

Systemvertrauen: Ein Versuch über einige Zusammenhänge zwischen Karte und Datenschutz

Herbert Burkert

All Rights reserved / Alle Rechte vorbehalten

© 1991

Eine gedruckte Version erschien (ohne Fussnoten) in:
à la Card Euro-Journal. Heft 1. 1991, 52-66.

Datenschutz und "Karte" : Ein erster Blick

Das erste Zusammentreffen der "Karte" mit dem Datenschutz führte zur Entwicklung des internationalen Datenschutzes¹.

Eine Gemeindeverwaltung in Schweden wollte zur Vereinfachung der Verwaltungsarbeit für die Patienten des Gemeindekrankenhauses eine Plastikkennkarte ausgeben. Diese Karte sollte das Personenkennzeichen, Name und Anschrift und den Namen der für den Patienten zuständigen Gemeinde enthalten. Da in Schweden kein Unternehmen zu finden war, das in der Lage gewesen wäre, die Karte herzustellen, sollte der Auftrag an eine englische Firma vergeben werden. Die schwedische Datenschutzbehörde, damals die erste *nationale* Behörde (in Hessen gab es auf Länderebene bereits seit 1970 ein Datenschutzgesetz) ihrer Art, untersagte in Anwendung des § 11 des schwedischen Datenschutzgesetzes die Übermittlung.

Diese Entwicklung hat über die Empfehlungen der OECD und die Konvention des Europarates zur Zeit ihren Höhepunkt in der Vorlage eines Entwurfes für eine EG-Direktive zum Datenschutz gefunden. Allerdings waren nicht die Karten selbst das Problem sondern der, wie es die schwedische Datenschutzbehörde damals nannte, "Massenexport" (es ging immerhin um 80.000 Datensätze) personenbezogener Daten. Seither hat der Datenschutz immer wieder in die *Verwendungszusammenhänge* der Karte eingegriffen, so etwa bei der Gestaltung und Nutzung des maschinenlesbaren Personalausweises.

¹¹ Hierzu Bing 1978, 18ff.

Ein zweiter Blick

Nicht aber den Anwendungsproblemen datenschutzgesetzlicher Regeln soll hier diese Betrachtung dienen. Beim Zusammentreffen von Karten"konzept" und Datenschutz"konzept" werden vielmehr Strukturen sichtbar, die unser Verständnis beider Konzepte vielleicht nicht notwendigerweise erweitern aber doch bewußter machen. Ein Ergebnis wird die Wahrnehmung sein, daß nicht nur der Datenschutz auf die Karte wirkt, sondern die Karte auch auf den Datenschutz. Dazu muß jedoch eine Perspektive gefunden werden, in der rechtliche, wirtschaftliche und soziale Phänomene gemeinsam betrachtbar bleiben, wir müssen zu einer allgemeineren Betrachtungsweise finden:

Die Karte erscheint dann als Symbol einer umfassenden gesellschaftlichen Entwicklung, die es keineswegs erstaunlich macht, daß sich ein eigener Zeitschriftentitel für sie gefunden hat, unter dem nun auch die wirtschaftswissenschaftliche Diskussion für die rechtswissenschaftliche und rechtspraktische Auseinandersetzung fruchtbar gemacht wird². Erstaunlicher ist vielmehr daß, soweit mir bekannt, noch keine umfassendere kulturwissenschaftliche Auseinandersetzung zu diesem Thema begonnen hat, denn wir müssen die "Karte" als ein Teilphänomen jener "technischen Großsysteme" wahrnehmen, die zu einem wesentlichen Kennzeichen nicht nur wirtschaftlicher sondern auch gesellschaftlicher Wirklichkeit geworden sind. Aus dieser Perspektive soll hier versucht werden, einige allgemeinere Bezüge zwischen Datenschutz und Karte anzudeuten. Die Karte sehen wir dabei vornehmlich in den ohnehin häufiger werdenden Verwendungsformen, bei denen der Kartennutzer unmittelbar mit einem technischen System in Verbindung tritt, also etwa bei technischen (Zugangs- oder Leistung-)systemen, so bei der Geldauszahlung, bei Point-of-Sale-Transaktionen, beim Ausdrucken von Kontoauszügen, bei Telefontautomaten, bei der Selbstaussstellung von Fahrkarten und Flugscheinen mit Kreditkarten, etc.

² Vgl hierzu von Usslar 1990 und von Usslar/von Morgen 1989

Technische Großsysteme

Wir haben die Karte als einen Teil technischer Großsysteme bezeichnet. Diese Systeme sind "(...) jene technischen Gebilde, die gesellschaftsweit, ja zwischengesellschaftlich ausgelegt sind und damit Voraussetzungen für das Funktionieren praktisch aller anderen "kleineren" technischen Systeme schaffen (...) "³. Zu diesen Infrastruktur- und Verkehrssystemen gehören die Informations- und Kommunikationsnetze. Im Unterschied zu herkömmlichen Verkehrssystemen wird mit ihnen nicht der Mensch selbst sondern seine informatischen Abbilder transportiert ("doubles informatiques" ⁴). Die Karte ist dabei das physische Verbindungsglied zwischen dem realen "Ich" und diesen jeweils verwendungsbezogenen Abbildern.

