Summary: Can privacy be saved? Is the personal completely public? Existing data protection regulations in the EU that are based on informed consent and opt-in clauses are not sufficient. Individual consumers are often unable to make good choices for themselves, and even if they are informed, they often have no real alternative. Instead of putting the entire burden on the consumers, it is necessary to develop technologies that can for example avoid the de-anonymization of large datasets. Nevertheless, consumers have to learn what to write in emails, what to post in social networks and the more.

Kurz gefasst: Ist die Privatsphäre noch zu retten, oder wird das Private total öffentlich? Datenschutzregelungen der EU, die auf dem Prinzip der informierten Zustimmung und auf „opt-in"-Regeln beruhen, greifen zu kurz. Die einzelnen Verbraucher sind überfordert, und selbst wenn sie informiert sind, haben sie kaum Wahlmöglichkeiten. Anstatt die ganze Last auf die Verbraucher abzuwälzen, müssen künftig auch technische Mittel genutzt werden, um zum Beispiel zu verhindern, Datensätze zu de-anonymisieren. Trotzdem muss jeder lernen, was man in E-Mails schreiben sollte und was nicht, was man nicht in sozialen Netzwerken teilen sollte.

Der freigiebige Verbraucher In der Ära der Digitalisierung schwindet die Privatsphäre – wie auch der Datenschutz

Dorothea Kübler

Der Schlachtruf, dass das Private politisch ist, war als emanzipatorische Aufforderung zur Ausleuchtung der häuslichen Verhältnisse gedacht. Heute ist der Schutz der Privatsphäre ein Politikum geworden. Dieser Wandel ist weniger einem Backlash zu verdanken als den veränderten technischen Bedingungen. Mit Hilfe von Facebook, aber auch durch die Datenspuren im Netz, die jeder Einkauf, jede Reise, jede Krankheit hinterlässt, wird fast alles öffentlich. Nicht alle Spuren sind für alle lesbar, aber es wird für immer mehr Leute immer einfacher.

Wie verhalten sich die Menschen angesichts dieser Situation? Sind sie vorsichtig oder misstrauisch, oder vertrauen sie darauf, dass die digitalen Spuren, die sie hinterlassen, ihnen nicht schaden werden? Diese Fragen haben Ökonomen untersucht. Und es zeigt sich immer wieder, dass die Menschen großzügig sind, was die Herausgabe persönlicher Daten angeht. Sie vertrauen darauf, dass ihre Daten nicht gegen sie verwendet werden: Sie geben gegen einen Preisnachlass ihre Telefonnummer und ihre Adresse heraus oder erlauben im Tausch für den Service einer App den Zugriff auf die gesamten Daten ihres Smartphones.

„Informed choice" ist einer der Pfeiler der Datenschutz-Grundverordnung der EU von 2016. Die Vorstellung ist, dass Verbraucher ausreichend Informationen zur Verfügung haben sollen, um selbst zu entscheiden, ob sie der Nutzung ihrer persönlichen Daten zustimmen möchten oder nicht. Der avisierte Prozess von „notice and consent" (in Kenntnis setzen und zustimmen), der informierte Entscheidungen und damit den gewünschten Schutz der Privatsphäre garantieren soll, ist allerdings zum Scheitern verurteilt. Die Gründe dafür werde ich im Folgenden kurz erläutern, auch mit Hilfe unserer experimentellen Untersuchungen. Daraus ergibt sich die Frage, was die Alternativen sind, um die Privatsphäre jedes Einzelnen effektiv zu schützen – denn politisch soll das Private schon sein, aber nicht öffentlich.

Es ist allseits bekannt und bestens erforscht, dass Verbraucher weder die Datenschutzbestimmungen noch das Kleingedruckte von Verträgen lesen. Die Datenschutzregelungen von Unternehmen sind oft absichtlich allgemein gehalten, damit die Verbraucher nicht abschätzen können, welche konkreten Folgen die Freigabe der Daten für sie haben kann. Außerdem erlaubt das den Unternehmen,

die Daten in der Zukunft für Analysen zu nutzen, von denen sie beim Abschluss des Vertrags mit dem Verbraucher noch gar nichts wissen. Es gilt zwar inzwischen die Regelung des „Opt-in", also die Notwendigkeit einer ausdrücklichen Zustimmung des Verbrauchers zur Nutzung seiner Daten. Praktisch gleicht die Zustimmung aber einem Blankoscheck für die Unternehmen, weil sie meist vollkommen unspezifisch ist. Selten geben Unternehmen den Verbrauchern die Möglichkeit, der Nutzung der Daten für bestimmte Zwecke zuzustimmen, sie für andere Zwecke aber abzulehnen. Und diese Möglichkeiten der differenzierten Zustimmung werden auch nur von wenigen Verbrauchern genutzt. Die Erfordernis des „Opt-in" bedeutet also keinen effektiven Zuwachs an Verbraucherschutz im Hinblick auf die Privatsphäre.

