

CRM und Datenschutz

– stirbt der Datenschutz im Data Warehouse?

Univ.-Prof. Dr. Jürgen Taeger

Juristisches Seminar
Fachbereich Wirtschafts- und Rechtswissenschaften
Carl von Ossietzky Universität Oldenburg
26111 Oldenburg
j.taeger@uni-oldenburg.de

Abstract: Moderne, das Internet nutzende Marketingkonzepte wie das One-to-One-Marketing erfordern detaillierte Informationen über Kundenverhalten und -bedürfnisse, um Kunden individuell ansprechen zu können. In der Praxis erweisen sich hierfür eingesetzten CRM-Systeme und Data Warehouses häufig als datenschutzrechtlich bedenklich. Verstöße gegen Datenschutzrecht verletzt nicht nur die Rechte der Betroffenen, sondern gefährden dadurch die Akzeptanz des E-Commerce überhaupt.

I. Elektronische Unternehmenskommunikation

Die Kommunikationskultur der werbenden Wirtschaft befindet sich im Umbruch. Unternehmenskommunikation setzt zunehmend auf das Internet. Die technischen Möglichkeiten, das elektronische Kommunikationsverhalten von Verbrauchern aufzeichnen, Kundeninteressen analysieren und mit individueller Ansprache reagieren zu können, faszinieren die Marketingbranche ebenso wie die um Absatzmärkte kämpfenden Unternehmen. Die Verlockungen der auch vergleichsweise preiswerten weltumspannenden elektronischen kommerziellen Kommunikation, fachsprachlich auch als Netvertising oder Webvertising bezeichnet, haben dem klassischen Marketing neue Kommunikationskanäle und Marketingmethoden eröffnet¹. Banner- und Pop Up-Werbung sowie die unaufgeforderte kommerzielle Kommunikation („Spamming“) sind nur die für jedermann augenscheinlichen Beispiele für die negativen Begleiterscheinungen dieser Entwicklung.

Im Vordergrund moderner Online-Kommunikation steht das One-to-One-Marketing, unter dem die kundenorientierte Ausrichtung aller Marketingaktivitäten auf elektronischem Weg verstanden wird, deren Ziel die persönliche Ansprache, u.a. durch Interactive Marketing anstelle der zu sehr streuenden Banner-Werbung, und individuelle Problemlösung ist². Customer Relationship Management-Systeme erweisen sich als geeignete Instrumente zur Unterstützung des One-to-One-Marketing.

¹ Siehe nur Matejcek, Newsletter und Mailinglisten – Marketing per E-Mail, Wien 2001.

² Hermanns, Online-Marketing im E-Commerce – Herausforderungen für das Management, in: Hermanns/Sauter (Hrsg.), Management-Handbuch Electronic Commerce, München 2001, S. 116.

1. Customer Relationship Management und Data Warehouse

Unternehmenserfolg wird im E-Business-Zeitalter wesentlich von der Fähigkeit der Unternehmung abhängen, nicht nur wirkungsvolle ERP-Systeme³ zur Optimierung interner Geschäftsprozesse einzusetzen. Der Focus zielt mehr denn je auf den Kunden; auf ihn ist die gesamte Wertschöpfungskette des Unternehmens auszurichten. Das Angebot an Produkten und Dienstleistungen erfolgreicher Geschäftsmodelle muss sich flexibel und zeitnah an den sich wandelnden, individuellen Kundenbedürfnissen orientieren. Vereinfacht ausgedrückt: es werden keine Kunden für ein Produkt, sondern Produkte und Service für den Kunden gesucht. Der Kundenkontakt bei Marketing, Vertrieb und Service ist intensiv zu pflegen. Kundenorientierte Konzepte erweisen sich somit als entscheidender Erfolgsfaktor für die Geschäftsentwicklung.

