

# Data Mining unter dem Gesichtspunkt des Datenschutzes

Matthias Leisi (leisi@astrum.ch)

24. Mai 2000

---

Ein Data Mining ohne Daten ist unmöglich.

Kann man Daten trotzdem mittels  
Data Mining analysieren, wenn die  
Daten geschützt sind?

# Inhaltsverzeichnis

<b>1 Was ist Datenschutz?</b>	<b>1</b>
1.1 Zielkonflikt zwischen Data Mining und Datenschutz . . . . .	1
1.2 Begriffe und Konzepte . . . . .	1
1.3 Übersicht datenschutzrechtlicher Regulierungen . . . . .	2
<b>2 Datenschutz im Kontext des Data Mining</b>	<b>6</b>
2.1 Datenerwerb und -beschaffung . . . . .	6
2.2 Datenbearbeitung und -richtigkeit . . . . .	8
2.3 Datenbekanntgabe und -handel . . . . .	9
2.4 Datensicherheit . . . . .	9
<b>3 Ausgewählte Fragestellungen</b>	<b>11</b>
3.1 Gesundheitswesen . . . . .	11
3.2 Grenzüberschreitende e-Commerce-Anwendungen . . . . .	12
3.3 Data Mining am Beispiel von Echelon . . . . .	14
3.4 Adress- und Datenhandel . . . . .	15
<b>4 Rechtsbehelfe und Rechtsfolgen</b>	<b>17</b>
<b>5 Folgerungen für den praktischen Einsatz von Data-Mining-Technologien</b>	<b>19</b>
<b>Literaturverzeichnis</b>	<b>21</b>

# 1 Was ist Datenschutz?

## 1.1 Zielkonflikt zwischen Data Mining und Datenschutz

Data Mining ist – in einer einfachen Definition – das nichttriviale und automatische ”Schürfen nach” Zusammenhängen in und Erkenntnissen aus vorhandenen Daten, die idealerweise aus einem Data Warehouse stammen.<sup>1</sup> Der Datenschutz wiederum bestimmt, dass ”Personendaten (... nur für den Zweck bearbeitet werden dürfen), der bei der Beschaffung angegeben wurde.”

Art. 4  
Abs. 2 DSG

Dieser offensichtliche Widerspruch zwischen den Zielen des Data Mining und des Datenschutzes wird durch aktuelle Entwicklungen auf technischer Ebene noch verschärft, zum Beispiel durch Methoden des User Tracking in Internet-basierenden Diensten.<sup>2</sup> Selbst ohne die technisch nur teilweise vollständig mögliche Überwachung ”im Internet” stehen Data Miner auf allen Ebenen ihrer Arbeit unter dem Eindruck des Datenschutzes, bei der Beschaffung der Daten, deren Verarbeitung mittels statistischer und anderer Methoden und bei der Anwendung der Erkenntnisse auf die Gesamtheit ihrer Daten oder auf die Datenbestände einzelner Personen.

Um diesem Dilemma zu entgehen, postulieren Datenschützer die Grundprinzipien der *Datensparsamkeit* und der *Datenvermeidung* ([Arbeitsgruppe ”Datenschutzfreundliche Technologien”, o. Datum], siehe auch Kapitel 5).

Im folgenden wird der Versuch unternommen, die aktuelle Situation aus rechtlicher und technischer Sicht greifbar zu machen und gewisse gefährliche Strukturen zu verdeutlichen.

## 1.2 Begriffe und Konzepte

Das Datenschutzgesetz<sup>3</sup> definiert auf dem Papier plausibel, was unter Datenschutz und den darin verwendeten Begriffen verstanden wird. In der Praxis entziehen sich die Definitionen gem. Art. 3 DSG allerdings einer praxistauglichen Auslegung und geben die Idee des Gesetzgebers nur teilweise wider [Belser, 1999]. Diese Definitionen sollen dennoch als Ausgangsbasis für weitere Erklärungen dienen (Art. 3 DSG, auszugsweise, Hervorhebungen durch den Autor):

- *Personendaten (Daten)*: Alle Angaben, die sich auf eine bestimmte oder *bestimmbare* Person beziehen.
- *besonders schützenswert*: Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten; die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit; Massnahmen der sozialen Hilfe; administrative oder strafrechtliche Verfolgungen und Sanktionen.<sup>4</sup>

Art. 3 DSG

<sup>1</sup> nach [Lusti, 1999]

<sup>2</sup> Beispielsweise webseitenübergreifendes User Tracking durch Werbebanner in Verbindung mit Cookies

<sup>3</sup> In dieser Arbeit wird primär auf das Schweizerische Datenschutzgesetz abgestellt. Die europäischen Regelungen sind über weite Strecken analog; auf allfällige Unterschiede und spezielle Probleme im grenzüberschreitenden Datenverkehr wird in Kapitel 3.2 ab Seite 12 eingegangen.

<sup>4</sup> Die Liste der besonders schützenswerten Personendaten im DSG stammt aus der Datenschutzkonvention des Europarates von 1981 (ER-Konv-108), Art. 6

- *Persönlichkeitsprofil*: Eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.
- *Bearbeiten*: Jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren und Vernichten von Daten.
- *Datensammlung*: Jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen *erschliessbar* ist.
- *Zweckbindung (Art. 4 Abs. 3 DSG)*: Daten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgeschrieben ist.

#### *Fallen Data Mining und Data Warehousing unter das Datenschutzgesetz?*

Das Datenschutzgesetz erfasst alle Bearbeitungsvorgänge, in denen Personendaten vorkommen, unabhängig von Medienart (analog, digital, Text, (Bewegt-)Bild, Ton, . . .) und der konkreten Bearbeitungsmethode (reine Erfassung oder Speicherung, administrative Fortschreibungen, Mutationen, statistische Auswertungen). Demzufolge sind auch sämtliche Data Mining-Vorgänge sowie die Speicherung in Data Warehouses oder Data Marts mit sämtlichen Technologien (OLAP, ROLAP, MOLAP, . . .) dem Datenschutzgesetz potentiell unterworfen.

Problematisch an der ständigen Bewertbarkeit von Personen ist der damit verbundene Verlust der Transparenz gegenüber den betroffenen Personen. Der Einzelne ist nicht mehr in der Lage zu beurteilen, welche Information zu welchem Zweck von wem bearbeitet werden.<sup>5</sup>

### **1.3 Übersicht datenschutzrechtlicher Regulierungen**

Massgebend für die Schweiz ist das Bundesgesetz über den Datenschutz [DSG, 1992] sowie die Verordnung vom 14. Juni 1993 zum Bundesgesetz über den Datenschutz (VDSG). Vom Datenschutzgesetz betroffen sind eine Reihe weiterer Gesetze z.B. aus den Bereichen Asylwesen, Staatsschutz, Bundesstatistik u.a.<sup>6</sup>

Für die Europäische Union massgebend ist die "Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" [EG-DRL, 1995]. Diese Richtlinie bindet a priori nicht die Bürger, sondern die Staaten, ist also nicht ohne Umsetzung in jeweils nationales Recht anwendbar. Viele Staaten der EU haben diese Richtlinie allerdings noch nicht umgesetzt, so dass der Europäische Gerichtshof eine direkte Anwendbarkeit unter gewissen Voraussetzungen anerkannt hat (siehe dazu [Haslach, 12/1998])

### **Verwandte Regelungen**

Dem Datenschutz gehen unter Umständen andere Regelungen vor. Namentlich das Bankgeheimnis sowie das Berufsgeheimnis von Ärzten, Amtsträgern usw. verbietet in diesen Fällen

<sup>5</sup> EDSB [1999]

<sup>6</sup> Eine Übersicht findet sich unter [http://www.admin.ch/ch/d/sr/2/z235\\_1.html](http://www.admin.ch/ch/d/sr/2/z235_1.html), Zitate des DSG.

nicht direkt die Anwendung von Data Mining-Methoden sondern vor allem die Bekanntgabe von personalisierten Daten an Dritte. Weiterhin *nicht* betroffen vom Datenschutz ist die rein administrative Datenverarbeitung.

Selbst wenn die Daten nicht mit Data Mining-Methoden ausgewertet werden ergeben sich hiermit datenschutzrechtliche Probleme in Bezug auf die Sozial-, Kranken- und Unfallversicherungen. Die Leistungs- und Kostenträger haben naturgemäss ein Interesse daran, aus den Daten besondere Risikogruppen und Missbrauchsfälle herauszufiltern, was angesichts der potentiellen Folgen für die betroffenen Personen aus der Sicht des Datenschutzes bedenklich sein kann (siehe auch Kapitel 3.1).

