www.bigbrotherawards.de

Autonome Akteure:
Wenn Daten die Realität gestalten

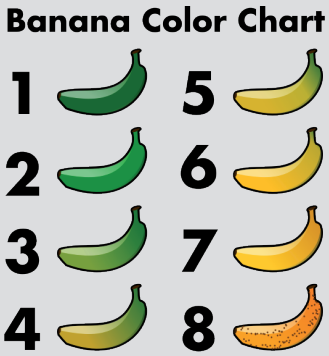
Daten werden erhoben, gespeichert, verarbeitet und ausgewertet. Für IT-Experten ist dies eine ebenso triviale wie unumstößliche Tatsache. Was aber passiert, wenn Daten ein Eigenleben entwickeln? Wenn gespeichertes Wissen zum Fakt erklärt wird, auf eine nahezu unwiderlegbare Weise? Wie kann eine Einzelperson ihre gesetzlichen Rechte einfordern? Und was geschieht, wenn datenbasierte Algorithmen das Ruder übernehmen, beispielsweise am Steuer eines Fahrzeuges? Wer haftet für potenzielle Schäden? Werden die Haftungsrisiken der Softwareentwicklung zukünftig noch versicherbar sein oder wird der Job zum existenziellen Risiko? Sind sich Politik und Gesellschaft ihres Gestaltungsauftrages bewusst und nehmen sie ihn aktiv wahr? Der Artikel beleuchtet einige Trends und setzt sich mit den Risiken auseinander.

Scoring

Fast jeder Verbraucher musste sich schon einmal einer Bonitätsprüfung unterziehen, sei es beim Online-Shopping, dem Abschluss eines Mobilfunkvertrages, dem Anmieten einer Wohnung oder beim Beantragen eines Kredites. Die Schufa ist die bekannteste Wirtschaftsauskunftei, die das „Scoring" – also die Beurteilung der Kreditwürdigkeit einer Person – auf Ebene der Endverbraucher betreibt (siehe Kasten 1).
Der Score bestimmt die Möglichkeiten und Chancen einer Person, in unserer Gesellschaft als Marktteilnehmer aufzutreten. Er hat Einfluss darauf, ob wir das online bestellte Notebook auf Rechnung bezahlen dürfen oder Vorkasse leisten müssen. Der Score kann entscheidend sein, wenn der Vermieter die schöne Altbauwohnung an einen konkurrierenden Interessenten vergibt. Der Score kann ein Eigenleben entwickeln, wie das folgende Beispiel zeigt.

Stefan L. ist auf der Suche nach einer Eigentumswohnung. Die Kreditzinsen sind niedrig und für die Altersvorsorge sind die eigenen vier Wände ein wichtiger Baustein.

Beim Scoring werden Personen einem Punktebewertungsverfahren unterzogen. Der ermittelte Punktwert (*Score*) soll die Wahrscheinlichkeit für ein zukünftiges Verhalten der Person angeben. Wirtschaftliche Bedeutung hat das Scoring bei der Beurteilung kreditorischer Ausfallrisiken, d.h. der Beantwortung der Frage, ob ein Geschäftspartner zukünftig in der Lage sein wird, seinen Zahlungsverpflichtungen nachzukommen.
In Deutschland wird das Scoring kommerziell von Auskunfteien betrieben, die bekannteste darunter ist die Schufa. Andere Unternehmen wie Arvato Infoscore, Creditreform, Bürgel oder Deltavista sind auf Grund ihrer geringeren Bedeutung für den Endverbraucher weniger bekannt.
Zur Berechnung eines Score müssen zu einer natürlichen Person eine Reihe von Merkmalen erfasst werden. Dazu gehören unter anderem:

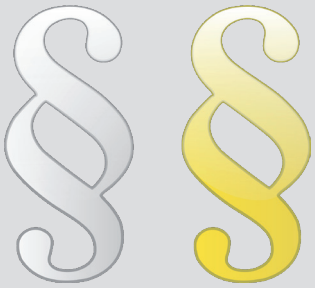


- *Persönliche Daten:* Geburtsdatum, Geschlecht, Familienstand, Anzahl Haushaltsmitglieder etc.
- *Adressdaten:* Verwendete Anschriften, Gebäudedaten, Wohndauer an der aktuellen Anschrift etc.
- *Zahlungserfahrungen:* Eventuell auch am Wohnumfeld
- *Kreditnutzung*
- *Zahlungsstörungen*
- *Insolvenzverfahren, Schuldnerverzeichniseinträge*

