Predictive Analytics im Spannungsfeld zur Privatheit

Holger Berens, Leiter KIS

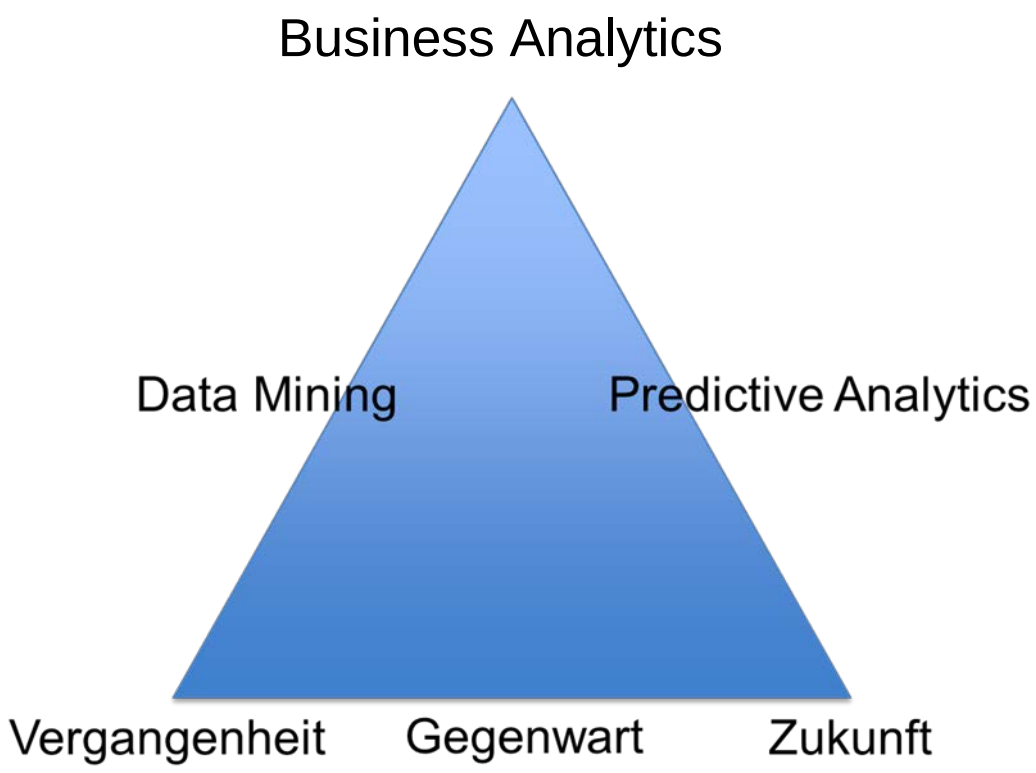
Google, Youtube, Whatsapp und Facebook vermelden, dass jeweils über eine Milliarde Menschen diese Dienste weltweit nutzen. Mit anderen Worten stellt jeder siebte Mensch in der Welt seine persönlichen Daten kostenlos zur Verfügung, ohne genau zu wissen, was mit seinen Daten passiert. Der Aufsatz soll in die Problematik der sogenannten **Predictive Analytics** einführen und den Bogen zum Datenschutz spannen.

Spiegel online vermeldet am 28.02.2015: „**Predictive Policing**: Polizei will Straftaten per Software vorhersagen“

Ohne in die Einzelheiten zu gehen, geht es darum Straftaten vorherzusagen. Anhand von Tatmustern in der Vergangenheit berechnet Software die Wahrscheinlichkeit, mit der in einer bestimmten Gegend z. B. ein Einbruch geschehen wird. In den USA wird im Laufe dieses Jahres flächendeckend Predictive Policing eingeführt. In Deutschland laufen die ersten Versuche. Aber auch die private Sicherheitswirtschaft setzt vermehrt auf diese Analysen, so sollen Einkaufscenter oder aber Großveranstaltung analysiert werden, um proaktiv Gefährdungslagen vorherzusagen und die Risiken zu minimieren.

Auf Unternehmen übertragen bedeutet das, dass wirtschaftliche, zukünftige Zusammenhänge prognostiziert werden können, um strategische Entscheidungen zu treffen und sich so einen Wettbewerbsvorteil zu verschaffen. Hier hat sich der Begriff **Predictive Analytics** eingebürgert.

