DIE INFORMIERTE EINWILLIGUNG

EIN DATENSCHUTZPHANTOM

von Jeanette Hofmann und Benjamin Bergemann

ISTOCK / PETROVICH9

Wer liest sie schon, die unzähligen Seiten der Geschäftsbedingungen aller möglichen Internetdienste? Die meisten haken einfach ab: klick und weg. Schließlich wollen sie den Dienst nutzen. Dabei legitimieren wir mit dieser so genannten »informierten Einwilligung« einen Eingriff in unsere Grundrechte. Wie kam es dazu?

Wenn wir ein Smartphone oder einen Computer kaufen, machen wir einen entscheidenden Klick, bevor wir das neue Gerät nutzen können: Wir willigen in die Datenschutzbestimmungen des Herstellers ein. Mit diesem Klick stimmen wir gleichzeitig der Aufzeichnung unseres Nutzungsverhalten zu. Ohne diesen Klick bleibt der Bildschirm schwarz. Auch Internetdienste verlangen in aller Regel ein Häkchen hinter ihren oft seitenlangen Datenschutzbestimmungen. Die informierte Einwilligung hat sich zur wichtigsten rechtlichen Grundlage für die Datenverarbeitung im Internet entwickelt. Die gegenwärtige Bedeutung ist das Ergebnis einer Transformationsgeschichte, die so sicherlich weder beabsichtigt noch vorhersehbar war und bis heute nicht systematisch aufgearbeitet worden ist. Dieser Artikel erklärt, wie die Einwilligung zu einem zentralen Instrument des Datenschutzes wurde – und warum das zunehmend zum Problem wird.

Bei genauerer Betrachtung zeigt sich, dass sich mit der Einwilligung heute sehr unterschiedliche, teils widersprüchliche Perspektiven verbinden. Aus rechtlicher Sicht stellt jedwede Form der Verarbeitung persönlicher Daten einen Eingriff in unsere Grundrechte dar: Mit der Einwilligungserklärung gestatten wir Anbietern erst, was andernfalls verboten wäre. Aus wirtschaftlicher Perspektive wiederum ist die informierte Einwilligung die vielleicht unverzichtbare Rahmenbedingung für den modernen Datenkapitalismus, der unsere persönlichen Daten in eine international akzeptierte Währung verwandelt hat. Aus alltagspraktischer Sicht ist die informierte Einwilligung dagegen zumeist nicht viel mehr als das zum Ritual gewordene Runterscrollen der Geschäftsbedingungen und das Häkchen, das wir abschließend setzen, um in den Genuss einer gewünschten App, also einer Informationsdienstleitung zu kommen, die anders heute praktisch nicht zu erwerben ist. Studien zeigen, dass die Datenschutzbestimmungen der Anbieter mehrheitlich nicht gelesen werden. Wir legitimieren den Eingriff in unsere Grundrechte also zumeist uninformiert.

Der Sozialwissenschaftler Alessandro Acquisti bezeichnet das Auseinanderklaffen von Anspruch und Wirklichkeit bei der Einwilligung als »Privacy Paradox«: In der Theorie ist uns am Schutz unserer Privatsphäre durchaus sehr gelegen; in der Praxis aber ziehen wir es vor, uns in sozialen Netzwerken auszutauschen und die Anzahl unserer Schritte mit Hilfe von Fitness-Trackern zu protokollieren – und das meist zu allem anderen als datenschutzfreundlichen Bedingungen. Aber diese Perspektive auf unser widersprüchliches Verhalten

greift zu kurz: Das Privacy-Paradox verortet den Widerspruch nämlich in unserem individuellen Verhalten. Das ist in etwa so, als wolle man heute die Nutzung einer Kreditkarte als Frage individueller Präferenzen darstellen und dabei außer Acht lassen, dass Online-Einkäufe, Flug- oder Hotelbuchungen oftmals den Besitz einer Kreditkarte voraussetzen. Berücksichtigt man, dass die informierte Einwilligung inzwischen Bestandteil eines globalisierten Geschäftsmodells ist, muss man sich fragen, ob wir es hier nicht eher mit einem grundlegenderen Problem zu tun haben. In Zeiten der allgegenwärtigen Datenverarbeitung kann die informierte Einwilligung kaum noch als Ausdruck unserer individuellen Handlungsfreiheit gelten. Und in dem Maße, in dem die Digitalisierung nun auch die Dinge erfasst und beispielsweise als Car-to-Car-Communication oder intelligentes Stromnetz infrastrukturelle Züge annimmt, wächst das Problem einer Einwilligung ohne ernsthafte Alternativen.