Die verschiedenen Auskunfteien arbeiten mit einer unternehmensspezifischen Teilmenge der oben genannten Datenkategorien. Sind exakte Werte zu einzelnen Merkmalen nicht bekannt, so scheuen die Unternehmen sich nicht, Daten auf Grund von Heuristiken zu schätzen. So werden das Geschlecht und das Alter mitunter auf Basis des Vornamens geschätzt. Neben den Stammdaten melden Unternehmen Angaben zum Zahlungsverhalten, zu Krediten sowie zu Zahlungsausfällen an die Auskunfteien. Schwerwiegende Vorfälle wie Insolvenzen ermitteln die Auskunfteien selbstständig aus öffentlichen Datenquellen (z.B. Schuldnerverzeichnissen).
Bei der Ermittlung eines Score wird eine Person auf Grund ihrer vorliegenden Daten einer passenden Vergleichsgruppe zugeordnet. Das historische Zahlungsverhalten der Gruppe wird auf die zu bewertende Person projiziert: Der Score der Person ist „berechnet". Was streng mathematisch klingt, könnte auch einer Kaffeesatzleserei nahe kommen. Die Auskunfteien verweigern eine Offenlegung ihrer Algorithmen mit Hinweis auf ihr Geschäftsgeheimnis, eine behördliche Genehmigung oder Überprüfung der Verfahren findet nicht statt. Für den Verbraucher ist der Zusammenhang zwischen seinen Daten und dem errechneten Score daher kaum nachvollziehbar oder überprüfbar.
Eine fehlerhafte Datenbasis senkt die Qualität der Prognosen zusätzlich. Für die Schufa ermittelten zwei Studien einen hohen Prozentsatz falscher oder unvollständiger Daten. Demnach wurden im Jahr 2009 noch 46 Prozent der überprüften Daten beanstandet (vgl. [Kor09]), während im Jahr 2013 mit einer Fehlerrate von 26,5 Prozent eine deutliche, aber dennoch unzureichende Verbesserung erzielt wurde (vgl. [ULD14]).

Kasten 1: Das Scoring-Verfahren.

Scoring: Datenschutz kaum durchsetzbar



Datenschutzrechtlichen Vorgaben entziehen sich die Auskunfteien mit der Argumentation, der Score einer Person sei kein personenbezogenes Datum, sondern eine freie Meinungsäußerung. Ein Argument, das juristisch kaum haltbar ist, aber dennoch Eingang in die Rechtsprechung gefunden hat. Die von Bundesministerium für Verbraucherschutz in Auftrag gegebene Scoring-Studie aus dem Jahr 2014 (vgl. [ULD14]) kritisiert die Rechtspraxis scharf und kommt zu dem Schluss, dass die Position der Verbraucher in Bezug auf Transparenz der Verfahren und *durchsetzbare* Korrekturrechte deutlich gestärkt werden muss.

Während das Bundesdatenschutzgesetz (BDSG) bei Behörden und sonstigen staatlichen Institutionen greift, eröffnen sich auf Seite der Privatwirtschaft große datenschutzrechtliche Lücken. Ein Beispiel aus dem Insolvenzrecht illustriert diese Kluft. Im Rahmen der Privatinsolvenz wird ein Schuldner nach Ablauf der „Wohlverhaltensphase“ von sechs Jahren aus dem Schuldnerverzeichnis gelöscht. Für Auskunfteien gelten diese Löschfristen nicht. Die Unternehmen entnehmen die Eintragungen den öffentlichen Schuldnerverzeichnissen, ohne jedoch mit den Löschungen gleichzuziehen. In den Score gehen Insolvenzinformationen noch lange nach der Löschung aus dem öffentlichen Verzeichnis ein. Manche Unternehmen argumentieren sogar, dass Insolvenzinformationen „lebenslänglich“ gespeichert bleiben müssten (vgl. [ULD14]). Die Idee einer zweiten Chance, die der Privatinsolvenz zu Grunde liegt, wird staatlich umgesetzt, aber privatwirtschaftlich konterkariert.

Darüber hinaus fehlt es den Behörden oft an wirksamen Möglichkeiten, datenschutzrechtliche Verstöße der Auskunfteien zu ahnden. Der im BDSG festgelegte Bußgeldkatalog lässt viele Verstöße, die das Scoring betreffen, außer Betracht. So ist beispielsweise das Geo-Scoring gesetzeswidrig, unterliegt aber keinem Bußgeld. Den Behörden fehlt damit die Möglichkeit zur Gewinnabschöpfung.

Bei einem ungerechtfertigten Score bleibt Betroffenen nur der aufreibende und teure Weg einer Zivilklage, um Rechte auf Korrektur oder Löschung durchzusetzen. Ein Recht darauf, *keinem* Scoring-Prozess unterworfen zu werden, existiert derzeit nicht.

Ein Vorschlag der Europäischen Kommission zu einer Datenschutz-Grundverordnung nimmt sich dieser Probleme an und will die Rechte der Verbraucher und der Aufsichtsbehörden deutlich stärken (vgl. [Eur12]). Eine Umsetzung in europäisches und nationales Recht steht jedoch aus.

Kasten 2: Scoring und der Datenschutz.

