Sven Türpe, Annika Selzer, Andreas Poller, Mark Bedner

Denkverbote für Star-Trek-Computer?

Big Data, statistische Modelle und lernende Maschinen

Big Data steht nicht nur für Datenberge, sondern auch für ein Paradigma ihrer Verarbeitung. Lernende Systeme leiten aus Daten statistische Modelle ab, die heuristische Voraussagen und Entscheidungen treffen. Das Speichern aussagekräftiger Angaben tritt in den Hintergrund, im Vordergrund steht die Dateninterpretation.

Sven Türpe

ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie SIT

E-Mail: sven.tuerpe@sit.fraunhofer.de

Annika Selzer

Wissenschaftliche Mitarbeiterin am Fraunhofer-Institut für Sichere Informationstechnologie.

E-Mail: annika.selzer@sit.fraunhofer.de

Andreas Poller

ist wissenschaftlicher Mitarbeiter im Security Test Lab am Fraunhofer Institut für Sichere Informationstechnologie (SIT). Zu seinen Hauptforschungsthemen gehören interdisziplinäre Studien zum Privatsphärenschutz in Sozialen-Online-Netzwerken und Entwicklung sicherer Software.
E-Mail: andreas.poller@sit.fraunhofer.de

Dr. Mark Bedner

Referent für Konzerndatenschutz in Mannheim.

Was tut das Internet mit unseren Daten? Craig Nevill-Manning fasst es so zusammen: *„At Google, we joke about building the Star Trek computer – except that we're not actually joking."* [5] Der Star-Trek-Computer, das ist fürs Erste eine Statistikmaschine, die Korrelationen in Daten analysiert und daraus Modelle für allerlei Anwendungen bildet. Statistischen Inferenzmodelle verallgemeinern die beobachteten Zusammenhänge zu Regeln für heuristische Prognosen und Entscheidungen. Diese Art der Datenverarbeitung ähnelt dem Scoring. Neu ist der Einsatz zu vielfältigen Zwecken und die automatisierte Modellbildung aus beobachtetem Nutzerverhalten. Werbung, Sprachverarbeitung, Empfehlungssysteme und andere Funktionen nutzen heute solche Verfahren, die Anwendungsmöglichkeiten reichen jedoch weiter.

Mit dem Datenbankparadigma, das trotz Anpassungen noch sichtbare Spuren im Datenschutzrecht hinterlässt, hat diese Datenverarbeitung nur noch wenig gemein. Im Mittelpunkt steht nicht mehr das Speichern von Fakten, sondern die Optimierung von Berechnungsvorschriften. Auf lange Sicht stellt sich die Frage nach angemessenen allgemeinen Regeln. Die gegenwärtig geltenden Vorschriften zum Scoring sind zu spezifisch auf Bonitätsbewertungen und vergleichbare Anwendungen ausgerichtet.

Die Forschung behandelt das Thema seit langem unter dem Stichwort Profiling [10]. Aktuell wird es wegen zunehmender Verfügbarkeit von Daten und Verarbeitungstechnologien [7]. Welche Verunsicherung davon ausgeht, zeigte die öffentliche Reaktion auf das Forschungsprojekt SchufaLab@HPI [8].

1 Anpassung mit Nebenwirkungen

Unternehmen setzen statistische Modelle ein, um ihre Dienste an das Kundenverhalten anzupassen. Das Kundenverhalten liefert auch die Datengrundlage zur Modellbildung. Die Anwendungsmöglichkeiten sind vielfältig, einige verbreitete Beispiele sind:

- Empfehlungssysteme, die Nutzern Inhalte gemäß ihren mutmaßlichen Interessen empfehlen. Als Grundlage dienen explizite oder implizite Interessensbekundungen aller Nutzer, aus denen Profile gebildet werden [11].
- Optimierte Werbung, die im Interesse des Unternehmens möglichst hohe Reaktionsraten erzielen soll. Daten lassen sich online unmittelbar erfassen, im Einzelhandel helfen Kundenkarten und Coupons dabei.

- Komfortfunktionen, zum Beispiel Vorschläge zur Eingabevervollständigung oder zur Tippfehlerkorrektur , die aus den Eingaben anderer Nutzer abgeleitet sind.

