Humanistische Union

Privacy by Design – Chancen eines programmierten Grundrechts

in: vorgänge Nr. 221/222 (1-2/2018), S. 65-78

Mit dem Konzept einer Privacy by Design verbinden manche Datenschützer die Hoffnung, Datenschutz ließe sich auch jenseits nachlässiger Nutzer realisieren. Aber lässt sich das Grundrecht auf Informationelle Selbstbestimmung rein technisch, durch Privacy by Design gewährleisten? Um diese Frage zu beantworten, geht Clemens Cap im folgenden Beitrag zunächst auf den Stellenwert der Privatheit ein: Brauchen wir Privatheit noch – oder kann das weg? Anschließend klärt er einige Begrifflichkeiten zum technischen Datenschutz und gibt eine (vorläufige) Prognose: Da das Problem weniger bei der Technik, sondern bei den Menschen zu suchen sei, kann auch nur dort eine Lösung gefunden werden.

1 Was heißt und zu welchem Ende brauchen wir Privatheit?

Privatheit ist ein alter menschlicher Wert. Bereits die Antike erkannte seine Bedeutung und formulierte im hippokratischen Eid die ärztliche Schweigepflicht. Veränderungen in der Informationstechnologie führten dann regelmäßig zu einem Nachjustieren des gesellschaftlichen und juristischen Konzepts: So definierten Warren und Brandeis[1] 1890 Privatheit als right to be left alone und das deutsche Bundesverfassungsgericht leitete 1983 im sogenannten Volkszählungsurteil[2] das Grundrecht auf informationelle Selbstbestimmung direkt aus der Menschenwürde und dem ersten Artikel des Grundgesetzes ab. Seine Forderung: Die Bürger müssen wissen können, wer was wann und bei welcher Gelegenheit über sie weiß, denn wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Diese Sorge würde die Selbstbestimmung und individuelle Entfaltung des Einzelnen und damit die Handlungsfähigkeit einer freiheitlichen, demokratischen Gesellschaft beschädigen.

Aus heutiger Sicht sind das damalige Urteil und seine Definition von Privatheit von bemerkenswerter Aktualität. Die Weiterentwicklung der Technologie, insbesondere die allgegenwärtige Präsenz des Internet und die mit ihm verbundenen Geschäftsmodelle und Überwachungsmöglichkeiten haben die Privatsphäre massiv beschädigt. Wesentliche Schuld an dieser Entwicklung trifft die Nutzer, da sie vielen Verletzungen ihrer Privatsphäre aus Unkenntnis, aus Bequemlichkeit, im Interesse angeblich erhöhter Sicherheit oder für kurzfristige ökonomische Vorteile zustimmen.

Die Preisgabe von Daten kann im heutigen Internet rasch teuer kommen. So verraten die meisten Internetbrowser, welche Webseiten ein Anwender besucht hat und welche Hardware er beim Surfen benutzt. Beim sogenannten Cookie-Pricing[3] macht ein Server die Preise angebotener Produkte von diesen Informationen abhängig. Nach einer amerikanischen Studie[4] zahlen Nutzer von Apple-Produkten (einer hochpreisigen Marke) bei Hotelbuchungen 30% mehr als andere Anwender. Selbstfahrende Staubsauger orientieren sich über Kameras und entwickeln dadurch neben einer Hinderniskarte auch eine gute Vorstellung über die Größe der Wohnung, die Anzahl der Möbelstücke und die Lebensqualität der Bewohner. Manche Systeme übertragen diese Informationen an den Hersteller, der daraus detaillierte Profile erstellt, um die Daten selber zu verwenden oder weiterzuverkaufen.[5] Bei Sicherheitslücken im System erfahren Kriminelle, wann niemand zu Hause ist und ob sich ein Einbruch angesichts der

Wohnungsausstattung der Opfer rentiert.

In sogenannten pay-as-you-drive-Tarifen[6] überwacht ein Sensor das Verhalten von Autofahrern. Neben nutzungsabhängigen Tarifen erlaubt das Gerät auch eine allgemeine Einschätzung des Risikoverhaltens seiner Nutzer. Aus Sicht der Versicherungswirtschaft gilt das als Vorteil, da die Datenbestände genutzt werden, um das asymmetrische Informationsverhältnis zwischen Versicherer und Versicherten zu reduzieren.[7] Bei anderen Versicherungsprodukten wird die Problematik noch deutlicher: Fitness-Tracker und Smart Watches beobachten die Sportaktivitäten und den Herzrhythmus ihrer Träger. Die Daten sind für Krankenversicherungen interessant, die Sammelgeräte werden von ihnen daher bezuschusst.[8] Je nach Lebenssituation kann sich daraus ein besonders günstiger oder teurer Tarif ergeben, eine Ablehnung bei der Abdeckung bestimmter Risiken oder eine Karriereentscheidung durch den Arbeitgeber. Sicherlich erzeugen diese Geräte vielschichtige Motivationslagen für den Nutzer, die sowohl für das Wohlbefinden des Einzelnen als auch für die Gesundheitskosten der Gesellschaft von Vorteil sein können.[9] Trotz der Beliebtheit und der finanziellen Förderung der Geräte zur Selbstvermessung bleiben die Effekte auf das individuelle Verhalten Studien[10] zufolge überschaubar. Übernehmen Versicherungen weiterhin die Rolle einer Solidargemeinschaft zum Ausgleich von Risiken und Schicksalsschlägen, wenn Datenbestände eine präzise Vorhersage der Schadenserwartung erlauben? Sobald konkrete Verhaltensweisen ökonomisch abgerechnet werden, tangiert das die Handlungs- und Entscheidungsfreiheit des Einzelnen viel stärker als bei einer simplen Volkszählung.

Die Nutzer erlauben die Weitergabe aller dieser Daten typischerweise durch den berühmten "OK-Klick" unter seitenlange, komplexe juristische Texte, die sie weder verstehen noch lesen.[11] Jeder gesetzliche Schutz wird aber ausgehebelt, wenn die Bürger ihre Rechte freiwillig preisgeben.