Der Jurist Spiros Simitis, der als Vater des deutschen Datenschutzes gilt, hat die Einwilligung bereits in den 1990er Jahren als Fiktion bezeichnet. Aller Kritik zum Trotz beweist sie gleichwohl große Beharrungskraft. Auch die jüngst verabschiedete europäische Datenschutz-Grundverordnung, die 2018 in Kraft treten wird, hält an ihr fest und sieht lediglich Optimierungsmaßnahmen, wie höhere Transparenzanforderungen an die Allgemeinen Geschäftsbedingungen beziehungsweise Datenschutzrichtlinien vor, in die wir Nutzer dann einwilligen. Wie konnte die Einwilligung, die sich im Alltag als so problematisch für die Menschen erweist, im Datenschutzrecht eine so starke Stellung gewinnen? Werfen wir einen Blick auf die Anfänge.

Die Einwilligung im ersten Bundesdatenschutzgesetz

Das Konzept der informierten Einwilligung ist fast so alt wie der Datenschutz selbst. Man findet es schon im ersten Bundesdatenschutzgesetz (BDSG) von 1977 als eine Möglichkeit der zulässigen Verarbeitung personenbezogener Daten: »Die Verarbeitung personenbezogener Daten, die von diesem Gesetz geschützt werden, ist in jeder ihrer in Paragraph 1 Abs. 1 genannten Phasen nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat.« (§3 BDSG 1977). Darauf folgende Daten-

