Securitas ex Machina.

Von der Bedeutung technischer Kontroll- und Überwachungssysteme für Gesellschaft und Pädagogik

Inauguraldissertation
zur
Erlangung des Doktorgrades
der Erziehungswissenschaftlichen Fakultät
der Universität zu Köln

vorgelegt von

Christine Ketzer

aus

Krefeld

September 2005

1. Gutachter: Prof. Dr. Wolf-Dietrich Bukow
(Universität zu Köln)

2. Gutachter: Prof. Dr. Kersten Reich
(Universität zu Köln)

Tag der mündlichen Prüfung: 31.05.2006

Securitas ex Machina.
Von der Bedeutung technischer Kontroll- und Überwachungssysteme
für Gesellschaft und Pädagogik

Einleitung

Technische Kontroll- und Überwachungssysteme werden in den letzten Jahren immer mehr Teil unseres Alltags. Besonders in Großstädten begegnen sie uns täglich in verschiedensten Formen und zu unterschiedlichsten Zwecken:

Wir steigen in eine Straßenbahn und werden durch Videoüberwachungssysteme erfasst. Wir steigen aus, gehen in eine Einkaufspassage oder Shopping-Mall und werden dort von einer nächsten Videokamera aufgenommen. Wir leihen uns einen Film in einer Videothek aus, und zur Identifizierung wird unser Fingerabdruck mit einer Datenbank abgeglichen. Beim Einkauf in einem Kaufhaus nutzen wir das Payback-System, um in den Genuss von Rabatten zu kommen und lassen dadurch unsere Einkaufsgewohnheiten elektronisch erfassen und sie mit unseren persönlichen Daten koppeln. Zur Vermeidung von Fehlmedikationen, und um an bestimmten Service-Leistungen partizipieren zu können, werden in unserer Barmer-Service-Apotheke[1] all unsere Einkäufe und die uns verschriebenen Medikamente zentral gespeichert. Aus Sorge um unsere Kinder, nehmen wir die Dienstleistung einer Firma in Anspruch, die das Kind über sein Handy jederzeit orten und uns seinen Standort über Internet auf einem Lageplan darstellen kann.

An diesen Beispielen wird deutlich, wie stark technische Kontroll- und Überwachungssysteme bereits unseren Alltag durchdringen, ohne jedoch von den Betroffenen weiter hinterfragt oder überhaupt als Kontrolle und Überwachung wahrgenommen zu werden. Diese Entwicklung vollzieht sich in nahezu allen (westlichen) Industrienationen und ist in anderen Ländern, wie beispielsweise Großbritannien, bereits erheblich weiter fortgeschritten als in Deutschland.

Neben der Videoüberwachung, die bisher im Fokus wissenschaftlicher Betrachtungen stand, sind auch andere technische Systeme verbreitet, die manches Mal erst auf den zweiten Blick ihr Kontroll- und Überwachungspotenzial offenbaren. Gerade Systeme wie die Payback-Karte oder die Kindersicherung über Handy und GPS verdeutlichen, dass Kontrolle und Überwachung immer mehr den Menschen als einzelnes Subjekt ansprechen und von dem jeweiligen Individuum *selbst* genutzt und gewollt werden.

Aber bereits das bloße Vorhandensein technischer Kontroll- und Überwachungssysteme greift in unser Leben ein und verändert es. Auf die Wirkmächtigkeit technischer Strukturen wies insbesondere der Medientheoretiker Marshall McLu-

[1] Die Barmer-Service-Apotheke ist ein Angebot der Barmer Ersatzkasse, das seit Anfang 2004 existiert. Barmer-Kunden wird das Angebot unterbreitet, sämtliche ihrer verschriebenen Medikamente und getätigten Einkäufe zentral in der Apotheke mittels EDV speichern zu lassen. Ziel soll es dabei sein, Fehlmedikationen zu vermeiden. Der Kunde kann im Gegenzug Vergünstigungen und Serviceleistungen in Anspruch nehmen.

han mit seinem viel zitierten Ausspruch „The medium is the message!“[2] hin, und technische Kontrollsysteme, die sich Medien- und Informationstechniken wie Computer, Video und Handy zunutze machen, sind letztlich ebenso unser Denken, unsere Wahrnehmung und unser Handeln beeinflussende Medien wie Fernsehen oder Internet.

Die zunehmende Videoüberwachung beispielsweise soll uns signalisieren, dass wir uns konform verhalten sollen, da wir sonst mit Repressalien rechnen müssen. Mit bereits fest in die Alltagstrukturen implementierter Technik lassen sich gesetzte Normen jedoch nicht mehr diskutieren, und sämtlichen heutigen Kontrollsystemen ging keine in der breiten Öffentlichkeit geführte Diskussion über deren Sinn, Zweck und die gewünschte gesellschaftliche Funktion voraus. Der allgegenwärtige Einsatz solcher Systeme bedeutet aber letztlich, dass die Technik Aufgaben übernimmt, die vorher pädagogischen Zusammenhängen zugeordnet wurden: Statt einer (sozial-) pädagogischen Intervention im gesellschaftlichen Zusammenleben kommt es zu einer Selektion mittels technischer Apparate, die Menschen ein- oder ausschließen.

Die heutige Pädagogik ist unter dem Einfluss der Moderne entstanden, die sich der Emanzipation des Individuums und seiner Autonomie verpflichtet fühlt. Allerdings hat sich die Disziplin bisher kaum mit dem Spannungsfeld Technik – Gesellschaft – Individuum auseinandergesetzt, welches die heutige Lebenswelt prägt. Bislang hat sich die Pädagogik mit den Neuen Medien nur im Kontext von Kommunikation und Information befasst. Unbemerkt blieb, dass die Techniken an anderen Stellen bereits wesentlich in das Erziehungsgeschehen eingreifen, indem sie nämlich erzieherisches Handeln durch Konformisierung, soziales Zusammenleben durch Normalisierung und das Recht auf Privatheit durch öffentliche Kontrolle ersetzen.

Der spezifische Beitrag dieser Arbeit soll sein, das Thema der technischen Kontrolle und Überwachung in die pädagogische Diskussion einzubringen und dabei auch die Bedeutung der Pädagogik für eine Gesellschaft zu reflektieren, die sich zwar demokratischen Grundwerten verpflichtet fühlt, in der aber zugleich das Schlagwort Sicherheit neue normative Kraft gewinnt, die derzeit oft mehr zu gelten scheint als die Autonomie des Einzelnen.[3]

Parallel zur Etablierung der beschriebenen Systeme wurden in den vergangenen Jahren beispielsweise Bürgerrechte zunehmend eingeschränkt - der Staat dringt in das *Private* seiner Bürger ein. So sind die Videoüberwachung von öffentlichen

---

[2] vgl. McLuhan 1968

[3] Dabei kann diese Arbeit, aufgrund der bisher fehlenden Bearbeitung des Themas, eher ein Problemaufriss sein, als dass an dieser Stelle schon konkrete Lösungsvorschläge gegeben werden könnten.

Plätzen und Veranstaltungen, das Verhängen von Aufenthaltsverboten, das Instrument der Schleierfahndung und der Große Lauschangriff[4] eingeführt worden. Derzeit steht die Verwendung biometrischer Daten in Personalausweisen zur Diskussion. Nach dem 11. September 2001 wurde es leichter, Gesetze zu beschließen, bei denen es unter anderen Umständen vermutlich zu Protesten gekommen wäre. Im Einzelnen kam es nach dem 11. September zu über hundert Gesetzesänderungen, beispielsweise einer Stärkung der Kompetenzen des Bundesamts für Verfassungsschutz, das nun die Befugnis hat, unter bestimmten Voraussetzungen bei Anbietern von Telekommunikationsdiensten und Telediensten, bei Kreditinstituten, Finanzdienstleistungsinstituten und bei Luftfahrtunternehmen[5] Auskünfte einzuholen. 2005 wurde das Bankgeheimnis de facto aufgehoben - der Fiskus hat Zugriff auf die Stammdaten des Kontoinhabers, seinen Namen, die Anschrift, Geburtsdatum und das Datum der Kontoeröffnung. Ferner erhielt das Bundeskriminalamt weit reichende Ermittlungskompetenzen im Bereich der Datennetzkriminalität. Im so genannten Sicherheitspaket II ist des Weiteren eine Auskunftspflicht der Sozialversicherungsträger gegenüber Sicherheitsbehörden zum Zwecke der Rasterfahndung vorgesehen.[6]

Ziel der vorliegenden Arbeit ist es, das Phänomen Technische Kontrolle und Überwachung theoretisch zu erfassen, seine Ausprägungen im Alltag zu erforschen und Konsequenzen für die Pädagogik zu erarbeiten. Da bislang eine Auseinandersetzung der Pädagogik mit technischen Kontroll- und Überwachungssystemen fehlt, bewegt sich die Arbeit auf zwei Ebenen:

Im ersten Teil werden die vorhandenen gesellschaftstheoretischen Modelle, die sich mit der wachsenden Verbreitung technischer Kontroll- und Überwachungssysteme auseinandersetzen, dargestellt. Weiterhin will die Arbeit im zweiten, dem empirischen Teil, zeigen, wie weit diese Techniken bereits in den Alltag des Bürgers vorgedrungen sind. Dabei wird danach gefragt, welche Aufgaben diese Systeme in der Praxis übernehmen und welche Konsequenzen daraus für eine Pädagogik erwachsen, welche sich vorrangig für die Erziehung und die Vermittlung demokratischer Werte verantwortlich sieht.

Das Bild vom *Big Brother*, der alles überwacht und gegen den man sich nicht wehren kann, scheint seit den Protesten der 80er Jahre gegen die damalige Volkszählung und einen Staat, der Informationen über die Lebensumstände seiner Bürger sammeln will, überholt zu sein. Vielmehr hat sich das Phänomen Überwa-

[4] Dieser ist in einem Urteil des Bundesverfassungsgerichts vom März 2004 allerdings als verfassungswidrig erklärt worden, vgl. Bundesverfassungsgericht 2004

[5] Bundesministerium des Inneren 2002

[6] vgl. dazu auch Ketzer 2003, S. 145ff

chung und Kontrolle dezentralisiert. Inzwischen wissen nicht nur staatliche Stellen über den einzelnen Bürger Bescheid, sondern das Individuum selbst macht in seinem Alltag von technischen Kontroll- und Überwachungssystemen Gebrauch, ohne dies jedoch mit Big Brother-Assoziationen zu belegen. Da das beobachtete Phänomen in anderen Ländern bereits stärker vertreten ist und auch theoretisch besser aufgearbeitet wurde, lohnt es sich, den Blick über die bundesdeutschen Grenzen hinaus zu erweitern und Forschungsergebnisse, insbesondere aus dem angloamerikanischen Sprachraum, für eine Beurteilung der Situation in Deutschland nutzbar zu machen.

Zu Beginn der Arbeit wird das theoretische Vorverständnis in Kapitel 1 dargestellt. Lyotard hat hier mit seinem Modell der postmodernen Gesellschaft und dem Hinweis auf die *Informatisierung* der Gesellschaft und der unklaren, aber zentralen Rolle von Wissen bereits Ende der 1970er Jahre die Grundgedanken für die in Kapitel 2 folgenden theoretischen Betrachtungen gelegt.[7] Aus der anschließenden Darstellung des Forschungsstandes ergeben sich die forschungsleitenden Fragestellungen der Arbeit.