Solche und andere Anwendungen erfassen das Verhalten eines Nutzerkollektivs in einer Vielzahl einzelner Datensätze, leiten daraus automatisiert ein Modell ab und benutzen dieses Modell als Berechnungsvorschrift, um in Einzelfällen Entscheidungen zu treffen oder Wahlmöglichkeiten zu bewerten. Dies hat Nebenwirkungen, die zunächst überraschend wirken, sich aber aus der Funktionsweise erklären lassen.

1.1 Schwangerschaftstest im Supermarkt

In Minneapolis ging ein Mann in einen Supermarkt, verlangte den Manager zu sprechen und beschwerte sich erregt über Werbesendungen der Supermarktkette. Die Werbung, gerichtet an seine Tochter im Highschool-Alter, hatte Produkte für werdende Mütter angepriesen. Ob der Supermarkt die junge Frau etwa für eine frühe Schwangerschaft begeistern wolle? Seine Beschwerde kam zu spät, wenig später beichtete ihm seine Tochter, dass sie ein Kind erwarte. Ihre Schwangerschaft war nicht Wirkung, sondern Auslöser der Werbesendungen. Die Supermarktkette hatte die Einkäufe ihrer Kundin erfasst und bestimmte Veränderungen im Einkaufsverhalten deuten auf eine Schwangerschaft hin. [4, 6]

1.2 AdWords mit Vorurteilen

In den Vereinigten Staaten bieten Dienste wie Instant Checkmate Auskünfte über Personen an, etwa über Vorstrafen und Verhaftungen; Polizeiprotokolle sind dort öffentlich zugänglich. Instant Checkmate verwendet Google AdWords, um bei der Suche nach Personennamen seine Dienstleistung anzupreisen, und verwendet dafür mehrere unterschiedlich formulierte Texte, in die der gesuchte Name eingesetzt wird. AdWords wählt Anzeigen in einem automatischen Auktionsverfahren unter anderem nach der gemessenen Klickrate aus [15].

Namen korrelieren mit der Zugehörigkeit zu Bevölkerungsgruppen, in den USA unter anderem mit der Hautfarbe. Eine Analyse der Anzeigen von *Instant Checkmate* zeigt, dass die Suche nach „weißen" Namen zum Anzeigentext *„[Name], Arrested?"* führt, während „schwarze" Namen Anzeigen wie *„Located: [Name]"* liefern. Ein nirgends explizit genanntes Merkmal führt zu unterschiedlicher Behandlung. Instant Checkmate bestreitet jede Diskriminierungsabsicht und verweist auf die Automatismen von AdWords[17].

1.3 Automatische Gerüchte

Die Suchmaschinen Google und Bing schlagen ihren Nutzern Suchbegriffe vor: Bei Beginn der Eingabe öffnet sich eine Auswahlliste möglicher Fortsetzungen, die sich nach jedem eingegebenen Zeichen ändert. Durch Auswahl eines Vorschlags kann der Nutzer den Vorgang abkürzen. Vorschläge folgen aus den Eingaben aller Nutzer.

Enthält die Eingabe einen Namen, so kann man Ergänzungsvorschläge als Aussagen über die benannte Person deuten. Weithin bekannt wurde dies, als die Ex-Präsidentengattin Bettina Wulff im Herbst 2012 ankündigte, Google zur Unterlassung bestimmter Vorschläge in Verbindung mit ihrem Namen auffordern zu wollen. Das Netz reagierte auf seine Weise: Nutzer suchten koordiniert nach dem Satz *„Bettina Wulff schmeckt lecker nach Hähnchen,"* den Google und Bing seitdem als Vorschlag anbieten. Einen vergleichbaren Fall entschied inzwischen der BGH: Verletzt ein Vorschlag Persönlichkeitsrechte, ist er nach Aufforderung zu entfernen (BGH VI ZR 269/12).