Die Nachteile einer Datenweitergabe werden gelegentlich erst über erstaunliche Umwege bemerkbar: Viele Benutzer von Fitness-Trackern laden ihre Sportdaten (teilweise unbewusst) in öffentliche Lauf-Foren hoch. Eine kürzlich veröffentlichte Studie zeigte, dass sich daraus die Positionen und die Belegungszahlen militärischer Einrichtungen ermitteln lassen.[12] Aber auch persönliche Nachteile sind denkbar. Bei einer Einreise in die USA werden die Benutzernamen für soziale Netze wie Facebook oder Twitter abgefragt. Damit können die Beamten die öffentlichen Beiträge den einreisenden Personen zuordnen. Medienberichten zufolge wird darüber nachgedacht, Reisende auch nach den Passwörtern für diese Dienste zu fragen – dann wäre auch ein Zugriff auf persönliche Nachrichten möglich.[13] Eine unbedachte Äußerung auf Facebook, von einem Beamten im falschen Kontext interpretiert, kann Probleme bei der Einreise machen.[14]

Häufig hört man in Datenschutz-Debatten den Satz 'Ich habe doch nichts zu verbergen.' Theoretisch und in einem ideal funktionierenden Staat können leichtgläubige Bürger hoffen, dass gesetzestreues Verhalten vor Strafverfolgung schützt. Diese Ansicht offenbart jedoch ein ungeheures Maß historischer Naivität und vollständige Unkenntnis über das Funktionieren der Wirtschaft im Zeitalter der Digitalisierung. Der Konkurrenzkampf fordert von heutigen Unternehmen, dass sie jede Information über Kunden zur Gewinnmaximierung nutzen – die Weitergabe von Daten wird daher nicht im Interesse der Kunden sein. Das staatliche Rechtssystem ist nicht vor Fehlinterpretationen und Justizirrtümern gefeit. Interpretationsrahmen ändern sich und mit ihnen auch die möglichen Vor- und Nachteile von Daten.[15]
Diskriminierung wird nicht erst zur Gefahr, wenn sie real wird: Bereits die Beobachtung durch Dritte lässt Menschen ihr Verhalten verändern und an die mutmaßlichen Normen der Beobachter anpassen. Einschüchterung und "chilling effects", also die berühmte "Schere im Kopf", wirken bereits bei der Datenerfassung, aber auch schon durch die grundsätzliche Möglichkeit einer Beobachtung und Erfassung unseres Verhaltens. "Wir fühlen uns frei, aber wir sind es nicht", meint Byung-Chul Han[16] und ergänzt: "Vertrauen macht Beziehungen zu anderen Menschen auch ohne genauere Kenntnisse über diese möglich. Die digitale Vernetzung erleichtert die Informationsbeschaffung dermaßen, dass Vertrauen als soziale Praxis immer unbedeutender wird."

Bis vor kurzem standen nur jene Daten im Brennpunkt der Diskussion, die sich unmittelbar auf identifizierbare Personen bezogen. Mit der Nutzung automatisierter Entscheidungen tauchen weitere Probleme auf, hier sei nur auf die mögliche Diskriminierung durch Algorithmen und den Zwang des

Normativen verwiesen.

In vielen Situationen dürfen[17] Menschen gegen Mitmenschen nicht aufgrund von Merkmalen wie Herkunft oder religiöse Orientierung diskriminieren. Nun gibt es Fälle, in denen Algorithmen genau dies tun und beispielsweise Schwarze bei Entscheidungen über strafrechtliche Rückfälle anders beurteilen als Weiße.[18] Handelt es sich hier um eine echte Benachteiligung, die ein Algorithmus etwa durch Beobachtung von Menschen gelernt hat? Wie ist damit umzugehen, wenn sich aus Datenbeständen tatsächlich für Menschen einer bestimmten Hautfarbe eine erhöhte Rückfallquote ergibt? Was macht unterschiedliche Behandlung aufgrund "objektiver" Eingangsdaten zur gesellschaftlich unerwünschten Diskriminierung? Will man die entsprechenden Algorithmen verbieten oder rechnet man die Ungleichbehandlung gegen "besseres", weil statistisch belegbares Wissen heraus?

Die statistische Analyse von Daten erzeugt eine fiktive Normalität: Die ermittelten Durchschnittswerte besagen, was als "okay" gilt. Durch die Bewertung üben sie einen Zwang auf das Individuum aus und verändern sein Verhalten. Das Wissen um angeblich mögliche Selbstoptimierung – nach welchen fremden Maßstäben und Wertvorstellungen auch immer – löst das Schicksalhafte der menschlichen Existenz auf zugunsten einer Illusion der Erreichbarkeit aller Ziele. Die – sinnvolle – Verantwortlichkeit für das eigene Dasein weicht dem Gefühl einer Schuld und erzeugt einen dauernden Druck zur Optimierung. Gesamtgesellschaftliches Resultat ist eine Müdigkeitsgesellschaft (Byung-Chul Han[19]), die in permanenter Selbstüberforderung gefangen ist und sich immer mehr einer Beschleunigung und Entfremdung (Hartmut Rosa[20]) ausliefert. Heute bietet es sich an, die Definition von Privatheit als "right to be left alone" zu erweitern zu einem "right to be different".[21]

2 Was ist und was leistet Privacy by Design?

Privacy by Design ist[22] der Entwurf eines (Informatik-)Systems auf eine solche Art, dass Fragen der Privatheit und des Schutzes personenbezogener und personenbeziehbarer Daten in allen Phasen der Verarbeitung umfassend beachtet werden.

In allen Phasen der Verarbeitung bedeutet beispielsweise, dass auch archivierte Daten einbezogen werden und nicht mehr benötigte Daten wirksam[23] zu löschen sind. Nachnutzungen gewonnener Daten in anderen Systemen, Kontexten oder Jurisdiktionen sind zu beachten, soweit sie nicht ohnehin verboten sind. Fragen des Datenschutzes müssen bereits ganz zu Beginn berücksichtigt werden, wenn der Ablauf eines Vorgangs beschrieben und seine technische Umsetzung geplant wird, sie dürfen nicht erst im Nachhinein oder gar als Reaktion auf einen Datenunfall umgesetzt werden.