Der enorme Wert von großen Mengen persönlicher Daten ist an mehreren Unternehmenskäufen der letzten Jahre direkt ablesbar. Ein prominentes Beispiel ist der Nachrichtendienst WhatsApp, der von Facebook für 16 Milliarden US Dollar übernommen wurde. Die Nutzer von WhatsApp erhalten für die Preisgabe ihrer Daten zwar den Service durch WhatsApp, aber keinen monetären Gegenwert. Aktivisten und Aktivistinnen haben versucht, das zu ändern, wie etwa die Organisation *commodify.us* mit dem Slogan: „They make money from your data. Why shouldn't you?" Die Forscher Omer Tene und Jules Polonetsky haben 2013 „big data for all" gefordert. Sie stellen sich vor, dass Verbraucher Zugang zu ihren Daten erhalten, und zwar in einem Format, das einfach zu nutzen ist. Auf die Weise könnten sie von ihren Daten zumindest selbst profitieren. Eine andere Form der Sensibilisierung von Verbraucher hat die Internetseite *Please Rob Me* gewählt. Sie erlaubt es ihren Nutzern, herauszufinden, was man im Internet über ihren gegenwärtigen Standort herausfinden kann, um zu demonstrieren, wie einfach es für potenzielle Einbrecher ist, sie zu schädigen. Die Internetseite *Fire Me!* zeigt ihren Nutzern, was Arbeitgeber im Internet über sie herausfinden können.

Aber keiner dieser Versuche, die Transparenz zu erhöhen und Aufmerksamkeit für die Gefahren zu wecken, hat zu signifikanten Veränderungen des Verhaltens geführt. In einem Experiment im Experimentallabor und auf der Plattform Amazon Mechanical Turk, die Crowdworking-Jobs anbietet, haben wir eine weitere Idee ausprobiert und sind am Ende zu ähnlichen Schlussfolgerungen gekommen. Die Frage, die wir untersucht haben, lautet: Verändert vollständige Transparenz darüber, welchen Wert die persönlichen Daten für das Unternehmen haben, das Verhalten der Verbraucher?

Ausgangspunkt ist die ökonomische Einsicht, dass Preise Informationen enthalten. Der Wert der Daten ist der Gegenwartswert aller zukünftigen Erträge, die mit Hilfe der Daten erreicht werden können (Verkauf der Daten, Nutzung für Gruppenprofile und Preisdiskriminierung etc.). Das bedeutet, dass der Wert, den persönliche Daten für ein Unternehmen haben, Informationen darüber enthält, ob und wofür es diese Daten in Zukunft nutzen möchte. Die Offenlegung des Werts der Daten könnte außerdem dazu führen, dass sich den Verbrauchern die Frage aufdrängt, ob der Deal eigentlich fair ist.

Um diese Fragen zu untersuchen, haben wir Teilnehmern im Experimentallabor und auf Mechanical Turk Geld angeboten für die Übermittlung ihrer persönlichen Daten an ein Unternehmen, mit dem wir für dieses Experiment kooperiert haben. Die Resultate lassen sich kurz zusammenfassen: Ob der Teilnehmer einen fairen oder nur einen minimalen Anteil am Wert der Daten erhält, beeinflusst seine Bereitschaft, persönliche Daten offenzulegen, kaum. Nur dann, wenn explizit angekündigt wurde, wie viel das Unternehmen und wie viel der Teilnehmer an den Daten verdienen, gab es Teilnehmer, die die Preisgabe ihrer Daten abgelehnt haben.