In Kapitel 2 werden derzeit diskutierte Erklärungsansätze und Modelle vorgestellt, die eine theoretische Einordnung des Phänomens Technische Kontrolle und Überwachung ermöglichen. Als Hauptbezugspunkte werden hier Ulrich Becks Theorie der Risikogesellschaft und Michel Foucaults Ausarbeitungen zur Gouvernementalität[8] vorgestellt, die in den folgenden Konzepten der Kontroll- und Sicherheitsgesellschaft und der Surveillance bzw. Maximum Surveillance Society vielfach aufgegriffen werden.

Ulrich Beck setzt sich innerhalb seiner *Risikogesellschaft* mit dem Präfix „post" auseinander und versucht, ihm auf die Spur zu kommen. Dabei entwickelt er die Leitidee der reflexiven Modernisierung[9], in der die Logik der Risikoproduktion und -verteilung eine bedeutende Rolle spielt. Becks *Risikogesellschaft* wird in zahlreichen theoretischen Ansätzen aufgegriffen und in Hinblick auf einen verän-

---

[7] Dieses Modell möchte ich nicht starr anwenden, sondern als Basis für weitere Überlegungen vorstellen. Es existieren auch alternative Begriffe und Weiterentwicklungen des Postmoderne-Begriffs. Beck spricht z.B. von einer Risikogesellschaft und einer reflexiven Moderne, er bezieht sich im Vorwort zur „Risikogesellschaft" aber ausdrücklich auf den Begriff der Postmoderne, wie andere Autoren auch. Es erscheint daher sinnvoll, den Lyotardschen Postmoderne-Begriff an dieser Stelle als Grundlage der theoretischen Betrachtungen vorzustellen.

[8] Dieser Neologismus Foucaults setzt sich aus den französischen Begriffen „gouverner" (regieren) und „mentalité" (Denkweise) zusammensetzt und stellt eine fragmentarisch gebliebene Weiterentwicklung der Machtanalyse Foucaults dar. Im Kapitel 2.2 werde ich ausführlich auf den Begriff der Gouvernementalität eingehen.

[9] „Modernisierung im Erfahrungshorizont der *Vor*moderne wird verdrängt durch die Problemlagen von Modernisierung *im Selbstbezug.* Wurden im 19. Jahrhundert ständische Privilegien und religiöse Weltbilder, so werden heute das Wissenschafts- und Technikverständnis der klassischen Industriegesellschaft entzaubert [...]", Beck 2003, S. 14

derten Kontroll- und Überwachungsbegriff weitergeführt und interpretiert. Er steht daher am Anfang der theoretischen Einordnung.

Ebenso lässt sich die Machtanalyse Michel Foucaults und sein Konzept der Gouvernementalität immer wieder in den Ansätzen finden. Hier soll der Frage nach der Nutzung der Technik durch das Individuum selbst nachgegangen werden. Beck und Foucault dienen somit als Hauptbezugspunkte der theoretischen Fassung des Phänomens.

Im Anschluss daran werden die Entwürfe der Kontroll- und der Sicherheitsgesellschaft vorgestellt, die sich stark aufeinander beziehen und ähnliche Einschätzungen bieten. Als dominierende Ansätze im angloamerikanischen Sprachraum werden danach die Perspektiven der Surveillance und Maximum Surveillance Society eingeführt.

Die vorgestellten Ansätze werden im Hinblick auf die Fragen, warum sich technische Kontroll- und Überwachungssysteme immer stärker verbreiten und warum immer stärker auch das Individuum selbst die Techniken nutzt, ausgewertet.

Nach dieser theoretischen Annäherung an das Thema werden in dem mit Kapitel 3 beginnenden empirischen Teil der Arbeit die Aspekte technischer Kontrolle und Überwachung untersucht. Wichtig ist zu prüfen, welche Techniken sich bereits im Alltag etabliert haben und welche Aufgaben diese übernehmen. Systeme, die derzeit verstärkt zum Einsatz kommen, werden exemplarisch vorgestellt. Wie schon im theoretischen Teil, wird auch hier ein Blick in jene Länder vorgenommen, in denen diese Systeme schon länger zum Einsatz kommen als in der Bundesrepublik Deutschland.

Im Rahmen dreier explorativ angelegter qualitativer Fallstudien wird in Kapitel 4 untersucht, wie sich technische Kontroll- und Überwachungssysteme vor Ort darstellen. Wo es sinnvoll erschien, wurden die qualitativen Ergebnisse durch quantitative Daten ergänzt. Als Fallstudien wurden exemplarisch ausgewählt: die Videoüberwachung im öffentlichen Nahverkehr, Datensammlungen mit Hilfe des Payback-Systems und Ortungssysteme für Kinder.

Durch diese Auswahl werden unterschiedliche gesellschaftliche Bereiche – das öffentliche Leben, der Konsumalltag, und der private Familienalltag - mit exemplarisch ausgewählten Beispielen der technischen Kontrolle und Überwachung untersucht. Die Untersuchungsfelder sind also so gewählt, dass die große Bandbreite des heutigen Einsatzes technischer Kontroll- und Überwachungssysteme deutlich wird.

Insgesamt war es ein Anliegen, ein möglichst umfassendes Bild des jeweiligen Forschungsfeldes aus unterschiedlichen Blickwinkeln darzustellen. Dies wurde

durch einen Methodenmix aus Ethnographie und unterschiedlichen Interviewtechniken realisiert. In diesem Rahmen wurden auch Sekundäranalysen vorhandener empirischer Forschung durchgeführt. Bei den Interviews wurde offenen Fragen der Vorzug gegeben, um den Einzelnen größtmöglichen Raum zur Meinungsäußerung zu bieten. Ziel der Untersuchung war herauszufinden, wie sich die Techniken für die jeweils Beteiligten darstellen.

Die Fallstudien werden anschließend vor dem Hintergrund der forschungsleitenden Fragestellungen ausgewertet und es wird geprüft, in wie weit es möglich ist, das vielschichtige Phänomen Technische Kontrolle und Überwachung mit den im Theorieteil erarbeiteten Einsichten zu fassen. Vor dem Hintergrund der Forschungsergebnisse werden im Resümee Konsequenzen für die Erziehungswissenschaft gezogen, die sich als Disziplin die Frage stellen muss, wie sie sich zu den veränderten gesellschaftlichen Bedingungen verhalten soll, wenn sie sich zugleich verpflichtet fühlt, zu zivilgesellschaftlicher Partizipation und Beteiligung an demokratischen Prozessen zu ermuntern.

Teil I: Theoretische Einordnung des Phänomens Technische Kontrolle und Überwachung

1 Theoretisches Vorverständnis und Fragestellung

Deutungen in der Wissenschaft Prozesse sind nie voraussetzungslos. Das eigene Vorverständnis beeinflusst die Untersuchung und Interpretation des Gegenstandes. Wichtig ist es deshalb, dieses Vorverständnis, das durch Lektüre, Beobachtungen, und eigene Schlussfolgerungen entstanden ist, zu Beginn offen zu legen, am Forschungsgegenstand schrittweise weiter zu entwickeln und so den Einfluss des Vorverständnisses für andere nachvollziehbar zu machen.[10]

In Kapitel 1.1 wird daher das dieser Arbeit zugrunde liegende gesellschaftliche Konzept - die postmoderne Gesellschaft - vorgestellt und anschließend, in Kapitel 1.2, das Verständnis des Kontroll- und Überwachungsbegriffs dargestellt. Kapitel 1.3 gibt eine Erläuterung technischer Kontroll- und Überwachungssysteme und skizziert die derzeitigen Möglichkeiten der Systeme. Im Anschluss wird in Kapitel 1.4 ein Überblick gegeben in welcher Art und Weise das Thema in den Disziplinen Soziologie, Pädagogik und Kriminologie derzeit diskutiert wird. Aus dieser Darstellung ergibt sich die Formulierung der Forschungsfragen.

1.1 Die postmoderne Gesellschaft

Der Begriff der postmodernen Gesellschaft bezeichnet eine Gesellschaft, die sich in deutlich von der Epoche der Moderne unterscheidet. Betrachtet man die Moderne als Zeitraum, der bei der Französischen Revolution einsetzt und bis in die letzten Jahrzehnte des 20. Jahrhunderts reicht, so war diese Epoche von einem Glauben an den Fortschritt und die Vernunft geprägt. Die Demokratie verbreitete sich, der Glaube an die Freiheit war ausgeprägt und die Emanzipation des Individuums wurde propagiert. Für einige Autoren[11] läutet aber bereits Friedrich Nietzsche[12] im 19. Jahrhundert das Ende der Moderne ein, indem er den Ausspruch „Gott ist tot“ prägte. Diese Aussage kündet bereits von der Tatsache, dass traditionelle Denkansätze in Frage gestellt werden und sich zunehmend eine Pluralität und Vielfalt des Denkens etabliert. Ein Aspekt, der in der Diskussion um die Postmoderne bedeutend ist. Die Postmoderne, so meint Honecker[13], stellt keinen Entwurf dar, nach dem die Wirklichkeit zu gestalten sei, sondern beschreibe eine geistige und kulturelle Verfasstheit. Diese Verfasstheit ist eine - wie bereits oben

[10] vgl. Mayring 1996, S. 18

[11] beispielsweise Lyon 1999

[12] Friedrich Nietzsche lebte von 1844 - 1900

[13] vgl. Honecker 1992, S. 263 - 266

erwähnt - der Pluralität und Differenzen, die sich vor allem auf der Ebene des Einzelnen, der Gruppen und Lebensstile zeigt.

Der Begriff Postmoderne wurde nach der Veröffentlichung von Jean-François Lyotards „La Condition Postmoderne“ im Jahr 1979 populär[14]. Andere, zuerst vornehmlich französische Autoren griffen den Begriff ebenfalls auf oder wurden mit ihm in Verbindung gebracht, darunter Jean Baudrillard, Jaques Derrida oder auch Michel Foucault, dessen Arbeiten im weiteren Verlauf der Arbeit immer wieder eine Rolle spielen.