Das Bankgeheimnis<sup>7</sup> bindet die davon betroffenen Firmen weitaus stärker als das Datenschutzgesetz. Daher sind für die Finanzindustrie gewisse Anwendungsgebiete des Data Mining a priori ausgeschlossen. Insbesondere der Einsatz der bereits vorhandenen umfangreichen Datenbestände zu Gunsten Dritter (etwa im Cross Selling) sind nicht zulässig.<sup>8</sup>

Ein Zielkonflikt besteht des weiteren zwischen dem Datenschutz und dem Bankgeheimnis auf der einen und dem Geldwäschereigesetz<sup>9</sup> auf der anderen Seite. Das Grundprinzip "Know your customer" des Geldwäschereigesetzes bedingt wesentlich mehr Informationen als zur Führung einer Kontobeziehung aus administrativer Sicht notwendig sind (zum Beispiel die Hintergründe einer in Höhe und Zeitpunkt aussergewöhnlichen Transaktion). Da es sich hier definitionsgemäss um einzelne Ereignisse handelt, die sich dem automatisierten Data Mining entziehen, soll darauf im Rahmen dieser Arbeit nicht weiter eingegangen werden.

In den genannten Bereichen nehmen zudem die organisatorischen Massnahmen des Datenschutzes und der Datensicherheit (siehe Kap. 2.4) breiten Raum ein und machen einen substantiellen Teil der Kosten des Datenschutzes aus.

## Regelungen für private und staatliche Stellen

Fokus der vorliegenden Arbeit sind die *privaten* Datensammlungen sowie die Anwendung von Data Mining-Methoden auf diese Bestände. *Staatliche* Stellen besitzen und verarbeiten zwar auch (und besonders) schützenswerte Daten, etwa in wirtschaftlicher oder gesundheitlicher Hinsicht, unterstehen jedoch speziellen Regelungen, die sich aus dem Datenschutzgesetz ergeben (gem. Art. 17 Abs. 1 lit. f DSGVO muss eine gesetzliche Grundlage für die Bearbeitung von Daten bestehen).

Art. 13 DSGVO

In der Praxis bestehen diverse *Rechtfertigungsgründe*, welche eine personenbezogene Erfassung, Speicherung, Verarbeitung und Auswertung von Daten erlauben. Dazu gehört vor allem ein unmittelbarer Zusammenhang mit einem Rechtsgeschäft (Kauf/Verkauf, Vertragsabschluss usw.) sowie Kreditauskünfte. Die Rechtfertigungsgründe werden als "überwiegendes Interesse der bearbeitenden Person" bezeichnet, sind jedoch nicht absolut formuliert. Gemäss [EDSB, 1999, p. 114 ff] "[Dürfte es] schwierig sein, einen Rechtfertigungsgrund im

<sup>7</sup> Art. 47 Bundesgesetz über die Banken und Sparkassen, SR 952.0, [http://www.admin.ch/ch/d/sr/952\\_0/a47.html](http://www.admin.ch/ch/d/sr/952_0/a47.html), Vereinbarung über die Sorgfaltspflicht im Bankwesen

<sup>8</sup> Persönliche Auskunft UBS AG, Legal & Compliance, sowie Visa Card Center, Mai 2000.

<sup>9</sup> Bundesgesetz vom 10. Oktober 1997 zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG), SR 955.0, <http://www.admin.ch/ch/d/sr/9/955.0.de.pdf>

Sinne von Art. 13 DSGVO zu finden, um vorliegend die Verletzung des Zweckbindungsgebots zu legitimieren“.

Spezielle Regelungen gelten für Personen des öffentlichen Lebens, die einen geringeren Schutz ihrer Persönlichkeitsrechte genießen, sofern die gesammelten Daten sich auf ihr Wirken in der Öffentlichkeit beziehen (siehe [Schweizer, 1999, Kap. 3.7.7] sowie [Schärli, 1998] zu den Unterschieden zwischen Privatpersonen und Personen des öffentlichen Lebens). Ausserdem bestehen Erleichterungen für Journalisten und andere Medienschaffende, sofern Daten für die Veröffentlichung in einem periodisch erscheinenden Medium verarbeitet werden. In diesem Bereich ist besonders auf die lange Aufbewahrungsfrist von Datensammlungen zu achten, wenn zum Beispiel Verlage grössere Datenbanken unterhalten, aus denen Beziehungsmuster gelegengewonnen werden können.

Art. 13 Abs.  
2 lit. d DSGVO

### **”Besonders schützenswerte Daten”**

Datensammlungen an sich sind, sofern sie bestimmte oder bestimmbare Personen aufführen, bereits dem Datenschutzgesetz potentiell unterworfen. Sobald besonders schützenswerte Daten enthalten sind, ergeben sich deutliche Einschränkungen der Bearbeitungsmöglichkeiten (insbesondere im Bereich des weit gefassten Begriffs der Bekanntgabe). Aus diesem Grund wird in der Praxis aus eigenem Geschäftsinteresse häufig bereits auf die Erhebung entsprechender Daten verzichtet.<sup>10</sup>

Durch die blosser Aufzählung der ”besonders schützenswerten Daten” im DSGVO ist jedoch ein wesentlicher Punkt nicht gelöst worden: die besonderen Umständen oder die geschickte Kombination von an sich ungefährlichen Daten kann zu Erkenntnissen führen, die besonders schützenswert sein können.

### **Persönlichkeitsprofile**

Das DSGVO definiert das Persönlichkeitsprofil als ”eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt”. Bemerkenswert ist, dass ein Persönlichkeitsprofil keine besonders schützenswerten Daten enthalten muss, um dem DSGVO unterworfen zu sein. Problematisch ist die Auslegung und die Handhabung in der Praxis.

Art. 3  
lit. d DSGVO

Weil juristisch die Persönlichkeit über die Persönlichkeitsrechte (wie Privatsphäre, familienrechtliche Beziehungen, Ehre, Wirtschaftsfreiheit usw.) definiert wird, steht zwangsläufig die Gefährdung der Persönlichkeitsrechte als Auslegungskriterium im Zentrum der Überlegungen. Nach [Belser, 1999, S. 2f] kann man danach für die Praxis etwas salopp ausdrücken:

Ein Persönlichkeitsprofil im Sinne von Art. 3 lit. d DSGVO liegt dann vor, wenn man mit einer systematischen Auswertung von einzeln an sich auch problemlosen Informationen einer natürlichen Person  
– nach dem Durchschnittsempfinden ”zu nahe tritt”

<sup>10</sup> Art. 3 lit. c DSGVO dürfte denn eher für staatliche Stellen sowie präventiv gegen eklatante Missbräuche relevant sein.

oder

– das Resultat der Auswertung sich auf ihr gesellschaftliches, berufliches oder wirtschaftliches Ansehen in einer Art nachteilig auswirken könnte, die man, ohne dass man besonders empfindlich ist, sich nicht einfach so gefallen lassen muss.

In Gesetz und Verordnung werden besonders schützenswerte Daten und Persönlichkeitsprofile durchwegs gleich behandelt (Anmeldung entsprechender Datensammlungen, Bekanntgabeverbot, eingeschränkte Rechtfertigungsgründe). Generell wird bei der Bearbeitung der genannten Kategorien von Daten ein strengerer Massstab angelegt als in anderen Bereichen.

Die blossе Anzahl der Merkmale kann kein ausreichender Massstab für die Qualifizierung als Persönlichkeitsprofil sein. Vielmehr kommt es auf die qualitative, sich aus den Umständen und den Verknüpfungen ergebende Aussage der Inhalte an.

Datensammlungen, welche besonders schützenswerte Personendaten und Persönlichkeitsprofile enthalten, müssen im Register der Datensammlungen des Eidgenössischen Datenschutzbeauftragten aufgeführt sein. Durch die Anmeldung in dieses Register ist es möglich, Datensammlungen auch *ohne Wissen* der betroffenen Personen zu führen. Im weiteren Text wird auf diese Unterscheidung verzichtet werden, "Wissen der Betroffenen" kann also jeweils durch "Eintrag im Register der Datensammlungen" substituiert werden.

## 2 Datenschutz im Kontext des Data Mining

Personendaten dürfen prinzipiell nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde. Wenn sich nachträglich eine Zweckänderung ergibt, so dürfen die erhobenen Daten nicht einfach weiterverwendet werden. Die Betroffenen müssen erneut um ihre Zustimmung gebeten werden. (Eidgenössischer Datenschutzbeauftragter, 1. Tätigkeitsbericht 1993/1994)

In jedem Schritt des Phasenmodell des Data Mining<sup>11</sup> müssen die datenschutzrechtlichen Anforderungen eingehalten werden: Bei der Spezifikation des Problems, bei der Sammlung und Aufbereitung der Daten, bei der Exploration, der Anwendung der Hauptmethoden und der Validierung sowie Anwendung der Ergebnisse.