MIT FRDL. GEN. VON JEANETTE HOFMANN

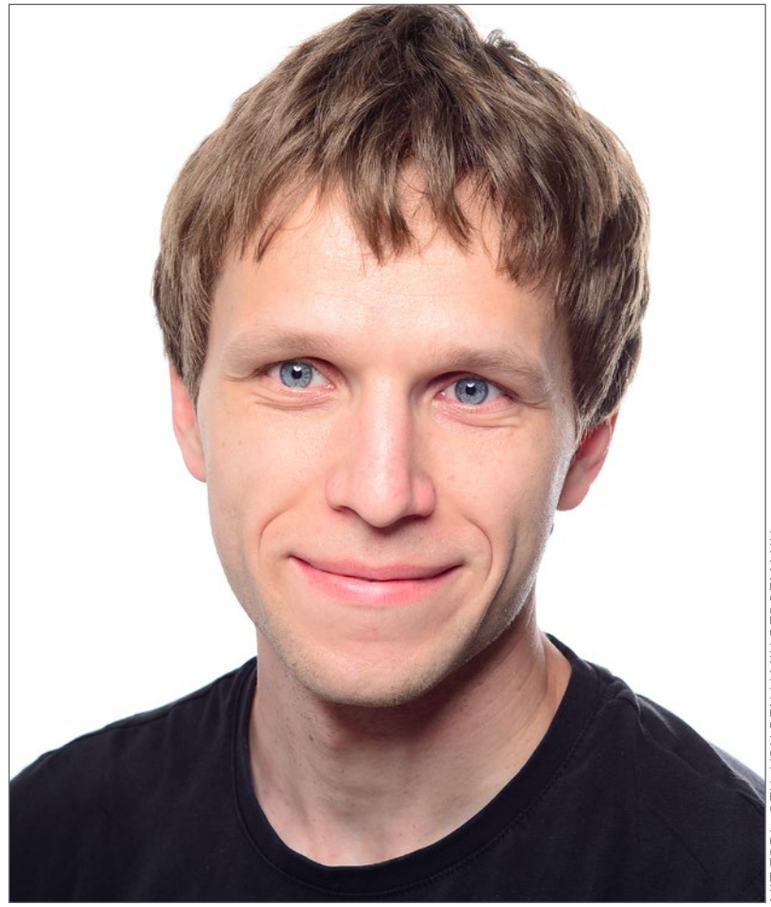
JEANETTE HOFMANN

Die Politikwissenschaftlerin Jeanette Hofmann forscht zu den Themen Global Governance und der Regulierung des Internets. Sie leitet die Projektgruppe Politikfeld Internet am Wissenschaftszentrum Berlin für Sozialforschung (WZB) und ist Direktorin am Alexander von Humboldt Institut für Internet und Gesellschaft (HIIG).

schutzgesetze definieren zudem eine Reihe von Anforderungen, denen eine Einwilligung genügen muss. Wesentlich ist, dass wir freiwillig und bewusst einwilligen. Wichtig ist außerdem, dass der Zweck der Datenerhebung und -verarbeitung, in den wir einwilligen, klar umrissen ist (§4a BDSG).

Die informierte Einwilligung stand (und steht bis heute) gleichberechtigt neben den gesetzlichen »Erlaubnistatbeständen« – ein Umstand, der in vielen juristischen Kommentaren hervorgehoben wird. Erlaubnistatbestände gestatten im Einzelfall, was die Regel eigentlich untersagt. Im Datenschutz verwirklichen Erlaubnistatbestände das Prinzip des »Verbots mit Erlaubnisvorbehalt«: Die Datenverarbeitung ist grundsätzlich untersagt, es sei denn, es liegt ein Erlaubnistatbestand vor, der die Ausnahme vom Verbot rechtfertigt. Praktisch besehen war die Bedeutung der Einwilligung zur Entstehungszeit des Datenschutzes jedoch so randständig, dass sich manche Beobachter fragten, warum sie überhaupt in das neue Gesetz aufgenommen wurde. Sofern beispielsweise Versicherungen personenbezogene Daten verarbeiteten, geschah dies normalerweise im Rahmen von Vertragsverhältnissen – einem der Erlaubnistatbestände. Die informierte Einwilligung beginnt ihre Karriere im Datenschutz als eine Art Residualkategorie oder Auffangbecken, um solche Formen kommerzieller Datenverarbeitung rechtlich abzusichern, die nicht zweifelsfrei durch Verträge zwischen Unternehmen und Kunden geregelt sind.

Schon hier kann man die zwei Gesichter erkennen, die die Bedeutung der informierten Einwilligung immer stärker prägen werden: Einesteils dient sie dazu, unerwünschte Eingriffe in unsere Grundrechte abzuwehren, und trägt somit unserem individuellen Recht auf Selbstbestimmung Rechnung. Anderenteils aber ermöglicht und erweitert sie auch die kommerzielle Datenverarbeitung, indem sie der Wirtschaft ein Instrument an die Hand gibt, das sich als weitaus flexibler erweisen wird als gesetzliche Bestimmungen. In der Frühphase des Datenschutzes stellte die informierte Einwilligung mithin einen Sonderfall dar, der bereits damals im Verdacht stand, den Rahmen der gesetzlich zulässigen privaten Datenverarbeitung zu sehr auszudehnen. Im öffentlichen Sektor spielt die informierte Einwilligung schon des-



MIT FRDL. GEN. VON BENJAMIN BERGEMANN

BENJAMIN BERGEMANN

Benjamin Bergemann studiert Politikwissenschaft (MA) an der Freien Universität Berlin und arbeitet für die Projektgruppe Politikfeld Internet am Wissenschaftszentrum Berlin für Sozialforschung (WZB). Seine Kernthemen sind Datenschutz und Überwachung.

halb keine Rolle, weil die staatliche Datenverarbeitung angesichts des Machtungleichgewichts zwischen Bürger und Behörde nicht durch unsere individuelle Einwilligung, sondern nur durch spezifische Gesetze legitimiert werden kann.

