mit seiner Privatsphäre.« Aber das stimmt nicht mehr, denn oft geht es gar nicht um einen Tausch, sondern die Interaktionen gleichen mehr einem Betrug, einer Täuschung. Durch Profilbildung wird der Zugang zu Produkten geregelt und häufig auch verteuert – Stichwort Preisdiskriminierung. Wer zum Beispiel einen Apple-Laptop für Online-Bestellungen nutzt, bekommt Preise, die bis zu 50 Prozent höher als normal ausfallen können, weil die Verwendung von Apple auf eine andere Präferenzordnung des Nutzers schließen lässt. In Wahrheit zahlt man also zweimal. Auf den Internetseiten von Big-Data-Firmen wird unverblümt mit Strategien der »emotionalen Beeinflussung« von Kunden geworben. Zweck der Datenverarbeitung ist also gerade die Überwindung der Nutzerselbstbestimmung, die deswegen nicht Grundlage von Datenschutz sein kann.

Im letzten Jahr hat US-Präsident Barack Obama seine Berater beauftragt, die Rolle von Big Data in Bezug auf die Privatsphäre zu untersuchen. In dem von John Podesta verantworteten Bericht wird das Problem treffend auf den Punkt gebracht: »Collective investment in the capability to fuse data is many times greater than investment in technologies that will enhance privacy.«[5] Das lässt das Machtverhältnis erahnen, in dem Nutzer und Unternehmen stehen. Und ein begleitender Bericht über die technologischen Grundlagen resümiert im Mai 2014: »As a useful policy tool, notice and consent is defeated by exactly the positive benefits that big data enables: new, non-obvious, unexpectedly powerful uses of data.«[6]

Medienkompetenz selbst beinhaltet kein Recht, sie verortet die Verantwortung für den Datenschutz beim Nutzer, also beim Bürger. Die informationelle Selbstbestimmung ist zwar ein Recht, das sich aber trotz bester Medienkompetenz nicht angemessen ausüben lässt. Es ist daher Zeit, die Verantwortung für den Schutz der Privatsphäre stärker bei den Unternehmen zu verorten, die jene Datenprodukte herstellen, die Menschen entblößen und gefährden.

Die Unternehmen können sich bislang unter dem rechtlichen Vorwand der AGBs ihrer Verantwortung entziehen. Es wird sogar befürchtet, dass eine Verschärfung des Datenschutzes, wie sie die geplante EU-Datenschutz-Grundverordnung bringen soll, dazu führt, dass das Datenschutzniveau faktisch sinkt, weil die AGBs noch länger, juristischer und damit unpraktikabler werden. So ist die Privatsphäre weiterhin nicht adäquat geschützt. Tim Berners-Lee, der Erfinder des World Wide Web, hat festgestellt, dass man heute wegen Copyright-Verletzungen hinter Gittern landen kann, für solche der Privatsphäre dagegen nicht.[7] Das würde ein Datenschutzrecht voraussetzen, das die Haftung für unsere Daten denen gibt, die die Daten sammeln und verarbeiten.

5 John Podesta, *Big Data: Seizing Opportunities, Preserving Values* (www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf).

6 White House, *Report to the President: Big Data and Privacy: A Technological Perspective* (www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf).

7 Jemima Kiss, *An online Magna Carta: Berners-Lee calls for bill of rights for web*. In: *The Guardian* vom 12. März 2014.

Um über die Pflichten von Datenverarbeitern nachzudenken, empfehlen sich Anleihen bei der ethischen Theorie des »Gerechten Kriegs«, in der eine recht ähnliche Problemstellung bearbeitet wird. Hier wie da geht es um die Frage, wie das Recht von Menschen respektiert werden kann, die selbst nicht gefragt werden können. Die in der Lehre des »Gerechten Kriegs« entwickelten Kriterien des legitimen Zwecks, der Notwendigkeit und der Proportionalität werden vor allem im Diskurs der Bürgerrechtsaktivisten über die Zulässigkeit von staatlicher Massenüberwachung aufgegriffen.

Staaten können die überwachten Bürger, deren Privatsphäre zu schützen ist, nicht fragen, deshalb müssen die Restriktionen in allgemeinen Prinzipien der Datenverarbeitung liegen. Ich sehe keinen Grund, weshalb dieses Modell nicht auch stärker in Bezug auf privatwirtschaftliche Datenverarbeitung angewandt werden könnte – tatsächlich enthält ja das deutsche Bundesdatenschutzgesetz auch allgemeine Prinzipien wie die Datensparsamkeit und Zweckbindung, die genau diesem Modell entsprechen. Sie stehen aber hinter dem Prinzip der Selbstbestimmung zurück und werden derzeit nicht mit Gewinn abschöpfenden Sanktionen durchgesetzt. Man mag in diesem Modell das Risiko von Datenpaternalismus erblicken, aber es ist gering im Vergleich zur gegenwärtigen Realität einer endemischen Privatsphärenverletzung.