### 2.1 Datenerwerb und -beschaffung

Gemäss dem Grundsatz der *Zweckbindung* dürfen Daten nur zu dem Zweck verwendet werden, der bei der Bekanntgabe durch die betroffene Person ersichtlich war. Dies kann etwa durch ein Antragsformular für eine Kreditkarte, durch Ankreuzen entsprechender Optionen auf einem Webformular oder auf anderen Wegen geschehen.

Art. 4 Abs. 3  
DSG

Generalklauseln wie sie zum Beispiel in den Allgemeinen Geschäftsbedingungen der Schweizer Post zu finden sind<sup>12</sup> dürften den Grundsatz der Zweckbindung gemäss DSG *nicht* erfüllen. Ebenso genügt es nach Ansicht von [EDSB, 1998, Kapitel 8.1: Adresshandel] nicht, die Einwilligung generell für "Marktforschung" oder "Marketing" zu erlangen. Insbesondere wenn Persönlichkeitsprofile erstellt werden sind wesentlich höhere Anforderungen an die Einwilligung zu stellen.

In Verbindung mit konkreten Vertragshandlungen ist der Zugriff auf weitere Quellen denkbar, etwa Anfragen bei Kreditauskunfteien und öffentliche Register (Handelsregister, Branchenverzeichnisse, Geschäftsberichte, Steuerregister (in wenigen Kantonen), ...) [Schweizer, 1999, p. 169]. Im Rahmen der Neukundenwerbung ist der Zukauf von unternehmensexternen Kundendaten ein wichtiges Element (auch wenn sog. "kalte Adressen" – d.h. Adressen mit denen noch nie ein Kontakt bestand – eine wesentlich niedrigere Responserate aufweisen<sup>13</sup>).

Um DSG-konform arbeiten zu können, müssen von Dritten zugekaufte Daten datenschutzrechtlich unbedenklich sein. Das bedeutet für den Verkäufer, dass er die explizite Einwilligung der betroffenen Personen eingeholt haben muss (und dies dem Käufer in der einen oder anderen Form schriftlich bestätigen muss).<sup>14</sup>

Neuere Entwicklungen anerkennen den Wert der Daten, indem die Auskunftswilligen für die Preisgabe der Daten direkt oder indirekt bezahlt werden. Das System der Hamburger Firma

<sup>11</sup> [Lusti, 1999, Kapitel 6.2]

<sup>12</sup> AGB "Postdienstleistungen", Stand 1.1.1999, Art. 8, Datenschutz: *Ohne gegenteilige Mitteilung ist die Post berechtigt, den Namen des Kunden und dessen Adresse an Dritte weiterzugeben.*

<sup>13</sup> Persönliche Auskunft von Schober Information Group vom 15. Mai 2000

<sup>14</sup> Zur Einwilligungsklausel siehe auch [EDSB, 1998, Kapitel 5.5.1]

Cocus etwa ordnet die erhobenen Daten nach verschiedenen Kriterien und Klassifizierungen ein und bezahlt den Konsumenten für jeden verkauften Datensatz einen bestimmten Betrag (die Firma selbst schätzt einen Betrag von 5 bis 20 DM pro verkauftem Datensatz) [NZZ, 5. Mai 2000]. Insbesondere in den USA existieren Modelle die mittels User-Tracking auf Webseiten Interessenprofile von Anwendern erstellen und euphemistisch "customized" genannte Werbung präsentieren. Die Gegenleistung ist häufig Internet-spezifisch, zum Beispiel in Form von reduzierten Onlinegebühren [Angwin, 1. Mai 2000]. Da in diesen Fällen von einer Einwilligung der Betroffenen ausgegangen werden kann, ist der Handel mit diesen Daten datenschutzrechtlich unbedenklich.

Andere Formen des Datenerwerbs, wie sie etwa von Microsoft<sup>15</sup>, Real Networks<sup>16</sup> und DoubleClick<sup>17</sup> betrieben werden, haben neben der prinzipiellen geschäftspolitischen Dimension auch eine direkte datenschutzrechtliche Relevanz, zumindest nach *europäischem* Datenschutzverständnis.

Die Unrechtmässigkeit der Datenbeschaffung kann sich auch aus Rechtsnormen ausserhalb der eidgenössischen und kantonalen Datenschutzgesetze ergeben. Zu denken sind etwa an besonders arglistige Beschaffungsmethoden, Täuschung (Art. 28 OR) oder auch das Gesetz gegen den unlauteren Wettbewerb (Schutz vor missbräuchlichen Geschäftsbedingungen).

Art. 179 bis, ter, quater, novies  
StGB

*Was heisst rechtmässige Beschaffung?* Die Beschaffung von Personendaten und die Einwilligung durch die Betroffenen kann auf vielfältige Art und Weise erfolgen, was vom Gesetz in dieser Fülle nicht abgedeckt werden kann. In diesen nicht explizit geregelten Fällen kommen die Grundsätze der Verhältnismässigkeit und von Treu und Glauben gemäss DSG zur Anwendung (Vgl. [Schweizer, 1999]). Für den Grundsatz der Beschaffung von Personendaten nach Treu und Glauben gilt insbesondere:

Art. 4 Abs. 2  
u. 4 DSG

- Vortäuschung anderer Verwendungszwecke (z.B. Marktforschung) verstösst nicht nur gegen das DSG, sondern auch gegen UWG.
- Die weitere Verwendung von Personendaten für andere Verwertungszwecke als ursprünglich angegeben ohne erneute Einwilligung der Betroffenen ist nicht zulässig.
- Eine verschleierte oder ungenaue Zweckangabe widerspricht ebenfalls dem Grundsatz von Treu und Glauben (in diese Kategorie kann man euphemistische Beschreibungen wie "administrative Datenverarbeitung" oder "to provide value added information" zählen).

<sup>15</sup> Heimliche Übermittlung von Kennzeichnungen installierter Software an einen Webserver; siehe zum Beispiel [Rötzer, 23. März 1999]

<sup>16</sup> heimliche Übermittlung von Namen und Kategorisierung heruntergeladener Multimediadateien; siehe *Privacy Forum Archive*, Vol. 9 Issue 15, 18. Mai 2000, <http://www.vortex.com/privacy/priv.09.15>, sowie [Heise Newsticker, 11. Nov. 1999] für einen früheren Fall

<sup>17</sup> User Tracking durch die Kombination von Werbebannern und Cookies auf Webseiten; die US-Firma DoubleClick.net ist ein führender Anbieter von Werbebannern im Internet und befindet sich in Fusionsverhandlungen mit dem US-Marktführer im Bereich des Adresshandels, Abacus Inc. (siehe [DoubleClick Inc., 14. Juni 1999]). Gegen diesen Merger hat die Federal Trade Commission (FTC) Einwände erhoben und untersucht auch die sonstigen Geschäftspraktiken von DoubleClick.net (siehe <http://www.ftc.gov/opa/2000/02/dblclickstajb.htm>).

- Die Betroffenen müssen auf die besondere Natur der Erkenntnisse, welche aus dem Einsatz von Data Mining-Methoden resultieren können, hingewiesen werden.

Die Verhältnismässigkeit der Beschaffung orientiert sich an drei Grundsätzen: Keine Datensammlung "auf Vorrat"; Reaktionsdaten, welche zusätzlich zu den Bestandsdaten gespeichert und ausgewertet werden, sind alleine für den Bearbeitungszweck der Vertragserfüllung erforderlich, eine Speicherung und Auswertung mit Data Mining-Methoden geht meist wesentlich über die Zweckbindung hinaus; durch die Kombination von Reaktions- und Bestandesdaten können eigentliche Persönlichkeitsprofile entstehen, die der besondere datenschutzrechtlichen Beachtung bedürfen und daher möglichst vermieden werden sollten.

## 2.2 Datenbearbeitung und -richtigkeit

"Bearbeitung" im Sinne des DSG umfasst den gesamten "Lebenszyklus" von Daten, unabhängig von den dabei angewandten Methoden. Im Kontext des Data Mining ist "Bearbeitung" enger gefasst, namentlich in die Aufbereitung der Daten, der Auswahl von Testgruppen und Methoden, sowie die Anwendung der parametrisierten Modelle auf die Grundgesamtheit respektive einzelne Datensätze (zum Beispiel Regelbasierte System bestehend aus Wissenserwerb, Wissensdarstellung, Wissensherleitung, Herleitungserklärung).