Hier setzen Customer Relationship Management-Systeme an. Sie verknüpfen Daten aus den Bereichen Marketing, Vertrieb und Service mit ERP-Systemen. Ziel ist es, die Kundenansprache zu verbessern, Kundenzufriedenheit und damit Loyalität und enge Unternehmens- oder Produktbindung zu erreichen. Voraussetzung für wirksame Kundenbindungssysteme sind Daten über individuelle Kundenprofile mit Angaben über Kundenverhalten, Kundenwünsche und nicht zuletzt über die Bonität des Kunden: was interessiert ihn, wofür ist er empfänglich, wie reagiert er auf Ansprache und kommerzielle Kommunikation, wie verhält er sich bei Leistungsstörungen und nachfolgenden Reklamationen. Erweist sich ein Kunde ausschließlich als Kostenverursacher, wird er nicht nur gern aufgegeben, sondern möglichst dem Wettbewerb empfohlen. Schließlich ist unternehmerisches Ziel das Gewinnen und Halten lediglich der profitablen Kunden, die Steigerung der Cross-Selling Rate (Umsatz pro Kunde).

Die Informationen über Kunden werden neben sonstigen für das Unternehmen bedeutsamen Daten idealer Weise im Data Warehouse gesammelt. In diesem zentralen Speicher fließen – innerhalb des Konzerns auch unternehmensübergreifend – aus ganz unterschiedlichen Quellen personenbezogene Daten zusammen. Eine Quelle für die Erhebung und Speicherung personenbezogener Daten ist – neben den Marktforschungs-Fragebögen der Haushaltsbefragungen⁴ – das Internet. Anfragen von Kunden, die sich unter Angabe ihres Namens und ihrer Adresse für Produkte oder Dienstleistungen interessieren, können ausgewertet und im System gespeichert werden. Mit Hilfe von Cookies, Java- und ActiveX-Funktionen lassen sich sogar dann Daten speichern, wenn der Kunde gar keinen Kontakt herstellen will, sondern lediglich auf die Website des Unternehmens gelangt ist und dabei eine Datenspur mit Informationen über die von ihm besuchten Seiten hinterlässt⁵.

Die im Data Warehouse gespeicherten Daten lassen sich mittels Data Mining multifunktional analysieren und für zielführende Unternehmensstrategien fruchtbar machen. Mit

³ Enterprise Resource Planning/Warenwirtschaftssystem.

⁴ Zur datenschutzrechtlichen Einordnung Podlech/Pfeifer, Die informationelle Selbstbestimmung im Spannungsverhältnis zu modernen Werbestrategien, RDV 1998, S. 139.

⁵ Nähere Hinweise bei Boehme-Neßler, Datenschutz in der Informationsgesellschaft, K & R 2002, S. 217; Wolters, Einkauf via Internet: Verbraucherschutz durch Datenschutz, DuD 1999, S. 277.

dem Data Warehouse und dem Data Mining stellen sich Unternehmen auch darauf ein, Informationen über bereits gewonnene oder potentiell künftige Kunden zu sammeln und nach beliebigen Kriterien für gezielte Marketingaktivitäten mit individueller Ansprache, also im One-to-One-Marketing einzusetzen.

Dieses Szenario ist keine Fiktion, sondern in weiten Bereichen Realität. Ein Internet-Unternehmen, das für seine Kunden Intershop-Anwendungen erstellt, bewirbt seine Dienstleistung wie folgt (2001):

„du wählst zwischen 100 digitalen tv-Programmen, das handy dient als fernbedienung und während der soap opera bestellst du das scharfe sakkko des titelhelden per knopfdruck. 2 tage später bringt der bote es an die haustür. der preis wird per handy überwiesen und mit dieser summe eine fülle von informationen: deine konfektionsgrösse, dein mode- und farbgeschmack sowie deine fernsehgewohnheiten ... zusammen mit deinen bereits gespeicherten daten ergibt dies ein plastisches bild deiner konsumgewohnheiten: du bist der glaeserne consumer ...

