
Datenschutz als Verbraucherschutz (2001)

Verbraucherzentrale
Bundesverband e.V.

Datenschutz als Verbraucherschutz

Vortrag Prof. Dr. Edda Müller

Sommerakademie 2001 des Unabhängigen Landeszentrums für Datenschutz am 10.09.2001 in Kiel zum Thema Datenschutz als Wettbewerbsvorteil

Sehr geehrter Herr Dr. Bäumler,
sehr geehrter Herr Landtagspräsident,
sehr geehrte Frau Ministerpräsidentin,
sehr verehrten Damen und Herren,

seit der letzten Sommerakademie, bei der wir bereits die Ehre und das Vergnügen hatten, die Sichtweise der Verbraucher zum Thema Datenschutz als Verbraucherschutz einzubringen, hat sich auf der Ebene der Verbraucherverbände einiges geändert. Ende des Jahres 2000 kam es zu einer **grundlegenden Reform der Verbrauchervertretung auf Bundesebene**. Um die Verbandsarbeit noch wirksamer zu gestalten, wurde der Bundesverband der Verbraucherzentralen und Verbraucherverbände (Verbraucherzentrale Bundesverband, vzbv) mit Sitz in Berlin als Dachorganisation der verbraucherpolitischen Organisationen in Deutschland gegründet. Im **Verbraucherzentrale Bundesverband** haben sich die drei Bundesorganisationen Arbeitsgemeinschaft der Verbraucherverbände e.V. (AgV), die Stiftung Verbraucherinstitut (VI) und der Verbraucherschutzverein (VSV) zusammengeschlossen. Mitglieder des vzbv sind die 16 Verbraucherzentralen der Länder sowie 18 weitere sozial orientierte Organisationen. Die Bündelung der Kräfte fiel zusammen mit einer neuen Prominenz und stärkeren Beachtung von Verbraucherbelangen im politischen Raum. Wir können uns heute also gestärkt zu Wort melden, wenn es um die Verbesserung des Schutzes von Verbraucherdaten geht. Ich will unsere Position im Folgenden anhand von sechs Thesen erläutern.

These 1: Moderne Verbraucherpolitik sollte sich am Leitbild der Vorsorge und der Verantwortung der Konsumenten orientieren. Der Schutz von Verbraucherdaten ist notwendiger Bestandteil einer solchen Politik.

Verbraucherpolitik ist immer dann gefordert, wenn Verbraucher ihre Interessen durch ihr individuelles Verhalten allein nicht wirksam befriedigen und verteidigen können, wenn der Marktmechanismus von Angebot und Nachfrage Verbraucherinteressen nicht ausreichend schützt oder wenn auch durch politik- und staatsferne Kooperationsformen Verbraucherschutzziele nicht erreicht werden können. **Leitbild moderner Verbraucherpolitik** muss daher zum einen die **Vorsorge** sein. Verbraucherpolitik darf also nicht erst bei den Produkten und Dienstleistungen ansetzen, sondern muss schon auf die der Vermarktung vorgelagerten Prozesse und Entscheidungen Einfluss nehmen. Zum anderen folgt aus dem **Leitbild des verantwortlich handelnden Konsumenten**:. Der Konsument sollte als aktiver Partner im Marktgeschehen verstanden werden, der als Einzelner das Recht auf Schutz hat und die Möglichkeit zur Gegenwehr haben muss, sich aber zugleich auch der Auswirkungen seiner Konsumentenentscheidung und seines Käuferverhaltens bewusst ist und Mitverantwortung übernimmt. Dies gilt auch für den Umgang mit den eigenen Daten.

