Bettina Sokol/Roul Tiaden

# Big Brother und die schöne neue Welt der Vermarktung personenbezogener Informationen

In der zweiten Hälfte des letzten Jahrhunderts war Big Brother das Synonym für einen Orwell´schen Überwachungsstaat, der alle Daten und Bewegungen seiner BürgerInnen erfasst und sie so – als gläserne Untertanen – umfassend kontrolliert. Heute wird mit Big Brother vor allem die gleichnamige Fernsehsendung assoziiert. Die schrieb Mediengeschichte, weil hier Menschen – in der Hoffnung auf Reichtum und Ruhm – mehrere Monate lang auf nahezu jede Privatsphäre verzichteten und sich rund um die Uhr einem Millionenpublikum zur Schau stellten.

Der Bedeutungswandel von Big Brother – von George Orwells Klassiker 1984 zum Fernsehformat eines Privatsenders – spiegelt die gesellschaftlichen Entwicklungen der letzten Jahrzehnte im Umgang mit personenbezogenen Informationen wider. Die im Zuge rasanten technischen Fortschritts exponentiell anwachsende kommerzielle Datenverarbeitung durch Private bringt neue Herausforderungen für die informationelle Selbstbestimmung mit sich. Gleichzeitig wandelt sich die Rolle der Betroffenen von bloßen Objekten verantwortlicher Stellen zu WirtschaftsbürgerInnen, die ihre personenbezogenen Daten zunehmend als HändlerInnen in eigener Sache vermarkten. Gibt es Grenzen der (Selbst-)Vermarktung? Degeneriert das Grundrecht auf informationelle Selbstbestimmung zum Recht auf informationelle Selbstveräußerung?

## »It´s the economy, stupid!« – Vom staatlichen zum privaten Leviathan

Mit der technischen Entwicklung von staatlichen Großrechnern zur allgegenwärtigen, vernetzten und miniaturisierten Datenverarbeitung und Digitalisierung wandelten sich auch die Herausforderungen für die informationelle Selbstbestimmung. Nicht mehr allein der volkszählende und rasterfahndende Staat, sondern auch datensammelnde Unternehmen werden verstärkt als Gefahrenquellen für die Selbstbestimmung betrachtet. So fürchten sich die BürgerInnen heute weniger vor dem Überwachungsstaat als vor kommerziellen Datenverarbeitern, die sie in gläserne Versicherungsnehmer, gläserne Internetnutzerinnen, gläserne Kunden und gläserne Beschäftigte verwandeln können.

Dies belegt eine repräsentative Befragung zum Datenschutz aus dem Jahr 2001 (Opaschowski 2001). Danach ist das Vertrauen der Befragten, dass ihre personenbezogenen Informationen stets datenschutzgerecht verwandt werden, bei Polizei (60%) und Verfassungsschutz (57%) deutlich größer als bei Versicherungen (37%), Internetanbietern (10%) und beim Versand- (10%) und Adresshandel (8%). Auch wenn subjektives Vertrauen und objektive Gefährdungslage nicht zwangsläufig übereinstimmen müssen, zeigt sich in den

Umfrageergebnissen jedenfalls ein erhebliches Misstrauen gegenüber kommerziellen Datenverarbeitern.

Diese Entwicklung – von der Furcht vor dem Überwachungsstaat zu einer verstärkt wahrgenommenen Gefährdung der Privatsphäre durch datenverarbeitende Unternehmen – könnte mit einem Wahlkampf-Slogan Bill Clintons aus den neunziger Jahren überschrieben werden: »It´s the economy, stupid!« In der Wirtschaft spielt (derzeit) die Musik für den Datenschutz – trotz der »Otto-Kataloge« des Bundesinnenministers und des Revivals der Rasterfahndung nach den Anschlägen vom 11. September. 2001. Die kommerzielle Nutzung der digitalen Revolution bringt die qualitativ neuen Herausforderungen für den Datenschutz. Vor allem in diesem Bereich wird sich das Recht auf informationelle Selbstbestimmung in den nächsten Jahren bewähren müssen.