Lyotard ging davon aus, dass die damals von ihm beobachteten Entwicklungen im Bereich Wissenschaft, Technik, Politik und Alltagsleben mit traditionellen Theorien nicht mehr fassbar sind. Er lieferte allerdings keine neue Gesellschaftstheorie, sondern entwickelte begriffliche Vorschläge und Überlegungen, die helfen sollen, der Neuheit der Veränderungen gerecht zu werden und sie in ihrem Zusammenhang zu erfassen. Lyotards Text wurde somit zum Vorläufer und Grundlagentext, der heute international - und kontrovers - geführten Diskussion um die Postmoderne.[15] Lyotard definiert die Postmoderne vereinfacht als *Skepsis gegenüber Meta-Erzählungen*[16]. Eine davon wäre beispielsweise der Fortschrittsglaube oder der wachsende Wohlstand für alle. Diese Meta-Erzählungen werden in der Postmoderne in Frage gestellt. Wolf-Dietrich Bukow und Erol Yildiz sprechen in diesem Zusammenhang von einer *Krise der Mythen*, die ihre gesellschaftsprägende Kraft und ihre Glaubwürdigkeit im globalen Zeitalter zunehmend verlieren.[17]

Lyotard beschäftigt sich als Philosoph mit dem *Wissen*[18] und dessen Veränderungen unter den Bedingungen der Postmoderne. Nicht alle seine Aussagen sind daher für die vorliegende Arbeit von Bedeutung. Herausgestellt werden soll an dieser Stelle allerdings Lyotards Sicht auf die Veränderungen, die durch den Einsatz der so genannten Neuen Medien in Bezug auf das Wissen innerhalb einer Gesellschaft stattfinden:

---

[14] vgl. Lyotard 1986, (Lyotards Text wurde 1982 unter dem Titel „Das postmoderne Wissen“ erstmals ins Deutsche übersetzt und 1986, nachdem die erste Auflage vergriffen war, erneut aufgelegt)

[15] vgl. Engelmann 1986, S. 11

[16] vgl. Lyotard 1986

[17] Bukow / Yildiz 2002, S. 13

[18] Wissen wird gemeinhin als Gesamtheit organisierter Informationen, mitsamt ihren wechselseitigen Zusammenhängen verstanden, auf deren Grundlage ein (vernunftbegabtes) System handeln kann; vgl. Wikipedia 2005

> „Man kann vernünftigerweise annehmen, daß die Vervielfachung der Informationsmaschinen die Zirkulation der Erkenntnisse ebenso betrifft und betreffen wird, wie die Entwicklung der Verkehrsmittel zuerst den Menschen (Transport) und in der Folge die Klänge und Bilder (Medien) betroffen hat.“19

Lyotard spricht von einer *Hegemonie der Informatik*[20], durch die das Wissen seine Qualität verändert und Wissen zur Ware wird, die auch im weltweiten Konkurrenzkampf um Macht - um die Beherrschung von Information - eine entscheidende Rolle spielen wird. Die Gesellschaft wird so *informatisiert*. Heute, 25 Jahre nach Erscheinen des französischen Originaltextes, erscheint Lyotards Einschätzung als sehr vorausschauend und zutreffend. Mit der Kommerzialisierung des Internets wurde das Wissen in der Tat zur Ware und derjenige, der Informationen über bestimmte Vorgänge oder Personen gesammelt hat, besitzt Macht. Lyotard stellt in seinem Text die - gerade für diese Arbeit – wichtigen Fragen:

> „Wer wird die verbotenen Daten oder Kanäle definieren? Wird es der Staat sein, oder wird dieser nicht vielmehr ein Benutzer unter anderen sein? Auf diese Weise werden neue Rechtsprobleme gestellt und durch sie die Frage: wer wird wissen?“[21]

Diese Fragen sind besonders im Hinblick auf demokratische Prozesse bedeutend. Wie wird das Wissen verwaltet? Wer hat Zugang zum Wissen und kann partizipieren? Was passiert mit dem Wissen, das gesammelt wurde? Lyotard betont, dass die Frage des Wissens im Zeitalter der Informatik mehr denn je eine Frage der *Regierung*[22] sei, die entscheide, was Wissen ist und die wissen müsse, was es zu entscheiden gälte.[23]

Zusammenfassung

Die postmoderne Gesellschaft stellt eine pluralistische und hoch differenzierte Gesellschaft dar, die sich nicht mehr einer großen, Einheit stiftenden Meta-Erzählung verschreibt. Die Gesellschaft ist heterogen und somit auch nicht mehr durch eine große Theorie zu fassen, was auch innerhalb der theoretischen Einordnung des Phänomens Technische Kontrolle und Überwachung deutlich werden wird (siehe Kapitel 2). Dies bedeutet allerdings nicht, dass Vielfalt mit Beliebig-

---

[19] Lyotard 1986, S. 22

[20] Lyotard 1986, S. 24

[21] Lyotard 1986, S. 28

[22] wie Lyotard den Begriff der Regierung genau versteht, wird von ihm nicht weiter ausgeführt, er scheint aber hier auf den Regierungs*staat* zu verweisen, was aus Äußerungen auf den Seiten zuvor zu schließen ist (vgl. Lyotard 1986, S. 33ff). Diese Bemerkung scheint an dieser Stelle angebracht, da Michel Foucault, der im weiteren Verlauf der Arbeit noch Bedeutung erlangt, einen anderen Regierungs-Begriff vertritt (siehe Kap. 2.6)

[23] vgl. Lyotard 1986, S. 35

keit gleichzusetzen ist. Vielmehr stellt der Zustand einer pluralistischen Gesellschaft den Auftrag, Werte neu zu diskutieren, zu hinterfragen und dieser vermeintlichen Beliebigkeit etwas entgegen zu setzen. Hier wäre also insbesondere die Pädagogik gefragt.

Jean-François Lyotard macht deutlich, dass es ihm um das *Wissen* geht, das sich unter postmodernen Bedingungen verändert. Wichtig für die Betrachtung meines Forschungsgegenstands erscheint Lyotards Einschätzung der *Hegemonie der Informatik*, durch die Informationen zur Ware und somit auch zum Machtmittel werden. *Wer* die Macht über den Zugriff auf Informationen hat, wird in Zukunft auch immer mehr für den Einzelnen und seine persönliche Freiheit zur entscheidenden Frage. Im Hinblick auf das Forschungsthema wird Lyotard so gelesen, dass die Frage nach den Auswirkungen postmoderner Wissensstrukturen auf demokratische Grundrechte, wie beispielsweise das Recht auf Informationelle Selbstbestimmung[24], gestellt wird und die Bedingungen, unter denen Informationen über Personen gesammelt werden, im Alltag untersucht werden.

Lyotard stellt mit dem *Postmodernen Wissen* ein Gedankengebäude vor, dass bereits alle Fragen und Probleme, die sich in heutiger Zeit mit dem Einsatz technischer Kontroll- und Überwachungssysteme verbinden, aufwirft.

1.2 Der Kontroll- und Überwachungsbegriff

Kontrolle und Überwachung spielen eine nicht zu unterschätzende Rolle im menschlichen Zusammenleben. Sie können positiv empfunden werden (Qualitätskontrollen, Verkehrsüberwachung) oder aber negativ besetzt sein und als hinterherspionieren und Beschneidung der Freiheit verstanden werden. Eine Begriffsbestimmung ist an dieser Stelle angemessen, um die unterschiedlichen Dimensionen der Begriffe Kontrolle und Überwachung zu markieren.

Kontrolle

Kontrolle wird gemeinhin definiert als *dauernde Überwachung* oder *Aufsicht*, der jemand oder etwas untersteht.[25] Ein spezielles Bedeutungswörterbuch bezeichnet

[24] BVerfGE 65, 1 – Volkszählung 1983, hier heißt es u.a.: 1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, vgl. Bundesverfassungsgericht 1983

[25] vgl. Duden 1999, S. 2228

Kontrolle als *Überprüfung,* der jemand oder etwas unterzogen wird. Sinnverwandt sind Begriffe wie Aufsicht, Beobachtung oder Bespitzelung.[26]

Kontrolle wird in der Soziologie als soziale Kontrolle verstanden. Sie ist in erster Linie ein Mechanismus der Integration und der Aufrechterhaltung sozialer Ordnung. Dem Zerfall der Gesellschaft aufgrund von Desintegration der Mitglieder soll durch normatives Ausmustern von unerwünschten Verhaltensweisen entgegengewirkt werden. Über soziale Kontrolle wird abweichendes Verhalten (Devianz / Delinquenz) auf gesellschaftlich lizenzierte Handlungsspielräume begrenzt. Kontrolle hat dabei etwas mit Macht zu tun. Wer kontrolliert, herrscht, weil er Wissen hat, mit dem er langzeitige Strategien planen kann und auch sonst überlegen ist.[27]

Anfang der 70er Jahre erlangte der Begriff im Zusammenhang mit Begriffen wie Gläserner Bürger oder Überwachungsstaat zeitweise den Status eines gesellschaftskritischen Kampfbegriffs. Zu dieser Zeit kam es zu einer Fiktion des lückenlosen Funktionierens von Kontrolle, was eine Steuerungseuphorie auslöste und Leitideen sozialtechnokratischer Gesellschaftsplanung bereitstellte. Soziale Kontrolle kann als Versuch der Beeinflussung und der Verhaltenssteuerung gesehen werden. Interessant im Bezug auf technische Überwachung ist die Tatsache, dass selbst ein vermutetes oder vorgestelltes Gehört- oder Beobachtetwerden Individuen oder Gruppen zu Einstellungen und Verhaltensweisen bewegen, die sie ohne Kontrollvermutung nicht an den Tag gelegt hätten.[28] Fortschritte im Bereich der Informations- und Kommunikationstechnik führen derzeit zu immer differenzierter ausgebildeten und auch zunehmend weniger kontrollierbaren Möglichkeiten der technikgestützten und medial vernetzten sozialen Kontrolle, wie beispielsweise der Telefon- oder Kameraüberwachung.[29] Mit den neuen Kontrollmöglichkeiten entstehen neue Kontrollhierarchien und weiter auch die Notwenigkeit einer Kontrolle der Kontrolleure.

Überwachung

Bei der Überwachung geht es darum, genau zu verfolgen, *was jemand (der verdächtig ist) tut*[30] oder jemanden bzw. etwas durch *ständiges Beobachten* zu kontrollieren, oder in einer weiteren Bedeutung beobachtend und kontrollierend für den richtigen Ablauf einer Sache zu sorgen und darauf zu achten, dass in einem

---

[26] vgl. Duden 1985, S. 391

[27] vgl. Endruweit / Trommsdorrf 2002, S. 292

[28] vgl. Endruweit / Trommsdorrf 2002, S. 293

[29] vgl. Endruweit / Trommsdorff 2002, S. 295

[30] Duden 1999, S.4041

bestimmten Bereich alles mit rechten Dingen zugeht.[31] Sinnverwandt sind Begriffe wie beobachten, beschatten oder bespitzeln.

Der Begriff Überwachung meint im Zusammenhang dieser Arbeit eine verdeckte Form der Kontrolle, eventuell auch eine dauerhafte. Während Kontrollen sporadisch erfolgen, kann Überwachung zu einem Dauerzustand avancieren. Überwachung wird in dieser Arbeit als Beobachtung und Sammlung von Daten, Kontrolle als aktiver Teil der Überwachung verstanden.

1.3 Technische Kontroll- und Überwachungssysteme

Kontrolle und Überwachung geschieht in erster Linie durch *Menschen*, die andere Menschen oder Objekte aus bestimmten Gründen überwachen oder kontrollieren. An dieser Feststellung ändern auch technische Systeme nichts - allerdings ändern technische Kontroll- und Überwachungssysteme bestehende *Strukturen*. Und zwar zum einen die Möglichkeiten und das Ausmaß der Überwachung und Kontrolle, zum anderen die Auswertungsmöglichkeiten und die Zusammenführung der gesammelten Daten.