Seit den Anfängen der Verbraucherarbeit ist **Datenschutz ein wichtiges Verbraucherthema**. So beschäftigte uns z. B. bereits in der Vergangenheit der Handel mit Kundenadressen. Durch den Eintrag in Sperrlisten konnte dem Missbrauch in der Offline-Welt begegnet werden. Auch wurden im Rahmen des **kollektiven Rechtsschutzes** Klauseln in den Allgemeinen Geschäftsbedingungen abgemahnt, die mit grundlegenden Regeln des Datenschutzes wie der Einwilligung des Betroffenen und einer gerechten Interessenabwägung nicht im Einklang standen. Ein weiteres Thema waren in diesem Zusammenhang Schweigepflichtentbindungserklärungen von Versicherungsgesellschaften.

Mit zunehmender Digitalisierung unser Gesellschaft werden solche Gegenmaßnahmen und damit der Selbstschutz des Verbrauchers immer schwieriger. Selbst für Experten wird zunehmend undurchschaubar, wo durch wen welche Daten erhoben, verarbeitet und weitergegeben werden. In der Online-Welt hinterlässt jede Lebensregung Datenspuren. Angesichts dieser unkontrollierbarer Datenströme nimmt potenziell auch die Einflussmöglichkeit der Verbraucher ab. Zugleich sind **personenbezogene Daten** für die Informationswirtschaft als weitere Einnahmequelle zunehmend interessant. Es gilt also, die

nachteiligen Folgen für den Verbraucherschutz zu begrenzen, und für eine **Chancen- und Waffengleichheit** zwischen Verbrauchern als „Datenträger" und Anbietern als „verantwortliche Stellen" zu sorgen. Gleichzeitig müssen die **Verbraucher als eigenverantwortliche Datensubjekte** im Sinne der Hilfe zur Selbsthilfe in die Lage versetzt werden, die Brisanz ihrer Daten zu begreifen, Risiken im Umgang mit diesen zu erkennen, um angemessen reagieren zu können.

Wesentliche Grundlage des Rechts auf informationelle Selbstbestimmung bildet immer noch das Volkszählungsurteil aus dem Jahre 1983, in dem der Bundesgerichtshof erstmals das Recht des Einzelnen aus unserer Verfassung hergeleitet hat, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Während es damals vor allem um den **Schutz vor staatlichem Zugriff** ging, geht es heute auch um den **Schutz vor der unkontrollierten Datenverwendung durch private Stellen.** Hier findet zunehmend eine Verschiebung der Quantitäten und Qualitäten personenbezogener Datenverarbeitung statt. Weiß der Einzelne schon in der herkömmlichen papiergebundenen Welt oftmals nicht, wer über seine persönlichen Daten verfügt, so wird es im world wide web schier unmöglich, die Verwendung der eigenen persönlichen Daten zu kontrollieren. Hinzu kommen **neue Verarbeitungstechniken**, die wiederum neue Gefährdungen personenbezogener Daten mit sich bringen, wie etwa die Biometrie. Wegen der unmittelbaren, vor allem auch datenschutzbezogenen Relevanz für den Verbraucher gestalten wir hier die Rahmenbedingungen in technischer, organisatorischer und rechtlicher Hinsicht aktiv mit.

Neue Probleme ergeben sich auch durch **neue Einsatzmethoden** der modernen Datentechnik. Aktuell geht es heute auf europäischer Ebene um das sog. spamming, d.h. um Werbe-emails, die unaufgefordert den elektronischen Briefkasten des Empfängers überfüllen und beim betroffenen Verbraucher neben Unbequemlichkeiten auch erhebliche Kosten verursachen können.

Sowohl hinsichtlich der Kontrolle der Datennutzer als auch der Sensibilisierung der Verbraucher beim Umgang mit seinen Daten in der Online-Welt sehen wir eine gemeinsame Aufgabe von Daten- und Verbraucherschützern. Mit vereinten Kräften werden wir Gefahren für die informationelle Selbstbestimmung wirksamer begegnen können, als wenn wir dies getrennt tun.

These 2: Das unterschiedliches Sicherheitsbewusstsein der Verbraucher muss zur Bündelung der Interessen in einer gesellschaftlich anerkannten Datenschutzkultur führen.