Art. 3  
lit. e DSG

Jeder Arbeitsschritt, der Daten bestimmter oder bestimmbarer Personen involviert ist prinzipiell datenschutzrechtlich relevant, doch die Resultate der Anwendung von Data Mining-Methoden sind mehr als die Summe der einzelnen Arbeitsschritte: *Ziel* des Einsatzes von Data Mining-Methoden *ist* ja gerade die Gewinnung bisher verborgener Zusammenhänge und Merkmale. Um den Grundsatz der Zweckbindung nicht zu verletzen muss daher spätestens vor dem Einsatz von Data Mining-Methoden die Einwilligung der Betroffenen vorausgesetzt werden können. Zudem sind die Betroffenen darauf hinzuweisen, dass durch Data Mining-Methoden neue Zusammenhänge und Merkmale aufgedeckt werden können [Schweizer, 1999, p. 107].

Betroffene Personen haben – unabhängig vom Verwendungszweck – ein Recht auf die Richtigkeit ihrer Daten (respektive die Feststellung der Unrichtigkeit, siehe Art. 3 lit. e DSG i.V.m. Art. 5 DSG). Gewisse statistische Methoden (zum Beispiel Clustering) können Daten in einer Art und Weise verändern, dass die Zuordnung zu gewissen Klassen und Kategorien in einer Einzelfallbetrachtung falsch sein kann respektive dass die Klassifizierung gemäss den Data Mining-Methoden nicht dem tatsächlichen Bild der Person entspricht. Das bedeutet für den Datenbearbeiter eine gesteigerte Pflicht zur Kontrolle der angewandten Modelle und eine erhöhte Sorgfaltspflicht bei der Auswahl von Stichproben und Kontrollgruppen.

Die *Qualität* der Data Mining-Resultate ist demnach nicht nur von der Richtigkeit der Ausgangsdaten abhängig (nach dem Motto "trash in – trash out"), sondern auch von der Wahl *angemessener* Methoden, welche die Gefahr einer Verletzung der Persönlichkeitsrechte betroffener Personen minimieren.

Über aktuelle Bearbeitungsfälle hinaus werden einmal gewonnene Daten zweckmässigerweise in reproduzierbarer Form abgespeichert, sinnvollerweise in Data Warehouses. Diese Speicherung und Archivierung erweist sich datenschutzrechtlich als bedeutsam, da durch die

Kombination von Personendaten und Bestandesdaten mit Data Mining-Resultaten wiederum Persönlichkeitsprofile entstehen können. Data Warehouses sind jedoch nicht a priori durch das Datenschutzgesetz verboten, müssen jedoch den üblichen Datenschutzerfordernungen gemäss DSG genügen (rechtsgültige und transparente Einwilligung, Need-to-Know-Prinzip und Zugriffskontrolle respektive -protokollierung, Datensparsamkeit und Datenvermeidung, Ermöglichung des Auskunftsrechts).

Art. 9 Abs. 2  
VDSG

[EDSB, o. Datumb] bemerkt dazu lapidar und einleuchtend: "Löschen Sie die nicht mehr benötigten Daten".

### 2.3 Datenbekanntgabe und -handel

Im Datenschutzgesetz ist der Begriff der "Bekanntgabe" weit gefasst – er umfasst sowohl die Einzelfallbezogene Weitergabe von Daten als auch das Massengeschäft. Nicht unter die Bekanntgabe fällt hingegen, wenn ein Unternehmen für Dritte an mehr oder weniger spezifisch spezifische Adressaten gelangt, da in dem Fall die Daten in der Hand des Datensammlers verbleiben.<sup>18</sup>

Art. 11 Abs.  
3 DSG

Nicht nur reine Personendaten, sondern auch die Resultate von Data Mining-Analysen können Handelsobjekte sein. Im Unterschied zu physischen Waren können Personenmerkmale hingegen mehrfach verkauft und in unterschiedlichen Kontexten eingesetzt werden, wodurch sich auch der relativ hohe Wert der Personendaten für Datensammler ergibt.

Beispielsweise lässt sich aufgrund der Merkmale "Einfamilienhaus" und "Zaun" mit einer Wahrscheinlichkeit von siebzig Prozent auf einen Hundehalter schliessen, was für einen Hersteller von Hundefutter interessant sein kann.<sup>19</sup>

### 2.4 Datensicherheit

Datensicherheit ist ein wesentlicher Bestandteil des Datenschutzes. Ohne Datensicherheit gibt es keinen Datenschutz. Die technischen und organisatorischen Massnahmen (Art. 7 DSG) sind primär zum Schutz der Betroffenen zu realisieren.

(Eidgenössischer Datenschutzbeauftragter, Leitfaden zu den technischen und organisatorischen Massnahmen des Datenschutzes)

Dass die verschiedenen Aspekte der Datensicherheit<sup>20</sup> nicht nur aus der Sicht des Datenschutzes relevant sind, versteht sich von selbst. Im Bereich besonders schützenswerter Daten und von Persönlichkeitsprofilen müssen jedoch zusätzliche Aspekte beachtet werden.

*Outsourcing:* Wenn unternehmensfremde Dritte Zugang zu Computersystemen und Daten haben, unterstehen diese ebenfalls den datenschutzrechtlichen Regelungen, ähnlich wie im Bereich des Bankgeheimnisses respektive allgemeiner im Kontext des Geschäftsgeheimnisses (siehe [EDSB, 1995, Kapitel I. 7.3, Softwarewartung] und [EDSB, 1995, Kapitel II. 15, Anwendbarkeit des Bundesgesetzes über den Datenschutz]). Der für die Datensammlung

Art. 14 DSG

<sup>18</sup> Persönliche Auskunft von Schober Information Group vom 15. Mai 2000

<sup>19</sup> Das Beispiel ist [Pietsch, Werner, Weber, Daniel, 1998] entnommen.

<sup>20</sup> Zugriffsrechte, Protokollierung, Sicherstellung von Datenintegrität und andere, siehe [Lusti, 1997]

Verantwortliche hat dafür zu sorgen, dass Dritte mit den Daten nur so umgehen, wie er es selbst dürfte.

*”Need to know”-Prinzip:* Die Einschränkung der Zugriffsrechte auf das zur jeweiligen Aufgabenerfüllung Notwendige entspricht dem datenschutzrechtlichen *”Need to know”-Prinzip*.

*Organisatorische Massnahmen:* Der Datenschutz bestimmt gewisse Mindestmassnahmen in Bezug auf die Protokollierung der Bearbeitung und des Handels (der Bekanntgabe) von Personendaten, insbesondere um das Auskunftsrecht sicherstellen zu können, aber auch um dem Datenschutzbeauftragten eine wirksame Kontrolle der angemeldeten Datensammlungen zu ermöglichen. Art. 9 VDSG

Die Einhaltung der technischen und organisatorischen Massnahmen ist Bestandteil des IT-Controlling respektive IT-Auditing; der Datenschutz schafft in diesem Bereich keine grundsätzlich neuen Anforderungen, sondern bedient sich der Mechanismen, die in einer seriösen Datenverarbeitung sowieso schon inhärent sein *sollten*. Art. 29 DSG

Weitergehend sind hingegen die möglichen Kontrollen durch den eidgenössischen oder die kantonalen Datenschutzbeauftragten, wobei der Inhaber der Datensammlung eine Mitwirkungspflicht innehat. Der Eidgenössische Datenschutzbeauftragte kann lediglich *Empfehlungen* aussprechen, welche jedoch gemäss Verwaltungsverfahrensgesetz von der Eidgenössischen Datenschutzkommission sanktioniert werden können.

### 3 Ausgewählte Fragestellungen

Data Mining-Methoden sind überall dort besonders erfolgversprechend, wo bereits grössere Datenmengen in ausreichender Qualität vorliegen. Insbesondere betrifft dies Banken und die mit ihnen häufig verbundenen Kreditkartenunternehmungen, Versicherungen, Telekommunikationsunternehmen, professionelle Datenhändler und staatliche Behörden. Andere Branchen, die sich vornehmlich an ein anonymes Publikum richten, haben in der Regel keine Notwendigkeit zur Speicherung personalisierter Datensätze, sondern arbeiten zum Beispiel mit anonymen Clusterdaten.

Im Folgenden werden einige Anwendungsgebiete des Data Mining – teilweise nach [Lusti, 1999, Kapitel 6] – herausgegriffen.

#### **Anwendungsgebiete des Data Mining und datenschutzrechtliche Implikationen**

Branchenunabhängiges Hauptanwendungsgebiet (mit zugleich grossen datenschutzrechtlichen Implikationen) ist das Database Marketing, und in dem Zusammenhang die Direktwerbung. [Schweizer, 1999, Kap. 2] unterteilt Data Mining in die Anwendungsgebiete "intern" und "kundengerichtet": Interne Anwendungsgebiete sind etwa die Kreditprüfung von Banken, das kundenindividuelle Risikomanagement von Versicherungen und Krankenkassen sowie die individuelle Kundenbeurteilung (Rentabilität, Bonität, ...).