Funktionen der Karte

Diese Funktion der Karte ist zunächst Folge einer technischen oder eher einer wirtschaftlichen Denkgewohnheit: physische Identifikation unmittelbar an der Systemgrenze, Hineinsprechen, selbst Eintippen verlangen aufwendigere, stör anfällige Apparaturen für den Systemübergang - sie sind zudem noch wenig diskret. Sie belassen Aufwand und Risiken noch zu weitgehend im Bereich des Systemanbieters. Verlagert man die Kommunikation in die Karte, so verlagert man damit auch einen Teil des Risikos auf den Inhaber der Karte. Je nach Systemausgestaltung haben Systemanbieter zwar nicht gänzlich darauf verzichtet, ihrerseits Sicherungen bereitzustellen. Physische Identität mit der Nutzung der Karte zu verbinden und diese Verbindung zu sichern bleibt dennoch in erster Linie Aufgabe des Nutzers; er soll die Karte nicht verlieren; er muß die gegenwärtig nur mentale Verbindung zwischen sich und der Karte, die "Geheimnummer" wahren. Diese Verteilung kann man zunächst als Entlastung des Systemanbieters sehen; sie ist aber auch -und das wird uns noch beschäftigen- ein symbolisches Vertrauensangebot.

Mit der Karte wird also in erster Linie der Austausch zwischen Maschine und Mensch optimiert: die Geschwindigkeit des Austausches wird vom System bestimmt; die Integrität der Übermittlung ist weitgehend sichergestellt. Die Karte vermittelt zugleich dem Nutzer den Eindruck eigener Unabhängigkeit und der Be-

³ Joerges 1990, 37, vgl. auch Joerges 1988.

⁴ Vitalis 1988.

herrschaft der Abläufe: die Karte trägt die sozialen und psychologischen Konnotationen eines "Schlüssels" (wie Schlüssel auch zunehmend durch Karten ersetzt werden). Die Karte vermittelt "Verfügbarkeit", sie gibt ein Zugangsprivileg zu Waren- und Dienstleistungen, zu physischem Zugang, zu technischer Kommunikation. Sie ist auch "Mitgliedskarte" zu mehr oder weniger exklusiven Gruppen. All dies sind Elemente, die uns aus der angewandten Psychologie des Kartenmarketings vertraut sind. In den hier uns beschäftigenden Zusammenhängen entlastet die Karte darüberhinaus von unmittelbarem physischem Kontakt mit anderen Menschen. Gerade diese Eigenschaft wird indes nicht immer als Entlastung empfunden. Auch die anderen Vorteile vermitteln sich nicht in allen Alltagssituationen der Kartennutzung, etwa in der Schlange vor dem Geldausgabeautomaten an einem regnerischen Samstagvormittag.

Gefährdungen von Großsystemen

Große technische Systeme sind jedoch nicht durch jeweils individuell wahrgenommene Dysfunktionen gefährdet. Zum einen werden diese eben nur individuell in persönlichen Kosten-Nutzen-Rechnungen verarbeitet. Aggregieren sie sich, so stellen sie doch nur die konkrete technische oder organisatorische Ausgestaltung in Frage. Insgesamt zeigt sich in der Alltagsnutzung und in der "Schlüssel"-Konnotation eine fortgeschrittene Eingewöhnung in die Großtechnik technischer Informations- und Kommunikationsnetze. Technische Großsysteme sind jedoch, allein schon wegen ihrer Größe, zumindest mit zwei grundsätzlichen und existenzgefährdenden Problemen behaftet: mit dem Kontrollproblem und dem Vertrauensproblem.⁵ Uns beschäftigt hier das Vertrauensproblem. Die ökonomischen Größenvorteile von Kommunikationsnetzen werden zu Größennachteilen: Zwar gewinnen alle bisherigen Netzteilnehmer durch einen neuen Teilnehmer, sie haben aber auch alle die Risiken, die mit dem Neuzugang auftreten, zu tragen. Hier braucht nur auf die in dieser Zeitschrift mehrfach ausgewiesenen Zahlen der Kriminalstatistik verwiesen werden.

Vertrauen

Technische Großsysteme funktionieren trotz ihrer Größe und Komplexität, weil die Nutzer in ihr Funktionieren vertrauen. Dieses Vertrauen kann jedoch kein individuelles Vertrauen mehr sein. Ich kenne vielleicht noch den Ladeninhaber, bei dem ich mit der Kredit-

⁵ Joerges 1990, 37.

karte bezahle, ich kenne aber weder die Mitarbeiter der Bank, noch die der eingeschalteten Verrechnungsstelle, noch die der Einrichtung, die für das Netz sorgt. Ich vertraue in die beteiligten Organisationen und in die Organisation ihres Zusammenwirkens. Bei den hier angesprochenen Systemen der unmittelbaren "Kommunikation" mit der Maschine entfällt die Möglichkeit ganz, auf individuelle Vertrauenserfahrungen mit anderen zurückzugreifen. An die Stelle des individuellen durch die eigene Biographie gestützten Vertrauens muß Systemvertrauen treten.