Im Bereich des Datenschutzes begegnet uns nicht ein einheitliches Sicherheitsbewusstsein der Verbraucher, auf das wir nur angemessen zu reagieren brauchen. Die Frage ist wesentlich komplexer und muss daher differenziert betrachtet werden. Auf der einen Seite gibt es eine große Zahl von Verbrauchern, die **besondere Sicherheitsbedenken** haben und aus diesem Grunde vor allem am elektronischen Geschäftsverkehr nicht oder nur sehr zögerlich teilnehmen. Auf der anderen Seite gibt es aber auch eine Gruppe von Verbrauchern, die **keine oder nur sehr gering ausgeprägte Sicherheitsbedenken** haben. Zu beobachten ist ein teilweise sorgloser Umgang mit den eigenen Daten. Die Gründe liegen oft im fehlenden Bewusstsein über die Brisanz der eigenen Daten, über den Geldwert für die anbietende Wirtschaft und in der Unkenntnis der technischen Möglichkeiten zur Erhebung, Verarbeitung und Übermittlung von Daten. Manche Verbraucher nutzen z. B. Angebote wie Kundenkarten[1], mailing-Listen. weitgehend bedenkenlos, oftmals ohne überhaupt auf den Gedanken zu kommen, dass sie damit Anbietern fast grenzenlose Möglichkeiten eröffnen, Kundenprofile zu erstellen, mit denen diese das individuelle Konsumverhalten nicht nur bewerten, sondern auch steuern und beeinflussen können.

So unterschiedlich beide Gruppen mit ihren Daten umgehen - **beiden mangelt es** vor allem **an hinreichender Transparenz**, was sowohl für die Möglichkeiten des Selbstschutzes als auch das Gefährdungspotenzial gilt. Durch **Sensibilisierung** der Verbraucherschaft muss diese über lautere und unlautere Möglichkeiten der Anbieter aufgeklärt werden. Die Verbraucher müssen daneben verstärkt über ihre Möglichkeiten zur **Prävention** informiert werden. Der präventive Schutz ist beispielsweise durch den Erwerb und die Inanspruchnahme datenschutzgerechter Produkte und Dienstleistungen möglich. Erforderlich ist auch hier das Wissen darüber, wie der Einzelne sich z.B. beim Surfen im Internet vor ungewollten Datenerhebungen und –verknüpfungen schützen kann. Dies fängt bei der technisch möglichen Verhinderung der Ablage von Cookies bzw. überhaupt deren Existenz an, geht über anonyme oder pseudoanonyme Möglichkeiten des Surfens im Internet und hört bei der Verschlüsselung sensibler Daten noch lange nicht auf.

[1] Wie z.B. das System PAYBACK, gegen das der vzbv derzeit in der zweiten Instanz vor Gericht steht

Um den Verbrauchern beides zu vermitteln, sind **Maßnahmen zur verbesserten Information** erforderlich. Dazu gehört eine verstärkte Informationspolitik seitens der Verbraucher- und Datenschutzverbände. Wir brauchen aber auch Anstrengungen im staatlichen Bildungsbereich und die Entwicklung einer Datenschutzdidaktik. Der Staat muss im Bereich des Datenschutzes seine mit fortschreitenden technischen Möglichkeiten ebenfalls wachsenden Schutzpflichten gegenüber dem Bürger wahrnehmen. Ziel sollte nicht nur die Bereitstellung einer Sicherheitsinfrastruktur sein, sondern es muss eine Sicherheitskultur geschaffen werden, indem jedem Bürger **Sicherheitskompetenz und Sicherheitsbewusstsein** vermittelt werden.. Dies müsste bereits im Schulunterricht durch Einführung eines Schulfaches „Datensicherheit in der Informationsgesellschaft" geschehen.

These 3: Zugang zu Informationen und Datenschutz sind in einer Informationsgesellschaft keine Gegensätze, sondern zwei Seiten der informationellen Selbstbestimmung.