Zu den internen Anwendungsgebieten kann man auch den Einsatz von Data Mining-Methoden zur Aufdeckung von Missbrauchs- und Betrugsfällen zählen. Da in diesen Fällen Rechtfertigungsgründe gem. Art. 13 DSGVO vorgebracht werden können (Überwiegendes privates Interesse, Zusammenhang mit Vertragsabwicklung), dürften diese Methoden datenschutzrechtlich unbedenklich sein.

Kundengerichtete Anwendungsgebiete betreffen Methoden, welche die Identifizierung potentieller Neukunden, die Analyse bestehender Kundenbeziehungen (Demographie und Fluktuationen) und Identifikation von Cross Selling-Potential ermöglichen (siehe [Lusti, 1999, p. 250])

#### **3.1 Gesundheitswesen**

Im Gesundheitswesen werden "besonders schützenswerten" Daten verarbeitet, welche wesentlichen Einschränkungen in Bezug auf Bearbeitung und Bekanntgabe unterliegen. Im komplexen Geflecht von datenschutzrechtlichen Anforderungen, bindendem und dispositivem Sozialversicherungsrecht, versicherungsmathematischen und marketingbestimmten Faktoren und dem Druck auf (administrative) Kosten bestehen vielfältige Widersprüche. Als weitere Verschärfung der Datenschutzvorschriften kann man die berufliche (ärztliche) Schweigepflicht auffassen.

Auswege aus diesem Dilemma sind zum Beispiel das "Need to know"-Prinzip (siehe [Landesbeauftragte für den Datenschutz, 19. April 2000]) und organisatorische Massnahmen des

Datenschutzes und der Datensicherheit sowie kryptographische Sicherungen, die den Datenzugriff auf einen möglichst kleinen Personenkreis beschränkt.

Dieses Minimalprinzip wird durch automatisierte Abrechnungssysteme zwischen Leistungserbringern und Kostenträgern potentiell gefährdet.

Wie auch in anderen Branchen ist das *Vertrauen* der Kunden in die Krankenkassen und andere Anbieter von Leistungen im Sozialbereich ein zentraler Erfolgsfaktor. Unter diesem Aspekt müssen die Anbieter den möglichen Nutzen aus der Anwendung von Data Mining-Methoden und den potentiell negativen Einfluss auf die Kundenbindung durch Vertrauensverlust gegeneinander abwägen. Eindeutige Regelungen und Rechtssprechungen gibt es in diesem Bereich (noch) nicht, obwohl dieser Problembereich schon seit mindestens 1984 bekannt ist (Bericht "Datenschutz im Medizinalbereich" einer vom Bundesamt für Justiz eingesetzten Experten-Gruppe, zitiert nach [EDSB, 1998, Kapitel I. 6.3, *Die H+ Spitalstatistik wird endlich mit anonymisierten Daten geführt*]).

Der Einsatz von Data Mining-Methoden hat für die betroffenen Personen (Patienten) auch gewisse Vorteile. So können durch den Vergleich von Krankheitsverlaufsdaten Ähnlichkeiten in verschiedenen Krankheitsbildern erkannt und darauf abgestimmt Behandlungsmassnahmen mit bekannten Nebenwirkungen ausgewählt werden oder die Wirkung von Medikamenten und Therapieformen für Patienten in unterschiedlichen Altersgruppen verglichen werden. Diese Anwendungsgebiete sind so lange datenschutzrechtlich unbedenklich, wie sie sich im Umfeld von Forschung und Behandlung bewegen (siehe auch [EDSB, o. Datum]).

### 3.2 Grenzüberschreitende e-Commerce-Anwendungen

Sogenannte "e-Commerce"-Anwendungen<sup>21</sup> liefern Daten, welche einfach in ein Data Warehouse übernommen werden können, da sie in der Regel bereits in strukturierter, elektronischer Form erhoben werden. Diese Daten machen die eigentlichen Kundenbeziehungen aus und stellen einen wesentlichen Teil des Unternehmenswertes dar, die optimale Verwertung dieser Daten ist für diese Firmen daher unabdingbar.

Ausserhalb Europas, namentlich in den USA, gibt es kaum datenschutzrechtliche Regelungen auf Gesetzes- oder Verordnungsstufe.<sup>22</sup> In den USA wird Wert auf eine Selbstregulierung der datenverarbeitenden Unternehmen – und hier insbesondere der Internet-spezifischen Datensammlungen – gelegt, auch wenn die FTC (Federal Trade Commission) gewisse Befugnisse aus anderen Gesetzestiteln, namentlich aus dem Bereich des Konsumentenschutzes, besitzt. Diese unterschiedliche Haltung führt im transatlantischen Datenverkehr dazu, dass die USA durch die EU *nicht* als "Safe Harbour" angesehen wird und dementsprechend keine dem Datenschutz unterstehenden Datensammlungen von EU-Bürgern in die USA ausgeführt werden dürften. Der Ausgang dieses Disputs ist noch offen [Rötzer, 16. März 2000]. Amerikanische Privacy Rights-Organisationen und neuerdings auch die FTC vertreten *subsidiär* zu den Selbstregulierungen gewisse gesetzliche Mindeststandards des Datenschutzes (siehe [Rötzer, 23. Mai 2000]).

<sup>21</sup> Im weiteren wird auf die modischen angelifzierten *e*-Auszeichnungen verzichtet

<sup>22</sup> Unter <http://www.datenschutz-berlin.de/infomat/heft24/inh.htm> findet sich eine Auflistung relevanter Regelungen.

Beispielsweise speichert der Versandhändler Amazon.com die gesamte Kontakthistory seiner Kunden und bietet ihnen bei der nächsten Anmeldung Produkte aus den gleichen oder ähnlichen Kategorien wie bei früheren Käufen auf der Einstiegsseite an. Die Amazon-Privacy Policy<sup>23</sup> postuliert für den Umgang mit Daten, die über reine Bestelldaten hinausgehen, gewisse Grundsätze, die auch mit EU- und schweizerischen Datenschutzrichtlinien konform gehen dürften. Allerdings ist der Passus auf der us-amerikanischen Webseite, welcher eine Blankovollmacht für die Bekanntgabe der Daten an Dritte enthält, nach europäischem Recht nicht zulässig. Auf der Webseite der deutschen Niederlassung steht denn auch (Hervorhebungen durch den Autor):

Amazon.de stellt Ihre persönlichen Daten *nicht Dritten* außerhalb der Amazon.com-Unternehmensgruppe zur Nutzung zur Verfügung. Um Ihnen auch in Zukunft das bestmögliche Einkaufserlebnis und sinnvolle Zusatzdienste anbieten zu können, schließen wir allerdings nicht aus, daß wir die Kundendatenbank von Amazon.de durch Dritte *anonym analysieren* und verbessern lassen.

Dies geschieht jedoch selbstverständlich unter strenger Wahrung der Vertraulichkeit Ihrer Daten. Es ist auch möglich, daß wir Statistiken über unsere Kunden, unseren Umsatz, Kundenverhalten und darauf bezogene Site-Informationen vertrauenswürdigen Dritten bereitstellen. Diese werden jedoch soweit zusammengefaßt sein, daß *einzelne Personen nicht mehr identifizierbar sind*.

Art. 6 DSGVO

Die Amazon.com-Unternehmensgruppe ist in den USA domiziliert; eine Bekanntgabe von Personendaten von Amazon.de an Amazon.com ist demnach zumindest nach Schweizerischem Recht nicht zulässig.

Um das Vertrauen der Kunden in den Onlinehandel zu stärken, schlägt [EDSB, 2000, p. 2] folgende Massnahmen vor:

- Das DSGVO ist flexibel und technologisch neutral verfasst. Daher drängen sich keine Gesetzesänderungen auf.
- Gesetzliche Regelungen alleine genügen nicht. Die Benutzer müssen entsprechend informiert und sensibilisiert werden. Mittelfristig ist die Sensibilisierung mittels Weiterbildungsmaßnahmen der Benutzer voranzutreiben.
- Um das Vertrauen der Benutzer in den elektronischen Geschäftsverkehr zu verstärken, sollen (wie dies auch vom DSGVO vorausgesetzt wird) die Anbieter von Dienstleistungen die Kundendaten transparent bearbeiten. Die Anbieter sollen die Benutzer informieren, welche Personendaten sie für welchen Zweck bearbeiten möchten. Wenn Personendaten aus einem Vertragsverhältnis zu anderen Zwecken (Bsp. Marketing, Werbung) bearbeitet werden, sollen die Benutzer Wahlmöglichkeiten haben.
- Technologien wie kryptografische Verfahren, Authentifizierungsverfahren und andere datenschutzfreundliche Technologien wie bspw. der Einsatz von Anonymisierungstools, sind für die Datensicherheit geeignet. Diese sollen im Umfeld des elektronischen Geschäftsverkehrs eingesetzt und den Benutzern zur Verfügung gestellt werden.