"Vertrauen", so Luhmann provokativ in seinem grundlegenden Essay⁶, "beruht auf Täuschung." Er fährt dann mildernd fort: "Eigentlich ist nicht so viel Information gegeben, wie man braucht, um erfolgssicher handeln zu können." Vermittelt auch die Karte physische Beherrschbarkeit, so bleibt doch ein Informationsdefizit. Der Nutzer weiß weder, wie das hinter der Karte stehende Informationssystem aussieht; er kennt noch nicht einmal die Informationen, die sich auf dem Magnetstreifen befinden. Er braucht dies alles auch nicht zu wissen, denn er kann auf all die anderen vertrauen, die dieses System entworfen haben und es täglich in Gang halten. Sozial gelerntes Vertrauen in die Technik, in die Wissenschaft, auch in das Wirtschaftssystem tragen das Kartenkonzept und machen es funktionsfähig. Allerdings ist dies kein "reines" Vertrauen: "Die Hochbauten des Vertrauens müssen auf der Erde stehen."⁷ Hierzu dient nun allerdings nicht etwa ein kontinuierlich beobachtendes und überprüfendes Kontrollsystem. Der Nutzer mag sich das Bestehen solcher Kontrolle "auf der anderen Seite der Karte" zwar vorstellen, für sein *Vertrauen* reichen ihm aber Schwellenkontrollen⁸: so die Beobachtung, daß das System die Autorisierung der Karte überprüft, so die Protokollauszüge, die ihm in regelmäßigen Abständen zugesandt werden. Wir haben es also mit einem funktionierenden Vertrauenssystem zu tun. Wie das Vertrauen auf Seiten der Systemanbieter beschaffen ist, mag hier dahin gestellt sein. Man mag vermuten, daß es hier um ein eher kalkuliertes Vertrauen (das wegen seiner Kalkuliertheit schon kaum noch als Vertrauen bezeichnet werden kann, sofern man Organisa-

⁶ Luhmann 1973, 33.; vgl auch Luhmann 1988.

⁷ Luhmann 1973, 62.

⁸ "Kontrolle durch Schwellen unterscheiden sich in Stil, Technik und Elastizität wesentlich von der Kontrolle durch bestimmte Zwecke, Normen oder Werte. Sie kann mit einfacheren Mitteln höhere Komplexität tolerieren, setzt aber voraus, daß die Schwellen, also die vertrauskritischen Verhaltensweisen hinreichend klar definiert und bekannt sind." Luhmann 1973, 31.

tionen überhaupt Vertrauensfähigkeit zugestehen will und diesen Begriff nicht auf Individuen beschränken will) handelt, bei dem auftretende Schäden durch die Solidargemeinschaft (die auch den Nutzer einbezieht) ausgeglichen werden. Das System "rechnet" mit dem Mißbrauch und vergleicht kalkulierend die Höhe der Prämie mit den Kosten der nächsthöheren Sicherheitsstufe; wird eine Prämienchwelle überschritten, weil der Verlust eine Anteilsgröße am Umsatz überschritten hat, wird die nächste Sicherheitsstufe eingeführt, etwa ein Hologramm-Logo. Hinzu kommen statistische Schwellenwerte, die aus der Beobachtung des Nutzungsverhaltens gewonnen werden können. Da Vertrauen zu seiner Stabilität der Gegenseitigkeit bedarf, muß aber jedenfalls nach außen auch dem Systemnutzer Vertrauen der Systembetreiber signalisiert werden: Er erhält die Karte mit einfacher Post zugesandt⁹; er hat sie erhalten, ohne daß er vorsprechen mußte; er konnte ein Antragsformular aus der Zeitung ausschneiden; er brauchte darauf nur einige wenige Fragen beantworten. An dieser Stelle stockt natürlich der datenschutzferne Leser, sowie er gestockt haben wird, wenn er einen solchen Antrag ausgefüllt hat. Zumindest in Deutschland enthalten diese Formulare nämlich ausführlich formulierte Einwilligungserklärungen in Informationsweitergaben.

Diese Einwilligungserklärungen sind nicht ohne Widerstand eingeführt worden. Es ist zu vermuten, daß dieser Widerstand auch auf der Befürchtung beruhte, daß hier in einer latenten Vertrauensbeziehung (so kennzeichnen zumindest die Banken in der Regel ihren Bezug zu ihren Kunden) "etwas" ausgesprochen wurde, was diese Vertrauensbeziehung problematisiert und eben nicht mehr latent sein läßt. Das mag auch ein Grund sein, neben zweifellos noch vorhandenen technischen Schwierigkeiten, die unter Sicherheitsgesichtspunkten problematische Brücke zwischen Person und Karte nicht oder noch nicht durch biometrische Verfahren zu stabilisieren. - Aus dieser Sicht ließe sich im übrigen die Existenz einer spezialisierten Zeitschrift zum Kartenrecht auch als Zeichen einer "Vertrauenskrise" deuten, nämlich der Krise des Vertrauens, das Rechtssystem werde ohne Schwierigkeiten auch die neuen Phänomene des Kartengebrauches bewältigen können. Allerdings ist dies (gegenwärtig) noch eher eine Vertrauenskrise derjenigen, deren Aufgabe es ist, Systemvertrauen zu generieren. Für den Kartennutzer wird die Existenz einer solchen Zeitschrift, wenn er denn von ihr Kenntnis erhält, wieder vertrauensstabilisierend, weil sie ein Zeichen dafür ist, daß sich Träger von Systemvertrauen um das Problem kümmern und im wissenschaftlichen Diskurs mit gelegentlicher Weitergabe an das politische System bewältigen werden. Das

⁹ Tatsächliches Motiv können dabei durchaus Wirtschaftlichkeitserwägungen sein.