## Datenhandel in Zeiten technischen Wandels

Der Handel mit personenbezogenen Daten ist kein neues gesellschaftliches Phänomen, sondern vielfach ein Gewerbe mit Tradition. Detekteien, Auskunfteien, Adresshandel und Medien, insbesondere die Boulevardpresse, verdienen seit mehr als hundert Jahren ihr Geld mit personenbezogenen Informationen. Bereits im 19. Jahrhundert gab es in Deutschland die ersten Adresshändler, die ersten Kreditauskunfteien – die jüngere SCHUFA feiert in diesem Jahr ihren 75. Geburtstag – und sogar Paparazzi: zwei Journalisten drangen 1898 in das Sterbezimmer Otto von Bismarcks und fotografierten den Verstorbenen, um die Bilder anschließend meistbietend zu verkaufen. Die rasanten wissenschaftlichen und technischen Entwicklungen der letzten Jahrzehnte haben indes qualitativ und quantitativ neue Dimensionen in den Handel mit personenbezogenen Daten gebracht.

## Online-Auskunfteien, Internet-Pranger und Credit-Scoring

Die Frage vieler Unternehmen, wie zahlungskräftig ihre (potentiellen) KundInnen sind, gewinnt in der Informationsgesellschaft stetig an Bedeutung. Mit der Entwicklung vom anonymen Barkauf zum personalisierten bargeldlosen Kreditkauf – innerhalb oder außerhalb des Internets – entsteht eine wachsende Nachfrage nach Bonitätsinformationen. Diese werden von Online-Auskunfteien und Internet-Warndateien angeboten. In Sekundenschnelle können Unternehmen per Knopfdruck automatisiert vielfältige Auskünfte über die Kreditwürdigkeit ihrer potentiellen (Online-) KundInnen abrufen.

Dabei beschränken sich die Auskunfteien längst nicht mehr darauf, nur Auskünfte über Personen zu liefern, zu denen sog. Negativdaten über vertragswidriges Verhalten vorliegen. Beim Credit-Scoring werden unbescholtene (potentielle) KundInnen automatisiert in statistische Risikogruppen eingeteilt. Diese prognostizieren die Wahrscheinlichkeit eines Kreditausfalls oder

einer Zahlungsunfähigkeit. Bei der Berechnung des Scorewertes spielen insbesondere statistische, soziodemographische Informationen, die mit personenbezogenen Daten verknüpft werden, eine große Rolle. Für die Betroffenen kann dies eine Schlechterbehandlung im Geschäftsverkehr bedeuten, auch wenn sie sich bislang stets vertragsgemäß verhalten haben.

Das Internet lässt mehr und mehr UnternehmensgründerInnen vom Aufbau einer eigenen Online-Warndatei träumen. Besonders bedenklich ist, dass einige Geschäftsleute eine mittelalterliche Praxis wiedereinführen wollen: SchuldnerInnen sollen – datenschutzwidrig – öffentlich angeprangert werden. Nur steht der Pranger nicht mehr auf dem städtischen, sondern auf dem weltweiten virtuellen Marktplatz, im Internet. Einmal – aus welchen Gründen auch immer – an den Internetpranger gestellt, kann die diskriminierende personenbezogene Information weltweit abgerufen werden und ist – wegen möglicher downloads – nicht mehr sicher rückholbar.

## Data Warehouse, Data Mining und Online Profiling

Die Adresshandel- und Direktmarketing-Branche boomt in den letzten Jahrzehnten. Unternehmen wollen wissen, wem sie was verkaufen können, wie sie bisherige KundInnen binden und neue KundInnen gewinnen können. Dafür benötigen sie möglichst umfassende Informationen über die KundInnen: Kaufkraft, Konsumeigenschaften, sozialer Status, Alter, Familienstand, Vorlieben, Hobbys, Lebenseinstellungen – je umfassender das Persönlichkeitsbild, desto berechen- und beeinflussbarer (scheint) das Verbraucherverhalten. Data Warehouse, Data Mining, Customer Relationship Management und Online Profiling sind einige der zahlreichen Schlagworte beim lukrativen Handel mit Kundendaten.