<sup>23</sup> <http://www.amazon.com/exec/obidos/subst/misc/policy/privacy.html> respektive <http://www.amazon.de/exec/obidos/subst/help/dataprotection.html> für die praktisch gleichlautende Policy von Amazon.de, der deutschen Niederlassung von Amazon.com

- Schliesslich kann der Schutz der Privatsphäre, insbesondere die transparente Datenbearbeitung, das Vertrauen der Benutzer im elektronischen Geschäftsverkehr verstärken. Dies kann für schweizerische Unternehmen durchaus als Wettbewerbsvorteil genutzt werden.

Nicht nur unter den Datenschutz, sondern allenfalls auch unter zivil- und strafrechtliche Regelungen fallen Akte von leichter oder grober Fahrlässigkeit, wie sie beispielsweise in Internetbasierten Anwendungen immer wieder zu beobachten sind. In diesen Fällen ist die Verletzung datenschutzrechtlicher Vorschriften nur ein Teil der gesamthaft zu betrachtenden Verstösse.<sup>24</sup>

### 3.3 Data Mining am Beispiel von Echelon

Der wohl weltweit grösste Anwender von Data Mining-Methoden ist die NSA, die National Security Agency, ein us-amerikanischer Geheimdienst. Während schon die Existenz der NSA an sich während Jahrzehnten negiert wurde (von den Abhör- und Auswertungsmethoden ganz zu schweigen), wurden in den letzten zwei Jahren (1999, 2000) auf journalistischen Druck hin entsprechende Gerüchte und Berichte bestätigt (siehe [Woolsey, 7. März 2000] und [Woolsey, 18. März 2000]). Im STOA-Bericht (siehe [Campbell, April 1999]) wurde die Existenz des weltweiten Abhör- und Auswertungssystems Echelon<sup>25</sup> einem grösseren Publikum erstmals quasi-offiziell dargelegt, obwohl die Existenz eines derartigen Systems aufgrund von Indizien (Patente, Installationen) schon lange vermutet worden war (eine Übersicht findet sich in [Feyerthum, 1998]).

Primärer Fokus von Echelon sind eher der wirtschaftliche und politische Kontext denn private Personen. Nichtsdestotrotz ist aufgrund der groben Rasterung der eingesetzten Data Mining-Technologien<sup>26</sup> anzunehmen, dass datenschutzrechtliche Grundsätze verletzt werden, zumal die nach europäischem Verständnis erforderliche gesetzgeberische Grundlage für Europäer fehlt.

Gegen den Eingriff in die Privatsphäre durch staatliche und nicht-staatliche Überwachung können sich Betroffene auf verschiedenen Wegen zur Wehr setzen:

- *Einsatz von (starker) Kryptographie:* Die Überwachung wird entscheidend erschwert, wenn die übermittelten Daten verschlüsselt werden. Aktuell sind ausserhalb der USA und Frankreichs Produkte mit starker Verschlüsselung frei erhältlich – starke Verschlüsselung bedeutet in dem Fall, dass eine Entschlüsselung nicht mit einem nutzungsgerechten Aufwand erfolgen kann (siehe als Einstieg etwa [Donnerhacke, 17. Dezember 1997] und [SIUG, 1999]).

<sup>24</sup> siehe [c't, 11/2000]

<sup>25</sup> Betreiber des Echelon-Systems sind: USA, Kanada, Grossbritannien, Neuseeland, Australien, Schottland

<sup>26</sup> Über die genaue Funktionsweise der eingesetzten Werkzeuge ist wenig bekannt. Aufgrund erteilter Patente (unter anderem zu Semantic Forests) ist anzunehmen, dass ein fortgeschrittener Keyword-Search mit kontextabhängiger Parametrisierung als Eingangsstufe in das System durchgeführt wird. Der Auswertung vorgelagert sind Systeme der Text-, Sprach- und Bilderkennung.

Nicht verhindern kann eine Verschlüsselung, dass die Kommunikationsbeziehung an sich festgestellt werden kann; dagegen hilft u.a. der Einsatz von pseudonymen oder "echt" anonymen Remailern (siehe [Donnerhacke, 20. Dezember 1996]).

- *Anwendung der datenschutzrechtlichen Sanktionsmöglichkeiten:* Wenn die Überwachung durch eine der lokalen Jurisdiktion unterstellte Körperschaft erfolgt, kann das gesamte Datenschutzrecht zur Anwendung gelangen (Auskunftsrecht, Widerspruchsrecht, zivilrechtliche Unterlassungsansprüche etc.).

Das Echelon-System wirft nicht nur, aber besonders, auf der Ebene des Datenschutzes und der Persönlichkeitsrechte Fragen auf, die allerdings mit datenschutzrechtlicher Argumentation alleine nicht gelöst werden können. Die Implikationen gehen weit über den Datenschutz hinaus.

### 3.4 Adress- und Datenhandel

Die Branche der Adress- und Datenhändler ist offensichtlich vom Datenschutzgesetz betroffen, insbesondere im Bereich privater Adressen und Daten.<sup>27</sup> Im Hinblick auf die erschwerte Verkäuflichkeit "besonders schützenswerter Daten" ist davon auszugehen, dass solche in der Regel gar nicht erst erhoben werden. Das Datenschutzgesetz an sich ist für die Branche positiv zu werten, weil es eine gewisse Seriosität bedingt (Anmeldung der Datensammlungen beim Eidgenössischen Datenschutzbeauftragten, generalpräventive Wirkung des DSG, ...).

Die Adress- und Datenhändler sind im gesamten "Lebenslauf" der Daten an das Datenschutzgesetz gebunden: etwa beim Datenein- und -verkauf werden vertraglich die Einhaltung der einschlägigen Bestimmungen ab- und zugesichert.

Data Mining- oder allgemeiner statische Methoden der Datenbearbeitung besitzen einen grossen Stellenwert, da diese das "Auswertungswissen" von Experten codifizieren. Mit zunehmenden Iterationen uebersteigt die Qualität der statistischen Methoden den Erfahrungsvorsprung der Experten.

Grenzüberschreitender Adresshandel ist noch relativ unbedeutend; Adressdaten sind primär eine nationale Angelegenheit und daher internationalen Unterschieden in der Datenschutzgesetzgebung nur wenig unterworfen. Das Problemgebiet ist jedoch bekannt und wird aufmerksam beobachtet. Unterschiede zwischen der Schweiz und der EU in Bezug auf den Datenschutz bestehen hauptsächlich in Bezug auf die mögliche Granularität der Daten: in der EU dürfen Daten nur auf *Haushalts-*, in der Schweiz auch auf *individueller* Ebene bearbeitet werden.

Wer überdie Data Warehousing- und Data Mining-Technologie verfügt und Personendaten auswertet, hat [...] eine Art künstlicher Geldmaschine, welche wie ein Perpetuum mobile immer wieder neue personenbezogene Merkmale,

---

<sup>27</sup> Dieser Abschnitt beruht auf einem persönlichen Gespräch mit der Schober Information Group vom 15. Mai 2000; siehe auch Kapitel 2.3

Gewohnheits- und Verhaltensmuster an das Tageslicht befördert. Der kommerzielle Datenhandel mit personenbezogenen Informationen ist ohne Zweifel zu einem sehr lukrativen und gewinnbringenden Geschäft geworden.<sup>28</sup>

Fraglich ist, welchen ökonomischen Wert solche Informationen tatsächlich haben, und inwiefern der Datenhandel datenschutzrechtlich solches Vorgehen zulässt. Besonders im Rahmen von Informationspools verschiedener Unternehmen (beispielsweise die Cross Selling-Programme von Swisscom (Joker) und UBS (Key-Club)) ist die Grenze zwischen erlaubtem Datenhandel und der Anfertigung von Persönlichkeitsprofilen eher schwammig.

Unter den weit gefassten datenschutzrechtlichen Begriff der Bekanntgabe fallen alle denkbaren Möglichkeiten und Formen, wie etwa Verkauf, Austausch, Leasing, Vermietung, Schenkung, Lizenzerteilung, Online-Abruf, Veröffentlichung in Druckerzeugnissen, via Telefon, Fax, mündliche, schriftlich usw. Voraussetzung ist jeweils, dass diese Daten personenbezogen sind – rein sachbezogene Daten, die sich auf keine bestimmte oder bestimmbare Person beziehen, fallen nicht unter den Anwendungsbereich des Datenschutzgesetzes.