Also macht er sich auf die Suche nach einer bezahlbaren und schönen Immobilie. Nach einigen Besichtigungsterminen wird Stefan L. fündig und kümmert sich um die Finanzierung. Mit Problemen rechnet er nicht, denn er hat ein gutes Einkommen und etwas Eigenkapital. Überraschenderweise erhält Stefan L. mehrere Absagen und nur ein einziges Kreditangebot – noch dazu ein schlechtes, denn die Konditionen beinhalten einem erheblichen Zinsaufschlag. Stefan L. hakt bei den Kreditinstituten nach und erfährt, dass eine negative Schufa-Auskunft zur Ablehnung seiner Anfrage führte.

Eine Schufa-Selbstauskunft soll Licht ins Dunkel bringen. Als Stefan L. die über ihn gespeicherten Daten überprüfen kann, ist er fassungslos: Ein Autohaus hat offene Forderungen aus einem Leasing-Vertrag gemeldet. Stefan L. hatte niemals Kontakt zu diesem Unternehmen, es muss sich um einen Fehler handeln. Er fordert die Schufa auf, den unberechtigten Eintrag zu löschen. Die Schufa entgegnet, dass der Autohändler zuvor eine korrigierte Meldung abgeben müsse. Ein Nervenkrieg beginnt, die Schufa und das Autohaus schieben sich gegenseitig die Schuld zu. Schließlich stellt sich heraus, dass die Fehleintragung auf einer Namens- und Geburtsdatumsgleichheit von Stefan L. mit dem säumigen Kunden beruhte. Einen Adressabgleich hatte man offenbar versäumt. Nach mehreren Wochen ist der Fehler bei der Schufa bereinigt – aber die schöne Wohnung wurde längst an einen anderen Kunden verkauft.

Der beschriebene Fall ist fiktiv (ebenso wie die anderen Fälle, die in diesem Artikel noch folgen werden), aber die Details beruhen auf Tatsachen. Ähnliche Vorfälle verletzen die Rechte von Verbrauchern Tag für Tag. Die Datenqualität ist bei der Schufa und anderen Auskunfteien nach wie vor inakzeptabel schlecht (**siehe Kasten 1**), sodass ein ungerechtfertigter schlechter Score jeden Verbraucher treffen kann. Ansprüche auf eine Berichtigung oder Löschung können nach derzeitiger Rechtslage nur schwer durchgesetzt werden (**siehe Kasten 2**).

Ein schlechter persönlicher Score kann dazu führen, dass man keinen Dispo erhält, keine Kreditkarte oder keinen Mobilfunkvertrag. In gravierenden Fällen schließt der Markt einen nahezu aus. All dies kann unverschuldet passieren, auf Grund einer fehlerhaften Datenbasis oder eines nicht nachvollziehbaren Scoring-Prozesses. Sind bei den Auskunfteien die eigenen Daten korrekt erfasst, so ist die Ausgangslage zwar besser, aber dennoch sind nicht alle Risiken beseitigt, wie das folgende Beispiel zeigt.

Robert K. hat sich während des Studiums eine preiswerte Drei-Zimmer-Wohnung mit drei Kommilitonen geteilt. Die Wohnung liegt am Rande eines Industriegebietes und die Verkehrsanbindung ist gut. Nach dem Ende der Studienzeit sind die Mitbewohner nach und nach ausgezogen. Robert K. hat die Wohnung behalten, eine Familie gegründet und wohnt mittlerweile mit seiner Partnerin und seinem Sohn dort. Aufgrund der günstigen Miete kann die Familie jeden Monat einen ordentlichen Betrag auf die hohe Kante legen, der Traum von Haus im Grünen rückt in greifbare Nähe. Robert K. informiert sich über Zinskonditionen und holt vorsorglich Selbstauskünfte bei verschiedenen Auskunfteien ein. Alles im grünen Bereich. Keine Datenfehler, keine Zahlungsauffälligkeiten, keine Kredite oder Verbindlichkeiten. Aber dennoch bewertet ihn eine Auskunftei mit einem miserablen Score. Wie kann das sein?

Robert K. wohnt in der falschen Gegend, im Stadtviertel häufen sich die Zahlungsausfälle. Ihm ist das „Geo-Scoring“[1]) zum Verhängnis geworden, denn er landet in einer Vergleichsgruppe mit mieser Zahlungsmoral und wird sozusagen mit seinen Nachbarn in „Sippenhaft“ genommen.

Das Geo-Scoring wird von Daten- und Verbraucherschützern, Stadtplanern und Kommunalpolitikern gleichermaßen verurteilt, da es eine Stigmatisierung ganzer Stadtteile begünstigt. Geo-Scoring birgt die Gefahr einer selbst erfüllenden Prophezeiung, denn

die Anwohner schlecht beleumdeter Viertel erhalten deutliche ungünstigere Konditionen am Markt als die Bewohner zahlungskräftigerer Stadtteile. Für Robert K. könnte es schwierig werden, Kreditinstitute oder Vermieter von seiner Bonität zu überzeugen. Sein miserabler Score nährt stets den Stachel des Misstrauens bezüglich seiner Zahlungsmoral.