Die dritte technische Revolution bringt sowohl exponentiell wachsende Datenbestände über die VerbraucherInnen als auch die technischen Hilfsmittel, um die Informationen intelligent und profitabel auswerten zu können. So ermöglichen die elektronischen Bestell- und Zahlungssysteme, die zunehmend an die Stelle des anonymen Barkaufs treten, enorme Datensammlungen über das Kauf- und Zahlungsverhalten der Kunden. Auch Kundenbindungs- und Rabattsysteme sowie die offene oder versteckte Erhebung von Daten im Internet helfen, Kunden- und Persönlichkeitsprofile zu erstellen (sog. Online Profiling). Um das Surf- und Nutzungsverhalten im Netz zu erfassen, werden unter anderem Log-Dateien und Registrierungsdaten systematisch ausgewertet und Spezialanwendungen wie Cookies, Packet-Sniffing-Technologien und Web Bugs eingesetzt (vgl. Buxel DuD 2001, 579; Schaar DuD 2001, 383).

Damit die in den unterschiedlichen Bereichen eines Unternehmens oder eines Konzerns anfallenden Kundendaten für das Direktmarketing verwertbar sind, müssen sie losgelöst vom bisherigen Zweck zeit- und funktionsgerecht zur Verfügung stehen, z.B. in einer operativen Datenbank. Das ist die Aufgabe

der sog. Data Warehouses, der Daten-Lagerhäuser. Ist der Zugriff auf die Datensammlungen möglich, werden daraus im Wege des Data Minings die für die Kundenbindung oder -gewinnung profitablen Informationen herausgearbeitet. Programme künstlicher Intelligenz analysieren die Daten unter speziellen Fragestellungen, stellen automatisiert neue Zusammenhänge her und decken Muster auf – etwa im Kundenverhalten. Angereichert mit soziodemographischen und mikrogeographischen Daten werden diese Informationen für zielgruppenorientiertes Marketing genutzt (vgl. Büllesbach CR 2000, 11; Wittig RDV 2000, 59 ff.)

## Von Untertanen zu WirtschaftsbürgerInnen – die neue Rolle der Betroffenen

Der anfangs erläuterte Bedeutungswandel von Big Brother spiegelt auch die wandelnde Rolle der Betroffenen wider: von der Untertanin zur Wirtschaftsbürgerin, vom bloßen Objekt verantwortlicher Stellen zur Händlerin in eigener Sache. Betroffene beteiligen sich heute aktiv an der Verwertung und Veräußerung ihrer personenbezogenen Daten. Personenbezogene Informationen sind eine Handelsware, die zunehmend auch DurchschnittsbürgerInnen in Geld umwandeln können.

So wie die Akteure bei Big Brother nicht Opfer einer versteckten Kamera wurden, so sind auch die TeilnehmerInnen eines modernen Kundenbindungs- und Rabattsystems keine Opfer einer heimlichen Kundenprofilierung. Die jeweiligen »Betroffenen« beteiligen sich vielmehr in Erwartung materieller Vorteile oder aufgrund finanzieller Anreize aktiv an der Erhebung und Kommerzialisierung ihrer Daten. Bonuspunkte in einem Kundenbindungsprogramm sind nicht mehr nur anonym gewährte Rabattmarken, sondern auch eine Gegenleistung für die Einwilligung, Daten über das individuelle Kaufverhalten erheben, verarbeiten und nutzen zu dürfen. Die TeilnehmerInnen lassen sich dabei die Preis-Gabe ihrer personenbezogenen Daten in Cent und Euro auszahlen.

Die Vermarktung von Daten mit aktiver kommerzieller Beteiligung der Betroffenen gewinnt in den Bereichen an Bedeutung, in denen personenbezogene Informationen nicht auf gesetzlicher Grundlage, sondern mit Einwilligung der Betroffenen erhoben, verarbeitet und genutzt werden sollen, wie zum Beispiel beim Handel mit detaillierten Kundendaten.

Bislang werden vor allem Preisausschreiben oder Gewinnspiele eingesetzt, um Anreize für die Teilnahme an VerbraucherInnen- und Life-Style-Umfragen zu schaffen. Ähnliches geschieht im Internet, wenn Personen unter der Bedingung an Spielen oder Wettbewerben teilnehmen dürfen, dass sie personenbezogene Daten als Grundlage für Kundenprofile beisteuern, sog. »Cybermarketing mit Anreizen« (Schaar DuD 2001, 383, 384).