Privacy by Default bedeutet: Wenn an bestimmten Stellen im System Nutzer den Schutz ihrer Privatsphäre aufgeben können, so ist bei den Voreinstellungen darauf zu achten, dass von einer Ablehnung der Zustimmung ausgegangen wird. Die Aufgabe der Privatheit darf den Nutzern nicht durch Vertrauen auf Bequemlichkeit oder Unwissenheit abgerungen werden, sondern muss als dokumentierter, informierter, aktiver Vorgang von den Anwendern bestätigt werden (Opt-In statt Opt-Out).

Die genutzten Prinzipien des Datenschutzes sollen dokumentiert werden, die Beschreibung wird in verständlicher Form den Endanwendern zugänglich gemacht. Die Überprüfung der Umsetzung durch eine unabhängige Stelle ist wesentlich. Natürlich sind weitere Konzepte des Datenschutzes zu beachten: Grundsätzlich sollen so wenig Daten wie nötig anfallen (Datenminimierung); es sollen nur jene Daten erhoben und verarbeitet werden, die für den entsprechenden Zweck unbedingt erforderlich sind, keine weiteren Daten (Datenvermeidung); die benötigten Daten sollen nur so lange gespeichert werden, wie es für den entsprechenden Zweck erforderlich ist (Datensparsamkeit); und sie dürfen nur für einen bestimmten,

bereits vor der Erhebung dokumentierten Zweck benutzt werden (Zweckbindung).

Zwei Beispiele sollen die Anwendung von Privacy by Design illustrieren:

Welche Informationen erhalten Sachbearbeiter, die über einen Antrag nach Hartz 4 befinden? Dürfen sie wissen, welche Fahrzeuge auf die Antragsteller zugelassen sind? Mit welchen Personen sie zusammenleben? Die Gesetzgebung bejaht beide Fragen und kennt den Begriff der Bedarfsgemeinschaft, in dessen Rahmen die Finanzkraft der Mitbewohner geprüft wird. Dürfen die Sachbearbeiter auf die Ortungsinformation von Mobiltelefonen zugreifen oder die in einem Lauf-Forum hochgeladenen Daten eines Fitness-Trackers mit GPS-Funktion nutzen, um aus dem regelmäßigen nächtlichen Aufenthalt von Antragstellern bei wohlhabenden Personen oder aus gemeinschaftlichem Freizeitverhalten Bedarfsgemeinschaften zu behaupten? Mit Privacy by Design könnte dieses Problem so gelöst werden: Die Beschreibung des Entscheidungsvorgangs muss (abschließend) alle Daten anführen, die in die Bewertung einfließen dürfen. Die technische Umsetzung darf in der spezifischen Beratungs-Situation dem Sachbearbeiter nur diese Daten vorlegen. Die Prozessbeschreibung soll die Einhaltung nachvollziehbar und überwachbar gestalten.

Ein weiteres Beispiel sind Hochleistungskopierer: Dabei handelt es sich meist um kleine Computer mit Scanner-Einheit und Drucker. Eingelesene Dokumente werden auf einem internen Speicher abgelegt. Verkauft ein Unternehmen später diesen Kopierer, so finden sich alle in der Vergangenheit kopierten Dokumente auf diesem Speicher und können vom neuen Inhaber ausgelesen werden. Privacy by Design müsste sich hier um ein dauerhaftes Löschen der Dokumente Gedanken machen, das in sinnvollem Verhältnis zur Protokollierung und Abrechnung der Kopierer-Nutzung steht.[24]

Privacy by Design ist in seiner Wirkung aber insofern eingeschränkt, da es sich (nur) um die Personenbezogenheit oder Personenbeziehbarkeit von Daten kümmert. Viele andere Schwierigkeiten umfassender Datenspeicherung und -auswertung, etwa die Diskriminierung oder ein normativer Druck, bleiben bestehen.

Datenschutz kann zudem auch unerwünschte Nebeneffekte verursachen. Naturgemäß sind in einer völlig transparenten Gesellschaft, die alle Vorgänge speichert, viele Dinge leichter kontrollierbar und die Menschen besser zu überwachen. Ob man diese Tatsache als Vorteil oder Nachteil empfindet, hängt von der eigenen Rolle in der Gesellschaft ab und ist eine Frage des persönlichen politischen Standpunkts sowie der Präferenzen für offene oder totalitäre Gesellschaftsformen.

Auf einer abstrakten Ebene scheint die Entscheidung für oder gegen Datenschutz einfach zu sein, am konkreten Beispiel zeigen sich die Schwierigkeiten: 2013 hatte ein Autobahnschütze über 700 Mal auf andere Lastwagen geschossen, bevor er durch eine eigens für diesen Tatbestand eingerichtete Kennzeichenerfassung verhaftet werden konnte. Die erforderlichen Bewegungsdaten wären bereits beim Mautbetreiber Toll Collect vorrätig gewesen, konnten aber aus Datenschutzgründen nicht genutzt werden.[25] Solche Beispiele führen immer wieder zu dem Vorwurf, dass Datenschutz eigentlich Täterschutz sei. Überwachung scheint zur Überführung von Tätern sinnvoll und kann als Präventionsmaßnahme das Sicherheitsgefühl der Bürger verbessern. Wie wirksam großflächige Datenerfassungen jedoch sind, ist aber stark umstritten.[26] Zudem kann ein abgestufter Datenschutz helfen: Dieser könnte bei Video- und Handyüberwachung aus einer strikten Zweckbindung bestehen, aus einem Richtervorbehalt vor der Datennutzung, aus engen Löschfristen, sowie aus Maßnahmen zur Verringerung des Missbrauchsrisikos, indem bspw. nur mehrere Personen die Daten einsehen können (technische Vorkehrungen) und dürfen (juristische Vorkehrungen).