2 Modellbildung aus Nutzungsdaten

Statistische Inferenzmodelle sind Verarbeitungsvorschriften, die aus detailreichen Eingaben eine spekulative Ausgabe berechnen. Die Eingabe beschreibt einen Vorgang, Sachverhalt oder Gegenstand durch eine Reihe von Merkmalsausprägungen und heißt deshalb Merkmalsvektor. Als Ausgabe liefert die Berechnung mutmaßliche Werte anderer Merkmale, die in der Eingabe nicht enthalten sind – eine statistisch begründete Schlussfolgerung aus den Eingaben, die als Prognose, Entscheidung oder Schätzung interpretiert werden kann.

Lernalgorithmen leiten Modelle aus Trainingsdaten ab und generalisieren die darin beobachteten Korrelationen zu allgemeinen Regeln. Anders als die klassische Statistik gehen algorithmische Verfahren nicht von einer Theorie über bekannte Zusammenhänge aus, sondern sie passen die Modellparameter nur den Daten an [1, 2].

Wir skizzieren die Funktionsweise hier am Beispiel eines einfachen Klassifikators. In ihren Einzelheiten unterscheiden sich die eingesetzten Verfahren, die Grundprinzipien sind jedoch stets dieselben [3, 13, 14, 15].

2.1 Merkmale

Die Menge möglicher Eingaben spannt einen vieldimensionalen Merkmalsraum auf. Jedem Merkmal entspricht eine Dimension mit seinen möglichen Ausprägungen als Werte, jeder Merkmalsvektor ist ein Punkt in diesem Raum. Merkmale können unmittelbar in verwendeten Daten enthalten sein oder durch eine Vorverarbeitung daraus gewonnen werden. So zerlegt man Text oft in Wörter oder N-Gramme – kurze Zeichenfolgen fester Länge – deren Häufigkeit sich zählen lässt. Bildanalysen liefern Merkmale, die aus einzelnen Pixelwerten nicht hervorgehen, zum Beispiel Kanten. Merkmale lassen sich auch durch Transformation oder Anreicherung vorhandener Daten gewinnen, etwa indem man einer IP-Adresse den Domainnamen und andere Metadaten zuordnet.

2.2 Modell und Klassifikation

Ein Modell beschreibt mit seinen Parametern Regionen im Merkmalsraum und ordnet ihnen Klassen zu. Damit lässt sich für jeden Punkt des Raumes, also jeden Merkmalsvektor, die zugehörige Region oder, bei überlappenden Regionen, eine Rangfolge derselben bestimmen. Dies ist die Ausgabe, welche zum Beispiel als Entscheidung oder Prognose weiterverarbeitet wird. Die variablen Modellparameter legen die Abbildungsregeln fest, den Zusammenhang zwischen Ein- und Ausgaben. Sie werden so gewählt, dass das Modell seine Aufgabe möglichst oft gut erfüllt. Die Klassifikationsleistung hängt unter anderem davon ab, wie genau sich Klassen und ihre Begrenzungen als Regionen modellieren lassen.

2.3 Modellbildung durch maschinelles Lernen

Lernverfahren passen das Modell schrittweise an Daten an und minimieren damit seine Irrtumshäufigkeit. Jeder Lernschritt betrachtet einen einzelnen Merkmalsvektor und verbessert das Modell geringfügig für diesen einen Datensatz. Dazu dienen Trainingsdaten, deren beabsichtigte Klassifikation bekannt ist, oder irgendein Verfahren, das die ausgegebene Klasse für eine Eingabe als passend oder unpassend bewertet. Nutzer liefern solches Feedback zum Beispiel, indem sie Angebote akzeptieren oder ablehnen. Nach und nach nähert sich das Modell der gesuchten Funktion an, so gut es Verfahren und Daten zulassen. Das Modell repräsentiert dann die statistischen Zusammenhänge zwischen Merkmalsausprägungen der Eingaben und der Klassen als Ausgaben. Ist die Leistungsgrenze erreicht, verbessert weiteres Lernen nicht mehr die Klassifikationsleistung, sondern kann sie sogar wieder verschlechtern.

3 Neuer Schwerpunkt: Schlussfolgern

In der klassischen Datenverarbeitung steht die strukturierte Speicherung im Mittelpunkt. Inferenzmodelle betonen demgegenüber Berechnungen anhand gespeicherter oder flüchtiger Daten. Darin ähneln sie Scoring-Verfahren.