Um zu verstehen, worum es überhaupt geht, ist es notwendig einen Überblick über die einzelnen Methoden der Datensammlung zu geben.



Ausgangspunkt der Methoden ist **Business Intelligence**. Hier werden Geschehnisse in der Vergangenheit untersucht und aus den Daten Antworten zur Gegenwart generiert. Es geht hierbei vor allen Dingen um Fragen zum Geschehen, zur Menge, Häufigkeit oder den Ursachen eines Ereignisses. Ziel von Business Intelligence ist es, aufgrund von geschäftsrelevanten Daten sich Überblick über das Unternehmen und die Querverbindungen zu verschaffen. Aufgrund der Auswertung dieser Daten können Unternehmensprozesse kontrolliert und gesteuert werden. Dies bedeutet betriebswirtschaftlich fundiert entscheiden zu können.

In diesem Zusammenhang fällt häufig der Begriff **Date Mining**. Data Mining ist die Anwendung von Methoden und Algorithmen zur digitalen Expertise empirischer Zusammenhänge. Zum Beispiel kann so eruiert werden, welche Waren von wem häufig zusammen gekauft werden (typische Warenkörbe) oder welche Bedingungen für die Kundentreue Voraussetzungen sind. Data Mining ist somit die Grundlage, um strategische unternehmerische Entscheidungen über Business Intelligence vornehmen zu können und Muster in Datenbeständen zu erkennen. In der Regel werden in den Unternehmen sogenannte **Data Warehouse** eingerichtet. Dies ist eine zentrale Datenbank, die alle verfügbaren Daten speichert. Aus verschiedenen Datenbanken werden Daten, die für unterschiedliche Zwecke gespeichert wurden, in das Data Warehouse integriert, um strategische Analysen und Entscheidungshilfen zu ermöglichen.

Business Analytics geht darüber hinaus und blickt in die Zukunft. Es werden Szenarien durchgespielt und darauf aufbauend Handlungsalternativen aufgezeigt. Es geht hierbei um die Datenveredelung Ziel ist es, Antworten nicht nur auf die Frage: „Was war?“, sondern auch: **„Was wird sein?“** zu finden, um so Zukunftsprognosen aufstellen zu können.

Predictive Analytics ist eine Unterart der Business Analytics. Predictive Analytics versucht mit Hilfe von Datenmodellen Vorhersagen über mögliche Ereignisse in der Zukunft zu treffen. Es werden Methoden wie maschinelles Lernen, Elemente der Spieltheorie oder Simulationsverfahren eingesetzt. Darüber hinaus können durch Einsatz von Text-Mining Aussagen auch aus sozialen Netzwerken (Artikel, Blogs, Tweets, Facebook-Inhalte etc.) untersucht und daraus gemeinsame Strukturen ermittelt werden.

Immer mehr wird in Unternehmen die **Human Resources** bzw. **People-Analytics** eingesetzt, um Personalentscheidungen zu treffen. Es werden nicht nur Mitarbeiterdaten aus dem eigenen Unternehmen ausgewertet, sondern externe Daten, die mit den internen Daten verglichen werden, um Personalentscheidungen auf Grund der erhobenen Daten zu treffen.

Ein Schlagwort in diesem Zusammenhang ist, dass das Unternehmen unter Umständen früher als der Mitarbeiter weiß, ob und wann er kündigen möchte.

So arbeitet schon ein deutsches Unternehmen mit einer solchen Software für die Personalgewinnung. Das Unternehmen hat zunächst ermittelt, welche Mitarbeiter besonders lange im Unternehmen arbeiten. Dann wurden die Gemeinsamkeiten untersucht. Bewerbungen werden daher auf diese Merkmale untersucht und dienen zur Entscheidung. Wichtig ist auch, dass die übermäßige Nutzung von sozialen Netzwerken ein Ausschlusskriterium ist.

All diese Methoden kann man auf einen einfachen gemeinsamen Nenner bringen. Erforderlich ist immer:

- Daten sammeln,
- Daten strukturieren,
- Daten auswerten.