Aber auch gegen derart abgesicherte Überwachungsmaßnahmen gibt es theoretische und praktische Einwände: Theoretische, weil eine solche Regelung einen demokratiepolitisch problematischen Generalverdacht gegen alle Bürger festschreibt; und praktische, weil der tatsächliche Umgang der Behörden mit bestehenden Einschränkungen von Überwachungsmaßnahmen wenig vertrauenserweckend ist. Das wurde zuletzt durch einen Sachstandsbericht über Abhörmaßnahmen des BND in Bad Aibling deutlich, aber auch ein älterer Bericht des Bundesbeauftragten für den Datenschutz zur Quellen-

Telekommunikationsüberwachung durch das BKA, der beim Chaos Computer Club als Leak[27] verfügbar ist, offenbart den hemmungslosen Eingriff in die Intimsphäre der Betroffenen. So zitiert der Bericht aus den Akten zu einem überwachten Skype Telefonat des Verdächtigen mit seiner Freundin: "Danach Sexgespräch. (Anm. Übers. Ab 15:52:20 bis 16:01:00 finden offensichtlich Selbstbefriedigungshandlungen statt)". Obwohl hier der gesetzlich geschützte Kernbereich privater Lebensgestaltung betroffen ist, wurden persönlichste Details rechtswidrig protokolliert. Die Tondateien zu diesen Gesprächen lägen ebenso noch vor und wären deshalb nicht wie vorgesehen gelöscht worden, weil "eine Teillöschung technisch nicht möglich gewesen sei" [sic].

Ein weiteres Problem entsteht durch jene Anwendungen, die auf einer umfassenden Datenspeicherung und -auswertung beruhen, beispielsweise im medizinischen Bereich. Gesundheitsdaten können in der Hand von Arbeitgebern, Krankenversicherungen oder Banken zu Entscheidungen führen, die nicht im Interesse der Betroffenen sind. Andererseits sind wir an medizinischem Fortschritt interessiert und wollen die Vorteile individualisierte ärztlicher Behandlung nutzen. Als datenschutzfreundlicher Ansatz bietet sich Anonymisierung von Gesundheitsdaten an, doch ist diese nicht so effektiv und zuverlässig, wie man sich das erhofft hat.[28]

Fazit: Privacy by Design ist ein wichtiges Entwurfsprinzip, das auf datenschutzfreundliche Informationsverarbeitung abzielt. In seiner praktischen Anwendung zeigen sich jedoch viele grundsätzliche Probleme.

3 Menschen zwischen Regulierung und Programmierung

In diesem Abschnitt untersuche ich den Menschen und sein Verhalten im Spannungsfeld zwischen einer de jure Position (Regulierung) sowie einer de facto Position (Programmierung). Die Analyse soll eine Antwort auf die Frage nach der Chance vertrauenswürdiger, datensparsamer Systeme und Dienste ermöglichen.

Regulierung: Die de-jure-Situation

Datenschutz wird unterschiedlich bewertet. Versucht man die einzelnen Positionen etwas zu sortieren, so kann man drei Doktrinen ausmachen:

> *1. Grundrecht: Datenschutz, Privatheit und informationelle Selbstbestimmung begründen ein Abwehrrecht des Einzelnen gegen Staat, Gesellschaft und Wirtschaft zur Wahrung seiner Menschenwürde. Als Grundrecht besteht es absolut, es ist konstitutiv für den Menschen als Person und Individuum, alle Eingriffe müssen vom Gesetzgeber besonders gerechtfertigt oder von Betroffenen genehmigt werden. Daten sind die virtuellen Entsprechungen menschlicher Wesen und sind als solche besonders zu schützen. Diese Position findet sich (derzeit noch) in Deutschland und einigen europäischen Staaten.*

> *2. Wirtschaftsgut: Daten und Aufmerksamkeit für Daten sind ein immaterielles Wirtschaftsgut mit hohem monetarisierbarem Wert. Es kann gehandelt und getauscht werden, etwa Verhaltensdaten auf Webseiten gegen Suchdienste und Speicherplatz auf Portalen, Fitnessdaten gegen Tarifreduktion oder Aufmerksamkeit auf Produktplatzierungen gegen Nachrichten. Es bestehen Besitz-, Eigentums- und Nutzungsrechte. Regulierung zielt auf die Sicherung dieser*

Rechte ab, auf die Vereinfachung des Austausches und den Abbau von Handelsschranken. Menschen und ihre Daten sind Objekte des Wirtschaftskreislaufs. Diese Position findet sich in den USA und Asien, sowie bei internationalen Handelsorganisationen; von dort dringt sie nach Europa.

3. Archaische Fiktion: Nach dieser Position ist Privatheit veraltet und in der heutigen digitalen Gesellschaft nicht mehr vorhanden. Wir sollten uns damit abfinden, da wir in einer Post Privacy Gesellschaft leben. Glaubt man dieser Position, bewegen wir uns hin zu einer radikalen Transparenz- und Abrechnungsgesellschaft, in der alles über jeden bekannt ist. In dieser werden die gesellschaftlichen Entscheidungen von uninformierten Massen, einem Smart Mob oder sogar von Algorithmen automatisiert getroffen. Angesichts der Brisanz dieser Zero-Privacy Doktrin[29] kann man leidenschaftliche Proteste[30] dagegen gut nachvollziehen. Diese Position findet sich in Dystopien, aber auch bei Unternehmen der Informations- und Kommunikationstechnologie sowie bei Sicherheitsfirmen und ihnen nahestehenden Lobbys.

Das Spannungsfeld zwischen der Position Grundrecht und der Position Wirtschaftsgut ist insofern von Bedeutung, als sich hier die Frage klärt, wem welche Rechte an Daten zukommen:[31] den Personen, von denen die Daten stammen und auf welche sich die Daten beziehen; oder den Unternehmen, welche diese Daten ermitteln, nutzen und mit ihnen handeln. Für beide Positionen können Gründe gefunden werden – jedoch mit gänzlich unterschiedlichen Auswirkungen auf die Würde des Menschen und seine Stellung in der digitalen Wirtschaft.