Gesundheitsdaten im Versicherungswesen

Versicherungsunternehmen sind in vielfacher Weise an den Daten bestehender oder potenzieller Kunden interessiert, um Risiko- und Leistungsprüfungen sowie Tarifkalkulationen bestmöglich zu verfeinern. Bei der Anbahnung eines Versicherungsvertrages in den Sparten Kranken-, Lebens-, Unfall- oder Berufsunfähigkeitsversicherung fordern die Unternehmen einmalig einen umfassenden Einblick in die Gesundheitsdaten ihrer potenziellen Kunden. Die Abwehr höherer Risiken wird damit für die private Versicherungswirtschaft möglich. Verglichen mit den gesetzlichen Sozialversicherungsträgern kann oft ein besseres Preis-Leistungsverhältnis angeboten werden.

Leider versiegen die Datenquellen, sobald der Versicherungsnehmer erst einmal im Bestand ist. Eine weitere risikobasierte Differenzierung der Beiträge kann nur noch rudimentär erfolgen: auf der Basis von Risikostatistiken bezüglich Geschlecht und Alter. Im Zeitalter von Big Data mutet dies an wie eine datentechnische Steinzeit. In den USA ist man bereits weiter und neue Trends schwappen über den großen Teich zu uns hinüber.

Versicherungsunternehmen wollen ihre Kunden dazu animieren, Gesundheitsdaten per App kontinuierlich zu übermitteln, neue *E-Health-Tarife* sollen bereits 2016 eingeführt werden. Man benötigt hierfür lediglich schmale Armbänder, vollgepackt mit Sensoren, welche die Körperdaten erfassen und mit Smartphones und der Cloud kommunizieren. Die so genannten *Health Tracker* können bereits heute den Herzschlag, die Körpertemperatur, den Hautwiderstand, den Körperfettanteil, zurückgelegte Schritte und die UV-Belastung erfassen. Auf dieser Grundlage lassen sich unter anderem Aussagen über sportliche Aktivitäten und den Kalorienverbrauch treffen sowie die Schlafqualität beurteilen (**siehe Abbildung 1**).

Lässt sich ein Versicherter auf die Auswertung seiner Daten ein, so können sportliche Betätigung, gesunde Ernährung oder andere Parameter einer gesunden Lebensweise zu einer Reduzierung seiner Beiträge führen. Klingt zunächst gut, aber was ist mit den Versicherten, die nicht können oder wollen? Zwangsläufig muss die Beitragsreduzierung der App-Nutzer mit Beitragserhöhungen der übrigen Kunden korrespondieren, da die Gesundheitskosten über die Gesamtgruppe der Versicherten unverändert bleiben werden. Eine weitreichende Umstellung der Lebensgewohnheiten aller Versicherungskunden ist kaum zu erwarten. Stattdessen könnten die bereits sportlich Aktiven in einen App-Tarif wechseln und die Übrigen die Zeche zahlen – also all jene Versicherte, die nicht mehr fit genug für einen sportlichen Lifestyle sind oder die sich dem Anspruch des gläsernen Kunden verweigern.

Denkt man das Modell etwas weiter, wird es der Versicherungswirtschaft zukünftig immer leichter möglich sein, „schlechte Risiken“ auch im Bestand zu identifizieren und Versicherungsnehmer über hohe Prämiensteigerungen aus dem Vertrag zu drängen. Die Risiken und deren Kosten werden dann von der privaten Versicherungswirtschaft in die Solidargemeinschaft verlagert, analog zum Vorgehen in der Finanzwelt: Risiken sozialisieren, Gewinne privatisieren.

Weitere Fragen drängen sich auf. Was passiert, wenn die Daten negative Veränderungen signalisieren? Wie wollen die Versicherer darauf reagieren? Das folgende Gedankenspiel zeigt, dass sich Kunden eventuell sehr weit entblößen müssten.

Julia K. ist 34 Jahre alt, schlank und sportlich. Bei ihrer privaten Krankenversicherung ist sie auf einen den neuen E-Health-Tarif umgestiegen. Sie freut sich über die Beitragsreduzierung und legt den Health-Tracker regelmäßig an. Ihre Gesundheitsdaten zeugen von ihrer aktiven und gesunden Lebensweise.

Aber zwei Jahre später wendet sich das Blatt, Julia K. hat fünf Kilo zugelegt, ihre sportlichen Aktivitäten sind kaum noch messbar. Was ist passiert? Ist Julia K. zur riskanten Couch-Potato mutiert? Die Krankenversicherung meldet sich bei ihr

Foto: Microsoft

Abb. 1: Health Tracking.

und fragt nach. Des Rätsels Lösung ist einfach: Julia K. isst für zwei und gönnt sich häufiger eine Ruhepause. Sie erwartet ein Kind. Es ist alles in Ordnung.