Ein politisches Thema

Privatsphäre ist ein politisches Thema, weil sie, erstens, ein Menschenrecht ersten Ranges ist und damit höchsten gesellschaftlichen Schutz verdient. Ihr moralisches Fundament ist so massiv, dass sie auch für diejenigen verteidigt werden kann, die meinen, darauf vorerst verzichten zu können. Der Informationsethiker Rafeal Capurro erblickt dieses Fundament in der uralten philosophischen Unterscheidung vom Menschen als materiellem und rationalem Wesen, aus der bei Kant die Begründung der Menschenwürde wird: Der Mensch ist nicht allein kausal determiniert, sondern kann über sich hinausgehen und die Welt der Moral, der Erfahrung, der Subjektivität betreten. »This experience of human autonomy and universality, with all its ambiguities and limitations, is at the core, it seems to me, of what we mean when we say that we must protect privacy.«[8] Die Privatsphäre schützt uns vor der Welt der Macht, der Wirtschaft, der Gewalt. Eine humane Gesellschaft, in der die Individuen nicht »Mittel« für fremde Interessen, sondern »Zwecke« sind, ist daher nicht ohne Privatsphäre möglich.

Derselbe Gedanke kann, zweitens, auf einer konkreteren Ebene von Rechten formuliert werden. Die Privatsphäre ist eine politische Angelegenheit, insofern sie ein *Recht* verleiht, das von anderen eingefordert werden kann. Das Recht auf Privatsphäre zu haben bedeutet, ein Recht auf eine Gesellschaft zu haben, die so organisiert ist, dass sie die Privatsphäre respektiert. Dabei wächst der Privatsphäre im Zuge der Digitalisierung der Status eines »basic right«

8 Rafael Capurro, *Privacy. An intercultural perspective*. In: *Ethics and Information Technology*, Nr. 1, 2005.

zu,[9] das grundlegender ist als andere Rechte, deren Geltung vom Recht auf Privatsphäre abhängt. Das gilt insbesondere für das Recht auf Informations-, Meinungs- und Versammlungsfreiheit, das Diskriminierungsverbot und das Recht auf einen ordentlichen Prozess – sie alle werden durch das Recht auf Privatsphäre nach beiden Seiten erweitert, sowohl was die »harten« als auch die eher alltäglichen Fälle betrifft. Wenn schon, dann ist also die Privatsphäre das neue »Supergrundrecht«, nicht die Sicherheit.

Drittens, und das ist eine Konkretisierung der ersten beiden Punkte, ist die Privatsphäre ein politisches Thema, insofern sie die Beziehung des Individuums insbesondere gegenüber dem Staat und der Wirtschaft ganz wesentlich mitregelt. Das jeweils zugestandene Maß an Privatsphäre beziehungsweise an Privatsphärenverletzung bestimmt ganz wesentlich darüber, welche Macht der Staat und die Unternehmen gegenüber den Individuen haben. In Diktaturen hat der Bürger keine Macht gegenüber dem Staat. Von einer Diktatur sind wir in den westlichen Demokratien zwar trotz endemischer Massenüberwachung gewiss weit entfernt, aber dennoch ist unbestreitbar, dass die Macht von Regierungen und Unternehmen im Zuge der digitalen Revolution in einer Weise zugenommen hat, dass es die individuelle Freiheit einschränkt und damit längerfristig auch die Grundlagen der Demokratie gefährdet.

Eine angemessene Reaktion auf die Gefährdung der Privatsphäre kann daher ebenfalls nur politischer Natur sein. Instrumente der digitalen Selbstverteidigung mögen taugliche Waffen gegen die staatliche Überwachung sein, aber es handelt sich dabei im Kampf um die Privatsphäre letztlich um die falsche Waffengattung: Jede technisch noch so ausgefeilte Strategie des Selbstdatenschutzes kommt zu ihrem abrupten Ende, wenn der Staat sie mit den politischen Mitteln des Gesetzes verbietet. Der britische Premier David Cameron hat angekündigt, im Falle seiner Wiederwahl die anonyme Kommunikation in England unter Strafe stellen zu wollen, der Staat müsse die Kommunikation seiner Bürger mitlesen können.

9 Henry Shue, *Basic Rights. Subsistence, Affluence, and U. S. Foreign Policy*. Princeton University Press 1996.