Die technischen Systeme, die innerhalb dieser Arbeit beschrieben werden, haben das Potenzial, Personen zu beobachten oder zu bespitzeln oder das Ziel, normierend ihr Verhalten zu bestimmen. Insbesondere wird dabei auf *Computertechnologie* zurückgegriffen. Einige der in der Arbeit vorgestellten Systeme werden in der Öffentlichkeit gar nicht als Kontroll- und Überwachungssysteme wahrgenommen, sind aber de facto durch die Nutzung von Datenbanken und Netzwerken, die im Hintergrund laufen, diesen zuzurechnen. Ohne die heutigen Möglichkeiten der elektronischen Datenverarbeitung (EDV) wären die beschriebenen technischen Systeme, wie die digitale Videoüberwachung, das Sammeln von Daten über Kaufverhalten oder Ortungsverfahren, die sich der Satellitentechnik bedienen, nicht denkbar. Ein wichtiger Aspekt technischer Kontroll- und Überwachungssysteme ist daher auch nicht die Tatsache, dass es sich dabei um elektronische Geräte handelt, sondern dass die Ergebnisse der Kontrolle und Überwachung per EDV erfasst und weiterverarbeitet werden. Oftmals kommt es dabei zur Speicherung in einer zentralen Datenbank und einer Auswertung und Kombination mit anderen bereits erhobenen Daten (Datamining[32]). Die bei Lyo-

[31] Duden 1999, S.4041

[32] *Data Mining* ermöglicht das automatische Auswerten großer Datenbestände, die in Unternehmen oder dem Internet etc. anfallen. Ziel dabei ist das Aufspüren von Regeln und Mustern bzw. statistischen Auffälligkeiten. So lassen sich z.B. Änderungen im Verhalten von Kunden oder Kundengruppen aufspüren und Geschäftsstrategien können darauf ausgerichtet werden. Es kann aber auch abweichendes Verhalten einzelner Personen erkannt werden. Unter Datenschützern wird das Verfahren kritisch gesehen.

tard formulierte *Informatisierung der Gesellschaft*[33] wird aufgrund des Einsatzes technischer Systeme erst möglich.

In den letzten Jahren haben sich Kontroll- und Überwachungssysteme innerhalb der westlichen Gesellschaften in allen Bereichen verbreitet.[34] Im Folgenden werden die derzeit gängigen Überwachungssysteme vorgestellt und kommentiert, um eine bessere Vorstellung über die Funktionsweise der Systeme zu erhalten. Anwendungsbeispiele und empirische Befunde zu ausgewählten Systemen werden im empirischen Teil der Arbeit vertieft.

Videoüberwachung

Videoüberwachung ist die Beobachtung von Räumen mit optisch-elektronischen Einrichtungen. Herkömmliche Videoüberwachung besteht in der Regel aus mindestens einer Überwachungskamera und einem Anzeigemonitor, optional erlauben die Systeme häufig auch eine Aufzeichnung der Bilder auf Videoband. Moderne Systeme bestehen aus Kameras, die via Netzwerk an einem Computer angebunden werden. Der Computer übernimmt die Funktion der Aufzeichnung. Zum Betrieb einer Videoüberwachungsanlage ist dann der Einsatz einer Videoüberwachungssoftware notwendig, die häufig weitergehende Funktionen wie beispielsweise Bewegungserkennung oder Gesichtserkennung ermöglicht. Die Kameramodelle für die Überwachung sind recht unterschiedlich und reichen von der gut sichtbaren Videokamera bis hin zu kleinen, an der Decke angebrachten und verspiegelten Dome-Kameras[35], die auf dem ersten Blick nur schwer als Kamera zu identifizieren sind. Die Bildauflösung der neueren Geräte kann sehr hoch sein, so dass sie gestochen scharfe Bilder auch aus größerer Entfernung liefern. Je nach Ausführung können die Kameras zoomen, schwenken oder haben die Möglichkeit über Infrarottechnik Nachtaufnahmen zu machen. Teilweise sind die Kameras über Funk oder Netzwerke mit Leitstellen vernetzt und können aus größerer Entfernung bedient werden.

Kundenbonuskarten

Diese Karten werden in der Regel nicht als klassische Kontroll- und Überwachungstechniken wahrgenommen. Sie haben aber in den letzten Jahren - beispielsweise als Payback- oder Happy Digits-Karte - in Verbindung mit der Nutzung von Datenbanken dazu beigetragen, den Kunden transparenter zu machen. Kundenbonuskarten arbeiten mit unterschiedlichen Kartensystemen. Für die

---

[33] vgl. Lyotard 1986, S. 30

[34] vgl. z.B. Datenschutzbericht 2003

[35] Unter einer Dome-Kamera versteht man kleine Videoüberwachungskameras, die halbkugelförmig an der Decke angebracht werden (siehe Abbildung 10, Kapitel 4.3.2).

Erfassung der Bonuspunkte ist es nicht notwendig, eine leistungsstarke Chipkarte einzusetzen. Der Marktführer Payback, der im empirischen Teil der Arbeit näher untersucht werden wird, verwendet für sein System beispielsweise Magnetstreifenkarten. Deren drei Spuren reichen aus um in zwei Spuren persönliche Daten zu codieren und in Spur drei aktuelle Daten, wie z.B. den Punktestand, zu speichern. Die erhobenen Daten müssen hier also fast zwangsläufig an Datenbanken o.ä. weitergeleitet werden, da die Speicherkapazität der Karte gering ist.

Ortungstechniken (GPS und GSM)

Bei diesen Systemen ist das Kontroll- und Überwachungspotenzial, ähnlich der Videoüberwachung, offensichtlicher. Das Global Positioning System (GPS) ist eigens zum Zwecke der Lokalisierung entwickelt worden, das Global System for Mobile Communications (GSM) macht es aufgrund der Einbuchung des Handys in Zellen ebenfalls möglich, die Geräte relativ genau zu lokalisieren.

Das Global Positioning System

Mittels GPS ist es möglich via Satellit einen GPS-Empfänger - einen kleinen Chip - bis auf wenige Meter genau zu orten. Das GPS besteht aus 24 Satelliten, die sich in sechs verschiedenen Umlaufbahnen um die Erde bewegen. Seit 1973 wird das GPS vom US-Verteidigungsministerium betrieben. Zur Überwachung des GPS existieren fünf Kontrollstationen, wobei sich die Hauptkontrollstation in Colorado Springs befindet.[36] Das GPS war noch bis Ende der 1990er Jahre vom amerikanischen Militär eingeschränkt worden und wurde erst dann für den zivilen Bereich freigegeben.[37] In Auto-Pilot-Systemen von Fahrzeugen verbreitet sich das GPS-System immer stärker, dort dient es zur Lokalisierung des eigenen Standortes, von dem aus dann, meist mittels einer CD-Rom, computerunterstützt das Fahrtziel ermittelt werden kann. In der öffentlichen Diskussion erlangte GPS verstärkt Beachtung, als es um die Einführung einer LKW-Maut in Deutschland ging.

Das Global System for Mobile Communications

Der Handy-Standard GSM stellt die Menge aller Spezifikationen und Schnittstellen dar, die für ein funktionierendes Mobilfunknetz benötigt werden. Er ist der

---

[36] vgl. Geosoft 2005

[37] Um nicht-autorisierte Nutzer von einer genauen Positionsbestimmung auszuschließen, wurde die Genauigkeit für Nutzer, die nicht über einen Schlüssel verfügen, künstlich verschlechtert (Selective Availability = SA, mit einem Fehler von größer 100 m). Am 1. Mai 2000 wurde diese künstliche Ungenauigkeit abgeschaltet, so dass das System seitdem auch außerhalb des bisherigen exklusiven Anwendungsbereichs zur präzisen Positionsbestimmung genutzt werden kann. Dies führte unter anderem zum Aufschwung der Navigationssysteme in Fahrzeugen und im Außenbereich.

Standard, mit dem inzwischen die Mehrheit aller mobilen Telefone betrieben wird. Mit dieser Technik ist es möglich, den Standort eines Handys zellengenau zu ermitteln, man kann also erkennen, in welcher Mobilfunknetz-Zelle das Handy sich gerade befindet, was eine Ortungsgenauigkeit von wenigen hundert Metern bedeutet. Diese Möglichkeit wird mittlerweile auch kommerziell genutzt und beispielsweise als Kindersicherungssystem angeboten.

Biometrische Verfahren

Biometrie meint die Erfassung und (Ver-)Messung von Lebewesen und ihrer Eigenschaften. Im Folgenden werden Verfahren vorgestellt, denen automatisierte Messungen zugrunde liegen und die ohne Computertechnologie nicht funktionieren würden. Zumeist geht es bei diesen Technologien um die Erfassung von individuellen physiologischen oder verhaltenstypischen Merkmalen einer Person zum Zwecke der Identifikation. Zur Identifikation eines Menschen ist das Gesicht eines der wichtigsten Merkmale. Vielfach gelingt es aber, durch Verkleidungen, z.B. ein angeklebter Bart, eine Brille etc., eine Täuschung vorzunehmen. Elektronische Gesichtserkennung soll an dieser Stelle Abhilfe schaffen, da typische geometrische Merkmale des Gesichts, wie Abstand der Augen, Anordnung von Kinn, Nase und Mund mittels einer Gesichtserkennungssoftware erfasst und ausgewertet werden können - aber auch die Form des Kopfes oder der Ohren können Aufschluss über die Identität einer Person geben. Die Daten werden in Datenbanken eingegeben und können beispielsweise in Verbindung mit den Bildern einer Videoüberwachungskamera zur Identifikation einer Person herangezogen werden.[38]

Fingerbilder, also das Muster der Hautleisten auf der Fingerkuppe, bieten eine weitere Möglichkeit der biometrischen Identifikation. Die Verzweigungs- und Endpunkte der Fingerlinien (die so genannten Minuzien) werden bei entsprechenden Verfahren in Betracht gezogen. Bei weiterer Betrachtung der Hand im Rahmen der Handgeometrie sind die Länge der Finger, ihre Dicke und ihr Abstand zueinander Merkmale. Auch das Profil der Hand und eventuell auch das Muster der Venen kommen für eine Identifikation in Betracht. Auch diese Methoden wären ohne die Möglichkeit eines digitalen Datenabgleichs nicht möglich. Fingerbilder werden nicht nur in der Kriminalistik verwertet, sondern halten auch Einzug in unseren Alltag. Im Personalausweis werden sie, nach der kürzlichen

[38] In London wurden bereits Systeme der amerikanischen Firma „Software and Systems“ erprobt, bei denen Menschenmengen mit Videokameras erfasst wurden, und die Gesichter dann mit den Bildern einer Datenbank abgeglichen wurden. Noch liegen die Fehlerquoten recht hoch, es ist jedoch nur eine Frage der Zeit, bis die Technik ausgereifter ist, vgl. STOA 2002

Verabschiedung des Anti-Terror-Paketes, zukünftig eingesetzt werden können, aber auch im privatwirtschaftlichen Bereich verbreiten sie sich.[39]

Die Augen des Menschen bieten einen weiteren Identifikationspunkt; sie können anhand des Musters der Iris und dem Muster der Retina (der Blutgefäße im Augenhintergrund) Aufschluss über die Identität einer Person geben. Selbst eineiige Zwillinge lassen sich eindeutig unterscheiden. Mit über 400 Strukturmerkmalen bietet die Iris sogar sechs- bis achtmal so viele Variablen wie der menschliche Fingerabdruck.[40]

Neben diesen passiven Merkmalen gibt es auch aktive Merkmale, wie die Unterschrift, die Handschrift oder die Stimme. Es gibt auch Systeme, die mehrere Merkmale vereinigen und aus der Mimik des Gesichts und der Stimme ihre Identifikationen vornehmen.