Haben Sie diese Informationen über Ihre Kunden? Dann unterschätzen Sie die Chancen nicht, die Ihnen eCommerce bietet. eCommerce ist mehr als eine alternative Vertriebschiene, sondern eine neue Ära des Marketing, eine gänzlich neue Verkäufer-Kunden-Beziehung: das 1-to-1-Marketing.“

2. Web-Scoring

Noch einen Schritt weiter geht das Web-Scoring, mit dem die Zahlungsfähigkeit potenzieller Kunden vor Vertragsschluss analysiert wird, um bei vermuteter fehlender Bonität den Vertragsschluss abzulehnen oder Vorkasse bzw. Nachnahmelieferung zu vereinbaren. Beim Web Scoring wird der potentielle Kunde je nach Wohnort, Alter oder Beruf bei Eingabe seiner Daten in das WWW innerhalb von Sekunden als „guter“ oder „schlechter“ Kunde eingestuft. „Gute“ Kunden können auf Rechnung einkaufen⁶. In Scoring-Programmen wird nicht nur die Wohnadresse und der Beruf berücksichtigt, sondern beispielsweise auch ein laufendes Inkasso- oder Verbraucherinsolvenzverfahren. Vor diesem Hintergrund erhält die elektronische Gebäudedatenbank, in der Fotos aller Gebäude nach Straßenverläufen gespeichert sind, eine neue Qualität⁷. Anhand der Lage und des Zustandes der Häuser soll auf das soziale Umfeld und die Kaufkraft ihrer Bewohner geschlossen werden. Ergänzt werden diese Daten mit Angaben über Hausbewohner, die Zeitungsverlage von ihren Inserenten haben oder von ihren Zeitungszustellern sammeln lassen und verkaufen. Gesammelt werden auch Informationen von Adresshändlern, die bei Preisausschreiben, Fragebogenaktionen und Straßenbefragungen Informationen über den Kunden erhalten und beim Scoring zu einem illustren Bild des Kunden zusammenführen.

⁶ Siehe etwa den für die Generaldirektion Gesundheit und Verbraucherschutz der EU erstellten Bericht von Alfred Töpfer, Confidence in e-commerce?, http://europa.eu.int/comm/dgs/health_consumer/events/event-32_wrks4-1.html.

⁷ Vgl. Günther, Elektronische Häuser- und Gebäudekarte, CI 2000, S. 70; Ernst, Zur rechtlichen Beurteilung der digitalen Erfassung von Gebäuden in Datenbanken, RTKom 2000, S. 4. Siehe auch LG Waldshut-Tiengen und VG Karlsruhe, CI 2000, 70 m. Anm. Günther.

3. Relevanz für den Datenschutz

Es liegt auf der Hand, dass die Erhebung, Speicherung, Verarbeitung und Nutzung von Kundendaten datenschutzrelevante Vorgänge sind. Die Respektierung des Datenschutzes gehört zu den vordringlichen Anforderungen an das im E-Business engagierte Unternehmen; denn es zeigt sich immer wieder, dass reale Marktchancen nur für diejenigen Unternehmen realisierbar sind, die das Vertrauen der Marktteilnehmer genießen. Dieses wird nicht nur über Produktqualität und Service, sondern gerade in der elektronischen Welt über Unsicherheit abbauende, vertrauensbildende, die Verbraucherrechte wahrende Maßnahmen erreicht⁸.

Deshalb ist zu fragen, unter welchen rechtlichen Voraussetzungen das Sammeln personenbezogener Daten im Data Warehouse, das Anlegen von Kundenprofilen über Data Mining-Prozesse und das Gewinnen und das Nutzen der Daten durch CRM-Systeme zulässig sind⁹.

II. Anforderungen des Datenschutzrechts

Es hat sich gezeigt, dass der Gläserne Verbraucher das Ziel vieler Marketingaktivitäten ist. Die Übermittlung digitaler Kunden-Informationen (Konsumgewohnheiten, Kreditdaten) über weltweite Netze im Internet als e-mail oder durch Abruf von webpages mit den daraus resultierenden Gefährdungen (Mitlesen privater mails; Erstellung von Nutzerprofilen durch Unbefugte z.B. über cookies; Offenbarung von Konten- und Kreditdaten) rückt das Problem des Datenschutzes immer mehr in den Vordergrund, weil technischer Selbstschutz durch Firewalls, Kryptographie und Sicherheitstechniken beim elektronischen Geldverkehr nur einen eingeschränkten Schutz gewährleistet. Teilnehmern sind die technischen Vorgänge (http-Protokoll, Cookies, Java- und ActiveX-Funktionen) und die damit verbundenen Risiken weitgehend unbekannt. Selbstschutz ist dann eine trügerische Forderung. Kontrollinstitutionen wie die externen Datenschutzbeauftragten sind überlastet. Externe Kontrolle findet weitgehend nicht statt.