Rechtlich wird die Speicherung und Nutzung personenbezogener Daten meist als Verbot mit Erlaubnisvorbehalt konstruiert. Dies besagt: Grundsätzlich dürfen personenbezogene Daten nicht gespeichert oder verwendet werden. Wie stringent dieses Verbot umgesetzt wird, ist von Land zu Land sehr verschieden. Noch wichtiger ist aber die Erlaubnis: Geben Betroffene Einblick in ihre Daten oder gestatten sie gar in aktiver Mitwirkung die Nutzung, so enden die Schutzmöglichkeiten dieses Rechtsansatzes. Die Freiheit einer offenen Gesellschaft erlaubt ihren Mitgliedern die Entscheidung zu selbstschädigendem Verhalten. Hat diese Selbstbeschädigung einen ökonomischen Vorteil für Dritte und verfügen diese über eine finanzstarke Lobby, dann wird die öffentliche Kommunikation über das Thema schwierig. Die Debatten über Tabak-Konsum und Tabak-Werbung sind bekannt und verlaufen entlang ähnlicher Linien wie die Warnungen vor einer datenschutztechnischen Selbstbeschädigung bei der Nutzung von Diensten wie Google oder Facebook.[32]

Rechtliche Probleme im Datenschutz bestehen viele: Zu den wichtigsten zählen uneinheitliche Standards in den Ländern, die zum Forum-Shopping einladen (d.h. Anbieter wählen das Recht jenes Landes, das ihnen die meiste Handlungsfreiheit bietet) oder wirkungslose Sanktionen, die für den Täter ökonomisch wenig schmerzhaft sind. Ob dies innerhalb der EU durch die neue Datenschutz-Grundverordnung besser wird, muss sich zeigen; im internationalen Umfeld bestehen diese Probleme fort.

Programmierung: Die de-facto-Situation

Programmierung ist ein faktisches Normativ. Code is law. Der technische Aufbau eines informationsverarbeitenden Systems erzeugt eine Datenschutz-Realität, die wirksam wird und unabhängig von den rechtlichen Rahmenbedingungen und den Präferenzen der Anwender von diesen hinzunehmen ist. Ich will hier exemplarisch drei Aspekte herausarbeiten:
Die Anwender wollen ihre Daten nicht schützen. Der Zugang zu wichtigen Kommunikationsdiensten, etwa

der Google-Suche, dem sozialen Netzwerk Facebook oder den vielen Diensten auf Smart Phones, wird erst freigegeben, wenn die Benutzer der weitgehenden Nutzung ihrer privaten Daten zugestimmt haben. Der Konstruktionsfehler ist, dass es zwar für die Grundversorgung mit unerlässlichen Diensten wie Wasser- und Stromversorgung Kontrahierungspflichten gibt, Verträge über digitale Dienste aber der Privatautonomie unterliegen. Aus der Sicht der Anbieter beruht die Finanzierung ihrer Dienste auf der Vermarktung der Nutzerdaten. Darauf lassen sich die Anwender "freiwillig" ein.

Problematisch ist dabei die Asymmetrie des Preises: Würden die Dienstleistungen in Euro oder Dollar bezahlt, könnten die Nutzer eine Vorstellung vom Wert ihrer Daten ableiten. Bei den „kostenlosen“ Angeboten können sie jedoch den "Wert" ihrer Gesundheits- und Verhaltensdaten– im Gegensatz zu den Dienst-Providern – nicht einschätzen.

Den Anwendern wird es praktisch verwehrt, ihre Daten zu schützen. Für Emails gibt es etwa relativ zuverlässige Verschlüsselungssysteme.[33] Sie werden von den Massenanbietern jedoch nicht eingesetzt, da diese die Mails ihrer Nutzer auswerten wollen.[34] Die verfügbaren Systeme erfordern vom Benutzer einen hohen Aufwand, sind schwer zu bedienen und verlangen für die tatsächliche Gewährleistung von Sicherheit fortgeschrittene technische Fertigkeiten.[35] Darüber hinaus gibt es Systeme, die zwar kraft Gesetz als sicher gelten, den Herstellern aber eine technisch unsichere Umsetzung erlauben. Das deutsche De-Mail-System etwa fordert nur eine Transport-Verschlüsselung (für die Übertragung zwischen den Providern), aber keine Ende-zu-Ende Verschlüsselung (vom Absender bis zum Empfänger). Damit können die Betreiber des Dienstes weiterhin auf die Inhalte der Mails zugreifen.[36]

Die Anwender können ihre Daten nicht schützen, wenn informationstechnische Systeme so (fehl-)konstruiert wurden, dass Dritte unerkannt auf ihre Datenbestände zugreifen können. Der amerikanische Geheimdienst NSA hat beispielsweise dafür gesorgt, dass die Normierungsbehörde NIST einen kryptografischen Algorithmus standardisierte, in den die NSA zuvor eine Hintertüre eingebaut hatte.[37] Der Forschung sind viele systematische Fehler in der Sicherheitsarchitektur der Mobilfunksysteme GSM, LTE sowie im Signalisierungssystem 7 bekannt.[38] Dabei handelt es sich nicht um theoretische Spitzfindigkeiten, sondern um Lücken, die von Kriminellen unter anderem bereits genutzt wurden, um sich Zugriff auf fremde Bankkonten zu verschaffen und diese abzuräumen.[39]

Bequemlichkeit und menschliches Verhalten – Plädoyer für die Digitale Aufklärung 2.0

Das schwächste Glied in der Kette zwischen Recht und System sind die Menschen mit ihren Verhaltensweisen. Aus Bequemlichkeit und Unkenntnis nehmen sie ihnen zustehende Rechte nicht wahr und verzichten auf ihre Möglichkeiten als Konsumenten und Stimmbürger. Die Wahlmöglichkeiten sind bereits eingeschränkt: Wir können aus hunderten Modellen von Mobiltelefonen und Computern nach Bildschirmgrößen, Farbe und Formen wählen, wir können Profile auf Facebook, Twitter, Instagram etc. gestalten. Die Freiheit, diese Systeme in datenschutzfreundlicher Weise zu nutzen, ist jedoch sehr eingeschränkt. Die Gestaltung des digitalen Lebensraums ist Informatikern unter Einsatz von sehr viel Zeit möglich, wird aber durch Unternehmen und Politik erschwert. Die digitale Gesellschaft entwickelt sich in Richtung eines Feudalismus 2.0. Es mehren sich daher die Stimmen, die nach einer Aufklärung 2.0 rufen. Mit Kant wollen wir fordern:[40]

Digitale Aufklärung ist der Ausgang des Menschen aus seiner selbst verschuldeten Unmündigkeit. Unmündigkeit ist das Unvermögen, sich seiner Daten und digitalen Endgeräte ohne Leitung, Bevormundung und Überwachung eines anderen zu bedienen. Selbstverschuldet ist diese Unmündigkeit, wenn die Ursache derselben nicht am Mangel technischer Möglichkeiten sondern der Entschließung und des Mutes liegt, sich seiner ohne Leitung, Bevormundung und Überwachung eines anderen zu bedienen.