Wird der Versicherer der erste sein, dem Julia K. die frohe Botschaft überbringt? Muss sie dem Unternehmen Rechenschaft ablegen? Kann sie damit eine Beitragserhöhung vermeiden? Und was wäre, wenn sie „einfach nur so“ zugenommen hätte? Vielleicht hat sie Liebeskummer und verbringt manchen Abend mit einer Packung Chips auf dem Sofa. Hat ihre Krankenversicherung ein Recht darauf, über ihr Seelenleben Bescheid zu wissen?

Darüber hinaus stellt sich die Frage, welche Befugnisse ein Versicherungsunternehmen im Umgang mit den erhobenen Daten hat. Kein Unternehmen ist eine Insel, die Versicherungskonzerne bedienen sich einer Vielzahl von Dienstleistern, die mit den erhobenen Daten in Kontakt kommt. Wer erhält Einblick? Dürfen meine Gesundheitsdaten an andere Unternehmen weitergegeben werden? Wie soll einem Missbrauch vorgebeugt werden?

Nach derzeitiger Rechtslage haben die Versicherungsunternehmen und ihre Geschäftspartner bereits weitreichende Rechte im Umgang mit den Gesundheitsdaten der Versicherten, wie das folgende Beispiel zeigt.

Martin S. steht mit 37 Jahren mitten im Berufs- und Familienleben. Von seinem abwechslungsreichen, aber fordernden Job als Vertriebsleiter eines Automobilzulieferers entspannt er sich gern im Skiurlaub. Nach den Weihnachtstagen fährt die Familie in die Berge, gemeinsam mit seiner Frau und den beiden Töchtern freut er sich auf zwei Wochen pures Skivergnügen. Doch leider ist es nach drei Urlaubstagen mit der Erholung vorbei: Martin S. stürzt auf der Piste und zieht sich einen kompliziert-

[1]) Scoring auf der Basis von Anschriften. Denkbar ist auch die Auswertung von IP-Adressen, Mobilfunkzellen, GPS-Daten etc. In Deutschland ist ein ausschließlich auf Adressdaten beruhendes Scoring verboten. Bei Hinzunahme eines zweiten Merkmals ist Geo-Scoring jedoch gestattet, die Gewichtung der Adressdaten im Vergleich zu anderen Merkmalen muss aber nicht offengelegt werden.

Versicherungswirtschaft – Global geltende Schweigepflichtsentbindung
Im Folgenden ein Auszug aus einem Leistungsantrag. Die Formulierung folgt dem Beschluss des Düsseldorfer Kreises vom 17.01.2012 und wird von den Datenschutzbeauftragten bereits als Fortschritt betrachtet (vgl. [Lep13]).

Übertragung von Aufgaben auf andere Stellen (Unternehmen oder Personen)
Die Versicherung XY führt bestimmte Aufgaben, wie zum Beispiel die Risikoprüfung, die Leistungsfallbearbeitung oder die telefonische Kundenbetreuung, bei denen es zu einer Erhebung, Verarbeitung oder Nutzung Ihrer Gesundheitsdaten kommen kann, nicht selbst durch, sondern überträgt die Erledigung einer anderen Gesellschaft, der XY-Gruppe oder einer anderen Stelle. Werden hierbei Ihre nach § 203 StGB geschützten Daten weitergegeben, benötigt die Versicherung XY Ihre Schweigepflichtentbindung für sich und soweit erforderlich für die anderen Stellen. Die Versicherung XY führt eine fortlaufend aktualisierte Liste über die Stellen und Kategorien von Stellen, die vereinbarungsgemäß Gesundheitsdaten für die Versicherung XY erheben, verarbeiten oder nutzen, unter Angabe der übertragenen Aufgaben. Die zurzeit gültige Liste ist als Anlage der Einwilligungserklärung angefügt [...] Für die Weitergabe Ihrer Gesundheitsdaten an und die Verwendung durch die in der Liste genannten Stellen benötigt die Versicherung XY Ihre Einwilligung.

Ich willige ein, dass die Versicherung XY meine Gesundheitsdaten an die in der [...] Liste genannten Stellen übermittelt und dass die Gesundheitsdaten dort für die angeführten Zwecke im gleichen Umfang erhoben, verarbeitet und genutzt werden, wie die Versicherung XY dies tun dürfte. Soweit erforderlich, entbinde ich die Mitarbeiter der XY-Unternehmensgruppe und sonstiger Stellen im Hinblick auf die Weitergabe von Gesundheitsdaten und anderer nach § 203 StGB geschützter Daten von ihrer Schweigepflicht.