Privatheit (Privacy)

Schöne neue Datenwelt, die unabdingbar innerhalb eines zuverlässigen und verhältnismäßigen Rechtsrahmen erfolgen muss. In diesem kleinen Aufsatz wird nur der deutsche Rechtsrahmen vorgestellt.

Privatheit umfasst viele Bereiche des menschlichen Lebens, weshalb die Definitionen von Privatheit auch sehr unterschiedlich sind.

Eine bekannte Definition stammt von Louis D. Brandeis:

„[Privacy is] The right to be left alone".

Das Bundesverfassungsgericht hat schon1983 im Volkszählungsurteil zur Privatheit das Recht auf **informationelle Selbstbestimmung** wie folgt definiert:

> „[Es ist die] Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen".

Damit hat das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung auf Grundrechtniveau gehoben, sodass dieses Recht verfassungsrechtlich determiniert ist. Allerdings sind die Grundrechte unserer Verfassung Abwehrrechte gegen den Staat. Der Staat also darf nicht ungerechtfertigt in die Grundrechte eingreifen und der Bürger kann sich gegen solche Eingriffe wehren.

Das bedeutet aber, dass diese Grundrechte nicht unmittelbar zwischen den Bürgern bzw. Bürger und Unternehmen gelten. Es besteht aber der Auftrag für den Gesetzgeber durch Gesetze, die auch zwischen den Privatpersonen gelten, die so definierte Privatheit schützen.

In Deutschland ist dieser Auftrag durch das Bundesdatenschutzgesetz umgesetzt.

Für die Wirtschaft ist vor allem die Verarbeitung und Weitergabe von Daten wichtig, die jeder Einzelne schützen möchte.

Privatheit kann man in zwei Bereiche aufteilen:

- Zugriffskontrolle,
- Verwertung der Daten.

Zugriffskontrolle

bedeutet, dass grundsätzlich personenbezogene Daten im System des jeweiligen Nutzers durch ihn selbst gespeichert sind und der Nutzer selbst den Zugriff für Dritte öffnen kann. Zugriffskontrolle liegt daher im Einflussbereich des Nutzers. Er hat es selbst in der Hand, das System sicher zu machen, durch entsprechende technische Maßnahmen oder aber durch die Vergabe von Zugriffsrechten.

Verwertung der Daten

Sobald allerdings personenbezogene Daten an Dritte übermittelt werden, hat der Nutzer keinen Einfluss mehr auf diese Daten. Daher muss es rechtlich gewährleistet sein, dass diese Daten nicht gegen den Willen des Nutzers ausgewertet, verändert oder weitergegeben werden. Da mithin der Nutzer keinen technischen Einfluss auf die Verwertung der Daten durch Dritte hat, muss der Staat durch ein funktionierendes Rechtssystem dafür sorgen, dass nicht rechtswidrig diese Daten genutzt werden.

Und genau hier setzt das Datenschutzrecht an.

Hinsichtlich des Datenschutzes ist zu unterscheiden, ob Daten personenbezogen sind oder nicht. **Personenbezogene Daten** sind alle Daten, die auf eine bestimmbare Person hinweisen oder ihr zugeordnet sind. Hier hilft das „Grundrecht" auf informationelle Selbstbestimmung zu (BVerfGE 65,1).

Jeder darf selbst bestimmen, welche Information über ihn zu welcher Zeit zur Verfügung stehen darf. Hier besteht allerdings das Spannungsverhältnis zu Business Analytics.

Um Aussagen über Personen**gruppen** machen zu können, ist die Sammlung und Auswertung personenbezogener Daten unabdingbar. Genau hierin besteht das Spannungsverhältnis zu Business Analytics.

Wenn man sich die Datenschutzprinzipien anschaut:

- Datensparsamkeit
- Zweckbindung
- Einwilligung
- Auskunftsrecht
- Eingriffsrecht

erkennt man, dass schon die ersten drei Prinzipien im Widerspruch zur Business Analytics stehen.

