Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut?*

Dr. Bruno Baeriswyl

Datenschutzbeauftragter des Kantons Zürich

1. Einleitung

Mit dem Einsatz von Informationstechnologie in fast allen Lebensbereichen ist die Menge der gespeicherten Daten dramatisch angewachsen. Da die Speicherung der Daten dank Neuerungen und Verbesserungen in der Computertechnologie immer weniger ein bestimmender Kostenfaktor ist, hat sich das Schwergewicht auf die Nutzbarmachung und Auswertung dieser Daten verlegt. Investitionen werden in Konzepte getätigt, die eine gewinnbringende Nutzung der Daten versprechen.

Die Aufbereitung von Daten mittels so genannter Data-Warehousing-Konzepte ist nicht neu. Vielmehr wurde in grossen Konzernen schon in den siebziger Jahren versucht, die immense Menge der gespeicherten Daten funktionsgerecht aufzubereiten, das heisst entsprechende Programme zu entwickeln, die die relevanten Daten in so genannten Management-Informationssystemen erfassten. Diese technischen Möglichkeiten und ihre Weiterentwicklungen haben in den letzten Jahren insbesondere die Marketingfachleute zu neuen Begeisterungen animieren können. «One-to-one»-Marketing – der einzelne Kunde im Fokus und nicht mehr nur ein Kundensegment, lange ein Schlagwort und kaum realistisch – ist plötzlich auf Knopfdruck verfügbar.

Die Diamantensuche im Informationsgebirge mit Data-Warehousing- und Data-Mining-Konzepten ist heute das Thema im so genannten «Customer Relationship Management». Einer, der nicht wenig zu diesem Datenberg beiträgt, ist der Konsument. Er hinterlässt seine Datenspuren, wenn er die Kreditkarte benutzt, ein Auto mietet, telefoniert, eine Flugreise bucht oder nur gerade seine Lebensmittel einkauft. Wenn man ihm noch einige Anreize gibt wie ein Vielfliegerprorgramm oder Rabatte und Boni und ihn mit einer Kundenkarte bestückt, fallen diese Daten vermehrt und regelmässig an.

2. Begriffe und Prozesse

Data Warehousing und Data Mining sind im vorliegenden Umfeld Begriffe, die vielfach miteinander verwendet werden. Jeder für sich beinhaltet indessen eine eigenständige Funktion.

Unter «Data Warehousing» («Daten-Lagerhaus») wird allgemein die Strategie – und eine damit verbundene Technik[1] – verstanden, welche zum Ziel hat, Daten zeit- und funktionsgerecht zur Verfügung zu halten.

«Data Mining» («Datenbergbau») hat als Ziel – mit Hilfe bestimmter Technik, insbesondere Methoden der künstlichen Intelligenz, wie sie in den achtziger Jahren erforscht wurden – Daten aufzuspüren und zu kombi-

* Erweiterte Fassung eines anlässlich des 4. Symposiums für Datenschutz und Informationssicherheit, 28. Oktober 1999, Zürich, und des 18. RDV-Forums, 17. November 1999, Köln, gehaltenen Referates.

1 Auf die Technologie wird im Rahmen dieser Darstellung nicht eingetreten.

nieren, um neue, bisher unbekannte Informationen zu finden. Mit anderen Worten: Aus dem Rohstoff Daten sollen Informationen gewonnen werden, die in dieser Form vorher nicht vorlagen.

Damit wird offensichtlich, dass ein strukturiert geführtes Data Warehouse eine gute Voraussetzung für die Implementation eines Data-Mining-Konzeptes ist.

Umfassend betrachtet ergibt sich somit im Rahmen des Kundenmarketings ein sequentieller Prozess, der durch die Wiederholung verfeinert wird und immer wieder neue Erkenntnisse liefern kann.

a. Beschaffung von Daten aus möglichst vielen internen und externen Quellen;
b. Erfassung der Daten in einem Data Warehouse;
c. Bearbeitung der Daten mittels Data Mining Tools;
d. Auswertung der Daten.

3. Fokus für Unternehmen

Die Unternehmen investieren heute hohe Summen in diesen Prozess, einerseits in der Überzeugung, dass sehr viel verborgener Wert in Daten liege, der bisher nicht genutzt wurde; andererseits soll in einem zunehmend gesättigten Markt die Bindung des einzelnen Kunden an das Unternehmen im Sinne des «One-to-one»-Marketing mit zusätzlichen Informationen über dessen Verhalten gefestigt werden.
Die Konzepte und Techniken ermöglichen es, die Marketingstrategien und Verkaufsprogramme zielgerichteter und effizienter zu gestalten. Insgesamt wird deshalb diesen Konzepten im heutigen globalisierten Markt als Teil zur Gewinnung eines Marktvorteils und insgesamt zur Steigerung der Profitabilität im Verkaufszyklus ein grosses Potential zugewiesen.