Verhältnis zwischen Rechtsvertrauen und Kartenvertrauen wird uns noch beschäftigen.

Die Rolle des Datenschutzes

Diese Problematisierung des Informationsaustausches ist Ergebnis der Datenschutzdiskussion, genauer der Interpretation des Datenschutzrechtes, insbesondere der Regeln zur Einwilligung.

Wir können die Datenschutzdiskussion als Reaktion auf eine Vertrauenskrise des technischen Großsystems "Information und Kommunikation" deuten und zwar insbesondere seiner Nutzung in Systemen der öffentlichen Verwaltung, die wiederum ihre eigene Vertrauenskrise zu bewältigen haben. Die Kartensysteme (des privaten Sektors) werden als solche nicht unmittelbar betroffen, sondern als Teil des technischen Großsystems. Dabei sind zwei Ebenen zu trennen: Datenschutz als gewissermaßen informationsethischer Satz von Verhaltensregeln und die "verrechtlichte" Datenschutzdiskussion unter den "Experten".

Diese Trennung ist deshalb bedeutsam, weil sich Datenschutz für den Nutzer dieser Systeme nicht primär als rechtlich normiertes System darstellt, wie etwa -zwar nicht tatbestandsgenau- Normen des Strafrechts. Beschäftigt sich nämlich der Nutzer eingehender mit dem Datenschutzrecht, so stößt er sehr bald auf eine Reihe von Eigenheiten: Wie wir an anderer Stelle ausführlicher versucht haben darzulegen¹⁰, läßt sich die Funktion des *Datenschutzrechtes*, und wir beschränken uns hier auf seine Ausprägung in Deutschland, als Legitimitätssicherung in informationstechnischer Systeme deuten. Ihre Nutzung wird an das Konsensprinzip geknüpft. Dieser Konsens wird entweder individuell generiert (durch ausdrückliche Einwilligung, durch Vertrag oder vertragsähnliche Beziehungen, die den Konsens zum Umgang mit Informationen implizieren) oder es wird auf kollektiv generierten Konsens verwiesen (Bezug auf eine spezifische Rechtsnorm, die den Umgang mit Informationen erlauben und die im parlamentarischen Prozeß geformt wurde oder doch zumindest auf diesen verweist). Zur Funktionsfähigkeit dieser Konsensverfahren werden Beobachtungsorganisationen institutionalisiert und Transparenznormen und Verfahren eingeführt (Mitteilungspflichten, Register, Auskunftsrechte). Die substantiellen Regeln knüpfen an die sehr generellen Prinzipien der Verhältnis-

¹⁰ Vgl. Burkert 1986.

mäßigkeit, Wahrhaftigkeit und Zweckdienlichkeit an, mit denen der Informationsumfang minimiert und die Informationsqualität gesichert werden soll. Diese Regeln, wie sie sich vielleicht deutlicher noch als im deutschen Datenschutzgesetz aus den internationalen Destillaten wie der Konvention des Europarates und den Richtlinien der OECD ablesen lassen, sind eher allgemeine Prinzipien sozialer Akzeptanz des Umgangs mit Informationen als ausziselierte rechtliche Regelungen¹¹. Dabei verlagert zumindest das deutsche Rechtssystem bei mangelndem Konsens, und das sind die eigentlichen Problemfälle des Datenschutzes, die "entscheidende Entscheidung" über die Zulässigkeit oder Unzulässigkeit einer Speicherung etwa oder einer Weitergabe in die Wertungssphäre des verantwortlichen Datenhalters, der speichernden Stelle. Dieser "Stelle" sind auch keine klaren Kriterien vorgegeben, sie muß vielmehr komplexe, in ihrem Ergebnis für den außenstehenden Betroffenen auch nicht klar vorhersehbare Abwägungsentscheidungen treffen.¹² Wohl können die Aufsichtsbehörden Handlungen aufdecken, die in ihrer Interpretation Verstöße sind und diese Auffassung dem Betroffenen mitteilen. Diese Behörden können auch durch Anordnungen in technische und organisatorische Abläufe im Extremfall eingreifen¹³. Letztlich jedoch muß der Betroffene selbst das Rechtssystem aktualisieren, um Unterlassung, Wiedergutmachung oder Strafe zu erreichen¹⁴.

Datenschutz ist in dieser Sicht eher ein Komplex erwartbaren Informationsverhaltens als ein unmittelbar rechtlich sanktioniertes Kontrollsystem. Wie die Diskussion um eine "Ethik der Datenverarbeiter" zeigt, ist dabei die technische Veränderung auch nicht ohne Probleme für eine Vertrauensstabilisierung durch ethische Regeln. Wegen der Ubiquität personenbezogener Datenverarbeitung muß

¹¹ Kirby 1980, 46; Vitalis 1988, 185 und Benyekhlef 1991, 140ff.