Gemäss dem 4. Tätigkeitsbericht des Eidgenössischen Datenschutzbeauftragten ([EDSB, 1997]) ist die private, kommerzielle Verwertung von öffentlich zugänglichen Registerdaten nicht zulässig, da diese zweckgebunden sind.

Gemäss Datenschutzgesetz müssen auch gehandelte Daten den üblichen Grundsätzen des DSG entsprechen (Zweckbindung, Einwilligung, Richtigkeit, Verhältnismässigkeit, Datensicherheit), andererseits greifen auch die vorgesehenen Rechtfertigungsgründe.

---

<sup>28</sup> [Schweizer, 1999, p. 281]

## 4 Rechtsbehelfe und Rechtsfolgen

Wichtigstes Mittel für betroffene Personen ist das Auskunftsrecht gegenüber den Betreibern von Datensammlungen. Bei Missbräuchen stehen eine ganze Reihe von Rechtsbehelfen zur Verfügung, die über das DSG hinausgehen, etwa nach ZGB (Art. 28a Abs. 1, Unterlassungs- und Beseitigungsklagen, sowie diverser weiterer Artikel, welche in extremis Schadenersatz für materielle und immaterielle Schäden ermöglichen).

Art. 8 DSG,  
Art. 15 DSG,  
Art. 28a ZGB

Ähnliche Ansprüche erwachsen aus dem DSG selbst, etwa auf Richtigstellung respektive Feststellung der Unrichtigkeit der Daten, Anspruch auf Sperrung und Vernichtung<sup>29</sup> sowie auf Durchsetzung des Auskunftsrecht.

Für die Datensammler kann sich aus dem Datenschutzgesetz die Pflicht ergeben, die Betroffenen über den Einsatz von Data Mining-Methoden zu orientieren<sup>30</sup>

### Datenschutzbeauftragte und Datenschutzkommission

Die Aufsicht über Datensammlungen und über datenschutzrechtliches Verhalten von Behörden und Privaten wird durch den Eidgenössischen Datenschutzbeauftragten ausgeübt. Diesem kommt primär eine Informations- und Auskunftsfunktion zu, etwa in Form der Tätigkeitsberichte zuhanden des Bundesrates oder sonstigen Publikationen zuhanden von privaten Personen und Inhabern von Datensammlungen.

Werden Empfehlungen des Datenschutzbeauftragten nicht befolgt oder abgelehnt, so kann er die Angelegenheit der Eidgenössischen Datenschutzkommission zum Entscheid vorlegen (Art. 29 Abs. 4 DSG).

Weiter führt der Datenschutzbeauftragte ein Register der privaten Datensammlungen und muss über die Ausführung von Personendaten ins Ausland informiert werden – dies betrifft sämtliche Personendaten, nicht nur allfällig durch Data Mining-Methoden gewonnene zusätzliche Daten.

### Auskunftsrecht

Wichtigstes Rechtsmittel für private Personen ist das Auskunftsrecht gemäss Art. 8 DSG. Inhaber von Datensammlungen sind dadurch verpflichtet, kostenlos und vollständig über die bei ihnen gespeicherten Personendaten Auskunft zu erteilen. Zur Erinnerung: Eine Datensammlung ist nach DSG jeder Bestand von Personendaten, der so aufgebaut ist, dass die Daten nach betroffenen Personen erschliessbar sind.

Art. 8 DSG

Der Eidgenössische Datenschutzbeauftragte ([EDSB, 1998, p. 66]) hat präzisiert, dass auch allfällig gespeicherte Data Mining-Resultate in die Auskunft mit einbezogen werden müssen, nicht jedoch Daten über Dritte (denn dadurch könnte wiederum deren Persönlichkeitsrecht verletzt werden).

<sup>29</sup> Die Vernichtung und Sperrung von Daten kann zu einem logischen Zirkelschluss führen: Wenn die Daten einer Person vernichtet werden können in Zukunft wiederum Daten über diese Person erfasst werden. Bei automatisierter Massenverarbeitung kann dies prinzipiell nicht ausgeschlossen werden.

<sup>30</sup> [EDSB, 1999]

Teil der Auskunft muss ebenfalls sein, welche Daten überhaupt gespeichert werden und welche Bedeutung den einzelnen Attributen zukommt, woher und von wem die Daten stammen. Die Auskunft hat in der Regel kostenlos zu erfolgen.

## 5 Folgerungen für den praktischen Einsatz von Data-Mining-Technologien

Datenschutz bedeutet nicht, dass Unternehmen auf Marktforschungsmechanismen oder auf die Bildung von massgeschneiderten Marketingprofilen gänzlich verzichten müssen. Für den Fall, dass Daten von Unternehmen auf diese Weise genutzt werden, sind die Betroffenen vorgängig genau darüber zu informieren, mit welchen Bearbeitungsmethoden und Bearbeitungszwecken sie zu rechnen haben. Auf diese Weise können sie sich gegebenenfalls der Bearbeitung widersetzen.

(Eidgenössischer Datenschutzbeauftragter, 6. Tätigkeitsbericht 1998/1999, p. 116)

Mit zunehmender Verlagerung von Wirtschaftsaktivitäten in elektronische Medien vergrössern sich die Möglichkeiten der Datengewinnung überproportional. Als Gegenstück zu den "klassischen" Persönlichkeitsrechten stellt der Datenschutz eine Möglichkeit für die Kunden und Bürger dar, ihr Recht auf informationelle Selbstbestimmung auszuüben.

Voraussetzung für die Wahrnehmung dieser Rechte ist die Aufklärung und Weiterbildung der betroffenen Personen, aber auch eine Sensibilisierung der Inhaber von Datensammlungen für die Belange des Datenschutzes. Fahrlässig (geschweige denn vorsätzlich) in ihren Persönlichkeitsrechten Verletzte sind schlechte Kunden.

Das datenschützerische *Ceterum censeo* des *Grundrechtes auf Datenschutz* hat insbesondere Implikationen auf die Methoden des Data Warehousing und des Data Mining als Schlüsseltechnologien zur Pflege von Kundenbeziehungen. Trotz – oder wegen – der Fülle an Daten und Informationen müssen Inhaber von Datensammlungen darauf bedacht sein, den Betroffenen jederzeit die grösstmögliche Transparenz zu garantieren und nicht aus falsch verstandenem Datenwert blindlings Archive von Persönlichkeitsprofilen zu akkumulieren.

Datenschutz ist jedoch nicht ein *Zustand*, sondern ein *Prozess*, dessen Fortschreibung im Kräftefeld zwischen wirtschaftlichen und persönlichen, politischen und Partikularinteressen nicht vorgezeichnet ist. Den überempfindlichen Betroffenen gilt es gleichsam im Rahmen der Angemessenheit zu beschützen wie es den Datensammelwütigen in der Wahl seiner Mittel einzuschränken möglich sein muss.

In Bezug auf die Anwender von Data Warehousing- und Data Mining-Methoden lassen sich die wichtigsten datenschutzrechtlichen Elemente zur Beachtung wie folgt zusammenfassen:

- *Datenvermeidung und Datensparsamkeit*

Daten, die gar nicht erst beschafft und bearbeitet werden, können keine Persönlichkeitsrechte verletzen. Mit jedem zusätzlichen Attribut steigt die Wahrscheinlichkeit, dass der Datensatz für sich alleine oder in Verbindung von mittels Data Mining gewonnenen Verknüpfungsinformationen ein Persönlichkeitsprofil darstellt. Die Zahl der Attribute konstituiert für sich alleine zwar noch keine datenschutzrechtlich Relevanz, führt aber umso leichter zur Unterstellung unter das Datenschutzgesetz, je einfacher die Daten mit anderen zu verknüpfen sind.

- *Organisatorische Massnahmen*

Datensicherheit in seinen verschiedenen Ausprägungen ist ein Grundelement des Datenschutzes (Art. 8ff VDSG). Geregelt werden muss insbesondere der Zugriff (unter Umständen unter Berücksichtigung der Bekanntgabe an Dritte) sowie die Protokollierung der Bearbeitung (Datenträger, Transport, Speicherung, Eingabe, Änderung, ...).

Bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen sollen höhere Anforderungen an die Protokollierung gestellt werden, welche zudem durch ein verantwortungsvolles IT-Auditing überprüfbar sein müssen.

Diese Massnahmen sind nicht allein aus datenschutzrechtlichen Gründen erforderlich, sondern sollten Bestandteil eines jeden IT-Controlling und der Qualitätssicherung sein.

- *Definition von Zielen und Überprüfung auf datenschutzrechtliche Unbedenklichkeit*

Reine Datensammlungen "auf Vorrat" um des Datensammelns willen macht weder ökonomisch Sinn noch ist es datenschutzrechtlich unbedenklich. Jede Datenbeschaffung und -archivierung muss einem bestimmten Zweck dienen, die Bearbeitung mit einem bestimmten Ziel erfolgen.