Die höchste Bereitschaft, persönliche Daten preiszugeben, zeigte sich dann, wenn das Unternehmen erklärt, dass die Daten des Teilnehmers einen hohen Wert besitzen, es aber keine Kompensation dafür anbietet und auch gar nicht erwähnt, dass so eine Kompensation möglich wäre. Die Ablehnung von unfairen Angeboten konnten wir nur im Experimentallabor beobachten. Die Teilnehmer auf der Plattform Mechanical Turk ließen sich dagegen auch mit unfairen Auf-

Dorothea Kübler ist Direktorin der Abteilung Verhalten auf Märkten. Sie forscht vor allem zu Verhaltensökonomik und experimenteller Wirtschaftsforschung, Matching-Märkten, Entscheidungsverhalten und strategischer Interaktion. *[Foto: David Ausserhofer]*

dorothea.kuebler@wzb.eu

teilungen abspeisen. Das Motiv, Geld zu verdienen, scheint bei den Studenten im Labor also etwas geringer ausgeprägt zu sein, beziehungsweise legen sie mehr Wert auf Fairness als die Teilnehmer über Mechanical Turk.

Insgesamt wird eine unfaire Aufteilung des Daten-Werts viel seltener abgelehnt als die Aufteilung einer Geldsumme in ähnlichen Experimenten zum sogenannten Ultimatumspiel, bei dem zwei Spieler sich einigen müssen, wie sie eine Geldsumme unter sich aufteilen. Die Ergebnisse suggerieren, dass die Verbraucher den Unternehmen mit ihren Daten helfen wollen. Eine abschreckende Wirkung durch die erhöhte Transparenz lässt sich nicht beobachten.

Aber was wäre, wenn jeder doch irgendwie die richtigen Entscheidungen für sich fällen würde? Wäre das Prinzip des „informed consent" zu retten, wenn viele Leute einfach sicher wären, dass sie mehr Nutzen als Kosten haben, wenn sie persönliche Daten preisgeben? Die Antwort bleibt negativ, denn die individuelle Zustimmung zum Gebrauch persönlicher Daten reicht noch nicht einmal dazu aus, die Personen zu schützen, die dem Gebrauch ihrer Daten nicht zustimmen. Zum Beispiel bedeutet die Möglichkeit, Profile für Gruppen von Verbrauchern zu bilden, dass Unternehmen viel mehr über Personen wissen, als das, was diese selbst preisgegeben haben. Die Kenntnis der Gruppenzughörigkeit in Kombination mit den Daten anderer Verbraucher ermöglicht das Erstellen sehr guter Prognosen über jede einzelne Person.

Solche externen Effekte der Bereitstellung persönlicher Informationen spielen auch eine Rolle, wenn es um die Freiwilligkeit der Zustimmung geht. Denn in Situationen, in denen jeder frei entscheiden kann, ob er oder sie persönliche Informationen offenlegt, kann die Entscheidung, keine Information preiszugeben, als ein schlechtes Signal interpretiert werden. In einer Studie untersuchen Volker Benndorf, Hans Normann und ich die Mechanismen, die die freiwillige Bereitstellung von Daten weniger freiwillig machen, als es zunächst erscheint. Autoversicherungen in einigen Ländern ermöglichen es ihren Kunden, niedrigere Beiträge zu bezahlen, wenn sie ihr Fahrverhalten mit GPS-Trackern aufzeichnen lassen. Krankenversicherungen verteilen Boni dafür, wenn ihre Mitglieder Fitness-Tracker nutzen und ihre Daten dann zur Verfügung stehen. Weitere Beispiele sind die freiwillige Bereitstellung eines polizeilichen Führungszeugnisses oder eines Gesundheitszeugnisses bei Bewerbungen.

Es geht hier um Situationen, in denen Menschen freiwillig persönliche Daten bereitstellen und wissen, wie diese Informationen genutzt werden. In gewisser Weise ist das ein Paradebeispiel für „informed consent", also für freiwilliges und informiertes Handeln. Wo also liegt das Problem? Diejenigen, die vorsichtig Auto fahren, die einen gesunden Lebenswandel haben, deren Führungszeugnis keine Einträge aufweist, sind gerne bereit, das offenzulegen. Auf diejenigen, die keine Information offenbaren, wirft das aber ein schlechtes Licht. Deswegen werden mittelmäßig Gesunde sich dann auch überlegen, ein Gesundheitszeugnis vorzulegen, um sich von den weniger Gesunden abzugrenzen. Das wiederum verstärkt den Druck auf die weniger Gesunden. Die Kettenreaktion kann dazu führen, dass alle ihre persönlichen Daten freiwillig preisgeben.

In Laborexperimenten lässt sich diese Kettenreaktion nachweisen. Das Phänomen tritt selbst dann auf, wenn die Menschen nicht beobachten können, was andere tun, sondern vorhersehen müssen, wer freiwillig Persönliches preisgibt und wer nicht.