Im O-Ton einer Beratungsfirma tönt das wie folgt: «Customer Relationship Management wird Marketing und Verkauf revolutionieren und zu Quantensprüngen in Produktivität und Profitabilität führen. Das Fokussieren auf investitionswürdige Kunden und das konsequente Ausschöpfen des Ertragspotentials jedes einzelnen Kunden durch systematisches Beziehungsmanagement kann auch in ihrem Unternehmen grosse Produktivitäts- und Profitabilitästreserven mobilisieren.»[2]

4. Sicht des Konsumenten

Für die Kundinnen und Kunden wird der Aufbau dieser Konzepte am ehesten sichtbar durch das Angebot immer neuer Kundenkarten. Jedes Kartensystem für sich ist in seiner Art attraktiv. Der kumulative Effekt beinhaltet indessen hohe Risiken für die Privatsphäre. Wir treffen hier auf eine Kehrseite der Medaille, die heute noch zu wenig beachtet wird: Data-Warehousing und Data-Mining-Konzepte sind eine Herausforderung für den Datenschutz in der Informationsgesellschaft, für die noch kaum eine adäquate Antwort vorliegt.
Die Auswertung des Konsumverhaltens einzelner Gruppen oder Bevölkerungsschichten war schon bisher das Ziel der Marketingstrategen. Die technologischen Möglichkeiten erlauben es nun aber, diese Analysen mit einer Präzision durchzuführen, die das Konsumverhalten einzelner Personen beinhaltet. Damit wird dieses Vorgehen auch datenschutzrechtlich relevant, indem Daten über eine bestimmte oder bestimmbare Person bearbeitet werden.
Mit der Zusammenstellung und Auswertung dieser Daten wird versucht, das Verhalten einer Person so weit zu steuern, dass sie entsprechend angebotene Produkte kauft respektive dass Produkte im Hinblick auf ihr mögliches Verhalten angeboten werden. Denn beim Einsatz von Data Mining Tools gibt der Kunde ungewollt mehr Daten bekannt, als er selber geben will: Mit der Auswertung der Daten fallen beispielsweise Angaben über bestimmte Präferenzen, die Zahlungswahrscheinlichkeit oder die Kundenprofitabilität an.
Je detaillierter solche Konsumprofile sind, desto eher ist von einem Persönlichkeitsprofil im datenschutzrechtlichen Sinne auszugehen. Von Persönlichkeitsprofilen wird gesprochen, wenn die Zusammenstellung der Daten eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer Person erlaubt. Als Beispiele gelten Aspekte des Verhaltens, z.B. Konsumverhaltens, oder die Beurteilung der Kreditwürdigkeit[3].
Das Bild des «gläsernen Konsumenten» ist bei diesen Konzepten nahe liegend und Besorgnis wird in den Medien oder in Umfragen sichtbar: «(...) beim Kunden löst die Vorstellung vom gläsernen Menschen natürlich Ängste aus. Er fürchtet sich davor, Opfer von Manipulationen zu werden. Auch das ist ein Thema, das intensiv in der Öffentlichkeit diskutiert werden muss.»[4] In den USA glauben gemäss einer Umfrage

75 Prozent der Bevölkerung, dass sie die Kontrolle über ihre persönlichen Daten verloren haben. Ebenso viele sind der Überzeugung, dass Unternehmen zu viele persönliche Informationen bearbeiten.[5]

5. Datenschutzrechtliche Grundprinzipien

Data-Warehousing- und Data-Mining-Konzepte haben eine hohe Relevanz in Bezug auf die datenschutzrechtlichen Grundprinzipien.
Die im vorliegenden Zusammenhang zu diskutierenden Prinzipien finden sich auf internationaler Ebene bereits in den Empfehlungen der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) aus dem Jahre 1980.[6] Sie sind ebenfalls Teil der Empfehlungen des Europarates von 1981[7] und der EU-Richtlinie[8]. Sie haben deshalb auch Eingang in die nationalen europäischen Gesetzgebungen gefunden.
Die folgenden fünf Prinzipien haben einen unmittelbaren Zusammenhang mit den vorliegenden Konzepten:

5.1. Zweckbindung

Das Kernprinzip in diesem Umfeld ist der Grundsatz der Zweckbindung. Daten sind nur zu dem Zweck zu bearbeiten, der bei der Beschaffung vorgesehen oder nach den Umständen ersichtlich war.
Am Beispiel eines Kauf- oder Dienstleistungsvertrages zeigt sich, dass diejenigen Daten bearbeitet werden können, die zur Abwicklung des Vertrages und insbesondere zur Wahrung der berechtigten Interessen beider Parteien notwendig sind. Insoweit dieser Vertrag abgewickelt und somit der Vertragszweck erfüllt ist, ist eine weitere Verarbeitung und Nutzung nicht mehr durch das Zweckbindungsgebot gedeckt[9].
Festzustellen ist, dass Data Mining immer eine sekundäre Zielsetzung ist, die durch die ursprüngliche Zielsetzung nicht abgedeckt ist. Selbst wenn Data Warehousing oder Data Mining als Zweckbestimmung einer Datenbearbeitung angeführt würden, wäre damit noch nicht gelöst, wie der Umgang mit den gewonnenen neuen Informationen und Kenntnissen zu erfolgen hätte.