3.1 Datenbanken

Eine Datenbank speichert verknüpfte Einzelangaben in einem vorgegebenen Strukturschema. Der Datenbankinhalt kann Lücken haben, sofern das Schema undefinierte Werte für eine Angabe erlaubt. Das Schema kann nachträglich um Felder für zusätzliche Angaben erweitert werden.

Nutzer und Anwendungen fragen Daten ab. Jede Abfrage legt einen Satz auszugebender Datenfelder fest sowie Werte oder Wertebereiche einzelner Angaben als Auswahlkriterium. Genutzt werden abgefragte Daten außerhalb der Datenbank zu irgendeinem Zweck, der technisch nicht eingeschränkt ist. Gespeicherte Angaben behalten von der Erfassung über alle Abfragen und Nutzungen dieselbe Bedeutung.

Verknüpft eine Datenbank Identitätsmerkmale mit anderen Angaben, so lassen sich alle vorhandenen Angaben zu einer Identität abfragen, aber auch alle Identitäten, auf die bestimmte Angaben zutreffen. Ein Profil im Sinne des Datenbankparadigmas entsteht durch Akkumulation von Einzelangaben zu einer Person als Ergebnis der Verarbeitung.

3.2 Scoring

Das Scoring [12, 18] verdichtet einen Satz von Einzelangaben (Merkmalen) zu einer Bewertung. Im Wesentlichen handelt es sich um eine Berechnungsvorschrift für die Bewertung, zum Beispiel um eine Scorecard, die einzelne Merkmale unterschiedlich gewichtet und miteinander verrechnet. Der Berechnung zugrunde liegt ein Modell des statistischen Zusammenhangs zwischen Merkmalswerten und der bewerteten Eigenschaft. Das Scoring liefert eine statistisch begründete Prognose, so dass die berechnete Bewertung häufig richtig ist, wenn die entsprechenden Merkmale vorliegen.

Scoring-Verfahren werden insbesondere eingesetzt, um die Bonität von Kunden einzuschätzen und damit das Risiko bei Kreditgeschäften zu prognostizieren. Das Scoring erfolgt dann anhand von Vertragsdaten, Angaben über die finanziellen Verhältnisse sowie soziodemografischen Daten. Das Ergebnis ist zum Beispiel eine Risikoklasse entsprechend dem prognostizierten Ausfallrisiko, die Entscheidungen über den Vertragsabschluss oder die Konditionen beeinflusst. Scoring-Verfahren können sowohl auf gespeicherte als auch auf flüchtige Daten angewandt werden.

Identitätsmerkmale sind für das Scoring als solches belanglos: Da eine individuelle Prognose nicht möglich ist, behilft man sich, indem man statistische Erfahrungswerte auf ein Individuum überträgt. Ein Profil im Sinne des Scorings ist zum einen das Merkmalsprofil einer Gruppe, deren statistisches Gruppenverhalten die Bewertung begründet [9], zum anderen das damit abgeglichene persönliche Profil eines Betroffenen. Individuelle Abweichungen und Sonderfälle bleiben unberücksichtigt – oder werden am Modell identifiziert.

3.3 Theorielose Modelloptimierung

Statistische Inferenzmodelle verallgemeinern die Prinzipien des Scoring; maschinelles Lernen automatisiert die Ermittlung von Erfahrungswerten und ihre Übersetzung in eine Berechnungsvorschrift. Anstelle ausgewählter Merkmale und einer Theorie über Zusammenhänge verwendet man alle verfügbaren Daten und sucht darin algorithmisch nach Korrelationen, die für eine Prognose, Entscheidung oder Dateninterpretation nützlich sind. Die Nützlichkeit bemisst sich nach gemessenen Erfolgsraten. So gewonnene Erfahrungswerte gelten für die konkrete Anwendung, sie sind nur durch die beobachteten Daten und den Prozess der Modellbildung begründet.

Interaktive Dienste können das Nutzerverhalten unmittelbar auswerten. Mit ihren Reaktionen auf gewählte Parameter und angebotene Inhalte bewerten Nutzer implizit das zugrundeliegende Modell, dieses Feedback dient der Modelloptimierung. Funktionen eines Dienstes passen sich so dem statistischen Verhalten der Nutzer an, unabhängig von seinen Gründen und Ursachen aufgrund automatisierter Experimente. Gegenstand der Modellierung sind Nutzungsvorgänge, etwa der Abruf von Inhalten, aber auch Sachverhalte, auf die sich Nutzungsvorgänge beziehen, zum Beispiel die Zuordnung von Namen zu Gesichtern und damit zu deren biometrischen Merkmalen.