Bei der Wahl der Ziele ist abzuwägen zwischen dem (ökonomischen und Erkenntnis-) Gewinn der Anwendung bestimmter Methoden und den daraus sich ergebenden datenschutzrechtlichen Implikationen.

Die Entscheidungsträger und Planer müssen auf die Belange des Datenschutzes sensibilisiert werden und sollen diese nicht als blosse Belastungsfaktoren, sondern als konstituierendes Element des Kundenvertrauens anerkennen können.

- *Verzicht auf individuell zuordenbare Attribute*

Viele Data Mining-Methoden müssen nicht zwingend mit Personendaten arbeiten, sondern können mit anonymisierten oder klassifizierten Daten durchgeführt werden, ohne einen nennenswerten Erkenntnisverlust hinnehmen zu müssen. Nur in den Fällen, in denen eine direkte Zuordnung unumgänglich ist, sollen Data Mining-Methoden angewandt werden, und auch dann nur, wenn die Daten nach ihrer Zweckbestimmung auch entsprechend bearbeitet werden dürfen.

Allgemeine Forderungen zum wirksameren Schutz der Privatsphäre finden sich etwa in [Landesbeauftragter für den Datenschutz Schleswig-Holstein, 4. November 1998]. Dort wird deutlich, dass Data Mining nur eines der Problemfelder im Umgang der Inhaber von Datensammlungen mit dem Datenschutz darstellt. Im eigenen Interesse und im Interesse ihrer Kunden sollten Anwender von Data Mining-Methoden bewusst versuchen, *datenschutzfreundliche Technologien* einzusetzen.

## Literaturverzeichnis

- Bundesgesetz über den Datenschutz (DSG)*. SR 235.1, 1992. (Stand am 7. Juli 1998).
- Julia Angwin. Web startup stirs up privacy concerns. *ZD Net*, 1. Mai 2000. URL <http://www.zdnet.com/zdnn/stories/news/0,4586,2558316,00.html>.
- Arbeitsgruppe "Datenschutzfreundliche Technologien". *Datenschutzfreundliche Technologie. Materialien des Arbeitskreises Technik der Landesdatenschutzbeauftragten*, o. Datum. URL <http://www.datenschutz-berlin.de/to/datenfr.htm>.
- Safe + Legal AG Belser. Das Persönlichkeitsprofil - Hinweise zur Interpretation von Art. 3 Bst. d DSG. Internes Rechtsgutachten Schober Information Group AG., 1999.
- Duncan Campbell. *DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION (An appraisal of technologies for political control)*. European Parliament, Directorate General for Research, Directorate A, The STOA Programme. Holdsworth, Dick, Head of STOA Unit, Luxembourg, April 1999. URL [http://www.iptvreports.mcmail.com/stoa\\_cover.htm](http://www.iptvreports.mcmail.com/stoa_cover.htm). The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition.
- c't. Sicherheitslücke bei Surf1. *c't – Magazin für Computertechnik*, Seite 76, 11/2000.
- Lutz Donnerhacke. Nichttechnische Einführung in PGP für Anfänger, 17. Dezember 1997. URL <http://www.iks-jena.de/mitarb/lutz/anon/pgp.html>.
- Lutz Donnerhacke. Anonyme Remailer, 20. Dezember 1996. URL <http://www.iks-jena.de/mitarb/lutz/anon/remail.html>.
- DoubleClick Inc. DOUBLECLICK INC. AND ABACUS DIRECT CORPORATION TO MERGE IN A \$1 BILLION STOCK TRANSACTION, 14. Juni 1999. URL [http://www.doubleclick.net/company\\_info/press\\_kit/pr.99.06.14.htm](http://www.doubleclick.net/company_info/press_kit/pr.99.06.14.htm).
- Eidgenössischer Datenschutzbeauftragter EDSB. *2. Tätigkeitsbericht 1994/1995*, 1995. URL <http://www.edsb.ch/cgi-bin/showme.cgi?Folder=d%2ft%2f2>.
- Eidgenössischer Datenschutzbeauftragter EDSB. *4. Tätigkeitsbericht 1996/1997*, 1997. URL <http://www.edsb.ch/cgi-bin/showme.cgi?Folder=d%2ft%2f4>.
- Eidgenössischer Datenschutzbeauftragter EDSB. *5. Tätigkeitsbericht 1997/1998*, 1998. URL <http://www.edsb.ch/cgi-bin/showme.cgi?Folder=d%2ft%2f5>.
- Eidgenössischer Datenschutzbeauftragter EDSB. *6. Tätigkeitsbericht 1998/1999*, 1999. URL <http://edsb.ch/pdf/tber99d.pdf>.
- Eidgenössischer Datenschutzbeauftragter EDSB. *Datenschutz und e-commerce: Umsetzungshilfe und Konkretisierungsvorschläge des Eidg. Datenschutzbeauftragten*, Februar 2000.

- Eidgenössischer Datenschutzbeauftragter EDSB. *Leitfaden für die Bearbeitung von Personendaten im medizinischen Bereich*, o. Datuma. URL <http://www.edsb.ch/cgi-bin/showme.cgi?Folder=d\%2fp\%2f1\%2f6>.
- Eidgenössischer Datenschutzbeauftragter EDSB. *Leitfaden für die Inhaber von Datensammlungen*, o. Datumb. URL <http://www.edsb.ch/cgi-bin/showme.cgi?Folder=d\%2fp\%2f1\%2f3>.
- EG-DRL. *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-DRL)*. Richtlinie 95/46/EG, 1995.
- Gundolf S. Feyermuth. Warum hast du so grosse Ohren? *NZZ Folio*, Seiten 38 ff., Juli 1998.
- Christian Haslach. Unmittelbare Anwendung der EG-Datenschutzrichtlinie. *Datenschutz und Datensicherheit (DUD)*, Seiten 693 ff., 12/1998.
- Heise Newsticker. Milliardenklage gegen RealNetworks. 11. Nov. 1999. URL <http://www.heise.de/newsticker/data/nl-11.11.99-000/>.
- Landesbeauftragte für den Datenschutz. Presseerklärung der Landesbeauftragten für den Datenschutz. 19. April 2000. URL <http://www.fitug.de/debate/0004/msg00354.html>.
- Landesbeauftragter für den Datenschutz Schleswig-Holstein. 10 Punkte für einen Politikwechsel zum wirksameren Schutz der Privatsphäre. 4. November 1998. URL <http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/presse/\%politikw.htm>.
- Markus Lusti. *Dateien und Datenbanken*. Springer, Heidelberg et al., 1997.
- Markus Lusti. *Data Warehousing und Data Mining*. Springer, Heidelberg et al., 1999.
- NZZ. Daten gegen Geld. *Neue Zürcher Zeitung*, Seite 75, 5. Mai 2000.
- Pietsch, Werner, Weber, Daniel. Ledig und 1500 m ü. M. *NZZ Folio*, Seiten 24 ff., Juli 1998.
- Florian Rötzer. Transatlantischer Kompromiss in Sachen Datenschutz. *Telepolis, Magazin für Netzkultur*, 16. März 2000. URL <http://www.heise.de/tp/deutsch/inhalt/te/5914/1.html>.
- Florian Rötzer. US-Handelskommission verlangt gesetzliche Regelung zum Schutz der persönlichen Daten beim E-Commerce. *Telepolis, Magazin für Netzkultur*, 23. Mai 2000. URL <http://www.heise.de/tp/deutsch/inhalt/te/8182/1.html>.
- Florian Rötzer. Ein sicherer Hafen für Microsoft. *Telepolis, Magazin für Netzkultur*, 23. März 1999. URL <http://www.heise.de/tp/deutsch/inhalt/te/1983/1.html>.
- Jacqueline Schärli. Was geht uns die Badehose des Bundesrats an? *NZZ Folio*, Seiten 10 ff, Juli 1998.

Alex Schweizer. *Data Mining, data warehousing: datenschutzrechtliche Orientierungshilfen*.  
Recht und Informatik. Orell Füssli, Zürich, 1999.

Swiss Internet Users Group SIUG. Positionspapier zum Thema Kryptographie, 1999. URL  
<http://www.siug.ch/positionen/SIUG-Krypto.shtml>.

R. James Woolsey. Why We Spy on Our Allies. *The Wall Street Journal*, 18. März 2000.  
URL <http://cryptome.org/echelon-cia2.htm>.

R. James Woolsey. FORMER CIA DIRECTOR WOOLSEY DELIVERS REMARKS AT  
FOREIGN PRESS CENTER . *FOREIGN PRESS CENTER*, 7. März 2000. URL <http://cryptome.org/echelon-cia.htm>.