Mithören - Überwachung der Telekommunikation

Bis in die 60er Jahre waren die meisten Überwachungsgeräte technologisch einfach, aber teuer, da sie voraussetzten, dass man den Verdächtigen auf Schritt und Tritt folgte, wozu ein hoher Personal- und Zeitaufwand nötig war. Alle Informationen und erzielten Kontakte wurden schriftlich festgehalten und abgelegt, wobei wenig Aussicht auf eine schnelle Überprüfung bestand. Auch die elektronische Überwachung war sehr arbeitsintensiv. Die ostdeutsche Polizei beschäftigte 500.000 Inoffizielle Mitarbeiter (IM), wovon 10.000 ausschließlich dazu eingesetzt wurden, die Telefongespräche der Bürger abzuhören und niederzuschreiben.[41] Bei der heutigen technischen Entwicklung sind solche Zahlen Geschichte. Nach Verabschiedung des Großen Lauschangriffs im Jahr 1998 stieg die Zahl der abgehörten Telefongespräche erheblich, die Auswertung ist durch die Möglichkeiten der Computertechnologie immer leichter. Im Grundrechte-Report 2002 wird vermeldet, dass die Zahl der Telefonüberwachungen im Jahr 2001 auf rund 15.000 angestiegen sei, betroffen seien 1,5 Millionen Menschen, die in der Regel nicht informiert würden.[42]

Genom-Kontrolle

Die DNA des Menschen ist in jeder Körperzelle in 23 Chromosomenpaaren enthalten. Modellhaft enthält sie in einer Abfolge von drei Milliarden *Buchstabenpaaren* 30.000 Gene und dazwischen nicht codierende Buchstaben-Sequenzen.

---

[39] vgl. Cinebank 2002

[40] Petermann / Sauter 2002

[41] vgl. STOA 1998

[42] vgl. Müller-Heidelberg 2002

Die Abfolge der *Buchstaben* wurde im Jahr 2000 entschlüsselt. DNS-Sequenzen, die nach bisherigen Erkenntnissen keine Gene bilden, aber bei jedem Menschen einmalig sind, sind als so genannter Genetischer Fingerabdruck bekannt. Das menschliche Erbgut ist in den letzten Jahren immer weiter in den Focus der Verwertbarkeit gerückt worden. Große Verbreitung erfährt die Genomkontrolle mittlerweile bei der Strafverfolgung, um z.B. Gewaltverbrechen auch noch nach Jahren aufzuklären. Mit Hilfe einer Genomdatenbank glaubt man Verbrecher eindeutig ausmachen zu können. Immer neue Erkenntnisse zu erblich bedingten Krankheiten, Merkmalen und Eigenschaften stehen ins Haus. Die Analysen der DNS werden heute weitgehend elektronisch unterstützt. Ohne die Informationstechnik sind Gentests - jedenfalls in größerer Zahl - nicht denkbar.[43]

1.4 Stand der Forschung

Das folgende Kapitel gibt einen Überblick, wie das Thema technische Kontroll- und Überwachungssysteme zurzeit in den Sozialwissenschaften und angrenzenden Fachgebieten diskutiert wird. Innerhalb der Soziologie findet sich das Thema fast ausschließlich im Bereich der Stadtforschung. Der urbane Raum kann somit als Ort gesehen werden, an dem die Auswirkungen technischer Kontroll- und Überwachungssysteme am deutlichsten zu Tage treten. Das Thema ist außerhalb der soziologischen Diskussion auch in der Kriminologie zu finden, in der es hauptsächlich um den Einsatz von technischen Systemen in der Polizeiarbeit geht. In der Pädagogik wurde das Thema theoretisch so gut wie gar nicht behandelt, obwohl die Anwendung im Alltag bereits weit fortgeschritten ist. Zur Darstellung des Forschungsstandes wird auch auf Literatur aus dem angloamerikanischen Sprachraum zurückgegriffen, wo technische Kontroll- und Überwachungssysteme bereits länger zum Einsatz kommen, als dies in Deutschland der Fall ist und diese Systeme auch wissenschaftlich stärker diskutiert wurden.[44]

1.4.1 Soziologische Aspekte

In Deutschland ist das Thema *Kontrolle und Überwachung* seit den 70er Jahren unter dem Begriff des *Überwachungsstaates* Gegenstand soziologischer Betrach-

[43] Schrader 2000 / 2001

[44] Ich möchte an dieser Stelle noch auf die journalistischen Arbeiten von Christiane Schulzki-Haddouti hinweisen, die sich kontinuierlich mit Datensicherheit und Überwachungstechnologien befasst und dazu sowohl in Fachzeitschriften als auch in eigenen Veröffentlichungen Stellung bezogen hat (vgl. Schulzki-Haddouti 2000, 2001, 2003, 2004). Ferner steht das Thema in juristischen Fachkreisen zur Diskussion, wo es im Bereich der bürgerlichen Grundrechte und im Datenschutz diskutiert wird.

tungen.[45] Damals war die grundsätzliche Stimmung in der Bevölkerung eine andere als heute, bedenkt man die Proteste, die in den 80er Jahren zur Volkszählung stattfanden und das bereits erwähnte Volkszählungsurteil[46] des Bundesverfassungsgerichts, welches das Recht auf Informationelle Selbstbestimmung konstituierte. Computertechnologie wurde zum damaligen Zeitpunkt kritischer gesehen und war noch nicht in dem Maße in den Alltag integriert, wie sie das heute ist.

Ende der 90er Jahre sind im Bereich der Stadtsoziologie Beiträge veröffentlicht worden, die sich - meist nur am Rande - den technischen Kontroll- und Überwachungssystemen widmen. Dabei werden diese als *ein* Mittel der Exklusion von Minderheiten oder unerwünschten Personen dargestellt. Die Darstellung beschränkt sich in der Regel auf den Einsatz von Videoüberwachung. Klaus Ronneberger und seine Kollegen[47] kritisieren beispielsweise innerhalb ihrer Forschung die wachsende Privatisierung öffentlicher Räume, aus denen unerwünschte Gruppen und Personen, wie z.B. Obdachlose, ausgeschlossen werden sollen, wozu auch die Videoüberwachung eingesetzt wird. Ähnliches stellt Pablo de Marinis[48] in seiner Arbeit dar, die sich mit Machtinterventionen in den urbanen Räumen der Kontrollgesellschaft beschäftigt. Diese Autoren werden innerhalb der theoretischen Einordnung in Kapitel 2 ausführlicher dargestellt.

An diese Autoren anschließend hebt Jan Wehrheim[49] in seiner 2002 veröffentlichten Dissertation auf Inszenierungen von Sicherheit in europäischen und US-amerikanischen Städten ab. Die Ausgrenzung von unerwünschten, weil nicht konsumierenden, Menschen ist Kern seiner Analyse. Dabei greift Wehrheim jüngere Ansätze zur Beschreibung aktueller Formen gesellschaftlicher Spaltung auf, wie sie in der Soziologie sozialer Ungleichheit, der Stadtsoziologie sowie der Kriminologie unter den Begriffen *soziale Ausgrenzung, Exklusion, soziale Ausschließung* und *Urban Underclass* diskutiert werden. Die zentrale Fragestellung ist, welche Auswirkungen Inszenierungen von räumlich orientierter Sicherheit in deutschen und US-amerikanischen Städten auf die genannten Diskussionsfelder haben. Die Videoüberwachung ist dabei *ein* Hilfsmittel, um Exklusion durchzusetzen.

---

[45] vgl. z.B. Bölsche 1979, Ruhmann 1985, Schoeler u.a. 1986

[46] hier ist das bereits in Fußnote 20 zitierte Urteil des Bundesverfassungsgericht aus dem Jahre 1983 gemeint, in dem festgelegt wurde, dass der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann, vgl. BVerfGE 65, 1 – Volkszählung 1983

[47] vgl. Ronneberger et al. 1999

[48] vgl. de Marinis 2000

[49] vgl. Wehrheim 2002

Im selben Jahr wurde das „Jahrbuch StadtRegion, Die sichere Stadt“ veröffentlicht, das Beiträge unterschiedlicher Autoren zum Thema bietet und sich teilweise auch mit Fragen der Videoüberwachung auseinandersetzt. Ebenfalls stellt darin Jan Wehrheim die Frage nach einer zunehmenden Abkehr vom Konzept einer integrativen Stadt zur Diskussion und berücksichtigt dabei auch Überwachungstechnologien.[50] Auch Katja Veil[51] und Detlef Nogala[52] hinterfragen kritisch Projekte der Videoüberwachung von Innenstädten, wobei Veil dabei auf die englische Stadt Coventry Bezug nimmt und Nogala Videoüberwachung als *urbane Einrichtung* definiert.

Für den angloamerikanischen Sprachraum hat der kanadische Soziologe David Lyon mit zahlreichen Veröffentlichungen[53] zum Thema die theoretische Diskussion gerade in Hinblick auf den Einsatz von technischen Kontroll- und Überwachungssysteme erweitert. Die Kombination von Überwachung und Bürokratie / Rationalisierung hat ihre Wurzeln in der Moderne, ändert ihre Strukturen aber zunehmend durch den Einsatz von Computertechnologie. Lyon verweist auf die Theorien Foucaults für eine weitere Betrachtung des Themas.[54] Schuurman[55], ebenfalls Kanadier, ergänzt das Bild mit einer Zusammenstellung der bisherigen Forschung im Bereich der *Videoüberwachung*. In seiner Dissertation stellt er heraus, dass nur wenige soziologische Arbeiten zu diesem Thema existieren. Bei seiner Auswertung von Studien seit den 70er Jahren, die sich mit der Effizienz von Videoüberwachung auseinandersetzen, kommt er zu dem Schluss, dass Videoüberwachung im Rahmen von Kriminalitätsbekämpfung nicht den gewünschten Effekt erzielten, sondern in einigen Fällen sogar kontraproduktiv seien, da sie ein falsches Gefühl von Sicherheit vermittelten und so die Aufmerksamkeit der Menschen herabsetzten.