Möglichst umfassender **Zugang zu Informationen** einerseits und der **Schutz der eigenen Daten** andererseits sind nach dem Bundesverfassungsgericht **elementare Grundbedürfnisse** des Menschen, um sich als Persönlichkeit zu entfalten. Dort, wo Schutzinteressen hinsichtlich sensitiver Daten verschiedener Parteien aufeinander treffen, müssen diese sorgfältig gegeneinander abgewogen werden. Die **gerechte Interessenabwägung** ist ein wesentlicher Grundsatz unserer Rechtsordnung. Somit müssen auch die berechtigten Interessen des informationsbegehrenden Verbrauchers gegen diejenigen des Unternehmers abgewogen werden, der seine Daten schützen will. Allerdings gilt hier wie in vielen anderen Bereichen auch, dass die potenzielle Unterlegenheit des Verbrauchers oftmals zu einem Zurücktreten der Anbieterinteressen führen muss. Wir fordern deshalb ein **Verbraucherinformationsgesetz**, mit dem der öffentliche Zugang zu staatlichen Prüfergebnissen und Bewertungen sichergestellt und im privaten Bereich Unternehmen verpflichtet werden, öffentlich zugängliche Transparenzdatenbanken aufzubauen.

These 4: Im E-Commerce ist der Datenschutz von besonderer Bedeutung.

Besonders im E-Commerce entstehen **datenschutzspezifische Risiken** wie etwa durch die Erstellung von Online-Profilen durch das. data-mining in sog. data-warehouses. Beim online-Einkauf hinterlässt der Kunde Daten im Klartext und Datenspuren, wenn er beispielsweise dazu veranlasst wird, umfassende persönliche Angaben zu machen, die für die Bestellung nicht notwendig sind, und er zusätzlich noch per Kreditkartennummer im voraus bezahlen soll, weil eine Bezahlung per Rechnung nicht angeboten wird. Hier müssen unter anderem Möglichkeiten verbrauchergerecht umgesetzt werden, sich **anonym** in der virtuellen Welt zu bewegen und nur dort, wo es wirklich darauf ankommt und auch die Zweckbindung gewährleistet ist, die wahre Identität zu offenbaren.

Bei der Gestaltung der gesetzlichen Rahmenbedingungen muss der Staat seinen Schutzpflichten gegenüber dem Bürger u.a. durch **Schaffung einer wirksamen Sicherheitsinfrastruktur,** wie etwa der digitalen Signatur, nachkommen. Notwendig sind Regelungen, die auch sanktionsbewährt sind. Die Schaffung geeigneter Sanktionsregelungen wird sicher einer der wesentlichen Diskussionspunkte im Rahmen der Modernisierung des Datenschutzrechts sein. Genauso wichtig ist angesichts des rasanten Fortschreitens der Technik eine wirksame und verlässliche **Selbstregulierung der Anbieter.**

Nach einer aktuellen **Studie unseres Weltverbandes Consumer International**, in der ca. 750 Internetseiten überprüft wurden, gaben 28 % der Internet-Händler **keinerlei Informationen zum Datenschutz**. Informationen über den Anbieter, Preis- und Lieferangaben etc. fehlten ebenfalls in erheblichem Umfang. Mehr als zwei Drittel der geprüften Seiten blieben hinter international anerkannten Minimalstandards zurück. Es wurden **persönliche Daten von Verbrauchern** solcher Art **abgefragt**, dass eine Identifizierung und Kontaktaufnahme ermöglicht wurde, ohne dass dies für die Nutzer eindeutig erkennbar gewesen wäre. Weit mehr als die Hälfte der Seiten bot **keine Möglichkeit** an, durch die der Nutzer selbstständig und bewusst **über die Weiterverarbeitung seiner persönlichen Daten durch Dritte hätte entscheiden** können. Trotz strengerer Gesetzgebung in der EU waren viele in der EU beheimatete Unternehmen nicht in der Lage, ihren Kunden hinreichende **Informationen über** ihre **Privacy Policy** zu geben. Die besten Ergebnisse fanden sich hier bei einigen US-Anbietern. Auch gab es bei den US-Seiten öfter als bei den EU-Anbietern die technische Möglichkeit für die Kunden, durch **bewussten Klick (opt-in) über die Aufnahme in die mailing-Liste** des jeweiligen