Resignierend wird das Internet dementsprechend als „Datenschutzfreier Raum“ bezeichnet¹⁰. Mit dem Internet und der E-Kommunikation wurde das tendenzielle Ende der Privatsphäre verkündet¹¹. Bei E-Commerce befindet sich der Datenschutz „an den Grenzen seiner Realisierbarkeit und Kontrollierbarkeit“¹². Informationelle Selbstbestimmung ist in der Tat dann nicht mehr möglich, wenn der einzelne nicht mehr in der Lage – oder

⁸ Siehe dazu Grabner-Kräuter, Konsumentenvertrauen im E-Commerce – Eine ökonomische Analyse, in: Horster (Hrsg.), Elektronische Geschäftsprozesse, Höhenkirchen 2001, S. 303.

⁹ Siehe zum Thema auch Bizer, TK-Daten im Data Warehouse, DuD 1998, S. 570; ders., Datenschutz im Data Warehouse, in: Fox/Horster (Hrsg.), Datenschutz und Datensicherheit, Wiesbaden 1999, S. 60; Möncke, Data Warehouses – Eine Herausforderung für den Datenschutz?, DuD 1998, S. 561.

¹⁰ Dazu schon Schaar, Datenschutzfreier Raum Internet?, CR 1996, S. 170.

¹¹ Charles J. Sykes, The end of privacy, New York 1999; Simson Garfinkel/Deborah Russell, Database Nation: The Death of Privacy in the 21st Century, 2001; Reg Whitaker/Reginald Whitaker, The End of Privacy: How Total Surveillance Is Becoming a Reality, 2000.

¹² Wächter, Personenbezogene Datenverarbeitung im E-Commerce, in: Moritz/Dreier, Rechts-Handbuch zum E-Commerce, Köln 2002, Rn. 655.

vielleicht auch gar nicht mehr Willens – ist, die Verwendung der sich auf ihn beziehenden Daten zu steuern¹³. Erstaunlich groß ist die Zahl derer, die für eine lächerlich geringe Gegenleistung wie eine kostenlose SMS pro Tag sehr persönliche, auch weltanschauliche Daten offenbaren. *Schneider* sieht die Privat- und Intimsphäre durch Selbstblößung und datenbankbasierte Segmentierung des Einzelnen durch die Data Warehouse-Konzeption als verloren gegangen an und fordert eine adäquate Neu-Modellbildung des Datenschutzes im Kommunikationszeitalter.

Es gibt daneben auch Stimmen, die fundamental zu einem 'roll-back' des Datenschutzgedankens auffordern und eine grundlegende "Neubesinnung" für erforderlich halten, weil Deutschland sonst zu einem informationellen Entwicklungsland würde, wenn der Gesetzgeber an seinem hohen Schutzniveau festhalte¹⁴.

Der Europäische und der nationale Gesetzgeber haben dagegen Anstrengungen unternommen, das Datenschutzrecht an die neuen Gefährdungslagen anzupassen. Die EU hat neben der allgemeinen Datenschutzrichtlinie eine bereichsspezifische Richtlinie erlassen¹⁵, deren Novellierung derzeit diskutiert wird¹⁶. Der Schutz der personenbezogenen Daten ist gar mit Art. 8 der Charta der Grundrechte der Europäischen Union an herausragender Stelle in den Grundrechtskatalog aufgenommen worden¹⁷.