Der Leitspruch einer digitalen Aufklärung könnte lauten:
Habe Mut, die eigene Hoheit über Deine Daten zurück zu gewinnen!

4 Ein Ausblick

Die Debatte über Privatheit ist nur ein Symptom der Krise unserer Gesellschaftsordnung. Die präzise Einschätzung des Gegenüber erlaubt gute Vorhersagen von Werten, Präferenzen und Interessen. Informationen über Mitmenschen werden umgerechnet in Chancen der Machtausübung. Die wirksamste Form struktureller Machtausübung ist jene, welche den Gegner eliminiert und dem Einzelnen die Illusion der Chance zur Selbstverwirklichung vermittelt: Aus Fremdausbeutung wird Selbstausbeutung. Ermöglicht wird diese durch glaubhafte Phantasien der Allmachbarkeit: das Versprechen, dank weitgehender Unterstützung durch digitale Systeme und smarte Assistenten das persönliche Optimum erreichen zu können. Diese Illusion ist auf vielen Ebenen wirksam, sie zieht sich von der Hochschule 4.0 bis zur Industrie 4.0.

Die Entwicklung ist nur schwer zu hinterfragen, da alles nur der Optimierung dient. Kritiker sehen sich rasch als Nörgler verunglimpft, deren angeblich rückständigen Argumente ins Lächerliche gezogen werden, da sie sich dem Rausch ewiger Verbesserung entgegenstellen.[41] Die philosophische Antwort gibt Byung-Chul Han in seinem Text über die Müdigkeitsgesellschaft mit dem Hinweis:[42] "Protect me from what I want". Eine treffende künstlerische Charakterisierung liefert das Lied 'Der Wilde mit seiner Maschin‘', in welchem der österreichische Kabarettist Gerhard Bronner 1956 die Begeisterung eines Halbstarken an seinem Motorrad beschreibt:[43]

"Zwar hab ich ka Ahnung wo ich hinfahr, aber dafür bin i g’schwinder dort."

Man kann die Situation mit Paul Watzlawick als ein systemisches Problem zweiter Ordnung betrachten, bei dem ein "mehr der bisherigen Lösung" das Problem nur weiter verschlimmert, und bei dem das Ignorieren der eigentlichen Problematik dafür benutzt wird, sich echten Lösungen zu verweigern.

Die Debatte über Privatheit ist wichtig. Sie ist aber nur ein Stellvertreterkrieg für die wichtigere Frage, wie ökonomische Probleme unseres Zusammenlebens gelöst werden sollen. Erstaunlich daran ist, dass sich diese Frage zu einer Zeit stellt, in der wir über unglaublich leistungsfähige Technologien und bemerkenswerte wissenschaftliche Erkenntnisse verfügen. Das Problem besteht daher nicht in einem Mangel an technischen Lösungen oder einer unerwarteten, unvermeidlichen Katastrophe. Nachhaltige Lösungen könnten bei den philosophischen Fragen nach der Bestimmung des Menschen und seinem Verhältnis zu Mitmensch und Umwelt ansetzen.

CLEMENS HEINRICH CAP *hat Mathematik, Informatik und Physik studiert und in Mathematik promoviert. Nach Tätigkeiten an den Universitäten Innsbruck, Mannheim und Zürich hat er derzeit den Lehrstuhl für Informations- und Kommunikationsdienste an der Universität Rostock inne. Seine fachlichen Interessen umfassen Internet-Anwendungen und Dienste, Systemsicherheit, verteilte Systeme und gesellschaftliche Auswirkungen der Informatik. Er ist Titularprofessor an der Universität Zürich und hält regelmäßig Vorlesungen im Baltikum.*

Anmerkungen:

1 Louis Brandeis and Samuel Warren: The Right to Privacy. Harvard Law Review 4 (1890-1891), pp 193-220.

2 BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

3 William J. McGee: How to Get the Lowest Airfares. Consumer Reports, 25. 8. 2016, https://www.consumerreports.org/airline-travel/how-to-get-the-lowest-airfares/ und Catherine McGloin: Do Browser Cookies Increase Flight Prices? Skyscanner v. 20.1.2017, https://www.skyscanner.net/ news/tips/do-cookies-increase-flight-prices/ sowie Jennifer Valentino-DeVries et al: Websites Vary Prices, Deals Based on Users Information. The Wall Street Journal v. 24.12.2012, https://www.wsj.com/articles/SB10001424127887323777204578189391813881534

4 Dana Mattioli: On Orbitz, Mac Users Steered to Pricier Hotels. The Wall Street Journal, 23. 8. 2012, https://www.wsj.com/articles/SB10001424052702304458604577488822667325882

5 Patrick Beuth: Wenn der Staubsauger die Wohnung filmt. Die Zeit v. 26.5.2015, http://www.zeit.de/digital/internet/2015-05/staubsauger-roboter-roomba-vernetzter-haushalt und Martin Holland: Roomba: Hersteller der Staubsaugerroboter will Karten der Wohnungen verkaufen. Heise Online v. 25.7.2017, https://www.heise.de/newsticker/meldung/Roomba-Hersteller-der-Staubsaugerrobot er-will-Karten-der-Wohnungen-verkaufen-3782216.html