Eine neue Variante im Handel mit Kundendaten beteiligt die Befragten aktiver an der Verwertung ihrer Daten und lässt sie am Erlös mitverdienen. Die Betroffenen entscheiden dabei selbst, welche personenbezogenen Informa-

tionen sie für den Verkauf an Firmen, Banken und Versicherungen preisgeben. Je umfassender, profilgenauer und aktueller die Daten, desto höher der Erlös, von dem die Betroffenen einen prozentualen Anteil erhalten. Kommentar der Konkurrenz: »Menschen sind halt käuflich.« Wer Big Brother gut finde oder sogar dabei mitmache, werde auch keine Hemmungen haben, seine Badegewohnheiten öffentlich zu machen (vgl. Langrock W&V 20/2000).

Eine andere Geschäftsidee ermöglicht es KundInnen, Computer zu mieten und den Mietzins zu reduzieren, indem sie als Gegenleistung personenbezogene Daten offenbaren. Wer beim Surfen im Netz gegenüber diversen Online-Unternehmen Angaben über Einkommensverhältnisse, Hobbys und Kreditkartennutzung macht, zahlt weniger Miete. Pro Angabe wird ein Betrag gutgeschrieben, so dass die Zahlungsverpflichtung maximal auf null sinkt (Weichert 2000, 158).

## Kommerzialisierung ohne Grenzen?

Angesichts einer immer umfassenderen und intensiveren Kommerzialisierung personenbezogener Informationen stellt sich die Frage, welche Grenzen es insoweit gibt oder geben sollte. Die bestehende Datenschutzrechtslage im Bereich wirtschaftlicher Betätigungen von Privatunternehmen und Privatpersonen ist davon geprägt, dass eine Verarbeitung personenbezogener Daten, die seit der Novelle des Bundesdatenschutzgesetzes 2001 bereits mit deren Erhebung beginnt, nur auf Grund einer Rechtsvorschrift oder mit einer Einwilligung der davon betroffenen Person erlaubt ist. Wollen die betroffenen Personen ihre Daten – mit oder ohne Einschaltung einer Maklerfirma – vermarkten, kann davon ausgegangen werden, dass sie in die Datenverarbeitung einwilligen wollen, da die Datenpreisgabe ja gerade die Erwerbsquelle ist. Ob ein solcher Sachverhalt juristisch als Vertragsverhältnis, beispielsweise als Datenüberlassungsvertrag (so Weichert 2000, 158) oder als Einwilligungsvorgang zu qualifizieren wäre, soll vorliegend nicht weiter verfolgt werden. Einwilligungen sind widerrufbar und Verträge in aller Regel kündbar. Die Vertragsfreiheit ist im Falle strukturell ungleicher Verhandlungsstärke nicht nur im Arbeits-, Miet- und Versicherungsrecht Beschränkungen unterworfen (vgl. BVerfGE 89, 214/299 ff.). Die datenschutzrechtlichen Grenzen der Einwilligung könnten möglicherweise auch entsprechend auf die Vertragsfreiheit übertragen werden. Dies zu prüfen ist hier allerdings nicht der Ort, so dass das Augenmerk auf die Einwilligung zu richten ist.

## Einwilligungsvoraussetzungen

Auch mit einer Einwilligung ist nicht alles erlaubt, was möglich wäre. Gesetzgebung und Rechtsprechung haben hier Grenzen gezogen und Anforderungen gestellt, die durch das Allgemeininteresse legitimiert sind.