1. Anonymität im Netz

Das CRM-Konzept steht in einem diametralen Widerspruch zu den Intentionen des Datenschutzes. Während CRM auf Identifizierung der Nutzer der elektronischen Kommunikation aus ist und dessen Verhaltens- und Persönlichkeitsprofil in einem Data Warehouse segmentieren will, strebt der moderne Datenschutz die Anonymität im Netz und das Agieren mit Pseudonymen an¹⁸.

Das Bundesdatenschutzgesetz verpflichtet mit § 3a BDSG zur Datenvermeidung und zur Datensparsamkeit. Die Anbieter von Tele- und Mediendiensten haben die Inanspruchnahme von Diensten und ihre Bezahlung in anonymer oder pseudonymer Weise zu ermöglichen (§ 3a BDSG; § 4 Abs. 1 TDDSG; § 13 Abs. 1 MDSStV) und die Prinzipien von Datenvermeidung und Datensparsamkeit zu beachten (§ 3 Abs. 4 TDDSG; § 12

¹³ Dazu *Schneider*, *Europäischer Datenschutz und E-Commerce*, in: *Lehmann (Hrsg.), Electronic Business in Europa*, München/Wien 2002, S. 561(562).

¹⁴ Siehe zuletzt in besonders pointierter, aber wenig überzeugender Form *Sutschet*, *Über Informationsverbote zur Wissensgesellschaft?*, RDV 2000, S. 107.

¹⁵ Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281/31); Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation (ABl. EG Nr. L 24/1).

¹⁶ Siehe den Vorschlag für eine Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, KOM/2000/0385 endg.; ABl. Nr. C 365 E vom 19.12.2000, S. 23, mit der übrigens auch das Verbot des Spamming entgegen einer früheren Haltung der EU-Kommission eingeführt werden soll (Art. 13).

¹⁷ ABl. EG Nr. C 364, S. 1 vom 18.12.2000.

¹⁸ Vgl. dazu näher *Rötzer*, *Das Recht auf Anonymität*, in: *Bäumler, H. (Hrsg.), E-Privacy*, Braunschweig/Wiesbaden 2000, S. 27.

Abs. 5 MDStV). Die Erstellung personenbezogener Nutzerprofile ist nach § 4 Abs. 4 S. 1 TDDSG unzulässig.

2. Verbot mit Erlaubnisvorbehalt

Ist anonymes Handeln nicht möglich und auch vom Nutzer, der eine ihm zu Gute kommende Leistung anstrebt und sich deshalb identifizieren muss, nicht angestrebt, gehen die europäischen Datenschutzrichtlinien, das BDSG sowie die bereichsspezifischen Datenschutzregelungen im Teledienstedatenschutzgesetz (TDDSG) und in der Telekommunikationsdatenschutzverordnung (TDSV) davon aus, dass das bußgeldbewehrte Verbot der Erhebung, Verarbeitung und Nutzung der Daten der Regelfall ist. Eine Ausnahme vom Verbot setzt eine Erlaubnis voraus. Die Erlaubnis kann sich aus einer Einwilligung, aus dem Datenschutzgesetz selbst oder aus einem anderen, die Datenverarbeitung erlaubenden oder anordnenden Gesetz ergeben.

An die Einwilligung sind hohe Anforderungen zu stellen. Zwar kann die jederzeit widerrufbare Einwilligungserklärung auch elektronisch abgegeben werden (§ 89 Abs. 10 TKG; § 3 Abs. 7 TDDG); wirksam ist sie aber nur, wenn der Nutzer über die gesamten Umstände und Folgen seiner Einwilligungserklärung informiert ist (informed consent) und die Tragweite seiner Einwilligung zu erkennen vermag. Er ist vor der Erhebung über Art, Umfang, Ort und Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten zu unterrichten (§§ 4 Abs. 1, 4a Abs. 1 BDSG; § 3 Abs. 4 TDDSG; § 12 Abs. 6 MDStV). Willigt der kooperationsbereite Kunde ein – ohne, dass Druck auf ihn ausgeübt wurde –, dürfen die Daten nur zu diesem Zweck verwendet werden (Zweckbindung). Sollen sie für andere Zwecke verwendet werden, bedarf es einer erneuten, darauf bezogenen Einwilligungserklärung. Eine Speicherung in einem Data Warehouse wäre mit diesen Grundsätzen von vornherein unvereinbar, weil es gerade das Prinzip des Data Warehouse ist, die Daten auf Vorrat und für beliebige Abfragekonstellationen zur Verfügung zu stellen.