5.2. Rechtmässige Beschaffung

Nach dem Grundsatz der rechtmässigen Beschaffung liegt ein Rechtfertigungsgrund für die Datenbearbeitung vor, wenn sie beispielsweise in unmittelbarem Zusammenhang mit dem Abschluss eines Vertrages erfolgt.

Data-Warehousing- und Data-Mining-Konzepte können sich indessen nicht auf Rechtfertigungsgründe stützen, da weder die Daten noch die Ergebnisse eine unmittelbare Notwendigkeit für einen vorliegenden wirtschaftlichen Vorgang mit einer betroffenen Person aufweisen. Der Aufbau von personenbezogenen Datensammlungen, deren Daten mittels Data Warehousing oder Data Mining gewonnen werden, ist daher mit diesen datenschutzrechtlichen Bearbeitungsgrundsätzen nicht vereinbar[10].

5.3. Einwilligung

Der rettende Anker in dieser Situation ist die Einwilligung der betroffenen Person. Eine Zweckänderung in der Datenbearbeitung ist mit der Einwilligung der betroffenen Person möglich. Damit stellen sich die Fragen, was eine Zweckänderung beinhalten kann und wie eine solche Einwilligung auszusehen hat.
Grundsätzlich ist festzuhalten, dass die Unternehmen, die ein Data Warehouse mit ihren Kundendaten führen wollen, regelmässig auf die Mitwirkung der betroffenen Personen angewiesen sind. Diese Mitwirkung wird in der Praxis in der Regel dadurch erreicht, dass der Kunde im Rahmen von allgemeinen Geschäftsbedingungen eine Vollmacht unterschreibt, die eine weitere Bearbeitung seiner Daten zu «Marketingzwecken» erlaubt. Damit wird indessen für den Kunden kaum transparent, was im Rahmen von Data Mining mit seinen Daten geschieht und welche Informationen damit zusätzlich gewonnen werden.

2 3. Fachtagung für Database Marketing und Customer Relationship Management, Zürich 1999
3 In der EU-Richtlinie 95/46/EG vom 24. Oktober 1995 wird der Begriff «Persönlichkeitsprofil» vermieden, aber in Art. 15 Abs. 1 von der Terminologie her erfasst.
4 Peter Quadri, Vorsitzender der Geschäftsleitung von IBM Schweiz, in: Tages-Anzeiger, 3. Juni 1999, S. 35
5 Joel R. Reidenberg, Lex Informatica: The formulation of Information Policy Rules through technology, in: Texas Law Review, vol. 76 (Feb 1998), No. 3, p. 561
6 Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten vom 23. September 1980; OECD Dokument C (80) 58 (Final). Die OECD hat weitere Dokumente zum Thema «Consumer privacy» veröffentlicht; siehe: http://www.oecd.org/dsti/sti/it/consumer/index.htm
7 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Konvention Nr. 108 vom 28. Januar 1981
8 Siehe Fn 3
9 Vgl. auch: Ulrich Möncke, Data Warehouse – eine Herausforderung für den Datenschutz? in: DuD, 22 (1998), S. 567
10 Eidgenössischer Datenschutzbeauftragter, 6. Tätigkeitsbericht, Bern 1998/99, S. 115

Das Konzept des Data Warehousing und des Data Mining ist darauf angelegt, mit dem vorhandenen Datenpool möglichst neue Erkenntnisse für die Beziehung Unternehmen – Kunden respektive Informationen über den Kunden zu finden, die in dieser Form gerade nicht vorliegen. Damit ist a priori eine unbestimmte Verwendung der ursprünglichen Daten vorgesehen. Es ist indessen fraglich, ob in eine unbestimmte Verwendung von Daten rechtsgültig eingewilligt werden kann. Vielmehr ist davon auszugehen, dass eine Vollmacht nur gültig erteilt werden kann, wenn die Datenbearbeitung für die betroffene Person ein Mindestmass an Transparenz aufweist. Es ist deshalb generell festzuhalten: Je sensibler die bearbeiteten Daten sind, je weiter weg vom ursprünglichen Bearbeitungszweck sie sind und je weiter der Zugriffsbereich auf diese Daten ausgedehnt wird, desto höhere Anforderungen sind an eine solche Einwilligungserklärung in Bezug auf die Transparenz zu stellen.