Nur freiwillig erteilte Einwilligungen sind nach § 4 a BDSG überhaupt wirksam. Zu den weiteren Einwilligungsvoraussetzungen gehören u.a. die vollständigen und in verständlicher Weise gegebenen Informationen über den Umfang und die Zwecke der beabsichtigten Erhebung, Verarbeitung oder Nutzung der dafür vorgesehenen personenbezogenen Daten. Dies soll der betroffenen Person nicht nur die bloße Kenntnis von den Einzelheiten des jeweils geplanten Vorhabens vermitteln, sondern sie in die Lage versetzen, die Tragweite ihrer Entscheidung überblicken zu können. Die grundsätzlich erforderliche Schriftlichkeit der Einwilligung nebst eigenhändiger Unterschrift soll einen gewissen Schutz vor einem übereilten Handeln und etwaigen Missverständnissen bieten. Die Erteilung der Einwilligung soll eine informierte, bewusste, beabsichtigte und völlig freie Entscheidung sein.

**Ausgleich von Machtungleichgewichten**

Eine freie und freiwillige Entscheidung ist eine Entscheidung »ohne Zwang«, wie es die EG-Datenschutzrichtlinie in ihrem Art. 2 Buchst. h) fordert. Wann sind Entscheidungen ohne jeden Zwang, auch ohne jeden faktischen Zwang? Allgemein anerkannt ist, dass bei Machtungleichgewichten von einer echten Freiwilligkeit höchst selten die Rede sein kann. Abhängigkeiten oder faktische Zwänge etwa – wie beispielsweise auf dem Arbeits- oder dem Mietwohnungsmarkt – sollen durch rechtliche Regulierungen teilweise ausgeglichen werden. Auch im Versicherungswesen gibt es in vielen Bereichen ausgehandelte Standardformulierungen, die regelmäßig nicht oder nur in engen Grenzen zur Disposition der Beteiligten stehen. Ausgehandelt und festgelegt werden sie aber nicht von den einzelnen Personen, um deren Daten es geht, sondern die Interessen der Betroffenen werden gegenüber den Unternehmen und deren Verbänden von den Datenschutzkontrollinstanzen wahrgenommen (vgl. Simitis, in: ders. u.a., BDSG, § 4 a Rn. 6 ff.). Zum Schutz der einzelnen Personen haben sie selber so gut wie keine Möglichkeiten mehr, die mit einer Einwilligung eigentlich verbundenen Fragen des Umfangs und der Bedingungen der Datenverarbeitung maßgeblich zu beeinflussen. Ihre Entscheidungsfreiheit besteht prinzipiell nur noch darin, vorgegebenen Bedingungen zuzustimmen oder zu verzichten.

**Unabdingbare Rechte**

Weitere Einschränkungen der Dispositionsbefugnis legt § 6 BDSG fest. Weder gänzlich ausgeschlossen noch auch nur beschränkt werden können danach die Rechte der betroffenen Person auf Auskunft und auf Berichtigung, Löschung oder Sperrung. Zwar muss niemand diese Rechte ausüben, jedoch ist es gesetzlich ausgeschlossen, in ihren Verzicht ausdrücklich einzuwilligen. Denn diese originären Bestandteile des Rechts auf informationelle Selbst-

bestimmung bilden zugleich Voraussetzungen seiner effektiven Ausübung. Die ausdrückliche Benennung der nach § 6 BDSG unabdingbaren Rechte der betroffenen Personen bedeutet allerdings nicht, dass alle dort nicht genannten Rechte zur freien Disposition stünden. Vielmehr ist das aufeinander abgestimmte System von Schutzinstrumenten im Bundesdatenschutzgesetz grundsätzlich zwingender Natur (Mallmann, in: Simitis u.a., BDSG, § 6 Rn. 17). Ausnahmen davon aufgrund von Einwilligungen sind gerade nicht unbegrenzt möglich.

## Elementare Funktionsbedingung der Demokratie

Mit einer freiwillig, auch ohne jeden faktischen Zwang erteilten Einwilligung in eine Datenverarbeitung wird ein Grundrecht wahrgenommen. Freilich ist stets zu prüfen, ob durch die Offenbarung eigener Daten auch (Grund-)Rechte Dritter betroffen sind, weil beispielsweise die Daten Informationen über andere Personen – etwa Verwandte – enthalten. Darüber hinaus verleiht die im Recht auf informationelle Selbstbestimmung verankerte Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung der Daten zur eigenen Person zu bestimmen (BVerfGE 65, 1/43), allerdings keine eigentumsähnlichen Verfügungsmöglichkeiten. Auch das allgemeine Persönlichkeitsrecht ist nicht im Interesse einer Kommerzialisierung der eigenen Person gewährleistet (BVerfGE 101, 361). Ein wesentliches Ziel des Rechts auf informationelle Selbstbestimmung besteht vielmehr darin, die Kommunikations- und Handlungsfähigkeit der einzelnen Menschen gegenüber staatlichen Stellen wie auch innerhalb der Gesellschaft sicherzustellen. Unter anderem soll die Transparenz von Datenverarbeitungen für die betroffene Person die Verhaltensfreiheit ermöglichen.