3. Einschränkungen bei der Verarbeitung

Die Speicherung der bei der Nutzung von Telekommunikationsleistungen (Netzebene) anfallenden personenbezogenen Daten zu Zwecken der Werbung oder der Marktforschung ist nur mit der ausdrücklichen Zustimmung des Betroffenen zulässig (§ 89 Abs. 7 TKG). Ansonsten dürfen personenbezogene Daten von Nutzern nur als Bestands- oder Nutzungsdaten im Rahmen des Vertragszwecks – soweit überhaupt erforderlich – gespeichert werden. Das gilt auch für die Nutzung von Telediensten (Dienste-Ebene, §§ 6, 7 TDDSG). Die Daten dürfen nur zusammengeführt werden, soweit dies zur Abrechnung erforderlich ist (§ 7 Abs. 2 TDDSG). Personenbezogene Nutzungsprofile sind verboten (§ 7 Abs. 3 TDDSG). Damit hat sich das Datenschutzrecht bei der Nutzung von Telekommunikationsanlagen und Telediensten darauf festgelegt, dass ohne Einwilligung nur Bestands- oder Abrechnungsdaten personenbezogen erhoben und verarbeitet werden dürfen. Auch die Regelung des § 28 Abs. 1 Nr. 2 BDSG, der es der speichernden Stelle zur Wahrung berechtigter Interessen erlaubt, personenbezogene Daten zu verarbeiten

und zu nutzen, wenn schutzwürdige Interessen des Betroffenen nicht entgegen stehen, berechtigt entgegen einer verbreiteten Ansicht nicht zur Nutzung der Vertrags- oder Nutzungsdaten zu anderen Zwecken¹⁹. Die gesetzlich geforderte Trennung zwischen Daten, die bei der Auswertung des Nutzungsverhaltens entstehen, und Vertrags-/Bestandsdaten wird in der Praxis regelmäßig nicht beachtet. So speichert der überwiegende Teil der auf dem Markt angebotene E-Mail-Marketing-Software das sogenannte Klickverhalten des Empfängers einer E-Mail-Newsletter und führt die Nutzungsdaten personenbezogen in das CRM.

4. Verbot von Scoring-Systemen

Scoring-Systeme ermöglichen die automatisierte Einzelentscheidung über die Kreditwürdigkeit auf der Grundlage vorgegebener, generalisierter Bewertungssysteme. Nach der Neufassung des Bundesdatenschutzgesetzes ist ein solches Verfahren unvereinbar mit der Vorschrift des § 6a BDSG, der eine automatisierte Einzelentscheidung verbietet²⁰.

III. Datenschutzrechtliche Beurteilung des CRM

Eine Umsetzung des technisch Möglichen und in der Praxis bereits realisierten Szenarios bei CRM-Systemen in Verbindung mit Data Warehouse und Data Mining verstößt gegen Datenschutzrecht. Auch die Datenschutzbeauftragten des Bundes und der Länder halten diese Datenverarbeitungspraxis für unzulässig²¹. Eine entsprechende Datenschutzsensibilität ist allerdings bei vielen Online-Händlern und ihren Software-Lieferanten nicht vorhanden²². Diensteanbieter kennen die Verpflichtungen des BDSG zumeist nur in groben Zügen und wenden es überwiegend nicht oder nicht richtig an. Die vorgehenden, strengeren Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) und der Telekommunikations-Datenschutzverordnung (TDSV) sind den Diensteanbietern, insbesondere den Anbietern beim E-Commerce, mit wenigen Ausnahmen unbekannt. Die Verletzung des TDDSG bzw. des Mediendienstestaatsvertrags und der TDSV ist heute die Regel.