6 Mia Franke: Pay-as-you-Drive-Versicherungen noch Zukunftsmusik? Individuelle Prämien. Auto Zeitung v. 12.10.2015, https://www.autozeitung.de/pay-as-you-drive-versicherungen-deutschl and-praemien-74153.html

7 Wiltrud Weidner im Interview mit Rafael Kurz. Versicherungswirtschaft Heute v. 11.4.2016, http://versicherungswirtschaft-heute.de/vertrieb/echter-pay-as-you-drive-bleibt-zukunftsmusik/

8 Stephan Dörner: Diese Krankenkassen bezuschussen die Apple Watch. Die Welt v. 4.8.2015, https://www.welt.de/wirtschaft/article144818188/Diese-Krankenkassen-bezuschussen-die-Apple-Watch.html sowie Irene Berres und Nina Weber: Zuschuss für Wearables: die Kasse trainiert mit. Spiegel Online v. 7.8.2015, http://www.spiegel.de/gesundheit/ernaehrung/apple-watch-und-co-was-soll-die-krankenkasse-bezuschussen-a-1046835.html

9 Oliver Budzinski und Sonja Schneider: Smart Fitness: Ökonomische Effekte einer Digitalisierung der Selbstvermessung. Diskussionspapier Nr. 105, TU Ilmenau, Institut für Volkswirtschaftslehre, März 2017, https://www.tu-ilmenau.de/fileadmin/media/wth/Diskussionspapier_Nr_105.pdf

10 Mitesh S. Patel et al: Wearable Devices as Facilitators, Not Drivers, of Health Behavior Change. JAMA, 2015; 313(5):459-460. doi:10.1001/jama.2014.14781

11 Nach einer Analyse von Rich Parris (Online T&Cs Longer Than Shakespeare Plays – Who Reads Them Which Conversation, 23.3.2012, https://conversation.which.co.uk/technology/length-of-75 Cap: Privacy by Design vorgänge #221/222 website-terms-and-conditions/) sind die Terms of Services von Paypal länger als Shakespeares Hamlet und die Bedingungen von Apples iTunes immerhin noch länger als Shakespeares Macbeth.

12 Martin Holland: Fitnesstracker: Strava-Aktivitätenkarte legt Militärbasen und Soldaten-Infos in aller Welt offen. Heise Online, 29.1.2018, https://www.heise.de/newsticker/meldung/Fitnesstracker-Strava-Aktivitaetenkarte-legt-Militaerbasen-und-Soldaten-Infos-in-aller-Welt-offen-3952875.html

13 S. http://www.sueddeutsche.de/digital/donald-trump-tausche-usa-visum-gegen-facebook-passwo rt-1.3369298

14 Bernd Kramer: Gescheiterte US-Einreise: Ich kam mir vor wie eine Schwerverbrecherin. Spiegel Online, 5.8.2015, http://www.spiegel.de/lebenundlernen/schule/usa-einreise-abgelehnt-20-jaehri ge-wegen-facebook-chat-abgewiesen-a-1046792.html

15 Das klassische Beispiel ist das sog. Judenregister, dass aus Mitgliederdaten jüdischer Gemeinden sowie Volkszählungsdaten erstellt wurde und den Nationalsozialisten dabei half, die "Effizienz" des Holocaust erheblich zu steigern, s. https://de.wikipedia.org/wiki/Judenkartei

16 Byung-Chul Han: Im digitalen Panoptikum. Spiegel Online, 6. 1. 2014, http://www.spiegel.de/spiegel/print/d-124276508.html

17 In Deutschland aufgrund des Allgemeinen Gleichbehandlungsgesetzes, das im Bereich der Arbeitswelt, des Sozialschutzes, der Gesundheitsdienste, der Bildung und der Versorgung mit öffentlich zugänglichen Gütern, Dienstleistungen und Wohnraum Benachteiligungen wegen Rasse, Ethnie, Geschlecht, Religion, Weltanschauung, Behinderung, Alter oder sexueller Orientierung verbietet.

18 Aaron M. Bornstein: Are Algorithms Building the New Infrastructure of Racism? Nautilus 55 (2017). http://nautil.us/issue/55/trust/are-algorithms-building-the-new-infrastructure-of-racism

19 Byung-Chul Han: Müdigkeitsgesellschaft. Reihe: Fröhliche Wissenschaft. Matthes & Seitz, 2010.

20 Hartmut Rosa: Beschleunigung und Entfremdung – Entwurf einer kritischen Theorie spätmoderner Zeitlichkeit. Suhrkamp, 2013.

21 Clemens H. Cap: Risks and Side Effects of Data Science and Data Technology. In: M. Braschler, T. Stadelmann, & K. Stockinger (Hrsg.): Applied Data Science – Lessons Learned for the Data-Driven Business, Springer, 2018.

22 Gürses Seda, Carmela Troncoso und Claudia Diaz: Engineering Privacy by Design. Computers, Privacy & Data Protection 14 (2011).

23 Im Unterschied zur oftmals gleich bezeichneten Löschmarkierung, die zwar den normalen Zugriff auf die Daten unterbindet, deren Rekonstruktion aber technisch gestattet.

24 Das deutsche Bundesamt für Sicherheit in der Informationstechnik hält dazu im Dokument SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte Richtlinien bereit: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_4_1_Drucke

25 Deutsche Vereinigung für Datenschutz e. V.: Polizei ermittelt Autobahnschützen mit Kfz-Kennzeichenerfassung und Funkzellenkontrolle. Datenschutznachrichten 3/2013, S. 115-116. https://www.datenschutzverein.de/wp-content/uploads/2015/04/DANA_13_3_Heft.pdf

26 Eine gute Zusammenfassung findet sich in der Stellungnahme von Thomas Feltes und Andreas Ruch zum Videoüberwachungsverbesserungsgesetz, A-Drs. 18 (4) 785 C des Innenausschusses, https://www.bundestag.de/blob/495434/95e763508e5400acbad1bc0b71386d98/18-4-785-c-data.pdf

27 S. https://www.ccc.de/system/uploads/103/original/Schaar-Bericht.pdf

28 Paul Ohm: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review 1701 (2010), 1701-1777, http://www.uclalawreview.org/pdf/57-6-3.pdf