[..] Liste der Dienstleister, die Datenverarbeitung in Funktionsübertragung oder im Auftrag erbringen:

Dienstleisterkategorie	Hauptgegenstand des Auftrags
IT-Dienstleister	IT-Entwicklungs- und Wartungsdienstleistungen
Wirtschaftsprüfungsgesellschaften	Jahresabschlussprüfung und Beratung
Beratungsunternehmen	Beratung
Aktenvernichter	Akten- und Datenträgervernichtung
Medizinische Gutachter	Leistungsfallprüfung
Kollektivpartner und Banken	Prämieneinzug in Teilbeständen
Wirtschaftsauskunfteien	Bonitätsauskünfte
Rechtsanwälte	Rechtliche Vertretung und Informationsbeschaffung
Postdienstleister	Postdienstleistungen
Adressermittler	Adressprüfung
Sicherheitsdienste	Bewachungs- und Empfangsdienst

Kasten 3: Global geltende Schweigepflichtsentbindungen für Gesundheitsdaten.

ten Oberschenkel- und Beckenbruch zu. Er wird mehrfach operiert, aber die Heilung gestaltet sich schleppend. Nach 43 Tagen endet die Lohnfortzahlung seines Arbeitgebers und das Haushaltseinkommen der Familie schmilzt deutlich zusammen. Fortan wird lediglich das Krankengeld gezahlt, das noch nicht einmal der Hälfte seines üblichen Einkommens entspricht. Zum Glück hat Martin S. eine Unfallversicherung abgeschlossen, welche die Versorgungslücke schließen soll.

Als Martin S. den Leistungsantrag ausfüllt, muss er seiner Versicherung umfangreichen Zugriff auf seine Gesundheitsdaten gewähren und eine Schweigepflichtsentbindung abgeben. Er hat damit gerechnet, dass er seine Ärzte von der Schweigepflicht entbinden muss, dies erscheint ihm sachgerecht. Als er sich jedoch dem Kleingedruckten widmet, erfährt er, dass er darüber hinaus neben den Mitarbeitern seiner Versicherung auch einer Vielzahl anderer Menschen Zugriff auf seine Untersuchungsergebnisse gestatten soll. Es handelt sich um die Mitarbeiter sämtlicher Firmen, die Dienstleistungen für seine Versicherung erbringen. Eine beigefügte Liste soll die Personen und Unternehmen näher eingrenzen.

Martin S. stutzt. Das erscheint ihm sehr weitreichend. Er will genau wissen, wem er seine Gesundheitsdaten zur Verfügung stellen soll. Also durchsucht er den Formularstapel, der ihm zugeschickt wurde, nach der Dienstleisterliste[2]) . Als er sie endlich findet, staunt er nicht schlecht: Anstelle namentlich genannter Unternehmen beinhaltet die Liste nur Branchenbezeichnungen (siehe Kasten 3). Vom Aktenvernichter über Sicherheitsdienste, vom Rechtsanwalt über Wirtschaftsauskunfteien, von Beratungsunternehmen bis hin zu Banken – allen Mitarbeitern aller derartigen Firmen soll Martin S. pauschal einen Freibrief zum Einblick in seine Krankenakte erteilen! Martin S. ist empört und forscht nach, ob er diese globale Schweigepflichtsentbindung verweigern kann. Das Ergebnis ist ernüchternd: Auf Grund seines Rechtes auf informelle Selbstbestimmung steht es ihm frei, die Zustimmung zu verweigern. Allerdings hat er dann keinen Anspruch mehr auf das Unfallgeld aus seinem Versicherungsvertrag. Sein Recht ist also ein Papiertiger. Martin S. ist auf die Versicherungsleistung angewiesen, um den Lebensunterhalt seiner Familie zu sichern. Zähneknirschend unterschreibt er die geforderten Erklärungen.

Der rollende Datenspeicher

Unsere modernen Autos sind zu Computern auf Rädern geworden. Die Elektronik assistiert dem Fahrer in alltäglichen und brenzligen Situationen mit Einparkhilfe, Start-Stopp-Automatik, Antiblockiersystem, Fahrdynamikregelung oder bei einem Unfall durch das Auslösen eines Airbags. Die Technologien basieren auf einer Vielzahl von Daten, erhoben von Sensoren und ausgewertet von der Bordelektronik. Die Airbag-Funktionalität erfordert beispielsweise die permanente Messung der Beschleunigung. ABS- und ESP-Systeme zeichnen Daten zum Bremsverhalten und den Drehzahlen der Räder auf.

Andere Daten werden zu Diagnosezwecken im Fahrzeug gespeichert, um Servicekräften die Fehlersuche zu erleichtern. Bei unklaren Fahrzeugdefekten oder einer Autopanne schließt der Techniker zunächst ein Diagnosegerät an die OBD-II-Schnittstelle[3]) des Fahrzeugs an, um sich einen Überblick zu verschaffen. Aber die Schnittstelle hat ein größeres Potenzial. Schon heute können GPS-fähige Zusatzgeräte die Fahrzeugdaten mit Ortsinformationen verknüpfen. Über eine SIM-Karte des Geräts gelangen die angereicherten Daten in die Cloud und können per Smartphone-App überwacht werden. In den USA werden auf Basis derartiger Daten bereits Services angeboten. Besorgte Eltern können sich per App benachrichtigen lassen, wenn der Junior mal wieder zu schnell auf dem Highway unterwegs ist. Vertrauen ist gut, Kontrolle scheint besser zu sein.