Das Speichern strukturierter Daten wird dabei zum Hilfsvorgang. Im Mittelpunkt steht nun das fortlaufend angepasste Modell als Verarbeitungsvorschrift, oft für flüchtige Daten. Das einzelne Modell hat einen spezifischen Zweck, seine Ausgaben können aber als Merkmal in Berechnungen anderer Modelle einfließen. Der Profilbegriff ähnelt dem des Scoring, aber Merkmalsprofile beschreiben anwendungsabhängig die unterschiedlichsten Gegenstände. Von der konkreten Anwendung hängen auch die möglichen Folgen für Nutzer und andere Betroffene ab.

4 Risiken

Als Verallgemeinerung des Scorings erben Anwendungen statistischer Modelle dessen Besonderheiten, Risiken und Probleme. Neue Aspekte ergeben sich aus der automatisierten Modellbildung aus Nutzungsdaten und dem breiten Anwendungsspektrum.

4.1 Scoring Reloaded

Viele grundlegende Fragen und Probleme im Zusammenhang mit dem Einsatz statistischer Modelle sind bereits aus der Debatte um das Verbraucher-Scoring [19, 20] bekannt:

- Persönlichkeitsrechte sind vor allem durch die Anwendung statistischer Modelle bedroht, weniger durch deren Entwicklung.
- Merkmale unterscheiden sich in ihrer Aussagekraft, Verlässlichkeit und Plausibilität. So sind etwa soziodemografische Merkmale ungenauer als persönliche Angaben. Unabhängig von ihrer statistischen Eignung sind bestimmte Merkmale als Bewertungskriterium inakzeptabel, insbesondere aufgrund von Diskriminierungsverboten.
- Modelle repräsentieren statistische Erfahrungswerte über Personengruppen, die durch Merkmale repräsentiert sind. Individuelle Unterschiede außerhalb dieser Merkmale bleiben unberücksichtigt. Modellgestützte Prognosen übertragen das Gruppenverhalten spekulativ auf Individuen, die resultierenden Aussagen können im Einzelfall falsch sein.
- Die Transparenz für und die Kontrolle durch Betroffene erfordert besondere Maßnahmen, etwa um den Zusammenhang zwischen Merkmalen und Bewertung zu erklären und um flüchtige Daten kontrollierbar zu machen.

Ein grundlegender Konflikt besteht zwischen dem Versprechen mathematischer Objektivierung auf der einen und dem heuristischen Charakter des Verfahrens auf der anderen Seite. Wahrscheinlichkeitsaussagen entziehen sich der direkten Prüfung und Korrektur.

4.2 Neue Risikofaktoren

Während sich die vorgenannten Besonderheiten des Scorings gut am repräsentativen Beispiel der Bonitätsbewertung diskutieren ließen, ist die Vielfalt neuer Anwendungen statistischer Modelle unübersichtlich. Einige Tendenzen lassen sich dennoch erkennen:

- Modelle entstehen automatisiert aus verfügbaren Daten über das Nutzungsverhalten und werden fortlaufend angepasst. Die Datenqualität variiert, Manipulationen sind möglich. Modelle bilden das statistische Nutzungsverhalten ab, ohne die Hintergründe zu analysieren.
- Gegenstand der Modellierung sind Nutzungsvorgänge. In welchem Maße die verwendeten Daten und gezogenen Schlüsse Aussagen über Personen treffen, unterscheidet sich von Anwendung zu Anwendung. Personenbezogene Aussagen können auch nachträglich durch Interpretation zustande kommen.
- Modelle und ihre Schlussfolgerungen bleiben selbst mit Erklärung schwer nachvollziehbar, da sie nur auf Beobachtungen und daraus abgeleiteten Regeln beruhen. Die offenkundigen Merkmale und Schlussfolgerungen können durch Korrelation implizite Informationen tragen.