Liest man den

> **„§ 3a Datenvermeidung und Datensparsamkeit BDSG**
>
> Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen ……."

so wird klar, wie schwierig die Abwägung zu den oben genannten Methoden rechtlich ist. Diese Vorschrift steht im klaren Widerspruch zu Data Mining usw. Sind doch gerade diese Methoden auf eine sehr große Menge an Daten angewiesen. Hier muss die Aufgabe des Rechts sein, ein rechtlich vernünftiges Verhältnis zwischen dem berechtigten Interesse der Wirtschaft an der Nutzung von Daten und dem Schutzinteresse des Einzelnen zu schaffen.

Es kommt hier zunächst auf den Einzelnen an, da es sich um **Verbote mit Erlaubnisvorbehalten** handelt:

> **„§4 BDSG: Zulässigkeit der Datenerhebung, -verarbeitung und –nutzung BDSG**
>
> ….Erhebung, Verarbeitung und Nutzung personenbezogener Daten [sind] nur zulässig, soweit gesetzlich erlaubt oder der Betroffene einwilligt …..".

Eine solche Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

Kurz gesagt muss also eine entsprechende Datenschutzerklärung so formuliert sein, dass der „einfache" Nutzer sie verstehen kann und selbständig entscheiden kann, ob er einwilligt oder nicht. Wenn man die entsprechenden Erklärungen der Unternehmen im Netz liest, erfüllen die allermeisten nicht diese Anforderungen.

Um das Rechtsproblem der Zulässigkeit von Business Analytics und alle anderen Arten von Datensammlungen zu wirtschaftlichen Zwecken zu verstehen, reicht es aus, den folgenden Paragraphen in Ruhe zu lesen:

> **„§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke BDSG**
>
> (1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig
>
> 1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
>
> 2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
>
> 3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt."

Es bedarf also einer Abwägung zwischen den berechtigten Interessen des einzelnen Unternehmens, Business Intelligence einzusetzen und dem Recht des Einzelnen an seinen personenbezogenen Daten.

Es ist unter Rechtsfachleuten streitig, ob zum Zwecke des Business Intelligence in all seinen Ausformungen eine Einwilligung vorliegen muss.

Wenn die geschilderten Methoden ausschließlich zur Marktanalyse und als Grundlage der Unternehmensstrategie eingesetzt werden, könnte man der Meinung sein, dass eine Einwilligung nicht erforderlich ist. Es geht ja gerade nicht um den einzelnen Kunden, Es sollen ja nur Muster erkannt werden.

Um jedoch Muster erkennen zu können, müssen personenbezogen Daten erhoben werden und darüber hinaus auch auf Vorrat gespeichert werden und das auch noch ohne Zweckbindung. Hinzu kommt, dass der Einzelnen dann auch nicht hierüber informiert wurde und auch nicht entscheiden kann, wie seine Daten verwendet werden. Damit muss man schlussfolgern, dass alle Formen und Business Intelligence einer Einwilligung bedürfen. Hierbei ist noch nicht der Spezialfall der Human Resources Analytics beleuchtet. Hier geht ohne Betriebsvereinbarung mit dem Betriebsrat gar nichts.

Ganz klar ist, dass wenn konkrete personenbezogene Kundenprofile erstellt werden auf jeden Fall eine Einwilligung unabdingbar ist.

Fazit:

Technisch ist alles möglich. Man kann Verhaltensmuster anhand von Datensammlungen erkennen und auch vorhersagen. Dies bedeutet eigentlich, dass wir als Einzelpersonen und auch Arbeitnehmer absolut gläsern sind. Berücksichtigt man auch noch, dass Daten aus den sozialen Netzwerken gefischt werden, die wir ja im Prinzip freiwillig offenlegen, wird es klar, dass eindeutige rechtliche Regelungen unabdingbar sind. Es ist darüber hinaus dringend erforderlich, den Begriff Privatheit rechtlich sicher einzuordnen. Wegen der Globalisierung ist ein einheitliches Datenschutzrecht unabdingbar und Predictive Analytics muss rechtlich geregelt werden.

Eine Möglichkeit wäre, dass die personenbezogenen Daten als sogenanntes verkehrsfähiges Gut angesehen werden und der Einzelne diese durch Vertrag an Dritte „verkauft". Man kann

grundsätzlich sagen, dass alle Dienste, die nichts kosten mit den personenbezogenen Daten bezahlt werden und Dritte – ohne Einfluss der Berechtigten – zur Zeit Geld damit verdienen.