5.4. Grundsatz der Transparenz

Das Verfahren des Data Warehousing und des Data Mining ist nach dem Grundsatz der Transparenz deshalb so anzulegen, dass der Kunde jederzeit die Risiken abschätzen und seine Rechte wahrnehmen kann, insbesondere auch eine erteilte Einwilligung wieder zurückziehen kann. Diese Transparenzanforderungen stellen für die Praxis eine grosse Herausforderung dar. In der Regel wird dem Kunden das Ergebnis eines Data-Mining-Prozesses nicht mitgeteilt, aber u. U. spürt er indirekt die Auswirkungen, wenn beispielsweise eine bestimmte Profitabilitätsrate aus einem solchen Prozess generiert wird und das Unternehmen sich ihm gegenüber entsprechend verhält. Der Grundsatz der Transparenz beinhaltet deshalb im vorliegenden Zusammenhang die Frage nach dem Umfang der Aufklärungspflicht, die indessen nicht allgemein beantwortet werden kann.

5.5. Grundsatz der Qualität

Nach dem Grundsatz der Qualität ist deshalb auch zu fragen, wieweit die Daten, die einem Data-Warehouse zu Grunde liegen oder aus einem Data-Mining-Prozess gewonnen werden, integer sind. Nicht nur die ursprünglichen Quellen mit ihren unterschiedlichen Fehleranfälligkeiten der Daten, sondern auch die gewonnene neue Information unterliegen – mangels Transparenz – kaum einer Kontrolle durch die betroffene Person.

Das Konzept des Data Warehousing setzt auch in Bezug auf die Aufbewahrung der Daten keine Grenzen. Im Gegenteil: Daten über eine möglichst lange Zeitspanne sind von Interesse, da sie ein Verhalten um so besser interpretieren lassen. Ist damit im Data Warehouse eine unbeschränkte Aufbewahrung der Daten definitionsgemäss enthalten, stellen sich besondere Risiken in Bezug auf die Datenintegrität.

6. Gefahren und Risiken

Data-Warehousing- und Data-Mining-Konzepte stehen offensichtlich in einem Spannungsfeld zu den datenschutzrechtlichen Grundsätzen. Den rechtlichen Rahmenbedingungen stehen Trends und Entwicklungen in der Praxis gegenüber, die sowohl für das Unternehmen wie auch für die betroffenen Personen zusätzliche Gefahren und Risiken beinhalten.
Die immensen Datenmengen und die Auswertungsmöglichkeiten führen zu einer generellen Überwachungs- und Kontrollmöglichkeit des Einzelnen, zu der das Unternehmen mit seinen Data-Warehousing-Konzepten aktiv beiträgt.

Einzelne dieser Risiken, die sich auf Grund von globalen Trends und Entwicklungen bestätigen, sind daher näher zu betrachten:

6.1. Datenzentralen

Data Warehousing Konzepte führen bei den Unternehmen zu riesigen Datensammlungen über die Konsumentinnen und Konsumenten. Was ursprünglich beim Staat befürchtet wurde, wird nun in der Privatwirtschaft aufgebaut: Datenzentralen, die Informationen über das Verhalten einzelner Personen enthalten, ohne dass hierzu eine primäre Notwendigkeit besteht. Das Risikopotential aus datenschutzrechtlicher Sicht zeigt sich etwa bei den Kreditkartenunternehmen, die Informationen über das Kaufverhalten von Millionen von Kundinnen und Kunden speichern, oder bei Fluggesellschaften, die über Bewegungsprofile von Tausenden von Passagieren verfügen.

6.2. Kombinationen durch Fusionen

Das Zusammenwachsen von Bank- und Versicherungsdienstleistungen zu so genannten Allfinanzgesellschaften bringt dem Kunden einen einzigen Ansprechpartner. Damit fliessen aber auch medizinische Informationen, die beispielsweise in einem Versicherungs-

formular Verwendung fanden, in den Bankenbereich. In den USA wurde dieses Problem bereits aufgegriffen und Präsident Bill Clinton hat am 4. Mai 1999 eine so genannte «Financial Privacy and Consumer Protection Initiative» angekündigt. Dazu führte er aus, dass durch gesetzgeberische Massnahmen bei Fusionen insbesondere zu vermeiden sei, dass medizinische Informationen in den Finanzbereich fliessen: «So we propose to severely restrict the sharing of medical information with financial services conglomerates.»[11]

6.3. Kommerzialisierung durch Datenmarkt

Das Ansammeln von Kundendaten bei den Unternehmen führt auch zu einer zunehmenden Kommerzialisierung dieser Daten. Supermärkte registrieren, wer was kauft, und verkaufen diese Informationen auch an Dritte, so beispielsweise in den USA Listen von Rauchern an Lebensversicherungsgesellschaften[12]. Ebenso befinden sich in den USA ca. 60 Mio. Krankengeschichten in privaten Händen: sie wurden verkauft bei Praxisauflösungen und bei Spitalaufhebungen.