Neben der Funktion, die subjektiv-individuelle Verhaltensfreiheit zu sichern, stellt die informationelle Selbstbestimmung eine elementare Funktionsbedingung »eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens« (BVerfGE, 65, 1/43) dar. Die gesetzliche Regelungsnotwendigkeit des Datenschutzes hat damit individuelle wie gesamtgesellschaftliche Bedeutung. Der Verzicht einzelner Personen auf beispielsweise Transparenz und Kontrollmöglichkeiten der Datenverarbeitung wirkt sich langfristig auf die gesellschaftlichen Strukturen aus, weil die Kommunikations- und Handlungsfähigkeit gemindert werden und sich die Manipulationsmöglichkeiten verstärken. Dies ließe die informationelle Selbstbestimmung in ihrer objektiven Funktion letztlich zu einer leeren Hülse werden.

**Gesetzgeberischer Handlungsbedarf**

Wenn »Einverständnis und Entgelt« die Datenschutzgesetze darauf reduzieren, »eine reibungslose Vermarktung sicherzustellen« (Simitis 1999, 5), die Kommerzialisierung personenbezogener Daten andererseits sicherlich nicht gänzlich unterbunden oder gar nur aufgehalten werden kann (Weichert 2000, 158), ist gleichwohl die gesellschaftliche Diskussion über diese Entwicklung notwendig und die Frage nach gesetzgeberischem Handlungsbedarf zu stellen. In Betracht zu ziehen sind die verstärkte Durchsetzung der Datenvermeidung ebenso wie eine Neuregulierung der Einwilligung. Das Recht auf informationelle Selbstbestimmung wird im Hinblick auf eine Preisgabepflicht bestimmter Daten – legitimiert durch Allgemeininteressen – schon vielfach gesetzlich beschränkt. Gleiches könnte im Hinblick auf eine Geheimhaltungspflicht bestimmter Daten überlegt werden. Diskutiert werden könnte auch, ob die Eindämmung des Datenhandels als berechtigtes Allgemeinwohlanliegen und die Sicherstellung der Freiwilligkeit durch Verbote – etwa unabdingbare Zweckbindungsregelungen – erreicht werden könnten. Damit hätten sich auch einwilligungsfähige Datenverarbeitungen grundsätzlich im Rahmen der gesetzlich festgelegten Verarbeitungsbedingungen zu halten.

Literatur:

Büllesbach, Alfred (CR 2000), Datenschutz bei Data Warehouses und Data Mining, CR 2000, 11.

Buxel, Holger (DuD 2001), Die sieben Kernprobleme des Online Profiling aus Nutzerperspektive, DuD 2001, 579.

Opaschowski, Horst W. (2001): Der gläserne Konsument. Die Zukunft von Datenschutz und Privatsphäre in einer vernetzten Welt, Hamburg 2001.

Schaar, Peter (DuD 2001), Persönlichkeitsprofile im Internet, DuD 2001, 383.

Simitis, Spiros (1999): Die Erosion des Datenschutzes. In: LfD NRW Sokol, Bettina (Hrsg.): Neue Instrumente im Datenschutz, Düsseldorf 1999, 5.

Simitis, Spiros u.a., Kommentar zum Bundesdatenschutzgesetz, 5. Aufl. (im Erscheinen).

Weichert, Thilo (2000): Zur Ökonomisierung des Rechts auf informationelle Selbstbestimmung. In: Bäumler, Helmut (Hrsg.): E-Privacy, Braunschweig/Wiesbaden 2000, 158.

Wittig, Petra (RDV 2000), Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken, RDV 2000, 59.