Betroffene können damit kaum noch intuitiv verstehen, was ihre Daten aussagen, denn dies hängt von den Interpretationsfähigkeiten des Verarbeiters ab: Was kann ein Supermarkt aus meinem Einkaufsverhalten herauslesen? In welchem Maße ist Werbung auf meine Person zugeschnitten, oder hängt die Auswahl doch nur vom Anzeigekontext und den Klickzahlen ab? Was ändert sich wenn ich Daten unterdrücke oder verschleiere? Gleichzeitig verbreitert sich mit dem Anwendungs- auch das Risikospektrum. Korrekturvorschläge für Tippfehler werden kaum Besorgnis auslösen, die technisch verwandte Eingabevervollständigung schaffte es bis vor den BGH. Risiken und Bedrohungen ergeben sich aus konkreten Anwendungen, weniger aus Daten und Technik schlechthin.

5 Passt das Recht noch zur Technik?

Das Recht auf informationelle Selbstbestimmung garantiert Bürgern, zu erfahren und zu entscheiden, „wer was wann und bei welcher Gelegenheit über sie weiß“ (BVerfGE 65,1). Den Datenschutz als Realisierung dieses Rechts stellt das neue Paradigma mit seiner Anwendungsvielfalt und zunehmender Verbreitung vor Herausforderungen [16].

Grundsätzlich lässt sich das geltende Datenschutzrecht nach dem Vorbild der Scoring-Diskussion [19, 20] auf modellbildende und modellgestützte Verfahren anwenden, zumal der Gesetzgeber vor einigen Jahren spezifische Regelungen zum Scoring (§ 28b, § 34 (2) und (4) BDSG) erlassen hat. Den Anbietern von Internetdiensten gestattet § 13 (3) TMG die Erstellung von Nutzungsprofilen, sofern Pseudonyme verwendet werden. Jedoch stellt sich die Frage, ob daraus ein angemessener Rechtsschutz resultiert.

5.1 Grundsätze

Big Data und das Schlussfolgern mit automatisiert angepassten Modellen kollidieren mit einigen Grundsätzen und Denkweisen des Datenschutzes, jedenfalls in ihrer gegenwärtigen Formulierung: Personenbezogene Daten, Datensparsamkeit, Transparenz und Kontrolle sowie der Betonung des Speicherns als Kern der Verarbeitung.

Der Personenbezug von Daten folgt aus der Möglichkeit, sie einer Person zuzuordnen, insbesondere anhand von Identitätsmerkmalen. Die Pseudonymisierung (§ 3 (6a) BDSG) ersetzt Identitätsmerkmale reversibel durch andere Kennzeichen. Die Anonymisierung (§ 3 (6) BDSG) verhindert jede Zuordnung zu einer Person mit vernünftigem Aufwand. Dem liegt die Vorstellung von strukturierten Datensätzen zugrunde.

Modelle als Berechnungsvorschriften haben demgegenüber einen Anwendungskontext, der die gewonnenen Aussagen explizit oder implizit auf Personen bezieht. Im Hinblick auf die Schutzziele kommt es auf den Gehalt der gewonnenen Aussage an sowie darauf, wer diese Aussage in welcher Weise nutzt und wie viel Kontrolle Betroffene darüber haben.

Die Forderung nach Datenvermeidung und Datensparsamkeit (§ 3a BDSG) unterstellt, dass Risiken proportional zur Menge verarbeiteter personenbezogener Daten wachsen, und betont die Pseudonymisierung und Anonymisierung als Lösungsansatz. Dagegen kommt es beim modellgestützten Schließen vor allem auf die Datenqualität an, auf die Aussagekraft verwendeter Merkmale und die Verwendung gewonnener Vermutungen. Je nach Anwendung folgen Risiken nicht immer aus höherer Genauigkeit der Berechnung, sondern umgekehrt aus Fehlern. Die großen Datenmengen, für die Big Data steht, sind vor allem als Kollektivdaten für die Modellbildung von Interesse; Risiken für einzelne Betroffene ergeben sich aber vor allem aus der Modellanwendung.