¹² In der neuen Fassung des deutschen Bundesdatenschutzgesetzes ist der Versuch unternommen worden, dies einzugrenzen, indem etwa bestimmte Typisierungen vorgenommen werden (so im § 28 (2) Ziff.1 b). Damit bleibt das Gesetz in der Leistung der Voraussehbarkeit jedoch immer noch hinter anderen Lösungen zurück, wie etwa den "normes simplifiées" nach dem französischen Datenschutzrecht. Solche Regeln bieten den Anwendern aus Beobachtung und Bewertung gewonnene Typisierungen rechtmäßigen Verhaltens an und machen solches Verhalten für die Betroffenen erwartbar.

¹³ § 38 (5) BDSG 1990.

¹⁴ Vgl. z.B: § 43 (4) BDSG 1990. Dies soll nicht als Kritik verstanden werden. Eine solche Kritik würde eine detaillierte Auseinandersetzung mit anderen äquifunktionalen Möglichkeiten voraussetzen (die möglicherweise aber zu Flexibilitätsverlusten führen). Erst dann könnte eine kritische Bewertung einsetzen (zur Methode: Luhmann 1973, 100 Fußnote 8).

aufgrund der so entstehenden Kontrollprobleme jedoch auf Verhaltenssteuerung durch Rat gebaut werden, wie es in den Berichten der Datenschutzbehörden auch immer wieder anklingt.¹⁵ Datenschutz aktualisiert also nicht unmittelbar das Rechtssystem zur Vertrauenssicherung in das technische Großsystem "Information und Kommunikation" sondern verweist auf die *Möglichkeit*, das Rechtssystem einzusetzen (im Gegensatz zu einem rein ethischen System, dessen Bezüge zum Recht nicht immer eindeutig sind). Die Funktion des Datenschutzes ist es, das generelle Vertrauen in das allgemeine Rechtssystem mit dem Vertrauen in das technische System "Information und Kommunikation" zu koppeln und letzteres von ersterem profitieren zu lassen. Datenschutz erzeugt (nicht allein, aber am deutlichsten) die Vorstellung, daß das technische System "Information und Kommunikation" sich nicht außerhalb dessen befindet, wofür man Leistungen des Rechtssystems erhoffen kann. Datenschutz wird zur vertrauensstützenden Maßnahme. Die geringe Anzahl der Fälle, in denen Datenschutz durch den Betroffenen rechtlich aktualisiert wird (durch Anzeige oder Klage etwa, aber auch schon in der Geltendmachung des Einsichtsrechtes) ist kein Indiz für das Versagen des Datenschutzes sondern gerade für seine Funktionsfähigkeit bei der Erzeugung und Stabilisierung von Vertrauen. Der andere Einwand, zunehmend weniger geäußert, der Datenschutz werde in seiner letzten (rechtlichen) Konsequenz so wenig mobilisiert, weil es eben sowenig Verstöße gebe, setzt voraus, daß der Betroffene zunächst aktiv geworden wäre, um sich zu vergewissern, daß keine Verstöße vorliegen. Der Rationalisierungsgewinn (im Sinne des ökonomischen Umgangs mit sozialen Ressourcen) liegt aber gerade darin, daß kein empirischer Befund über die Einhaltung erhoben werden muß.

Datenschutz ist somit in seiner Gesamtheit symbolisiertes Vertrauen der Informationsgesellschaft in ihre technischen Kommunikationsmittel durch eine Koppelung des Vertrauens in das jeweils genutzte technische System mit dem Vertrauen in das Rechtssystem.

Allerdings können fortgesetzte Meldungen über die Nichteinhaltung dieses Vertrauens gefährden. In diesem Sinne könnte man dann die Verlängerung der regelmäßigen Berichterstattung des Bundesdatenschutzbeauftragten von ein auf

¹⁵ Stellvertretend hierzu: Der Bundesbeauftragte für den Datenschutz. Erster Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs.2 Satz 2 des Bundesdatenschutzgesetzes (BDSG). Deutscher Bundestag. 8. Wahlperiode. Drucksache 8/2460 vom 10.1.1979, 6f.

zwei Jahre¹⁶ nicht zu sehr als Entlastung der zuständigen Ausschüsse sehen, sondern als eine "vertrauensschützende" Maßnahme.

Instabilität

Diese letzte, selbstverständlich als ironisch zu kennzeichnende Bemerkung verweist dennoch auf ein grundsätzliches Problem von Vertrauen. Vertrauensstützende Systeme sind wie individuelles Vertrauen instabil. Diese Instabilität kann verstärkt werden durch Enttäuschungen, durch nicht eingetretene Erwartungen, durch beständige Warnmeldungen von den eingerichteten Kontrollschwellen. Bei gekoppelten Vertrauenssystemen können Vertrauensstörungen auch über die Kopplung aufeinander einwirken. Der Datenschutz im öffentlichen Bereich, ist dadurch besonders problembeladen, weil hier nicht nur Vertrauensprobleme der Technik und des Rechts sondern auch des politischen Systems bewältigt werden müssen, die sich aus historischen und noch sehr aktuellen Enttäuschungserfahrungen speisen. Ähnliche Kopplungseffekte können sich im übrigen gerade auch für die Kartensysteme im wirtschaftlichen Bereich ergeben, denn ihre Funktionsfähigkeit beruht nicht nur auf einer Kopplung von Technik- und Rechtsvertrauen, sondern verbindet diese mit dem grundsätzlichen Vertrauen in die Funktion des Geldsystems, das es informationell abbildet.¹⁷