6.4. Verwertung historischer Daten

In Frankreich[13] haben die Telefongesellschaften damit begonnen, bei der Mobiltelefonie neben den Verbindungsdaten insbesondere auch die geografische Lokalisation des Gespräches zu erfassen. Damit wird in den Grossstädten auf 100–350 Meter und in den ländlichen Gebieten auf ca. 15–30 Kilometer genau erfasst, von wo ein Gespräch geführt wird[14]. Diese Aufzeichnungen werden auf drei Jahre zurück aufbewahrt mit der Begründung, dass dem Kunden individuelle Angebote in Bezug auf die Tarifierung gemacht werden sollen, indem beispielsweise die häufige Benutzung zwischen zwei bestimmten geografischen Zellen in einem massgeschneiderten Vergünstigungsangebot resultieren soll. Diese Datenbank kann indessen unterschiedliche Interessen wecken, da sie einwandfreie Bewegungsprofile der Telefonbenutzerinnen und -benutzer enthält.
Hier – und dies sei nur ein Nebenhinweis – scheint auch das Telefongeheimnis aufgeweicht zu werden, indem so genannte Verbindungsdaten nicht mehr unter das Telefongeheimnis fallen sollen[15].

6.5. Staatliche Zugriffe

Die Kundendaten unterliegen in den wenigsten Fällen einem Spezialgeheimnis. Solche Spezialgeheimnisse bestehen beispielsweise im Bereich der Medizinalberufe oder der Rechtsanwälte. Im Bereich der Telekomindustrie ist das Telefongeheimnis zu erwähnen, dessen Tragweite aber unterschiedlich interpretiert wird[16]. Soweit demnach kein Spezialgeheimnis besteht, haben staatliche Behörden, insbesondere Untersuchungsbehörden, einen relativ offenen Zugang zu den Kundendatenbanken.

So kommt es zumindest in der Schweiz des Öfteren dazu, dass Personen in Verfahren involviert werden, weil ihr Kassenzettel in einem nicht offiziellen und daher verbotenen Kehrichtsack gefunden wurde. Ein Grossverteiler versieht auf Grund der Kundenkarte die Kassenzettel mit einer individuellen Nummer, weshalb jeder Zettel identifizierbar wird. Das achtlose Fortwerfen eines Kassenzettels kann deshalb dazu führen, dass er von anderen Personen missbraucht wird, um falsche Fährten zu legen.

Die Vielfliegerprogramme der Luftfahrtgesellschaften gestatten die Erstellung von Bewegungsprofilen. Die Fluggesellschaften sind mit zunehmenden Anfragen staatlicher Behörden konfrontiert[17]. In den USA werden bereits heute Personen, die des Öfteren in bestimmte Länder fliegen, durch staatliche Stellen herausfiltriert, um sie einer speziellen Kontrolle zu unterziehen, da hier potentiell Terrorverdacht bestehe[18].

6.6. Treuwidrige Datenquellen

Das Internet ist heute in verschiedener Weise eine Rohstoffquelle für Data Mining. Nicht nur werden der Besuch von Homepages, das Interesse an bestimmten Angeboten und das Verhalten des jeweiligen Benutzers

11 Privacy Laws & Business Newsletter, No 49, July 1999, p. 22
12 c't 1999, Heft 4, S. 42
13 Marcel Pinet, La localisation des téléphones portables dans les réseaux de communication mobile, CNIL Paris 1999
14 Im Gegensatz zu der in der Schweiz eine Zeit lang diskutierten Möglichkeit der geografischen Ortung (mit Speicherung) des eingeschalteten Handys geht es hierbei um die Speicherung des geografischen Ortes im Zeitpunkt der Gesprächsführung.
15 Vgl. zur Diskussion in der Schweiz: ZR 98 (1999) Nr. 1, S. 1 ff. In der BRD ist das Telekommunikationsgeheimnis durch § 85 TKG umfassend geschützt. Vgl. hierzu: Johann Bizer, TK-Daten im Data Warehouse, in: DuD 22 (1998), S. 570 ff.
16 siehe Fn 15
17 Vgl. hierzu auch: Hans Jürgen Kranz, Datenschutz im internationalen Luftverkehr, in: DuD 4 (1998), S. 215 ff.
18 Der Spiegel, 27/1999, S. 115