Unternehmens zu entscheiden. Nur 10 % der **an Kinder gerichteten Angebotsseiten** forderte die Zustimmung der Eltern ab oder verzichtete ganz auf die Erhebung persönlicher Daten über die jugendlichen Nutzer.

Innerhalb der Europäischen Union werden diese Probleme nicht primär durch mangelnde Gesetze verursacht. Zu beklagen sind vielmehr der **mangelhafte Gesetzesvollzug** und insbesondere die praktischen Schwierigkeiten, Rechte im **grenzüberschreitenden Rechts- und Geschäftsverkehr** auch durchzusetzen. Hier muss über geeignete Wege gesprochen werden, Verbraucherrechte und Verbrauchervertrauen zu stärken und Missbräuche zu bekämpfen. In dem in Schleswig-Holstein entwickelten Datenschutzaudit sehen wir .ein interessantes und praktikables Instrument, um dieses Ziel zu erreichen.

These 5: Wirksamer Datenschutz ist ein Wettbewerbsvorteil.

Die wirtschaftlichen Möglichkeiten des e-commerce werden derzeit wegen der dargestellten Probleme einer häufig **fehlenden Vertrauenswürdigkeit** und **Intransparenz** bei weitem nicht genutzt. Wirksamer Datenschutz kann deshalb zu einem entscheidenden Wettbewerbsvorteil werden. Voraussetzung ist allerdings, dass Datenschutzmaßnahmen für den Verbraucher konkret und praktikabel sind.. Erst wenn der Verbraucher **Datenschutz als im Alltag praktikabel** erlebt, wird er Produkten, Anbietern und Dienstleistern den Vorzug geben, deren Datenschutzangebot überzeugend ist. Ein Teil der Wirtschaftsakteure hat die Zeichen der Zeit erkannt.. Wir erhalten vermehrt Anfragen von Anbieterseite, die den Dialog mit den Verbraucherverbänden zum Datenschutz suchen und unsere Zustimmung zu bestimmten Angebotsformen erfragen, um das Verbrauchervertrauen zu gewinnen. Diese Unternehmen haben erkannt: **„Privacy sells“**

These 6: Nötig sind Qualitätstests für datenschutzgerechte Produkte und Dienstleistungen

Datenschutz sollte wie andere Merkmale auch ein **wichtiger Faktor zur Beurteilung der Qualitätseigenschaften von Produkten und Dienstleistungen sein.** Während es auf dem Gebiet der Verbraucherprodukte seit langer Zeit und mit Erfolg der Stiftung Warentest und anderen Einrichtungen gelingt, dem Verbraucher anhand von Waren- und Dienstleistungstests Entscheidungskriterien für den Erwerb von Produkten und die Inanspruchnahme von Dienstleistungen an die Hand zu geben, fehlt derartiges bisher auf dem Gebiet des Datenschutzes. Denkbar wäre die Einbeziehung von Datenschutzkriterien in die bereits bestehenden Testreihen. Geeigneter wären vermutlich jedoch spezifische Tests, die die besonderen Anforderungen des Datenschutzes, Aspekte der Datensicherheit und Datenschutzpolicies überprüfen könnten.. Die Datenschutzbehörden haben schon erste Ansätze entwickelt. Sie sollten weiter ausgebaut werden, um Datenschutz für den Verbraucher in Zukunft alltagstauglich zu machen. Wir bieten ihnen hierbei unsere Kooperation und Unterstützung an.