Bewältigung von Enttäuschungen

Soziale Vertrauenssysteme sind jedoch, ähnlich wie individuelle Vertrauenssysteme, in der Lage bis zu einem Schwellenwert Enttäuschungen zu verarbeiten; nicht jede Enttäuschung zerstört Vertrauen. Vielmehr ist es dem Einzelnen, aber auch Organisationen möglich, durch Verdrängung etwa oder durch Uminterpretation Vertrauen aufrecht zu erhalten. Diese Reaktion tritt vor allem dann auf, wenn der Aufwand der Umstellung auf Nichtvertrauen zu groß ist. Der Rat, Schecks und Scheckkarte getrennt aufzubewahren, ist zwar eine Regel der Sicherheit, eine Mißtrauensregel, die auf Enttäuschungen aufbaut, sie ist in der Praxis jedoch nicht umsetzbar, da im Nutzungsakt beide zusammengeführt werden müssen und Zusammenführung erst dann die zeitliche Flexibilität des Zahlungsmediums so einschränken, daß auf seine Nutzung auch

¹⁶ §26 (1) BDSG 1990.

¹⁷ Hierzu Luhmann 1973, 54f. Zum Zusammenhang von Wirtschaftssystem und Vertrauen: Barber 1983, 100ff.

verzichtet werden könnte. Eine weitere Möglichkeit ergibt sich dann, wenn "(...) der Ausfall des Vertrauensobjektes nur partielle und isolierbare Schäden stiften kann und das Vertrauensobjekt durch Substitution funktionaler Äquivalente ersetzbar ist."¹⁸ In der Diskussion um die soziale Bewertung technischer Großsysteme wird daher immer darauf hingewiesen, daß diese Systeme so ausgestaltet sein sollen, daß keine *ausschließliche* Abhängigkeit entsteht.¹⁹ Für den spezielleren Zusammenhang, die Kartensysteme als Zugangsmittel zu technischer Information und Kommunikation, folgt daraus die Ablehnung "der" Karte, die Zugang zu allen Systemen verschafft, mit ihrem Verlust aber zu einem Zugangsverlust zu technischer Information und Kommunikation überhaupt führt.

Eine Gefährdung soll hier jedoch ausführlicher aufgegriffen werden, um das Versprechen einzulösen und das Vertrauen des Lesers nicht zu enttäuschen, auch das "Gegenseitigkeitsverhältnis" von Karte und Datenschutz aufzugreifen: Datenschutz wurde als vertrauensbildende oder zumindest stabilisierende Kopplung von Vertrauen in technische Systeme und Vertrauen in das Rechtssystem qualifiziert. Diese Kopplung führt jedoch nicht nur zu einer gegenseitigen Stärkung sondern, wie bei dem kurzen Hinweis auf den Datenschutz im öffentlichen Sektor schon angedeutet, auch zur Erhöhung des Gefährdungspotentials. Versucht man durch den Verweis auf das Rechtssystem das Vertrauen in das technische System zu stärken, so kann sinkendes Vertrauen in die Leistungsfähigkeit des Rechtssystems auch das Vertrauen in das technische System gefährden. Datenschutz hat, wie ausgeführt, durch primär an ethischen Informationsverhaltensregeln ausgerichteten Prinzipien (mit sekundärem Verweis auf das Rechtssystem) sich zugleich auch einer zu starken Bindung an den "Stand der Technik" weitgehend zu enthalten versucht. Zwar hat sich Datenschutz technikunabhängig darzustellen versucht. Durch seinen, wenn auch nur sekundären Verweis auf Recht stellt er aber zugleich auch die Frage, wie denn Recht die technische Weiterentwicklung bewältigen kann. In dem Zeitraum, in dem die rechtliche Bewältigung technischer Kommunikationssysteme ein beinahe eigenständiges internationales Rechtsgebiet hervorgebracht hat, sind zugleich auch die Zweifel an der Fähigkeit des Rechtes gewachsen, technische Gefährdungspotentiale überhaupt noch bewältigen zu können.²⁰ Dies trifft nicht nur das "Informa-

¹⁸ Luhmann 1973, 28.

¹⁹ Vgl. Roßnagel u.a. 1989.

²⁰ Hierzu Simitis 1987, Pouillet 1987 und Burkert/Rankin 1989.

tionsrecht“, wie die Diskussion um Technikfolgenbewältigung und die Rolle des Rechts dabei belegen. Eine Form der Anstrengung, die das Rechtssystem dabei unternimmt, und nicht nur im Informationsrecht, sind Anpassungsversuche durch bereichsspezifische Regelungen und die grundsätzliche Bereitschaft, als lernendes System zu operieren. Die Probleme, die daraus für das Technikrecht und insbesondere für seine Vorausssehbarkeit entstehen, sollen hier nicht weiter verfolgt werden. Einige der beim Datenschutzrecht beobachteten Kennzeichen sind vielleicht bereits schon Ausdruck derartigen Technikrechts.