Das Aufkommen der automatisierten Datenverarbeitung

Die ersten Datenschutzgesetze, und mit ihr die Einwilligungsklausel, entstanden gegen Ende der 1970er Jahre vor dem Hintergrund der allmählich in Schwung kommenden automatisierten Datenverarbeitung. In Zeiten, in denen die digitale Datenverarbeitung kaum mehr einen Lebensbereich unberührt lässt, fällt es schwer nachzuvollziehen, welche Zäsur der Einzug der Großrechenanlagen in die öffentlichen Verwaltungen einst darstellte. Daher ist auch das Volkszählungsurteil des Bundesverfassungsgerichts von 1983 so bedeutsam, weil es die Risiken, die in der maschinellen Datenverarbeitung gesehen wurden, mit großer Hellsichtigkeit ausbuchstabierte: Die automatische Datenverarbeitung gefährde die Befugnis des Menschen, »grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden«, weil Entscheidungsprozesse nicht mehr den Rückgriff auf »manuell zusammengetragene Karteien und Akten« erfordern, sondern personenbezogene Informationen »technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind«. Sie können zu einem »Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsichtnahme und Einflussnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen«. Die Datenverarbeitung, so auch der Datenschutzexperte Simitis knapp 30 Jahre später, verschärfe »um ein Vielfaches die Verletzlichkeit des Einzelnen, ja der Gesellschaft überhaupt«. Die Datenschutzdiskussion der 1980er-Jahre ähnelt damit bemerkenswerterweise den Debatten, die wir heute über Big Data führen.

In den 1980er Jahren konzentrierten sich die Bedrohungsszenarien allerdings nicht auf die kommerzielle Datenverarbeitung, sondern auf den Datenhunger des Staates, der zu Planungszwecken, aber auch aus Gründen der inneren Sicherheit immer mehr Informationen verlangt und den »gläsernen Bürger« schaffte. Die private Datenverarbeitung war zwar bereits absehbar wichtig genug, um unter dem bezeichnenden Titel »Datenverarbeitung nichtöffentlicher Stellen für eigene Zwecke« ein eigenes Kapitel im Datenschutzrecht zu erhalten, im Kern aber zielte die Gesetzgebung darauf, die Grundrechte der Bürger durch neue Abwehrrechte gegenüber dem Staat zu stärken. Informationsbeziehungen, so formuliert es der Jurist Kai von Lewinski in einem jüngeren Beitrag zur Geschichte des Datenschutzes, sind auch Machtbeziehungen. Entsprechend besteht das genuine Ziel des Datenschutzes im »Schutz vor Datenmacht«.

Die Geburt der informationellen Selbstbestimmung: Das Volkszählungsurteil

Das Volkszählungsurteil des Bundesverfassungsgerichts von 1983 spielte eine wichtige Rolle für die weitere Entwicklung der informierten Einwilligung. Auf dieses Urteil geht das international einzigartige Grund-

recht auf informationelle Selbstbestimmung zurück, auf das sich heute auch die informierte Einwilligung beruft. Das neue Grundrecht sollte sicherstellen, dass jeder Mensch »grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann«. Die Auslegung des Datenschutzrechts im Lichte des Persönlichkeitsrechts begründet seinen Grundrechtscharakter und damit zugleich ein starkes Abwehrrecht gegenüber den Möglichkeiten staatlichen Machtmissbrauchs.

Auch wenn der persönlichkeitsrechtliche Bezug das Individuum klar ins Zentrum der informationellen Selbstbestimmung stellt, lässt das Volkszählungsurteil keinen Zweifel daran, dass die automatisierte Datenverarbeitung nicht nur die Entfaltungschancen des Einzelnen gefährdet, sondern auch das öffentliche Gemeinwohl. Selbstbestimmung, so das Bundesverfassungsgericht, sei eine »elementare Funktionsbedingung« einer Gesellschaftsordnung, die in der »Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger« gründet. Insofern erschöpft sich der Datenschutz nicht in einem individuellen Abwehr- beziehungsweise Selbstbestimmungsrecht, sondern er verfolgt auch gesellschaftspolitische Ziele, wie Kai von Lewinski betont. Gerade diese Verknüpfung von individuellen und gesellschaftlichen Bezügen im Volkszählungsurteil gerät leicht in Vergessenheit: Die Befürworter der informierten Einwilligung stützten sich in den folgenden Jahren hauptsächlich auf die individuelle Dimension des Datenschutzes. Seine gemeinwohlorientierte Dimension ist darüber ins Hintertreffen geraten.