29 “You have zero privacy. Get over it”. Scott Mc Nealy in: Polly Sprenger: "Sun on Privacy: 'Get Over It'". Wired, 26. 1. 1999,

http://www.wired.com/politics/law/news/1999/01/17538

30 "I've heard quite a lot of people that talk about post-privacy, and they talk about it in terms of feeling like, you know, it's too late, we're done for, there's just no possibility for privacy left" in vorgänge #221/222 Schwerpunkt: Perspektiven des Datenschutzes nach der DSGVO "[...] and we just have to get used to it. And this is a pretty fascinating thing, because it seems to me that you never hear a feminist say that we're post-consent because there is rape. And why is that? The reason is that it's bullshit." Jacob Appelbaum an der re:publica 2012 in: Appelbaum & Kleiner – Resisting the Surveillance State and its Network Effects., https://www.youtube.com/watch?v=Y3h46EbqhPo&t=7m46s

31 "Meine Daten gehören mir". Es drängt sich ein Vergleich mit dem Satz aus der Abtreibungsdebatte auf: "Mein Bauch gehört mir".

32 Clemens H. Cap: Verpflichtung der Hersteller zur Mitwirkung bei informationeller Selbstbestimmung. In: Friedewald, M., Lamla, J. & Roßnagel, A. (Eds.): Informationelle Selbstbestimmung im digitalen Wandel. Springer Vieweg, DuD-Fachbeiträge, 2016 und Clemens H. Cap: Vertrauen in der Krise: Vom Feudalismus 2.0 zur Digitalen Aufklärung. In: Haller, M. (Ed.): Öffentliches Vertrauen in der Mediengesellschaft. Halem Verlag.

33 Etwa die Systeme PGP (Pretty Good Privacy) oder GPG (Gnu Privacy Guard).

34 Jose Pagliery: Microsoft Defends Its Right to Read Your Email. CNN Tech, 21. 3. 2014, http://money.cnn.com/2014/03/21/technology/security/microsoft-email/index.html, Russell Brandom: Microsoft Just Exposed Email's Ugliest Secret. The Verge, 21.3.2014, https://www.theverge.com/2014/3/21/5533814/google-yahoo-apple-all-share-microsofts-troubling-email-privacy-policy und Janko Roettgers: Google Will Keep reading Your Emails, Just Not for Ads. Variety, 23.6.2017, http://variety.com/2017/digital/news/google-gmail-ads-emails-1202477321/

35 Alma Whitten und J. D. Tygar: Why Johnny Can't Encrypt. In: L. Cranor und G. Simson (Hrsg.): Security and Usability: Designing Secure Systems that People Can Use. O'Reilly, 2005, pp. 679-702, https://people.eecs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/Oreilly.pdf; 10 Jahre später: Scott Ruoti, Jeff Andersen et al: Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client. https://arxiv.org/pdf/1510.08555.pdf

36 Einige Anbieter haben nachgebessert. Siehe auch Holger Bleich: De-Mail: Ende-zu-Ende-Verschlüsselung mit PGP gestartet. Heise Security v. 22.4.2015, https://www.heise.de/security/meldung/De-Mail-Ende-zu-Ende-Verschluesselung-mit-PGP-gestartet-2616388.html Die Nachbesserungen – Javascript-basierte Verschlüsselung oder Browser-PlugIns – sind aus technischer Sicht problematisch und erlauben dem Anbieter ein einfaches Unterlaufen der angeblich sicheren Verfahren.

37 Nicole Perlroth, Jeff Larson und Scott Shane: NSA Able to Foil Basic Safeguards of Privacy on Web. The New York Times, 5.9.2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html sowie Thomas C. Hales: The NSA Back Door to NIST. Notices of the AMS, Vol 62 No 2, 2014, http://www.ams.org/notices/201402/rnoti-p190.pdf

38 Mohsen Toorani und Ali A. Beheshti: Solutions to the GSM Security Weaknesses, Proc. 2nd IEEE International Conference on Next Generation Mobile Applications, Services, and Technologies, pp. 576–581, Cardiff, UK, September 2008, arXiv:1002.3175 sowie Syed Raiful Hussain, Omar Chowdhury et al: LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. Network and Distributed Systems Security Symposium, San Diego, 2018, http://homepage.divms.uiowa.edu/~comarhaider/publications/LTE_NDSS18_paper.pdf und Swati Khandelwal: Real-World SS7 Attack — Hackers Are Stealing Money from Bank Accounts. The Hacker News, 3.5.2017, https://thehackernews.com/2017/05/ss7-vulnerability-bank-hacking.html

39 Fabian Scherschel: Deutsche Bankkonten über UMTS-Sicherheitslücken ausgeräumt. Heise Online, 3.5.2017, https://www.heise.de/newsticker/meldung/Deutsche-Bankkonten-ueber-UMTS-Sicherheitsluecken-ausgeraeumt-3702194.html

40 Clemens H. Cap: Verpflichtung der Hersteller zur Mitwirkung bei informationeller Selbstbestimmung. In: Friedewald, M., Lamla, J. & Roßnagel, A. (Eds.): Informationelle Selbstbestimmung im digitalen Wandel. Springer Vieweg, DuD-Fachbeiträge, 2016.

41 August-Wilhelm Scheer: Hochschule 4.0. Whitepaper Nr 8, AWSi Institut, 2015. Hier: Seite 32.

42 Niels Boeing und Andreas Lebert: Interview mit Byung-Chul Han. Zeit Online v. 7.9.2014. 77 Cap: Privacy by Design vorgänge #221/222 http://www.zeit.de/zeit-wissen/2014/05/byung-chul-han-philosophie-neoliberalismus/komplettansicht

43 Gerhard Bronner: "Der Wilde mit seiner Maschin'". Weltmusik Edition International. Aufgeführt auf https://www.youtube.com/watch?v=vM3CmTkwHVM 78

---

https://www.humanistische-union.de/publikationen/vorgaenge/221-222/publikation/privacy-by-design-chancen-eines-programmierten-grundrechts-1/
Abgerufen am: 05.12.2023