Richard Posner, einer der Doyens von Law and Economics, Richter und Professor in Chicago, hat so argumentiert: Weil freiwillige Offenlegung mehr freiwillige Offenlegung nach sich zieht, müsse Datenschutz scheitern und sei daher unnütz. Ihm ist insoweit zuzustimmen, dass die Politik des „informed consent" in solchen Situationen nicht ausreicht. Es bedarf anderer Politikinstrumente. Eine Möglichkeit besteht darin, die Nutzung bestimmter Informationen von vorneherein ganz zu verbieten. Das gilt für genetische Daten, die nicht von Versicherungen und Arbeitgebern verwendet werden dürfen. Die Genetic Information Nondiscrimination Act (GINA), die 2008 in den USA erlassen wurde (ein ähnliches Gesetz gilt in der Europäischen Union), hat der damalige Senator

Ted Kennedy als „first major new civil rights bill of the new century“ bezeichnet.

Schließlich sind die Wahlmöglichkeiten, was die Freigabe persönlicher Daten angeht, auch aus einem weiteren Grund häufig begrenzt. Im Forschungssemester in Stanford, mitten im Silicon Valley, konnte ich das am eigenen Leib erfahren. Der tägliche Schulstoff bereits eines Sechstklässlers steht im Netz, die Hausaufgaben werden hochgeladen, die Abwesenheiten und sämtliche Schulnoten lassen sich von allen Familienmitgliedern bequem einsehen, das Fußballteam wird per App zusammengerufen, ohne Uber (das den Zugriff auf sämtliche Daten des Smartphones verlangt) kommt man nicht zum Flughafen. Ob mit oder ohne Vertrauen in die Datensammler – es gilt „friss‘ oder stirb‘“. Informieren kann man sich schon, aber echte Alternativen zur Zustimmung gibt es keine.

Wie ist der Schutz der Privatsphäre noch denkbar? Es gibt inzwischen viele, die argumentieren, dass Datenschutz nur noch zentral und mit Hilfe von Mathematik und Informatik zu leisten ist. Daten fallen an und werden aufgezeichnet und gesammelt, überall, ob wir wollen oder nicht. Die entscheidende Frage ist, was mit diesen Daten geschieht. Kurz gesagt: Die Idee ist, dass Computerprogramme und Datenbankarchitekturen die Nutzung der Daten so begrenzen und kontrollieren, dass die Privatsphäre geschützt wird. „Differential privacy“ heißt eines der Schlagworte. Das Forschungsgebiet befasst sich damit, wie sich Datenbanken so anlegen lassen, dass es nicht möglich ist, Personen zu identifizieren, aber die Daten gleichzeitig dafür zu nutzen, statistisch valide Aussagen zu machen. Es gilt dabei, durch kluges Design der Datenbanken die De-Anonymisierung von anonymisierten Daten auszuschließen. Computerprogramme können außerdem dabei helfen, sicherzustellen, dass die Verarbeitung persönlicher Daten unter Einhaltung von Regeln und Gesetzen geschieht. In anderen Fällen können sie helfen, den Missbrauch von Daten aufzudecken und die Verantwortlichen zu identifizieren. Bisher ist nicht viel davon reif für die Implementierung. Die Entwicklung von Systemen, die den Menschen die Kontrolle über ihre Daten geben und sicherstellen, dass die Daten verantwortungsvoll genutzt werden, ist eine Herausforderung für die Wissenschaft, aber auch für die Gesellschaft, die die Spielregeln und Rahmenbedingungen formulieren muss. Davon unbenommen werden wir neue Regeln der E-Mail-Etikette entwickeln müssen, denn Datenleaks wird es auch in Zukunft geben. Und wir werden lernen, welche persönlichen Daten wir in sozialen Netzwerken preisgeben wollen. Aber die Last kann nicht allein auf dem Verbraucher liegen.

Literatur

Benndorf, Volker/Kübler, Dorothea/Normann, Hans-Theo: „Privacy Concerns, Voluntary Disclosure of Information, and Unraveling. An Experiment“. In: European Economic Review, 2015, Vol. 75, April, pp. 43–59.

Tene, Omer/Polonetsky, Jules (2013): „Big Data for All: Privacy and User Control in the Age of Analytics“. In: Northwestern Journal of Technology and Intellectual Property, Vol. 11, No. 5, pp. 239–273.