gespeichert, sondern das Internet wird auch mit Angeboten bestückt, die als primäres Ziel das Aushorchen der Benutzerinnen und Benutzer zum Ziele haben.
In den USA sind die 14–17-jährigen Jugendlichen eine beliebte Quelle solcher Aushorchaktionen: Bevor ihnen ein bestimmtes Angebot zur Verfügung gestellt wird, haben sie Fragebogen zu den Lebensverhältnissen ihrer Eltern auszufüllen.
Aber auch Banken bedienen sich dieser Methoden: Beim Update ihrer Online-Banking-Software hat die Bank «Credit Suisse» gleichzeitig einen Fragebogen zu den Familienverhältnissen, der beruflichen Situation, der Ausbildung usw. ausfüllen lassen[19]. Der Datenaufbau wird mit dem Motto «Profitieren Sie dank Ihren Angaben von unseren Anregungen und Tipps» aktiv gefördert. Die Feststellung, «das Internet ist ein überaus offenes Medium, mit dem uns die Benutzer sehr viele Informationen über ihre persönlichen Präferenzen liefern»[20], sagt auch etwas über den Erfolg solcher Aktionen aus.

6.7. Verwertung neuer Informationen

Genanalysen werden das Wissen über den Menschen radikal verändern. Der Umgang mit diesen Informationen ist äusserst sensibel. In Bezug auf ein Data-Warehousing- und Data-Mining-Konzept stellen sich aber bereits heute Fragen: Was machen Lebensversicherungsgesellschaften, die heute für den Abschluss einer Lebensversicherung die Vorlage einer Genomanalyse verlangen, mit solchen Daten? Wie ist beispielsweise deren Verwendung in Bezug auf verwandte Personen?
Auch Geografische Informationssysteme (GIS) erschliessen neue Informationen: Die Veröffentlichung von Risikokatastern wird zur Kombination dieser Daten führen und eine Versicherungsgesellschaft wird beispielsweise feststellen können, dass eine bestimmte Person schon seit Jahren in einem Gebiet mit erhöhtem Krebsrisiko wohnt. Die Konsequenzen der Verarbeitung und Kombination dieser zusätzlichen Informationen sind heute kaum abschätzbar.

6.8. Diskriminierung

Mit so genanntem «Scoring» wird ermittelt, welcher Nutzen der Kunde dem Unternehmen bisher gebracht hat respektive welcher potentielle Nutzen in Zukunft zu erwarten ist.[21] Bereits die Hälfte der Banken in den USA sollen solche Rentabilitätsprofile erstellen und für die Kundinnen und Kunden entsprechende Konsequenzen ziehen.[22]
Die Kunden werden nach «Kundenwert» behandelt. In der Regel kennt der Kunde weder «seinen Wert» noch die Daten und Informationen, die zu diesem Wert geführt haben. Das Verhalten des Unternehmens ihm gegenüber kann sich deshalb auf Grund von Daten, die – von bestimmten Annahmen ausgehend – ausgewertet wurden, ändern.

So hat beispielsweise eine Fluggesellschaft bereits heute ihre Top-1000-Kunden identifiziert, die jederzeit auch ohne Ticket an einen Schalter kommen können und einen Platz erhalten werden[23]. Dies natürlich auf Kosten desjenigen, der bereits im Flugzeug sitzt, aber nicht so viele Meilen auf seinem Konto hat oder vielleicht sogar keine Kundenkarte besitzt.

6.9. Globale Information

Mit der Globalisierung der Kommunikation ist immer damit zu rechnen, dass lokale Informationen weltweit zur Verfügung gestellt werden. Das Festlegen einer prozentualen Zahlungswahrscheinlichkeit, die vielleicht daher rührt, dass eine Person mit einem lokalen Händler Auseinandersetzungen in Bezug auf eine Lieferung hatte, kann losgelöst vom lokalen Erklärungsumfeld als Datum erscheinen, das in der globalisierten Welt kaum mehr zu relativieren ist.

6.10. Staatliches Data Mining?

Auf den ersten Blick scheint der Gedanke, dass auch der Staat diese Konzepte sich zu Nutze machen könnte, abwegig. Doch im Rahmen von Reformbemühungen, die insbesondere auch eine Kommerzialisierung von Personendaten nicht ausschliessen[24], sind solche Überlegungen bereits im Gange.

In den USA haben verschiedene Staaten die Fotos aus den Führerausweisen an eine private Firma verkauft, die damit eine zentrale Datenbank aufbauen wollte, um Namen und Fotos miteinander abzugleichen[25].
Auch sollen beispielsweise bei der Börsenaufsicht in Deutschland Data-Mining-Analysetools geprüft werden, die aus den täglich etwa eine halbe Million Meldungen über Käufe und Verkäufe von Aktien und Optionen verdächtige Transaktionen herausfiltern, um Insiderhandel aufzudecken[26]. Daher ist es auch nicht auszuschliessen, dass dereinst Steuerämter, Sozial-

ämter oder Polizeibehörden mittels solcher Methoden nach neuen Informationen über die einzelnen Bürgerinnen und Bürger suchen[27].