Der Datenbestand eines Wagens birgt statische und dynamische Informationen, er beschreibt den Zustand des Wagens und protokolliert das Verhalten des Fahrers. Er ähnelt damit einem Flugschreiber, ohne jedoch auf vergleichbare Weise gegen Manipulationen gesichert zu sein. Die Besitzverhältnisse der erhobenen Daten sind derzeit gesetzlich nicht geregelt. Einige Experten vertreten die Ansicht, dass die Daten als „immaterielle Informationen“ besitzlos seien (vgl. [Ver14]). Die Fahrzeughersteller hingegen reklamieren die Datenhoheit für sich. Der Fahrer des Wagens bleibt in diesen Diskussionen zumeist außen vor.

Foto: Audi

Abb. 2: Pilotiertes Fahren wird bereits erprobt.

Ereignet sich ein schwerer Unfall, so können Versicherungen und Ermittlungsbehörden an Hand der Fahrzeugdaten Details zum Unfallhergang rekonstruieren – mit erheblichen rechtlichen Konsequenzen für die beteiligten Personen. Der Fahrer eines Unfallfahrzeugs kann mit einer erdrückenden und kaum widerlegbaren Beweislast konfrontiert werden. Daher ist es unerlässlich, dass die Daten fehlerfrei aufgezeichnet wurden und Manipulationen unmöglich sind. Ist es denkbar, dass ein technischer Mangel datentechnisch verschleiert und die Schuld auf den Fahrer abgewälzt wird oder dass fehlerhafte oder manipulierte Messdaten eine überhöhte Geschwindigkeit vermeintlich belegen?

Momentan deutet nichts darauf hin, dass besondere Vorkehrungen zum Schutz der Integrität der Fahrzeugdaten getroffen werden. Es verbleiben offene technische und juristische Fragen bezüglich der Datensicherheit, den Zugriffsberechtigungen und der Beweislast sowie die Aufforderung an Politik und Justiz, den rechtlichen Rahmen für den Umgang mit Fahrzeugdaten zu definieren.

Richtet man den Blick weiter in die Zukunft, so erscheinen die selbstfahrenden Autos am Horizont (**siehe Abbildung 2**). Fahrzeuge, die bis unters Dach vollgepackt sind mit Sensoren, Prozessoren und Bordelektronik, Fahrzeuge, die niemals abgelenkt sind, die am Steuer weder mit ihrem Partner streiten, noch mit dem Chef telefonieren oder in der Musiksammlung nach dem Lieblingstitel suchen.

Wenn tatsächlich alle Systeme fehlerfrei funktionieren, so ist es nicht vermessen anzunehmen, dass ein solches Fahrzeug weniger Unfälle verursachen könnte als ein menschlicher Fahrer. Allerdings lehrt die Erfahrung, dass technische Fehler nicht vollständig zu vermeiden sind und dass es schwierig ist, Anforderungen an ein System vollständig zu erfassen und umzusetzen. Wehe, wenn ein Fehler oder eine im System nicht definierte Situation eintritt. Wehe, wenn es knallt.

Wie lässt sich dann nachweisen, dass das Fahrzeug zum Zeitpunkt des Unfalls im autonomen Modus unterwegs war? Muss der Innenraum permanent per Kamera überwacht werden? Wer haftet bei einem Unfall? Der Fahrer, der im Wagen saß, ohne einzugreifen? Ein Fahrer, der vielleicht gar nicht eingreifen konnte, weil das System dies verweigert hat? Oder der Fahrzeughersteller? Und was heißt das, „der Fahrzeughersteller“? Neben zivilrechtlichen Ansprüchen des Schadensersatzes können strafrechtliche Gesichtspunkte ins Spiel kommen. Dabei ist zu bedenken, dass es in Deutschland kein Strafrecht für Firmen gibt. Strafrechtlich können ausschließlich natürliche Personen belangt werden. Im Falle des Fahrzeugherstellers müssten Beschäftigte des Unternehmens zur Verantwortung gezogen werden.

Wen würde es dann treffen? Den Ingenieur, der eine fehlerhafte Komponente entwickelt hat? Den Softwareentwickler, der eine unzureichende Lösung implementiert hat? Den Analytiker, der die Anforderungen unzureichend spezifiziert hat? Den Mitarbeiter der Qualitätssicherung, der einen Fehler übersehen hat? Schon heute kündigen Versicherungsunternehmen in Europa an, dass

[2]) Derartige Listen sind abgesegnet durch den „Düsseldorfer Kreis“, dem Gremium der Datenschutzbeauftragten des Bundes und der Länder.

[3]) OBD = „On board diagnostics“, standardisierte Schnittstelle für Fahrzeugdiagnosesysteme.

sie zukünftig auch selbstfahrende Autos versichern wollen, nicht ohne darauf hinzuweisen, dass sich das Risiko vom Fahrer auf den Entwickler verlagert.