Ähnlich wie beim verwandten Scoring beeinträchtigen die Funktionsprinzipien der Technik die Transparenz und Kontrolle, so dass kompensierende Maßnahmen nötig werden. Das Problem stellt sich nun nicht mehr für eine relativ überschaubare Anzahl von Anwendungen und Zwecken, sondern grundsätzlich: Den Grundsatz der Direkterhebung beim Betroffenen (§ 4

(2) BDSG) hat die Technik überholt, die interessierenden Angaben werden nun aus anderen berechnet. Explizite Angaben und gespeicherte Daten sind nur noch ein Mittel zum Zweck, und ihre Aussagekraft lässt sich ohne Kenntnis der anwendbaren Modelle nicht bewerten. Umgekehrt können aus Modellen gewonnene Angaben Rückschlüsse auf andere Merkmale erlauben, auch auf solche, die nicht explizit als Eingabe verwendet wurden und deren Verwendung vielleicht gar nicht zulässig wäre.

Im Fokus des BDSG steht die Verarbeitung personenbezogener Daten – das Speichern, Verändern, Übermitteln, Sperren und Löschen (§ 3 (4) BDSG) – sowie das Erheben als Voraussetzung dafür. Alle anderen Vorgänge fallen unter den Auffangbegriff der Nutzung. An die Stelle der Speicherung, die zum Hilfsvorgang wird, tritt nun aber die wiederholbare flüchtige Berechnung als Kern der Verarbeitung. Deutlich gehen darauf bislang nur die Auskunftspflichten über Scorewerte (siehe unten) ein, während die allgemeinen Benachrichtigungs- und Auskunftspflichten (§§ 19, 19a, 33 und 34 BDSG) ihrem Wortlaut nach bei der Erhebung bzw. der herkömmlichen Verarbeitung ansetzen.

Diese vier Punkte mögen genügen, um den Diskussionsbedarf zu illustrieren. Eine tiefere Analyse würde mehr Raum erfordern als hier zur Verfügung steht.

5.2 Scoring-Regeln als Vorbild?

Das Verbot automatisierter Einzelentscheidungen, soweit sie rechtliche Folgen oder erhebliche Beeinträchtigungen nach sich ziehen (§ 6a BDSG), lässt sich ohne Schwierigkeiten auf die hier behandelten Verfahren anwenden. Die Einschränkung erlaubt die erforderliche Differenzierung zwischen unterschiedlich kritischen Anwendungen, so dass etwa bloße Komfortfunktionen wie Eingabehilfen oder Empfehlungssysteme davon ausgenommen sind.

Mit der Einführung von § 28b BDSG und darauf aufbauenden Regelungen in § 34 BDSG ist der Gesetzgeber auf einige grundsätzliche Probleme bereits eingegangen: auf den Wahrscheinlichkeitscharakter modellgestützter Prognosen, auf die Flüchtigkeit von Berechnungen anstelle der Speicherung sowie auf das Transparenzproblem und die Abwägung zwischen Betroffenenrechten und Geschäftsgeheimnis. Allerdings zielen diese Vorschriften formal und ihrem Inhalt nach klar auf das klassische Scoring durch Unternehmen und Auskunfteien. Analoge Regelungen für den öffentlichen Bereich fehlen gänzlich.

Eine Verallgemeinerung dieser Regelungen müsste auf die Anwendungsvielfalt eingehen. Sinnvoll erscheint die Differenzierung nach Auswirkungen und Risiken, etwa analog zu § 6a BDSG. Hinsichtlich der Auskunftspflichten ist zu beachten, dass anders als beim Scoring nicht unbedingt eine Person Gegenstand der Berechnungen ist, sondern dass häufig Nutzungsvorgänge mit Personenbezug behandelt werden. Dabei werden Vorgangsmerkmale und persönliche Angaben gemischt und Modellanwendungen erfolgen mit höherer Frequenz. Alle Ergebnisse über längere Zeit zu speichern, um gegebenenfalls Auskunft erteilen zu können, könnte sich als ungeeignetes Mittel erweisen.

Soweit Datenschutzprobleme spezifisch für Internetdienste sind, bietet sich die Ergänzung des TMG um geeignete Regelungen an. Wünschenswert erscheint auch die Ergänzung der elektronischen Auskunftsmöglichkeit (§ 13 (7) TMG) um eine Grundlage für direkte Eingriffe der Nutzer, wie sie etwa bei Empfehlungssystemen und personalisierter Werbung zum Teil angeboten wird.