Der Siegeszug der Einwilligung

Als Folge der Digitalisierung hat sich der Schwerpunkt der Datenverarbeitung von der öffentlichen Hand auf die Privatwirtschaft verlagert. Mit der Zunahme der kommerziellen Verarbeitung personenbezogener Daten begann auch der Aufstieg der informierten Einwilligung zur wichtigsten Rechtsgrundlage in diesem Bereich. Vor die Wahl gestellt zwischen dem unsicheren Geltungsbereich gesetzlicher Datenschutzregelungen und der großen Flexibilität, die das Instrument der Einwilligung bietet, haben sich viele Unternehmen für letztere Option entschieden, auch schon bevor persönliche Daten selbst zum Wirtschaftsgut avancierten.

Der Aufstieg der informierten Einwilligung spiegelt auch einen politischen Wandel im Datenschutz wider. Allgemeine Rechte und Pflichten machen einer stärker individualisierten Verantwortung für den Datenfluss Platz. Je mehr sich die Gefahren für die informationelle Selbstbestimmung in den Bereich der privaten Datenverarbeitung verlagern, so der Datenschutzexperte Alexander Roßnagel in einem Gutachten zur Modernisierung des Datenschutzes von 2001, desto stärker müssten die Individuen in die »Gewährleistung ihrer Selbstbestimmung« einbezogen werden. Generell sollte es in der »Entscheidungsautonomie« der Betroffenen liegen, welchen Datenverarbeitungen sie zustimmen.

Die Aufgabe eines solchermaßen modernisierten Datenschutzrechts wäre es dann nicht länger, detaillierte Regeln für eine sich fortwährend weiterentwickelnde Datenverarbeitung festzuschreiben, sondern stattdessen Voraussetzungen dafür zu schaffen, dass Individuen im privatwirtschaftlichen Umfeld selbstbestimmt entscheiden können. Der datenschutzrechtliche Fokus sollte sich demgemäß auf die Anforderungen konzentrieren, die eine informierte Einwilligung erst ermöglichen,

etwa klare Transparenz- und Zweckbestimmungen.

Es ist also nicht allein das Wachstum der kommerziellen Datenverarbeitung, dem wir die zunehmende Relevanz der informierten Einwilligung verdanken. Auch die Popularität staatsfernerer Regulierungsprinzipien unter Datenschutzexperten hat sie gestärkt. Marktförmige Regelungen gewinnen an Überzeugungskraft und treten an die Stelle dessen, was Spiros Simitis als das einst vorherrschende »interventionistische Regelungsmodell« bezeichnet. Indem der Gesetzgeber die Gewährleistung des Datenschutzes an die beteiligten Individuen und Unternehmen delegiert, soll das Datenschutzrecht entlastet und von seiner »Normenflut« befreit werden, so Alexander Roßnagel.

Die Vorrangstellung der Einwilligung hat sich in den 1990er Jahren zum europäischen Standard entwickelt. Nicht nur die Europäische Datenschutzrichtlinie, auch die EU-Grundrechtecharta erwähnt die Einwilligung unter den möglichen Legitimationsformen der Datenverarbeitung nun als erste und mutmaßlich wichtigste Option – noch vor gesetzlichen Lösungen.