Da erscheint es nicht unwahrscheinlich, dass es den Versicherern im Gegenzug wenig attraktiv erscheint, Entwickler und Konstrukteure gegen die Haftungsrisiken ihrer Berufsausübung abzusichern. Die Versicherungsprämien für Berufshaftpflichtversicherungen könnten unbezahlbar werden[4]) und der Job wird zum existentiellen Risiko. Vielleicht wird es in naher Zukunft einmal selbstfahrende Autos geben. Aber die Entwickler, Analytiker und Konstrukteure, die in dieser Branche tätig sein werden, könnten eine aussterbende Spezies sein.

Fazit

Vor mehr als 30 Jahren begründete das Volkszählungsurteil mit der Etablierung des *Grundrechtes auf informelle Selbstbestimmung* in Deutschland einen Meilenstein des Datenschutzes. Damals vermutete man vor allen bei staatlichen Institutionen den Willen und die Technologien, umfassende Datensammlungen auszuwerten. Es war die Zeit der Großrechner, der PC tauchte erst am Horizont auf. Die Datenschutzgesetze des Bundes und der Länder lassen noch heute die damalige IT-Landschaft erahnen, Kontroll- und Sanktionsmöglichkeiten beziehen sich überwiegend auf Behörden und Telekommunikationsunternehmen – eine Folge der Privatisierung des ehemals staatlichen Postunternehmens.

Gesetzliche Vorgaben für den Datenschutz gelten zwar auch in der privaten Wirtschaft, aber deren Einhaltung wird kaum kontrolliert. Verstöße bleiben für die Unternehmen fast immer folgenlos, betroffene Bürger erleiden jedoch teils erhebliche Nachteile und wirtschaftliche Schäden.

Big Data ermöglicht es beliebigen Firmen – vom großen Konzern bis hin zum Startup – Benutzerprofile in bisher kaum vorstellbaren Umfang zu speichern und auszuwerten. Nicht ohne Grund bezeichnete ein Versicherungsvorstand die Daten als das neue „Gold der Branche“. Als Kunden sollten wir uns gut überlegen, wem wir dieses Gold anvertrauen. Aber in vielen kommerziellen Bereichen haben wir heute keine echte Wahl. Internationale Konzerne ignorieren in ihren Geschäftsbedingungen häufig nationales Recht, ohne dafür belangt zu werden. Stattdessen appellieren Minister an den guten Willen der Unternehmen oder löschen demonstrativ ihre Benutzerkonten. Bisher weitgehend folgenlos.

Der technische Fortschritt hat Big Data ermöglicht. Nun müssen Gesellschaft und Politik Schritt halten und sich der neu entstandenen Probleme annehmen. Es gilt, Gesetze weiterzuentwickeln, wirksame Sanktionen gegen Verstöße zu etablieren und dem Bürger durchsetzbare Rechte an die Hand zu geben. Ein Recht auf informelle Selbstbestimmung, das nur mit langem Atem und hohen Prozesskosten durchgesetzt werden kann, widerspricht dem Gedanken eines Grundrechts für alle Bürger. ||

Literatur & Links

[Eur12] Europäische Kommission, Vorschlag für „Verordnung des Europäischen Parlaments und des Rates“ zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 2012, siehe:
`http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf`

[Kor09] D. Korczak, M. Wilken, Verbraucherinformation Scoring, Bericht im Auftrag des Bundesministeriums für Ernährung, Landwirtschaft und Verbraucherschutz, 2009

[Lep13] U. Lepper, 21. Datenschutz- und Informationsfreiheitsbericht des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, S. 144ff, siehe:
`www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/Inhalt/21_DIB/DIB_2013.pdf`

[ULD14] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), GP Forschungsgruppe, Scoring nach der Datenschutz-Novelle 2009 und neue Entwicklungen, siehe:
`www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Scoring-Studie.pdf`

[Ver14] Verkehrsgerichtstag 2014, Datendiskussion in Goslar, siehe:
`www.vkuonline.de/verkehrsgerichtstag-datendiskussion-in-goslar-1324023-vku_article.html`

Die Autorin

|| Kerstin Dittert
(kerstin.dittert@oocon.de)
ist freie Beraterin mit den Schwerpunkten Softwarearchitektur, agile Methoden, Java/JEE und Anforderungsmanagement. In diesem Beitrag verlässt sie die engen Grenzen der Technik und fragt, ob unsere Gesellschaft angemessen auf die sozialen Herausforderungen von Big Data reagiert.

[4]) Eine ähnliche Kostenexplosion konnte man vor einigen Jahren bei den Prämien für Berufshaftpflichtversicherungen von Hebammen beobachten. Sie zeigt, dass ein Fortschritt (hier der medizinische) zu Verwerfungen an anderer Stelle führen kann. Durch einen Geburtsfehler schwer behinderte Kinder können heute mit langen Lebenserwartungen rechnen, Rentenzahlungen und Behandlungskosten sind über Jahrzehnte zu finanzieren. Die Haftungsrisiken sind daher extrem gestiegen, die Versicherungen wurden für Hebammen nahezu unbezahlbar. Die Politik versucht, regulierend einzugreifen, bisher ohne Erfolg.