Uns interessiert hier ein anderer Aspekt: Die Kopplung, die durch den Datenschutz vorgenommen wurde, ermöglicht es seinerseits dem Rechtssystem bei der Suche nach vertrauensschützenden Maßnahmen im technischen System selbst fündig zu werden. Das Vertrauen in das Rechtssystem läßt sich auch durch das Vertrauen in Technik stärken. Auf Rechtsvertrauen verweisender Datenschutz läßt sich durch auf Technik vertrauenden Datenschutz ergänzen.

Um Mißverständnissen vorzubeugen: Hier geht es nicht um Datensicherheit, wie sie etwa im § 9 des Bundesdatenschutzgesetzes 1990 angesprochen ist. Diese Art von Technik und sie umgebende organisatorische Maßnahmen haben, ohne ihre komplementäre Bedeutung hier mindern zu wollen, insoweit nur sekundären Charakter als sie immer die Rechtmäßigkeit des Umganges mit Informationen voraussetzen. Technisch sicher aufbewahrte unzulässig erhobene Daten sind für die Generierung von Vertrauen kontraproduktiv.²¹ Hier geht es vielmehr um die technische Vergegenständlichung von Grundprinzipien des Datenschutzes. Es geht um die technische Abbildung (und Kontrolle) von Konsensverfahren, um die Minimierung von identifizierenden Datenbeständen, um die “Verdrahtung” von Zweckbindung.

Bei der Suche nach solchen technischen “vertrauensbildenden” Maßnahmen bietet nun gerade die Kartentechnologie ganz neue Perspektiven: Im Kontext des OSIS (Openshops for Information Services)-Projektes der GMD (Gesellschaft für Mathematik und Datenverarbeitung)²² und in den späteren TeleTrusT-Aktivitäten²³, in den

²¹ Gambetta 1988,159 ff. weist darauf hin, daß Vertrauenssysteme auch gesellschaftlich unerwünscht sein können.

²² Vgl. hierzu Lenk/Goebel/Schmalz 1986, Burkert 1987.

²³ Hierzu: u.a. Struif/Herda/Goebel 1988.

Arbeiten von Pfitzmann und seinen Kolleginnen und Kollegen²⁴, in den von Chaum²⁵ vorgeschlagenen Verfahren werden Ansätze deutlich, die die eingangs geschilderten positiven Konnotationen von Kartenkonzepten für die Vertrauensbildung nutzbar machen. Derartige Konzepte verbinden kryptographische Methoden (insbesondere Systeme, die mit "öffentlichen" Schlüsseln operieren) mit einer Technologie, die Datenverarbeitungs- und Speicherkapazität noch stärker auf die Karte verlagert. Derartige Verfahren ermöglichen es zum Beispiel, Anonymität mit Zurechenbarkeit zu verbinden, in Zahlungsvorgängen eine Äquifunktionalität mit Bargeld herzustellen (bei gleichzeitig höherer Sicherheit) und technische Lösungen für den Grundkonflikt zwischen Sicherheit und Offenheit von technischen Kommunikationssystemen anzubieten. In solchen Systemen kann bereits die Erzeugung personenbezogener Daten erheblich reduziert und Konsens jeweils aktuell und für den Nutzer wahrnehmbar realisiert werden. Durch die Aufteilung von Funktionen auf verschiedene physische Karten mit unterschiedlichen "Pseudonymen" können Datenbestände nach Zweckbereichen entflochten und das Risiko von Zusammenführungen gemindert werden. Diese Kartensysteme haben zugleich Vorteile bei der Handhabbarkeit und Verfügbarkeit gegenüber anderen ähnlichen Lösungen etwa komplexen "verdrahtete" dedizierte Hardwaresysteme.

Diese Lösungsvorschläge sollen hier nicht im einzelnen diskutiert und bewertet werden. Es muß jedoch auch angemerkt werden, daß dieser Versuch, Datenschutzprinzipien durch technische Äquivalente umzusetzen, nicht unproblematisch ist. Mit Hilfe dieser Systeme kann das Entstehen von "Datenspuren" in viel stärkerem Maße reduziert werden, als dies gegenwärtige Regeln verlangen. Da aber diese Informationen, ob gewünscht oder nicht, einen Marktwert haben, verändern sich die Rentabilitätserwartungen bei Investitionen in Kommunikationssysteme. Sind dies möglicherweise Hindernisse für die Akzeptanz bei denen, die derartige Systeme bereitstellen, so hängt die Vertrauensleistung für den Nutzer solcher technischen Lösungen vom Vertrauen in das technische System ab. Dieses Vertrauen wiederum verlangt, daß zumindest Schwellenwerte für Vertrauensverlust bereitgestellt werden, die ohne großen Aufwand zu überprüfen sind²⁶. Das wiederum setzt unter anderem ein auch "in der Laiensphäre" nachvollziehbares "Verstehen" voraus, das zum

²⁴ Pfitzmann 1990; Pfitzmann/Waidner/Pfitzmann 1990; Pfitzmann/Waidner 1988.

²⁵ Chaum 1989 und 1987.

²⁶ Luhmann 1973, 31.

gegenwärtigen Zeitpunkt noch nicht vorhanden ist. Dieses Verstehen zu fördern wäre eine Aufgabe der Spezialisten der Vertrauensbildung, der Datenschutzeinrichtungen.