Die Reaktion kann nicht der Abschied vom Datenschutz sein. Es sind ausgereifte Datenschutzkonzepte erforderlich, die das Vertrauen der Kunden in elektronische Geschäfte

¹⁹ Ebenso Büllesbach, Datenschutz bei Data Warehouses und Data Mining, CR 2000, S. 11(13f.).

²⁰ Siehe dazu auch Wächter, Personenbezogene Datenverarbeitung im E-Commerce, in: Moritz/Dreier, Rechts-Handbuch zum E-Commerce, Köln 2002, Rn. 646.

²¹ Vgl. die Nachweise bei Jürgens, Grenzen für Videoüberwachung, Data-Warehousing und Data-Mining, DSB 4/2000, S. 8, und unter <http://www.datenschutz-berlin.de/doc/de/konf/index.htm>. Siehe auch Büllesbach, Datenschutz bei Data Warehouses und Data Mining, CI 2000, S. 65; Baeriswyl, Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut?, RDV 2000, S. 6, und Imhof, One-to-One-Marketing im Internet – Das TDDSG als Marketinghindernis, CR 2000, S. 110.

²² Ausführlich dazu Computer Zeitung vom 23.3.2000, S. 20. Siehe auch Wanckel, Persönlichkeitsschutz in der Informationsgesellschaft, Frankfurt/M. 1999.

erobert werden²³. Die bereits jetzt nach nicht-hoheitlichen Kriterien stattfindende Auditierung der e-shops und die Verleihung von Siegeln wie 'trusted shops'²⁴ können dafür geeignete Maßnahmen sein.

Richtig ist, dass neue, 'moderne' Formen des Datenschutzes wie mehr Schutz durch Selbstregulierung (codes of ethics; vgl. § 38a BDSG), Technischer Schutz (privacy enhancing technologies), Systemdatenschutz (z.B. Zahlungen ohne Datenspur) neben die hoheitliche Verantwortung und Kontrolle treten müssen, um Defizite der bisherigen Regelungen durch neue Instrumente zu beheben²⁵. Daneben bietet sich an, „Mechanismen der indirekten Verhaltenssteuerung unter Einbeziehung marktwirtschaftlicher Methoden zu etablieren“²⁶. In den jüngeren Datenschutzgesetzen sind bereits Ideen des Schutzes durch Marktmechanismen in Form eines Datenschutz-Audits eingeführt (§ 9a BDSG).

Auch die Verbände der Werbewirtschaft und einige Unternehmen²⁷ haben erkannt, dass sich auf lange Sicht der elektronische Geschäftsverkehr nur durchsetzt, wenn über eine datenschutzfreundliche Systemgestaltung das – glaubt man den Umfragen – bislang nicht sehr ausgeprägte Vertrauen der Kunden nachhaltig gewonnen werden kann.

Literaturverzeichnis

Baeriswyl, B.: Data Mining und Data Warehousing: Kundendaten als Ware oder geschütztes Gut?, RDV 2000, S. 6.

Bizer, J.: TK-Daten im Data Warehouse, DuD 1998, S. 570.

Bizer, J.: Datenschutz im Data Warehouse, in: Fox, D./Horster, P. (Hrsg.), Datenschutz und Datensicherheit, Wiesbaden 1999, S. 60.

Boehme-Neßler, V.: Datenschutz in der Informationsgesellschaft, K & R 2002, S. 217.

Büllesbach, A.: Datenschutz bei Data Warehouses und Data Mining, CR 2000, S. 11.

Büllesbach, A.: Datenschutz bei Data Warehouses und Data Mining, CI 2000, S. 65.

²³ Computer Zeitung vom 23.3.2000, S. 20: "Der sensible Umgang mit Kundendaten (wird) zu einem K.O.-Kriterium im elektronischen Handel.". Daniel Ebert: "A group of CEOs, representing several of the Internet's largest companies, have sent a joint letter to more than 400 of their colleagues, urging them to strengthen their online privacy policies." (Brief dokumentiert unter <http://www.netcoalition.com/>). Vgl. auch den Konzern-Datenschutzbeauftragter bei DaimlerChrysler Büllesbach, Datenschutz in einem globalen Unternehmen, RDV 2000, S. 1.