6 Fazit

Big Data steht für einen technischen Umbruch, der für den Datenschutz ähnlich bedeutsam scheint wie einst der Übergang vom Karteischrank zur Datenbank. Computer speichern nicht mehr Angaben über Personen mit klarer Bedeutung, sondern sie berechnen heuristisch Aussagen, die ihnen so niemand mitgeteilt hat. Die Berechnungsregeln lernen sie statistisch aus beobachtetem Verhalten. Echte Star-Trek-Computer sind das noch nicht, doch auf Nutzer und Betroffene wirken sie so, zumal sich ihre Funktionsweise nicht intuitiv erschließt.

Die Ziele des Datenschutzes haben damit mehr Berechtigung denn je. Seine Mittel müssen sich der Entwicklung anpassen, um weiterhin effektiv die informationellen Selbstbestimmung zu ermöglichen. Das Anwendungsspektrum ist breit, die Risiken variieren ebenso wie der Nutzen, viele Einsatzmöglichkeiten sind noch gar nicht erkundet. Vielleicht muss sich der Datenschutz am Ende von den Daten lösen und stattdessen auf Persönlichkeitsrechte in einem denkenden – und irrenden – Netz konzentrieren.

Literatur

[1] Anderson, C.: The End of Theory: The Data Deluge Makes the Scientific Method Obsolete, *Wired Magazine*, 16 (2008) 07.

[2] Breiman, L.: Statistical Modeling: The Two Cultures. *Statistical Science*, 16 (2001) 3, S. 199–231.

[3] Domingos, P.: A Few Useful Things to Know About Machine Learning. *Commun. ACM*, 55 (2012) 10, S. 78–87.

[4] Duhigg, C.: How Companies Learn Your Secrets. http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

[5] Interview mit Craig Nevill-Manning, Research at Google, https://plus.google.com/+ResearchatGoogle/posts/Cto6zsujfJo

[6] Greengard, S., Advertising gets personal. *Commun. ACM*, 55 (2012) 8, S. 18–20.

[7] Hartzog, W. & Selinger, E., Big Data in Small Hands. *Stanford Law Review Online*, 2013.

[8] Hasso-Plattner-Institut kündigt Schufa-Forschungsprojekt, heise.de, 08.06.2012.

[9] Hildebrandt, M.: Profiling: From Data to Knowledge. *DuD*, 30 (2006) 9, S. 548–552.

[10] Hildebrandt, M. & Gutwirth, S. (Hrsg.): *Profiling the European Citizen*. Springer, 2008.

[11] Konstan, J. A. & Riedl, J., Recommended for You. *IEEE Spectrum*, 49 (2012) 10, S. 54–61.

[12] Korczak, D.: *Verantwortungsvolle Kreditvergabe*. GP Forschungsgruppe, 2005.

[13] MacKay, D. J. C.: *Information Theory, Inference, and Learning Algorithms*. Cambridge University Press, 2003.

[14] Mitchell, T. M. (1999) Machine Learning and Data Mining. *Commun. ACM*, 42 (1999) 11, S. 30–36.

[15] Rajaraman, A. & Ullman, J. D.: *Mining of Massive Datasets*. Cambridge University Press, 2011.

[16] Schermer, B. W.: The Limits of Privacy in Automated Profiling and Data Mining. *Computer Law & Security Review*, 27 (2011) 1. 45–52.

[17] Sweeney, L.: Discrimination in Online Ad Delivery. *Commun. ACM*, 56 (2013) 5, S. 44–54.

[18] Kamp, M. & Weichert, T.: *Scoringsysteme zur Beurteilung der Kreditwürdigkeit – Chancen und Risiken für Verbraucher*. ULD, 2006.

[19] Weichert, T.: Datenschutzrechtliche Anforderungen an Verbraucher-Kredit-Scoring. *DuD*, 29 (2005) 10, S. 582–587.

[20] Weichert, T.: Verbraucher-Scoring meets Datenschutz. *DuD*, 30. (2006) 7, S. 399–404.