Der Kreis dieser Betrachtung schließt sich: Datenschutz, die Kopplung von Vertrauensmechanismen des Rechts und der Technik, notwendig durch die Größe und die Intransparenz der technischen Großsysteme wird in seiner Wirksamkeit zurückgeworfen auf das Vertrauen in technische Systemleistungen. /--

Literaturangaben:

Barber 1983

Barber, B.: The Logic and Limits of Trust. Rutgers, The State University of New Jersey 1983.

Benyekhlef 1991

Benyekhlef, K.: La protection de la vie privée dans le cadre des échanges internationaux d'informations. Thèse de doctorat. Montréal 1991.

Bing 1978

Bing, J.: Transborder Data Flows: Some Legal Issues and Possible Effects on Business Practices. In: Transnational data regulation (Online Conferences Ltd.). London 1978.

Burkert 1986

Burkert, H.: Datenschutz und Informations- und Kommunikationstechnik . Eine Problemskizze. Düsseldorf 1986.

Burkert 1987

Burkert, H.: Une experience positive de solution juridico-technique: Le projet "OSIS (Open Shop for Information Services)". In: Vivant, M. (Hrsg.), Les transactions internationales assistées par ordinateur. Bibliothèque de droit de l'entreprise. Paris 1987, 139-152.

Burkert/Rankin 1989

Burkert, H.; Rankin, M.: The Future of the OECD Privacy Protection Guidelines: Building Trust in Electronic Data Networks", (ICCP), Paris, OECD, 26 June 1989.

Chaum 1987

Chaum, D.: Sicherheit ohne Identifizierung. Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen. In: Datenschutz und Datensicherung 1988, 26-41.

Chaum 1989

Chaum, D.: Privacy Protected Payments - Unconditional Payer and/or Payee Untraceability. In: SMART CARD 2000 : The Future of IC Cards. Proceedings of the IFIP WG 11.6 International Conference. Laxenburg (Austria), 19 - 20 October 1987. Amsterdam 1989, 69-93.

Gambetta 1988

Gambetta, D.: Mafia: The Price of Distrust. In: Gambetta, D. (Ed.) : Trust. Making and Breaking Cooperative Relations. New York 1988, 158-175.

Joerges 1988

Joerges, B.: Large Technical Systems: Concepts and Issues. in: Mayntz, R; Hughes, Th.P. (Eds.) : The Development of Large Technical Systems. Frankfurt/Main 1988, 6 - 36.

Joerges 1990

Joerges, B.: Große technische Systeme. Aspekte eines Forschungsprogrammes. in: WZB-Mitteilungen 1990, No. 48, 36-48.

Kirby 1980

Kirby, Justice M.D. Transborder Data Flows and the "Basic Rules" of Data Privacy . In: Stanford Journal of International Law, Vol.XVI (Summer 1980), 27-66.

Lenk/Goebel/Schmalz 1986

Lenk, K; Goebel, J.W.; Schmalz, R.: Das elektronische Informationsgeschäft. Rechts- und Organisationsprobleme im Zusammenhang mit dem Projekt OSIS (Open Shop for Information Services). Frankfurt/Main 1986.

Luhmann 1973

Luhmann, N.: Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. 2. erweiterte Auflage. Stuttgart 1973.

Luhmann 1988

Luhmann, N.: Familiarity, Confidence, Trust: Problems and Alternatives. In: Gambetta, D. (Ed.) : Trust. Making and Breaking Cooperative Relations. New York 1988, 94-108.

Pfitzmann 1990

Pfitzmann, A.: Dienstintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. Heidelberg 1990.

Pfitzmann/Pfitzmann/Waidner 1988

Pfitzmann, A.; Pfitzmann, B.; Waidner, M.: Datenschutz garantierende offene Kommunikationsnetze. In: Informatik-Spektrum 11 (1988), 118-142.

Pfitzmann/Waidner/Pfitzmann 1990

Pfitzmann, B.; Waidner, M.; Pfitzmann, A.: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. In: Datenschutz und Datensicherheit 1990, 243-253, 305-315.

Poulet 1987

Poulet, Y.: Les concepts fondamentaux de la protection des données et les nouvelles technologies de l'information", Texte présenté à la Conférence sur les problèmes législatifs de la protection des données, Athènes, Conseil de l'Europe, Octobre 1987.

Roßnagel u.a. 1989

Roßnagel, A.; Wedde, P.; Hammer, V.; Pordesch, U.: Die Verletzlichkeit der "Informationsgesellschaft". Opladen 1989.

Simitis 1987

Simitis, S.: Privacy in an Information Society. In: University of Pennsylvania Law Review Vol 135 (1985), 707-746

Vitalis 1988

Vitalis, A.: Informatique, pouvoir et liberté. 2e édit. Paris 1988.

von Usslar 1990

von Usslar, L.: Die Kreditkarte - Vehikel der europäischen Währungsunion. In: à la Card Eurojournal 1990, 2-3.

von Usslar/ von Morgen 1989

von Usslar, L.; R.D. von Morgen: Aktuelle Rechtsfragen dewr Kreditkarten-Praxis. Hamburg 1989.

Fußnoten