7. Lösungsansätze

Die Diskussion um die datenschutzrechtlichen Aspekte von Data-Warehousing- und Data-Mining-Konzepten steht am Anfang. Wir haben eine klare Rechtslage, aber ebenso klare und starke Tendenzen in der Praxis, die diesen Grundsätzen wenig Beachtung schenken und sogar neue Risiken für die betroffenen Personen schaffen.
Die Data-Warehousing- und Data-Mining-Konzepte sind deshalb umfassend in ihrem wirtschaftlichen, rechtlichen und sozialen Umfeld zu betrachten. Hierzu drei Feststellungen:

a) Ein wirtschaftlicher Blick auf die Beziehung Unternehmen – Kunden und Data-Warehousing rückt das Interesse an einer Optimierung des Leistungsaustausches in den Vordergrund. Durch eine genaue Analyse des Kundenverhaltens soll dieser seine Leistung zu einem optimalen Preis-Leistungs-Verhältnis erhalten. Dieser Ansatz setzt gleichgewichtige Partner voraus, die Angebot und Nachfrage im Markt dynamisch aushandeln.

Mit dem Konzept des Data-Mining- und Data-Warehousing wird indessen das Informationsgewicht eindeutig zu Gunsten des Unternehmens verschoben. Dieses hat nicht nur die Möglichkeit, das Angebot auf eine bestimmte Person auszurichten, sondern ebenso – durch Zusatzinformationen – eine bestimmte Person von einem Angebot auszuschliessen.

b) Data-Warehousing- und Data-Mining-Konzepte beinhalten zusätzliche Risiken für die Privatsphäre der betroffenen Personen. Die Gesetzgebung vermag indessen hier nur schwer eine Grenze zu ziehen. Der Datenschutz als ein Grundrecht verliert an Gewicht, wenn in der Rechtswirklichkeit dessen Schutz nicht gewährleistet werden kann.

c) Als dritter Faktor kommt die technologische Entwicklung hinzu. Wer an der elektronischen Gesellschaft teilnehmen will, muss zwangsläufig Daten preisgeben. Aus dieser Tatsache ergibt sich ein Grundrisiko: Wo Daten anfallen, ist ein Missbrauchspotential vorhanden. Dies um so mehr, als die Verwendung der Daten nicht transparent ist und die Preisgabe von persönlichen Daten unter verschiedenen Deckmänteln (Konsumentenbefragungen etc.) aktiv gefördert wird. Damit wird auch eine soziale Grundsatzfrage aufgeworfen, nämlich diejenige nach der Rolle des Individuums als Privatperson in unserer Gesellschaft. Die Informationsgesellschaft als Risikogesellschaft bedarf der Risikodiskussion gerade auch in diesem Bereich. Eines dieser Risiken, dessen Konsequenzen kaum zu Ende gedacht sind, ist, dass das Individuum in der Masse untergeht, da seine Privatsphäre völlig aufgehoben wird[28].

8. Fazit

Auf Grund der tatsächlichen Entwicklung, der Rechtslage und der sozialen Risiken ist ein Interessenausgleich zwischen Unternehmen und Konsumenten nur möglich, wenn das Gebot der Fairness spielt. Offensichtlich nutzt heute das Unternehmen die neuen Technologien vorwiegend zur Optimierung seiner eigenen Interessen, die (wirtschaftlichen) Vorteile des Konsumenten sind meistens marginal, und die Gesetze zum Schutze der Privatsphäre haben nur beschränkte Wirkung.
Wie lange eine solche Situation von den Konsumentinnen und Konsumenten toleriert wird, kann indessen auch einem Unternehmen nicht gleich sein. Datenschutz ist dabei nicht als strategischer Nachteil zu sehen, wie Umfragen zeigen:
Eine neue Umfrage in Deutschland, Grossbritannien und den USA zeigt, dass in allen drei Ländern über