²⁴ <http://www.trusted-shops.de>.

²⁵ Vgl. neben vielen Lanfermann, Datenschutzgesetzgebung – gesetzliche Rahmenbedingungen einer liberalen Informationsgesellschaft, RDV 1998, S. 1; Wolters, Einkauf via Internet: Verbraucherschutz durch Datenschutz, DuD 1999, S. 277.

²⁶ Boehme-Neßler, Datenschutz in der Informationsgesellschaft, K & R 2002, S. 217(221).

²⁷ Siehe dazu etwa das Projekt DASIT unter <http://www.dasit.myshop.de>. Inzwischen gibt es einige Unternehmensinitiativen, die die Selbstregulierung propagieren, siehe dazu <http://www.gbde.org>, und Unternehmen dazu aufrufen, sich einem strengen Code of Conduct zu unterwerfen. Gibt es einen solchen, ist auf diesem übrigens gem. § 312 c BGB i.V.m. der BGB-Informationspflichtenverordnung auch auf der Website hinzuweisen.

- Büllesbach, A.: Datenschutz in einem globalen Unternehmen, RDV 2000, S. 1.
- Ernst, St.: Zur rechtlichen Beurteilung der digitalen Erfassung von Gebäuden in Datenbanken, RTKom 2000, S. 4.
- Garfinkel, S./Russell, D.: Database Nation: The Death of Privacy in the 21st Century, 2001.
- Grabner-Kräuter, S.: Konsumentenvertrauen im E-Commerce – Eine ökonomische Analyse, in: Horster, P. (Hrsg.), Elektronische Geschäftsprozesse, Höhenkirchen 2001, S. 303.
- Günther, A.: Elektronische Häuser- und Gebäudekarte, CI 2000, S. 70.
- Hermanns, A.: Online-Marketing im E-Commerce – Herausforderungen für das Management, in: Hermanns, A./Sauter, M. (Hrsg.), Management-Handbuch Electronic Commerce, München 2001, S. 116.
- Imhof, R.: One-to-One-Marketing im Internet – Das TDDSG als Marketinghindernis, CR 2000, S. 110.
- Jürgens, U.: Grenzen für Videoüberwachung, Data-Warehousing und Data-Mining, DSB 4/2000, S. 8.
- Lanfermann, H.: Datenschutzgesetzgebung – gesetzliche Rahmenbedingungen einer liberalen Informationsgesellschaft, RDV 1998, S. 1.
- Matejcek, K.: Newsletter und Mailinglisten – Marketing per E-Mail, Wien 2001.
- Möncke, U.: Data Warehouses – Eine Herausforderung für den Datenschutz?, DuD 1998, S. 561.
- Podlech, A./Pfeifer, M.: Die informationelle Selbstbestimmung im Spannungsverhältnis zu modernen Werbestrategien, RDV 1998, S. 139.
- Rötzer, F.: Das Recht auf Anonymität, in: Bäuml, H. (Hrsg.), E-Privacy, Braunschweig/Wiesbaden 2000, S. 27.
- Schaar, P.: Datenschutzfreier Raum Internet?, CR 1996, S. 170.
- Schneider, M.: Europäischer Datenschutz und E-Commerce, in: Lehmann, M. (Hrsg.), Electronic Business in Europa, München/Wien 2002, S. 561.
- Sutschet, H.: Über Informationsverbote zur Wissensgesellschaft?, RDV 2000, S. 107.
- Sykes, Ch. J.: The end of privacy, New York 1999.
- Wanckel, E.: Persönlichkeitsschutz in der Informationsgesellschaft, Frankfurt/M. 1999.
- Wächter, M.: Personenbezogene Datenverarbeitung im E-Commerce, in: Moritz, H.-W./Dreier, Th., Rechts-Handbuch zum E-Commerce, Köln 2002, Rn. 655.
- Whitaker, R./Whitaker, R.: The End of Privacy: How Total Surveillance Is Becoming a Reality, 2000.
- Wolters, S.: Einkauf via Internet: Verbraucherschutz durch Datenschutz, DuD 1999, S. 277.