Die Fusion von Einwilligung und informationeller Selbstbestimmung

Ihren vielleicht stärksten Ausdruck findet die rechtliche und wirtschaftliche Aufwertung der Einwilligung in der bis heute viel zitierten Formel von Alexander Roßnagel, wonach die Einwilligung »der genuine Ausdruck des Rechts auf informationelle Selbstbestimmung« sei. Die informationelle Selbstbestimmung, als Grundrecht knapp 20 Jahre zuvor vom Bundesverfassungsgericht durchgesetzt, um die Abwehrrechte der Bürger gegen den Staat und mit ihnen die demokratische Gesellschaftsordnung zu stärken, hat im Zuge ihrer Vermählung mit der informierten Einwilligung in den 1990er Jahren eine zusätzliche Bedeutung gewonnen. Im Kontext der privatwirtschaftlichen Datenverarbeitung ist sie nicht mehr primär Abwehrrecht gegen die Möglichkeiten eines staatlichen Machtmissbrauchs. Stattdessen verkörpert sie die freie Entfaltung der Persönlichkeit, indem sie den freien Willen der Individuen zum obersten Legitimationsgrund erhebt.

Zugespitzt formuliert, bildet die informationelle Selbstbestimmung im Zusammenhang mit der staatlichen Datenverarbeitung einen gesetzlichen Schutz angesichts einer offenkundigen Machtasymmetrie zwischen Bürgern und Staat; als Ausdruck der informierten Einwilligung steht sie gegenwärtig für (wirtschaftliche) Handlungsfreiheit, nämlich das Recht – und die Verantwortung –, selbst über die Verwendung der eigenen Daten zu bestimmen. Die Machtasymmetrie, die nicht nur im Verhältnis zwischen Bürger und Staat, sondern auch zwischen Individuen und Unternehmen besteht, wird von Datenschutzexperten zwar durchaus wahrgenommen, allerdings mit sektoral unterschiedlichen Schlussfolgerungen. Während im öffentlichen Bereich angesichts des Machtungleichgewichts zwischen Staat und Bürger auf Einwilligungslösungen weitgehend verzichtet wird, zielt die jüngere Datenschutzgesetzgebung für den privatwirtschaftlichen Bereich darauf, ihre Wirksamkeit zu erhöhen. Um die Entscheidungsfreiheit und Verhandlungsposition des Einzelnen zu stärken, soll etwa die Informationsbasis der Betroffenen verbessert und die Zweckbindung der Datenverarbeitung geschärft werden.

Solche Optimierungsversuche lassen die Kritik an der Einwilligungsregelung jedoch nicht verstummen. Einwilligungs-

gegner argumentieren, dass selbst eine reformierte Einwilligungslösung die Selbstbestimmung der Menschen in Zeiten von Big Data immer nur unzureichend schützen kann. Zwei ihrer Kritikpunkte erscheinen uns besonders gravierend.

Macht- und Wissensgefälle

Die wohl wichtigste Kritik an der informierten Einwilligung betrifft die Machtasymmetrie zwischen den Anbietern und Nutzern von digitalen Kommunikationsdiensten. Angesichts der schwachen Verhandlungsposition der Individuen, so argumentieren die Datenschützer Meike Kamp und Martin Rost, geraten die Anforderungen der Freiwilligkeit und Informiertheit, die das Datenschutzrecht an die Einwilligung stellt, zu bloßen Wunschvorstellungen.

Tatsächlich steht und fällt das Konzept der informierten Einwilligung mit der Freiwilligkeit der Preisgabe von Informationen. Freiwilligkeit als Maßstab beruht auf der Annahme, dass Individuen in ihrer Lebensführung unabhängig sind und sich auch gegen die Nutzung von digitalen Informationsdiensten entscheiden können, und zwar abhängig davon, welchen Wert sie dem Schutz ihrer Privatsphäre zuschreiben. In der Praxis zeigt sich allerdings, dass der Verzicht auf informationelle Dienstleistungen und soziale Netzwerke wie Facebook oder Twitter erhebliche Einschränkungen des Alltags und der gesellschaftlichen Teilhabe mit sich bringen können. Wer wird sich schon freiwillig aus dem Kreis seiner Freunde ausschließen, wenn diese vorzugsweise über Messengerdienste wie Whatsapp kommunizieren?