19 Weltwoche Nr. 38, 23. September 1999, S. 37
20 Hanspeter Kurzmeyer, GL-Mitglied der Credit Suisse, in: Tages-Anzeiger, 30. Juli 1998, S. 23; im zitierten Beispiel haben 65 Prozent der Online-Kunden der Credit Suisse den Fragebogen ausgefüllt (Quelle: Fn 19)
21 Vgl. hierzu: Frank Möller, Data Warehouse als Warnsignal an die Datenschutzbeauftragten, in: DuD, 22 (1998), S. 557
22 Sonntags-Zeitung, 17. Januar 1999
23 Reinhold Rapp, Datenbankgestütztes Beziehungsmarketing bei der Lufthansa, Fachtagung Database Marketing und Data Mining, Zürich 1998
24 Siehe hierzu grundlegend: Herbert Burkert, Personendaten als Handelsware?, in: Fakten Nr. 4 / 1996, S. 23 ff.; Spiros Simitis, Datenschutz – Rückschritt oder Neubeginn?, in: NJW 1998, Heft 34, S, 2476 f.
25 The Economist, May 1st 1999, p. 20; die Verkäufe wurde rückgängig gemacht, als sie publik wurden und 14 000 Personen sich mittels E-Mail beschwerten.
26 Frank Möller, a.a.O., S. 557
27 Vgl. Landesbeauftragter für den Datenschutz Schleswig-Holstein, 21. Tätigkeitsbericht 1999, S. 117 f.
28 Solche Szenarien werden vermehrt auch in den Medien diskutiert: Vgl.: The Economist, The end of privacy, May 1999; Der Spiegel, Das Ende des Privaten, Nr. 27, Juli 1999.

70 Prozent der Personen sich über einen möglichen Missbrauch ihrer Daten im Wirtschaftsumfeld Sorgen machen[29].
In der Schweiz hat eine Umfrage gezeigt, dass 72 Prozent der Kunden lieber Nettopreise bezahlen würden als sich mit diversen Kundenbindungs-Programmen herumschlagen zu müssen[30].

Daher zwei konkrete Lösungsansätze:
a) Die anonyme Auswertung von Daten beinhaltet grundsätzlich keine datenschutzrechtlichen Konsequenzen[31]. Mit anderen Worten: Data-Mining- und Data-Warehousing, die zwar zum Ziel haben, das Verhalten von Kundinnen und Kunden zu analysieren, aber auf eine personenbezogene Bearbeitung und Auswertung verzichten, sind a priori als datenschutzkonform
zu bezeichnen. Anonymisierungskonzepte stehen aber im Spannungsfeld zu den Zielsetzungen des «One-to-one»-Marketing, weshalb sie in der Praxis nur beschränkte Bedeutung haben.

b) Unternehmen geben sich einen Datenschutz-Standard, wobei der Kunde die Möglichkeit haben muss, darüber zu entscheiden, wieweit er seine Privatsphäre für eine bestimmte geschäftliche Transaktion aufgeben will, zum Beispiel im Rahmen seines Telefonverhaltens oder als Nutzer eines Vielfliegerprogrammes. Dies bedingt, dass die Unternehmen einen solchen Standard garantieren und sich nicht auf gesetzliche Regelungen berufen, die der Entwicklung der Technik gerade im vorliegenden Bereich weit hinterherhinken. Datenschutz muss der «default»-Standard sein.

Das bedeutet im Einzelnen, dass
- das Unternehmen Transparenz über die Verwendung seiner Kundendaten schafft. Insbesondere informiert es über die Änderung in der Verwendung oder die Weitergabe dieser Daten;
- die Konsumentinnen und Konsumenten einen angemessenen Gegenwert für die Verwendung ihrer Daten erhalten;
- die Konsumentinnen und Konsumenten jederzeit das Recht haben, sämtliche ihrer Daten zurückzuziehen oder zu löschen.

Ein solches System ist nicht unbekannt: Statt dass Kunden Geld bei einer Bank anlegen, legen sie persönliche Daten bei einem Unternehmen an und erhalten einen angemessenen Gegenwert dafür. Wie bei den Banken will der Konsument aber Transparenz und insbesondere die Herrschaft über sein Geld respektive seine Daten behalten, indem er diese(s) zurückziehen kann.
Die Verantwortung in diesem Prozess liegt dabei nicht nur beim Unternehmen, das sich einen Datenschutz-Standard gibt und Transparenz schafft, sondern auch bei den Kundinnen und Kunden, die sich vermehrt auch Gedanken machen müssen, ob und für welche Zwecke sie persönliche Daten weitergeben. Aber auch der Staat hat die rechtlichen Rahmenbedingungen zu schaffen, die eine angemessene Reaktion auf die technischen Entwicklungen erlauben und das Grundrecht auf Datenschutz nicht durch das Faktische aushöhlen lassen.

29 IBM/Harris Study 1999, in: Alan F. Westin, Consumers, E-Commerce and Privacy: US, UK and Germany, Conference Proceedings, 21st International Conference on Privacy and Personal Data Protection, Hong Kong 1999, p. 264
30 Umfrage IHA/GfM, in: Facts Nr. 5 (4.2.1999), S. 64 ff.
31 Siehe hierzu im Einzelnen: Ulrich Möncke, a.a.O., S. 568