Norris und Armstrong aus Großbritannien heben ebenfalls auf das exkludierende Moment der Videoüberwachung ab. Sie kommen in ihren Untersuchungen in Großbritannien zu dem Ergebnis, dass der Schwerpunkt bei der Videoüberwachung hauptsächlich auf Jugendlichen liegt. Dabei werden eher Farbige als Weiße, eher Männer als Frauen und eher die Arbeiter- denn die Mittelschicht in den Fokus der Kamera genommen.[56] Auch Betrunkene, Bettler, Obdachlose und Straßenverkäufer werden intensiv mit der Kamera beobachtet. Dieser Umstand der

---

[50] vgl. Wehrheim 2002, S. 16ff

[51] vgl. Veil 2002, S. 117ff

[52] vgl. Nogala 2002, S. 33ff

[53] vgl. z.B. Lyon 1994, 2001, 2003

[54] vgl. Lyon 2001, S. 118ff

[55] Schuurman 1995

[56] vgl. Norris / Armstrong 1999, S. 119

Diskriminierung übermittele, so die Autoren, eine negative Botschaft an deren Position innerhalb der Gesellschaft und kann schwerwiegende Konsequenzen für die gesellschaftliche Ordnung haben.[57] Norris und Armstrong weisen in ihren Untersuchungen weiter auf den Umstand hin, dass die Installation von Kameras meist andere ordnungspolitische Maßnahmen nach sich ziehen. Sie berichten von einem kameraüberwachten Platz, auf dem nach geraumer Zeit das Verbot zum öffentlichen Konsum von Alkohol erteilt wurde. Damit wurde auch die Zugriffsmöglichkeit der Polizei erhöht und neue Möglichkeiten der Kriminalisierung und Exklusion eröffnet. Die Autoren gehen davon aus, dass Straftäter in Bereiche, die außerhalb der Kameraüberwachung liegen, verdrängt werden. Probleme werden durch diesen Umstand zwar nicht gelöst, allerdings ist nicht von der Hand zu weisen, dass auf diese Weise bestimmte Stadtgebiete gesäubert werden können, um z.B. ungestörten Konsum zu ermöglichen.[58] Zusammen mit der Durchsetzung der Verfügungen durch die Polizei kann Videoüberwachung mächtige exkludierende Effekte haben und ihren Beitrag dazu leisten, dass mehr und mehr Verhaltensweisen, die eigentlich nicht wirklich bedrohlich oder gefährlich sind, Gegenstand von offizieller, autoritärer Intervention werden. Dabei werden hauptsächlich Personen von der Kameraüberwachung erfasst, die schon vorher als deviant stereotypisiert waren oder deren Erscheinungsbild Aufsehen erregt. Videoüberwachung kann so ein Instrument der Ungerechtigkeit werden, wenn Menschen nur wegen äußerer Kriterien oder aufgrund von Vorurteilen exkludiert werden.

Auffällig ist auch, dass die Ziele der Videoüberwachung sich laufend verändern, bzw. neue Einsatzmöglichkeiten ersonnen werden. Ein Beispiel aus London zeigt, dass die in der Vergangenheit zur Terrorismusbekämpfung und Sicherheit der Bevölkerung installierten Videokameras nun zur Ermittlung der Identität der Fahrzeughalter der Wagen eingesetzt werden, die in die Innenstadt von London gelangen wollen. Eine neu eingeführte Stau-Gebühr kann so abgerechnet werden.[59]

Ein aktuelles internationales Projekt, das am Zentrum für Technik und Gesellschaft an der Technischen Universität in Berlin koordiniert wird, widmet sich dem Phänomen der urbanen Videoüberwachung und trägt den Titel *Urbaneye, - On the Threshold to Urban Panopticon?*. Das seit 2001 laufende, mehrere Städte vergleichende Forschungsprojekt hat das Ziel, den Einsatz von Videoüberwachung in der Öffentlichkeit in Europa zu analysieren und die gesellschaftlichen Effekte und politischen Auswirkungen herauszuarbeiten. Es sollen Strategien zur Regulierung

---

[57] vgl. Norris / Armstrong 1999, S. 150f

[58] vgl. Norris / Armstrong 1999, S. 200

[59] vgl. WDR 2003

des Einsatzes von Videoüberwachung erarbeitet werden. Dabei wurde ein multidisziplinäres Team zusammengestellt, dass sich aus Kriminologen, Philosophen, Politologen, Soziologen und Stadtgeographen aus sieben Ländern zusammensetzt. Das Forschungsprojekt wird von der Europäischen Kommission gefördert und soll aufgrund der vielfältigen Ergebnisse, die es zur Verfügung stellt, hier etwas ausführlicher vorgestellt werden.

Die bereits durchgeführten Forschungsprojekte beziehen sich auf Videoüberwachung in Großbritannien, Norwegen, Dänemark und speziell auch auf die Städte Oslo, Kopenhagen und London. Im deutschsprachigen Raum wurde die Videoüberwachung in Wien und Berlin in den Fokus genommen.[60] Dabei wurde beispielsweise für Berlin herausgefunden, dass sich die befragten Personen einer Untersuchung[61] erst einmal sicherer fühlen, wenn Videokameras, beispielsweise in einem Einkaufszentrum, installiert sind. Dabei ist es aber auch so, dass das Vertrauen in die Technik größer ist, als das in das Personal, das hinter den Überwachungsmonitoren sitzt; das Sich-sicherer-Fühlen durch die Videokameras wird durch die Ungewissheit, was die Aufsichtspersonen wirklich mit dem Bildmaterial tun, wieder unterwandert.[62] Als Ergebnis dieser Ambivalenz haben die Autoren herausgefunden, dass alle Befragten dazu neigen, ihr Verhalten zu regulieren, wenn sie bemerken, dass sie von Kameras überwacht werden. Eine Folge der Überwachung ist es, die Aufmerksamkeit im städtischen Umfeld zu reduzieren, also nicht mehr so genau hinzusehen, wenn etwas passiert, da ja nun die Kameras installiert sind – ein Umstand, der auch beim Kanadier Schuurman bereits Erwähnung fand. Eine andere Folge der Kameraüberwachung ist es, Videoüberwachung als Zeichen einer wachsenden Sicherheit oder aber auch einer wachsenden Überwachung zu interpretieren. Diejenigen, die sich mit Videoüberwachung sicherer fühlen, betonen die Notwendigkeit zur Regulation und des Datenschutzes. Sie möchten Videoüberwachung auch nicht flächendeckend eingesetzt sehen, sondern nur an Orten, die als besonders riskant gelten, da dort eventuell schon Straftaten verübt worden. Es wurden aber auch negative Dinge durch die Interviewten geäußert, die zu dem Schluss kamen, Videoüberwachung könne keine Hilfe zur Kriminalitätsbekämpfung sein, sondern ihr sozialer Effekt sei es, ein umfassendes Kontrollsystem zu installieren, das zu unterschiedlichen Zwecken und aus unterschiedlichen Interessen eingesetzt werden kann.[63]

---

[60] vgl. Urbaneye 2004

[61] Bei der Studie wurden 203 standardisierte Interviews geführt, die teils offene Fragen enthielten und zwischen 15 und 30 Minuten dauerten. Im Anschluss wurden aus den Interviewten 10 Personen in einem längeren, qualitativen, Interview befragt.

[62] vgl. Helten / Fischer 2004, S. 50

[63] vgl. Helten / Fischer 2004, S. 51

Forscher derselben Gruppe, die sich mit Videoüberwachung in Oslo auseinandergesetzt haben, kommen zu dem Schluss, dass es durch Videoüberwachung zu Diskriminierungen kommt und äußern sich besorgt, dass der öffentliche Raum ghettoisiert werden könnte:

> „In extension of this, we are also concerned, that publicly accessible spaces will thereby become „ghettoized", will come to be populated by an ever-narrower spectrum of society. Societies need meeting places. If we are to build cosmopolitan societies, societies rich in cultural impulses, societies where democracy is secured by mutual trust amongst social groups with diverse interests and perspectives, then we need those meeting places to be diversely populated."[64]

An der gleichen Forschungseinrichtung, die auch Urbaneye koordiniert, dem Zentrum für Technik und Gesellschaft, forscht die Kanadierin Heather Cameron zum Thema, wie neue Überwachungstechnologien den öffentlichen Raum beeinflussen und wie diesen Technologien widerstanden werden kann. Ergebnisse ihrer Arbeit liegen derzeit noch nicht vor.

Ein weiteres internationales Projekt zum Thema Überwachung und Gesellschaft bietet die Internet-Plattform Surveillance and Society[65], die von britischen Wissenschaftlern ins Leben gerufen wurde. Sie hat das Ziel, die Surveillance-Studies einer breiteren Öffentlichkeit zugänglich zu machen und einen Überblick über aktuelle Forschung zu geben. Primär liegt der Fokus auf Videoüberwachungssystemen und weiterführenden theoretischen Modellen, wobei die Theorien Michel Foucaults stark diskutiert werden.

1.4.2 Pädagogische Aspekte

Technische Kontroll- und Überwachungssysteme stellen in der pädagogischen Diskussion bisher allenfalls ein Randthema dar. In den späten 80er Jahren rückte das Thema unter dem Blickwinkel der Vernetzung von Computern und den Risiken von Datennetzen in die pädagogische Praxis. Dort wurden entsprechende Themen vereinzelt für den Schulunterricht aufbereitet.[66] In der damaligen Diskussion ging es aber nicht speziell um Technikeinsatz *zur* Kontrolle, sondern eher um Aufklärung und kritische Auseinandersetzung mit neuen technischen Entwicklungen, die mit der wachsenden Verbreitung des Personal Computers (PC) ihren Anfang nahmen.

---

[64] vgl. Saetnan / Dahl / Lomell 2004, S. 39

[65] vgl. Surveillance and Society 2004

[66] vgl. z.B. Schorb u.a. 1991

In der aktuellen Diskussion findet eine Auseinandersetzung mit technischen Systemen, die zur Kontrolle und Überwachung von Menschen eingesetzt werden, nicht statt. Eine zusätzlich zur eigenen Literaturrecherche in Auftrag gegebene Nachforschung beim Deutschen Institut für internationale pädagogische Forschung[67] in Frankfurt ergab Ende des Jahres 2000 lediglich *eine* Literaturangabe für den deutschsprachigen Raum. Eine Anfang 2005 neuerlich in Auftrag gegebene Literaturrecherche kam zum selben Ergebnis.[68] Bei dem erwähnten Treffer handelt es sich um einen Artikel[69], in dem der Einsatz von Videoüberwachung in Kindergärten diskutiert wird, bei dem die entstandenen Bilder über das World Wide Web von den Eltern eingesehen werden können. Diese, in den USA bereits gängige Praxis wird von deutschen Erzieherinnen und Erziehern abgelehnt, welche die Autonomie ihrer Arbeit gefährdet und die Ablösungsprozesse zu den Eltern behindert sehen. Auch das Missbrauchspotenzial von Kinderbildern, die über das World Wide Web übertragen werden wird als Minuspunkt gegenüber der Technik gesehen. Pädagogische Arbeit könne unter einer solchen Beobachtung und Überwachung nicht geleistet werden.[70]

Im journalistischen Bereich ist das Thema der Kontrolltechniken in der pädagogischen Praxis in letzter Zeit gelegentlich diskutiert worden, hier wird aber - genau wie innerhalb der soziologischen Diskussion - allein auf die Videoüberwachung als technisches Überwachungssystem Bezug genommen. In einer Beilage der Frankfurter Rundschau wird das auch von Hohn behandelte Thema unter dem Titel „Big Brother im Kindergarten“[71] diskutiert und kommt, mit Verweis auf bereits bestehende amerikanische Projekte zu einem ähnlichen Ergebnis wie Hohn. Deutlich wird, dass das Thema in der Fachdiskussion überhaupt keine Rolle spielt und bisher lediglich journalistisch aufbereitet wurde. Angeführt sei in diesem Zusammenhang noch die immer wieder aufkommende Diskussion zum Thema „Videoüberwachung von Schulhöfen“[72] oder die Kommentare zu einer Überwachung eines Schulbusses in Brandenburg durch Videokameras.[73] Eine wissenschaftliche Begleitung oder theoretische Aufarbeitung des Themas fehlt jedoch - genau da müssten Pädagogen sich aber ihrer Verantwortung stellen und diese Systeme in ihre theoretische Reflexion einbeziehen.