In der Regel unterscheiden sich die Geschäftsbedingungen der Anbieter nur wenig, aber selbst wenn es eine datenschutzfreundliche Alternative am Markt gibt, hängt ihr Nutzen immer auch von der Popularität im sozialen Umfeld ab. Auf Grund von Netzwerkeffekten entwickeln sich beliebte Dienste zu unverzichtbaren Quasi-Monopolen, deren Betreiber nahezu unbegrenzt hohe Datenforderungen stellen können. Kann man aber von einer freiwilligen Einwilligung ausgehen, wenn die gewünschte App nur im Tausch gegen die Freigabe der Kontaktliste, aller Fotos, Dokumente und Standortdaten auf dem Telefon zu bekommen ist? Mit der Integration digitaler Dienste in den Alltag verlieren die Menschen schleichend die Unabhängigkeit im Handeln, die die Einwilligungsregelung zwingend unterstellt.

Die Individuen werden zunehmend abhängiger, so dass sich ihre Entscheidungsfreiheit in eine Abfolge wiederkehrender Zielkonflikte verwandelt. Immer wieder neu sollen wir wählen zwischen der irreversiblen Preisgabe von Daten und den als nützlich oder unterhaltsam befundenen Angeboten im Netz. Unter solchen Umständen stellt sich die freie Entfaltung der Persönlichkeit eher als Bürde denn als rechtliche Errungenschaft dar.

Wie der US-amerikanische Philosoph Gordon Hull anmerkt, sind wir als Nutzer zwar beständig mit der Frage nach mehr oder weniger Datenschutz konfrontiert, aber die jeweilige Situation ermuntert uns systematisch dazu, uns für weniger Datenschutz zu entscheiden. Diese Präferenz erzeugt im Lauf der Zeit so große Gewöhnungseffekte, dass die Neigung zu weniger Datenschutz als der Normalfall erscheint. Aufsehen oder gar Misstrauen erregen dann diejenigen Menschen, die von diesem Normalfall abweichen und beispielsweise keine sozialen Netzwerke benutzen. Nicht nur die Freiwilligkeit, auch die Informiertheit der Einwilligung erweist sich als

Problem. Zweifelhaft ist, ob die Menschen zu dem Zeitpunkt, an dem sie sich für die Nutzung einer App interessieren, tatsächlich beurteilen können, welche Folgen die Einwilligung in die Speicherung und Verarbeitung ihrer Daten haben kann. Zumeist machen wir uns keine Vorstellung darüber, welche weit reichenden Informationen sich heute oder in Zukunft aus unseren Daten gewinnen lassen. Der Datenanalyst Eric Siegel illustriert dies an einem besonders abwegigen Zusammenhang.

So fand ein kanadisches Unternehmen heraus, dass der Kauf von Filzgleitern für Möbel, die den Fußboden schützen sollen, offenbar verlässliche Rückschlüsse über die Kreditwürdigkeit der Konsumenten zulässt. Der Aha-Effekt dieses Beispiels demonstriert, wie wenig wir über den Aussagewert unserer Daten wissen.

Daraus ergibt sich wiederum die Frage, ob man denn überhaupt von einer informierten Einwilligung sprechen kann, wenn wir den tatsächlichen Informationsgehalt unserer Daten nicht abschätzen können. Daten sind relational, ihr Wert erschließt sich häufig erst in der Zukunft durch die Zusammenführung mit weiteren Daten. Unser Bewertungsmaßstab ist jedoch situativ und orientiert sich üblicherweise am einzelnen Tauschgeschäft, nicht an der Summe aller Daten, die wir über uns preisgeben.

Obwohl uns also wichtige Voraussetzungen fehlen, um den täglichen Handel mit unseren persönlichen Daten angemessen bewerten zu können, nimmt uns die informierte Einwilligung ausdrücklich in die Verantwortung für etwaige Folgeschäden, die uns daraus für unser künftiges Leben entstehen mögen. Die individuelle Eigenverantwortung, stellt der Datenschutzexperte Simitis dazu fest, sei »Prolog und Bestätigung eines potenziellen Eigenverschuldens«.

