

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. Der Datenschutz wiederum bestimmt, dass ”Personendaten (. . . nur für den Zweck bearbeitet werden dürfen), der bei der Beschaffung angegeben wurde.”

Problematisch an der ständigen Bewertbarkeit von Personen durch Data Mining ist der damit verbundene Verlust der Transparenz. Der Einzelne ist nicht mehr in der Lage zu beurteilen, welche Informationen zu welchem Zweck von wem bearbeitet werden.

Begriffe und Konzepte

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.

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.

Rechtfertigungsgründe: Unter gewissen Umständen ist auch eine Bearbeitung von besonders schützenswerten Daten und Persönlichkeitsprofilen möglich (etwa im Zusammenhang mit Verträgen, Bonitätsprüfung, Journalisten).

Der Datenschutz steht nicht isoliert da. Alternativ oder zusätzlich können auch Bestimmungen des Bankgeheimnisses, des Geldwäschereigesetzes oder anderer Berufsgeheimnisse greifen.

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. Um DSGVO-konform mit den Daten 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

Die Datenbeschaffung muss *rechtmässig* sein und nach Treu und Glauben erfolgen. Bei der Anwendung von Data Mining-Methoden muss explizit darauf hingewiesen werden.

Datenbearbeitung und -richtigkeit

”Bearbeitung” im Sinne des DSGVO umfasst den gesamten ”Lebenszyklus” von Daten, unabhängig von den dabei angewandten Methoden. 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.

Betroffene Personen haben – unabhängig vom Verwendungszweck – ein Recht auf die Richtigkeit ihrer Daten (respektive die Feststellung der Unrichtigkeit).

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.

Datenhandel (Bekanntgabe)

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 ausgewählte Adressaten gelangt, da in dem Fall die Daten in der Hand des Datensammlers verbleiben.

Die Bekanntgabe "besonders schützenswerter" Daten und von Persönlichkeitsprofilen sowie eine Bekanntgabe ins Ausland sind in der Regel nicht möglich (respektive Meldepflichtig).

Datensicherheit

Datensicherheit ist ein wesentlicher Bestandteil des Datenschutzes. Ohne Datensicherheit gibt es keinen Datenschutz. Die technischen und organisatorischen Massnahmen sind primär zum Schutz der Betroffenen zu realisieren. Im Bereich "besonders schützenswerter" Daten und von Persönlichkeitsprofilen müssen über den konventionellen Datenschutz hinausgehende Punkte beachtet werden:

Outsourcing: Wenn unternehmensfremde Dritte Zugang zu Computersystemen und Daten haben, unterstehen diese ebenfalls den datenschutzrechtlichen Regelungen.

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

Organisatorische Massnahmen: Die Bearbeitung und die Bekanntgabe muss in geeigneter Art protokolliert werden, damit das Auskunftsrecht sichergestellt werden kann.

Folgerungen

Bestimmte Klassen von Data Mining-Anwendungen sind vordergründig datenschutzrechtlich unbedenklich, können aufgrund der potentiellen Erkenntnisse aber datenschutzrechtliche Fussangeln bergen. Gerade die Klasseneinteilung kann je nach Wahl von exogenen und endogenen Variablen ausreichen, um ein Persönlichkeitsprofil zu konstituieren.

Mit zunehmender Verlagerung von Wirtschaftsaktivitäten in elektronische Medien vergrössern sich die Möglichkeiten zur 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 auf die Belange des Datenschutzes. Fahrlässig (geschweige denn vorsätzlich) in ihren Persönlichkeitsrechten Verletzte sind schlechte Kunden.

- *Datenvermeidung und Datensparsamkeit*
- *Organisatorische Massnahmen*
- *Definition von Zielen und Überprüfung auf datenschutzrechtliche Unbedenklichkeit*
- *Verzicht auf individuell zuordenbare Attribute*

In der aktuellen Diskussion stehen die Bereiche Polizeiwesen, Ausländer- und Asylrecht, Telekommunikation, Personalwesen, Versicherungswesen, Gesundheitswesen, Kreditwesen, Direktmarketing, Statistik sowie Mietrecht im Vordergrund. Diese Diskussion wird sich im Umfeld internationaler Bemühungen der Überwachung und "Entanonymisierung" der Internetbenutzer auf grundlegendere datenschutz- und persönlichkeitsrechtliche Fragen verlagern – insbesondere im Hinblick auf die in ihrer rechtlichen Stellung noch nicht gefestigte Online-Ökonomie. Dort werden Aspekte des Data Mining auf Seiten der Anbieter und der zur Überwachung möglicherweise befugten Stellen die Diskussion beeinflussen.