---

[67] vgl. DIPF 2005

[68] Dabei wurde in der „FIS Bildung“ Literaturdatenbank recherchiert, die den umfangreichsten bildungsbezogenen Datenpool im deutschsprachigen Raum darstellt.

[69] vgl. Hohn 1998, S. 23-24

[70] vgl. Hohn 1998, S. 24

[71] vgl. Siering 1999, S. 34-36

[72] vgl. Zips 1999, S. 10

[73] vgl. Jaeger 2000, S. 142

In den USA, Kanada und Großbritannien finden sich unter den Hochschulschriften ebenfalls nur wenige Arbeiten, die sich mit dem Thema technische Kontroll- und Überwachungssysteme aus einem pädagogischen Blickwinkel heraus beschäftigen. Dabei liegt der Schwerpunkt hier auf dem Einsatz von Videoüberwachung zur Steigerung der Sicherheit an Schulen und zur Gewaltprävention. Technik wird in den USA hauptsächlich zur Herstellung von *Sicherheit* diskutiert, ein Aspekt, der in der weiteren Betrachtung des Themas eine wichtige Rolle spielen wird. Die Ergebnisse der Arbeiten lassen jedoch vermuten, dass die Technik nicht geeignet scheint, soziale Probleme zu lösen. Holmes[74], der in seiner Arbeit herausfinden wollte, ob sich das Sicherheitsgefühl von Schülern und Lehrern nach dem Umzug in ein neues Schulgebäude mit Videoüberwachung und einem computerisierten Türschließsystem verbessert, fand heraus, dass die Schüler glaubten, das Sicherheitssystem diene nur dazu, sie beim Brechen der Schulregeln zu überführen und zu überwachen. Das Sicherheitsgefühl konnte demnach also nicht gesteigert werden, wohl aber das Gefühl der Überwachung.

Balen[75] beschäftigt sich mit dem Gebrauch und Nutzen von Videoüberwachung in zwei Schulcaféterien von Middle Schools. Seine Studie zeigt, dass unter der Videoüberwachung zwar kleinere Vergehen wie Schubsen oder das Tablett nicht zurücktragen, reduziert wurden, es aber zu keiner Veränderung des Verhaltens in Hinblick auf Kämpfe oder Respektlosigkeit gegenüber Aufsichtspersonen kam.

In den letzten Jahren sind verschiedene technische Systeme in der pädagogischen Praxis erprobt worden. Dabei eilt die Praxis der Forschung, wie so oft, voraus. Ob es um Videoüberwachung in Schule und Kindergarten, um elektronische Waffenkontrollen in US-amerikanischen Schulen geht, oder ob Kinder durch GPS-Empfänger stets auffindbar sind – eine wissenschaftliche Betrachtung aus pädagogischer Sicht fehlt weitestgehend.

1.4.3 Kriminologische Aspekte

Unter kriminologischen Gesichtspunkten wurde das Thema technische Kontroll- und Überwachungssysteme hauptsächlich unter dem Aspekt der sich verändernden Bedingungen des Umgangs mit Straftaten behandelt. Kontrollsysteme, die in diesem Zusammenhang in der Literatur Beachtung finden, sind in erster Linie die Videoüberwachung, aber auch Systeme, wie die elektronische Fußfessel für Gefangene, die das GPS nutzen. Eine Betrachtung der Kriminologie an dieser Stelle erweitert den Blickwinkel und liefert einige neue Aspekte in der Diskussion des Themas.

---

[74] vgl. Holmes 1998

[75] Balen 1997

Detlef Nogala hat 1998 eine Dissertation[76] zum Thema *Soziale Kontrolltechnologien* verfasst, die die Verwendungsgrammatiken, die Systematisierung und die Problemfelder technisierter sozialer Kontrollarrangements, insbesondere im Hinblick auf die Polizeiarbeit thematisiert. Nogala stellt fest, dass Technik schon längere Zeit innerhalb der Instanzen sozialer Kontrolle eine Rolle spielt, es aber in den letzten 30 Jahren mit der Entwicklung der Mikroelektronik und der Computertechnologie zu einer "Dynamisierung der ´Beziehung` von Technikoption und Kontrollentwurf"[77] gekommen ist. In einem ersten, explorativen Teil untersucht Nogala den Einsatz von Kontrolltechnologien in der Praxis und versucht dabei bereits in den Technologien angelegte Möglichkeiten für zukünftige Kontrollarrangements zu finden. Er stellt dabei die Frage nach der Freiheit des Individuums unter technisierter sozialer Kontrolle.[78] Die technischen Kontrollsysteme, die Nogala in den Fokus nimmt, sind insbesondere aus dem Bereich der polizeilichen Arbeit entnommen (Genetischer Fingerabdruck, Abhöranlagen, Videoüberwachung). Nogala kommt zu dem Ergebnis, dass Polizeistrategen und andere Verantwortliche in den Kontrolltechnologien *den* Schlüssel sehen, um weiterhin den Eindruck aufrecht erhalten zu können, sie wären im Stande, die geltende Ordnung gegen das Risiko ihres Verfalls zu versichern. Sicherheit ließe sich demnach in der Risikogesellschaft nicht mehr ohne modernste Technik herstellen und zu jeder Risikopopulation gäbe es die passende technische Methode. Bezogen auf Bürgerrechte, die Nogala als „Abwehrrechte, individuelle Autonomie und Privatheit“[79] versteht, befürchtet er, dass diese auf einen kläglichen Rest zusammenschrumpfen und die sozialen Kontrolltechnologien ein prototypisches, technisch mediatisiertes Verhältnis zwischen den Kontrolleuren und den Kontrollierten verfestigen, bzw. konstituieren.

Einen theoretischen Background liefern die viel zitierten US-amerikanischen Kriminologen Feeley und Simon[80]. Sie konstatieren einen Paradigmenwechsel innerhalb der Strafrechtslehre, der auch den Einsatz technischer Systeme zu erklären vermag: es habe ein Wechsel von der *Old Penology* zur *New Penology* stattgefunden. In der *Old Penology* ging es um das Individuum, um Begriffe wie Schuld, Verantwortung, Intervention und die Behandlung des individuellen Straftäters. Ein Verbrechen zu begehen war ein antisozialer Akt, der eine Reaktion des Staates und der Gesellschaft forderte. In der *New Penology* vollzieht sich eine Umori-

[76] Die Arbeit ist innerhalb der Politologie entstanden, wird aber in dieses Kapitel eingeordnet, da sie hier hinsichtlich der kriminologischen Aspekte bedeutend ist.

[77] Nogala 1998, S. 10

[78] vgl. Nogala 1998, S. 19

[79] vgl. Nogala 1998, S. 321

[80] vgl. Feely / Simon 1994

entierung: Techniken der Identifizierung, Klassifizierung und dem Management von Gruppen nach deren unterschiedlichen Gefährlichkeit stehen im Vordergrund. Kriminalität wird als selbstverständlich angesehen, Abweichungen als normal. Man möchte die Kriminellen nicht verändern und wieder in die Gesellschaft eingliedern, sondern bestimmte Gruppen unter Kontrolle halten, um ein Gefahrenmanagement zu betreiben. In diesem Zusammenhang bietet sich der Einsatz technischer Kontroll- und Überwachungssysteme an. Die Gesellschaft wird durch diese Einteilung in In- und Out-Zonen fragmentiert, statt Integration erfolgt eine Desintegration bestimmter Bevölkerungsgruppen. Das Bild von der Gesellschaft als sozialer Einheit scheint demnach überholt.

1.5 Forschungsleitende Fragestellungen

Die bisher vorliegenden Untersuchungen legen ihren Fokus zumeist auf das Thema Videoüberwachung, lassen jedoch andere Systeme technischer Kontrolle und Überwachung außer Acht. Auch die Perspektive auf die alltägliche Begegnung mit technischen Kontroll- und Überwachungssystemen und den *freiwilligen* Gebrauch solcher Systeme wurde bislang nicht eingenommen. Außerdem wurde übersehen, dass technische Kontroll- und Überwachungssysteme immer stärker auch in erzieherische Domänen eindringen, was von der Pädagogik noch nicht wahrgenommen und reflektiert wurde. Das Forschungsinteresse dieser Arbeit liegt daher auf mehreren Ebenen:

Zum einen wird im theoretischen Teil der Arbeit versucht, einen Überblick über derzeit diskutierte Gesellschaftsmodelle zu geben, die das Moment der Kontrolle und Überwachung[81] zu fassen suchen. Insbesondere wurde nach Erklärungsmodellen gesucht, die erklären:

- Warum sich technische Kontroll- und Überwachungssysteme immer stärker innerhalb der Gesellschaft verbreiten und
- warum es zur wachsenden Nutzung solcher Systeme durch das Individuum selbst kommt.

Da die Diskussion zu Kontrolle und Überwachung international geführt wird, ist es ein Anliegen dieser Arbeit, zumindest einen Ausschnitt der internationalen Diskussion, sofern sie die westlichen Industrieländer betrifft, wiederzugeben. Insbesondere wurde dazu Literatur aus Großbritannien, den USA, Kanada und Frankreich ausgewertet.

[81] Dabei wird in den einzelnen Modellen unterschiedlich stark auf *technische* Kontroll- und Überwachungssysteme eingegangen.

Zum anderen wird im empirischen Teil der Arbeit die Frage gestellt, welche Aufgaben ausgewählte technische Kontroll- und Überwachungssysteme in der alltäglichen Praxis übernehmen.

- In welchen Bereichen des täglichen Lebens kommen die Systeme bereits zum Einsatz und wo werden sie vom Individuum freiwillig eingesetzt?

Innerhalb des empirischen Teils wurde ebenfalls auf internationale Erfahrungen zurückgegriffen, da, wie im Fall Großbritannien, dort bereits eine größere Anzahl empirischer Untersuchungen vorliegen.