Individualisierung durch Einwilligung

Die Aufwertung der informierten Einwilligung als Ausdruck des Grundrechts auf informationelle Selbstbestimmung akzentuiert die individuelle Entscheidungsfreiheit und Verantwortung im Datenschutz. In der Summe haben die Güterabwägungen jedes Einzelnen zwischen Privatsphäre und Informationsdiensten allerdings auch gesellschaftliche Auswirkungen. Aus der Perspektive eines individualistisch argumentierenden Datenschutzes bleiben diese jedoch unterbelichtet. Dass sich individuelle Datengeschäfte auch auf Dritte auswirken, die nicht eingewilligt haben, zeigt sich schon daran, dass unsere Kontaktlisten derzeit zu den häufig eingesetzten Tauschgütern für Smartphone-Apps gehören. Es sind jedoch nicht nur einzelne Dritte, sondern die Gesellschaft insgesamt, die von der Monetarisierung unserer Privatsphäre betroffen ist.

Die Verwertung von Daten als »Informationskapital« kann gesellschaftliche Kollektivgüter wie Gleichheit und Nichtdiskriminierung, Meinungsfreiheit und Anonymität in gleicher Weise bedrohen wie ein Missbrauch staatlicher Informationsmacht. Man denke nur an die Bestrebungen der Versicherungsindustrie, Tarife abhängig vom individuellen Fahrverhalten oder der körperlichen Fitness einzuführen. Solche Tarifmodelle rütteln am Solidaritätsprinzip, das Versicherungen zu Grunde liegt. Der US-amerikanische Rechtswissenschaftler Daniel Solove merkt dazu an, dass die Lebensqualität einer Gesellschaft auch von der Freiheit abhängt, die sie dem Einzelnen vor der Zudringlichkeit anderer gewährt. Eine Gesellschaft ohne Privatsphäre, so Solove, würde

die Toleranz für Verschiedenheit und Abweichung und damit auch die Grundlage für gesellschaftlichen Wandel und Innovation gefährden. Der Fokus des Datenschutzes auf die Entscheidungsfreiheit des Einzelnen unterschätzt die Gefahr kollektiver Gemeinwohlverluste, die langfristig von den vielen individuell gewährten Einwilligungen ausgeht.

Das Volkszählungsurteil, auf das sich die Befürworter der informierten Einwilligung berufen, hat die Brücke geschlagen zwischen den Entfaltungschancen, die sich aus der individuellen Kontrolle von Daten ergeben, und den Funktionsbedingungen einer demokratisch verfassten Gesellschaft – allerdings primär für die Datenverarbeitung durch staatliche Stellen wie Verwaltungs- und Sicherheitsbehörden. Im Bereich der privatwirtschaftlichen Datenverarbeitung steht dieser Brückenschlag zwischen individueller Entscheidungsfreiheit und gesellschaftlichem Gemeinwohl noch aus. Kritiker argumentieren, dass die Aufwertung der Einwilligungslösung im Datenschutz nicht nur ein Symptom, sondern auch eine Ursache dieser Verengung der Regelungsperspektive ist.

Fazit: Die zwei Gesichter der Einwilligung

Die informierte Einwilligung hat in den letzten Jahren eine Zwitterrolle eingenommen. Zum einen verkörpert sie unser Verständnis von informationeller Selbstbestimmung im Internet. Zum anderen aber legitimiert sie die Geschäftspraktiken der Datenwirtschaft, die diese Selbstbestimmung in Frage stellen: Leistung nur gegen Einwilligung. Angesichts der voranschreitenden Digitalisierung und dem Wachstum der digitalen Wirtschaft muss man sich fragen, ob die Einwilligungslösung nicht längst an die Grenzen ihrer Wirksamkeit gestoßen ist und einer neuen Ausbalancierung mit anderen Instrumenten des Datenschutzes bedarf. ⮌

(Beitrag zum 20. Berliner Kolloquium der Daimler und Benz Stiftung: »Der Datenmensch – Über Freiheit und Selbstbestimmung in der digitalen Welt«, 11. Mai 2016)