Die in Kapitel 4 vorgestellten explorativ angelegten Fallstudien ermöglichen es im Anschluss, ein detaillierteres Bild vom Einsatz technischer Kontroll- und Überwachungssysteme im Alltag zu erhalten. Hier wurde eine Auswahl getroffen, welche die Videoüberwachung im öffentlichen Nahverkehr[82], Datensammlungen mit Hilfe des Payback-Systems und Kinderortungssysteme umfasst. Dadurch werden unterschiedliche gesellschaftliche Bereiche mit exemplarisch ausgewählten Beispielen der technischen Kontrolle und Überwachung untersucht. Die Untersuchungsfelder sind dabei so gewählt, dass die große Bandbreite des heutigen Einsatzes technischer Kontroll- und Überwachungssysteme deutlich wird. Hier interessierte insbesondere:

- Wie stellt sich die jeweilige Technik im Alltag des Durchschnittsbürgers dar?
- Was versprechen sich diejenigen, die diese Technik einsetzen, von diesen Systemen, und welche Ziele verfolgen sie?
- Welche Einstellungen haben die Adressaten der technischen Systeme? Aus welchen Gründen nutzen *sie selbst* die Technik?

Die Leitfragen dieser Arbeit können in folgender Weise nochmals zusammengefasst werden:

- Welche theoretischen Ansätze können zur Erklärung des vielschichtigen Phänomens Technische Kontrolle und Überwachung nutzbar gemacht werden?
- Welche Techniken begegnen uns bereits im Alltag und wie stellen sie sich aus der Sicht der Betreiber und Adressaten der Technik dar?
- Welche Konsequenzen ergeben sich aus den Forschungsergebnissen für eine Pädagogik, die sich einer freiheitlich-demokratischen Grundordnung verpflichtet fühlt?

[82] Diese besondere Form der Videoüberwachung wurde gewählt, da hier vermutet wurde, dass neue Erkenntnisse zum Einsatz der Videotechnik gewonnen werden können.

2 Erklärungsansätze und diskutierte Modelle

Innerhalb dieses Kapitels sollen derzeit diskutierte Modelle[83] zu Kontrolle und Überwachung in der Postmoderne vorgestellt werden. Es existiert in diesem Zusammenhang nicht die *eine* Theorie, doch wird gezeigt werden, dass sich bestimmte Erklärungsmotive durch nahezu alle hier vorgestellten Ansätze hindurch ziehen. Ein Fokus auf technische Kontroll- und Überwachungssysteme wird in den wenigsten Fällen gelegt. Hier haben sich einzig die Ansätze der Surveillance und Maximum Surveillance Society explizit mit den Auswirkungen technischer Systeme beschäftigt.

Zu Beginn werden Ulrich Becks *Risikogesellschaft* und Michel Foucaults Machtanalysen vorgestellt, die in zahlreichen theoretischen Ansätzen aufgegriffen und in Hinblick auf einen veränderten Kontroll- und Überwachungsbegriff weitergeführt und interpretiert werden. Beck und Foucault stehen daher am Anfang der theoretischen Einordnung und bilden deren Hauptbezugspunkte.

Im Anschluss werden die Modelle der Kontroll- und der Sicherheitsgesellschaft vorgestellt, die sich stark aufeinander beziehen und ähnliche Einschätzungen bieten. Als dominierende Ansätze im angloamerikanischen Sprachraum werden danach die bereits erwähnten Perspektiven der Surveillance und Maximum Surveillance Society vorgestellt.

Die vorgestellten Perspektiven werden im Hinblick auf die Fragen, warum sich technische Kontroll- und Überwachungssysteme immer stärker verbreiten und warum immer stärker auch das Individuum selbst die Techniken nutzt, ausgewertet.

[83]Der Begriff *Modell* mag an dieser Stelle etwas irreführend sein, denn teilweise handelt es sich bei den vorgestellten Analysen nicht um ausgearbeitete Gesellschaftsmodelle, sondern um Einschätzungen und Perspektiven, die unter einer bestimmten Überschrift eingenommen werden.

2.1 Andauernder Ausnahmezustand: Die Risikogesellschaft

Die von Ulrich Beck in den 1980er Jahren beschriebene Risikogesellschaft wird in der aktuellen Diskussion um Kontrolle und Überwachung immer wieder aufgegriffen. Der Ansatz der Risikogesellschaft wurde von anderen, auch internationalen Autoren weitergeführt, die im weiteren Verlauf vorgestellt werden.

2.1.1 Die Risikogesellschaft nach Beck

Beck konstatiert, dass es im Übergang von der Klassen- zur Risikogesellschaft, als zwei Typen moderner Gesellschaften, zu einem Wechsel im Wertesystem gekommen ist. Bleiben Klassengesellschaften in ihrer Entwicklungsdynamik auf das Ideal Gleichheit bezogen (z.B. Chancengleichheit), so ist die Risikogesellschaft nicht daran interessiert, das Gute zu erreichen, sondern daran, das Schlechte zu verhindern:

> „Ihr normativer Gegenentwurf, der ihr zugrunde liegt und sie antreibt, ist die *Sicherheit.* An die Stelle des Wertsystems der »ungleichen« Gesellschaft tritt also das Wertsystem der »*unsicheren*« Gesellschaft.“[84]

Während Beck als treibende Kraft der Klassengesellschaft den Satz: „Ich habe Hunger!“ betrachtet, ist die Risikogesellschaft mit der Aussage: „Ich habe Angst!“ zu fassen. Beck postuliert eine Epoche, in der eine Solidarität aus Angst statt einer Solidarität aus Not zu Tage tritt und zu einer politischen Kraft wird.[85] Diese Angst hat sich laut Becks Analyse auf die Zerstörung der Lebensgrundlagen gerichtet, auf die Verschmutzung von Wasser, Luft und Boden. Die Risiken haben sich heute teilweise verlagert. Im Bereich Umweltschutz haben sich einige positive Veränderungen vollzogen; die von Beck aufgestellten Merkmale einer Risikogesellschaft sind aber aktueller denn je. Heute ist der Terrorismus oder einfach nur die Angst vor dem, was passieren *könnte*, das Risiko, das jeden betrifft. Angst hat man heute vor Terror-Anschlägen, vor Einbrüchen oder schlicht vor belästigenden Situationen.

Die Angst vor den Risiken und deren Vermeidung stellen neue Herausforderungen für die Demokratie dar. Aus Becks Sicht enthält die Risikogesellschaft eine Tendenz zu einem *legitimen Totalitarismus der Gefahrenabwehr*, der

---

[84] Beck 2003, S. 65

[85] vgl. Beck 2003, S. 66

> „mit dem Recht, das eine Schlimmste zu verhindern, in nur allzu bekannter Manier das andere Noch-Schlimmere schafft. Die politischen »Nebenwirkungen« der zivilisatorischen »Nebenwirkungen« bedrohen das politisch-demokratische System in seinem Bestand. Es gerät in die ungute Zwickmühle, entweder angesichts der systematisch produzierten Gefahren zu versagen oder aber durch autoritäre, ordnungsstaatliche »Stützpfeiler« demokratische Grundprinzipien außer Kraft zu setzen.“[86]

Eine neue politische Kultur entsteht - die Aufgaben und Möglichkeiten des Staates ändern sich. Allein in den Bereichen der Außen- und Militärpolitik und im Einsatz staatlicher Gewalt für den Erhalt der Inneren Sicherheit behält er sein Monopol, während er sich aus anderen Bereichen zurückzieht.[87]

Schon in den 1980er Jahren skizziert Beck die Risikogesellschaft als eine Gesellschaft, in welcher der Ausnahmezustand zur Regel wird. Einige von Becks Analysen in Bezug auf die Risikogesellschaft sind im Rahmen meines Forschungsthemas von Bedeutung und lassen sich auf die Betrachtung der gesellschaftlichen Bedeutung von technischen Kontroll- und Überwachungssystemen übertragen. Spätestens seit dem 11. September 2001 und den darauf folgenden Gesetzesänderungen[88] gewinnt Becks Aussage an Aktualität:

> „Die Risikogesellschaft ist eine katastrophale Gesellschaft. In ihr droht der Ausnahmezustand zum Normalzustand zu werden.“[89]

Laut Beck läuft die technische Entwicklung am Parlament vorbei. Sie ist so schnell, dass althergebrachte politische Prozesse viel zu langsam sind, als dass sie diese aufhalten könnten. Entscheidungen werden innerhalb der Subpolitik, in ihren Teilarenen der Rechtsprechung, Medienöffentlichkeit, Privatheit, in Bürgerinitiativen und neuen sozialen Bewegungen getroffen. Beck führt aus:

> „Die Gestaltung der Zukunft findet versetzt und verschlüsselt nicht im Parlament, nicht in den politischen Parteien, sondern in den Forschungslabors und Vorstandsetagen statt. Alle anderen – auch die Zuständigsten und Informiertesten in Politik und Wissenschaft – leben mehr oder weniger von den Informationsbrocken, die von den Planungstischen technologischer Subpolitik fallen.“[90]

Becks Ansatz der Risikogesellschaft wurde von mehreren Autoren weitergeführt, von denen die relevanten Arbeiten im Folgenden vorgestellt werden.

---

[86] Beck 2003, S. 106

[87] vgl. Beck 2003, S. 317

[88] Stichwort ist hier das bereits erwähnte „Sicherheitspaket II“

[89] Beck 2003, S. 31

[90] Beck 2003, S. 358

2.1.2 Präventive staatliche Überwachung und neue Formen der Machtausübung

Umgang mit Straftaten in der Risikogesellschaft – ein Paradigmenwechsel

Die Briten Clive Norris und Gary Armstrong heben auf den veränderten Umgang mit Straftaten innerhalb der Risikogesellschaft ab. Hier geht es darum, schon im Vorfeld Straftaten (Risiken) zu verhindern und nicht mehr nur darum, bereits Geschehenes aufzuklären. Die Polizeiarbeit wird *proaktiv* statt *reaktiv,* und auch dort, wo sie reaktiv ist, verlangt sie, dass Informationen zur späteren Risiko-Bewertung gesammelt werden. Ist man als Individuum in die Klassifikationsschemen hineingerutscht und auffällig geworden, wird man ein Kandidat für intensivere technische oder menschliche Überwachung.[91] Bürger werden solange für schuldig gehalten, bis ihr Risikoprofil das Gegenteil belegt. Damit ändert sich das Paradigma der Unschuldsvermutung gegenüber dem Bürger:

> „Everyone is assumed guilty until the risk profile assumes otherwise.“[92]

Die Kanadier Ericson und Haggerty sehen Überwachung als Motor der Risikogesellschaft, welche die notwendigen Informationen bereitstellt. Die Verwendung des Begriffes der *Biomacht* verweist auf Foucault, dessen Theorien noch später aufgegriffen werden.[93]

> „Risk society is fuelled by surveillance, by the routine production of knowledge of populations useful for their administration. Surveillance provides biopower, the power to make biographical profiles of human populations to determine what is probable and possible for them. Surveillance fabricates people around institutionally established norms – risk is always somewhere on the continuum of imprecise normality.“[94]

Devianz hat in der Risikogesellschaft nichts mehr mit Moral zu tun. Sie ist weder schlecht noch verwerflich; sie ist einfach ein existierendes Risiko, mit dem man umgehen muss.[95] Hier spielt Überwachung eine immer größer werdende Rolle. Wissen über die Bevölkerung zu erlangen und zu speichern ist hilfreich, um Risiken abschätzen zu können. Bezogen auf die Kriminalitätskontrolle vertritt der britische Soziologe Stanley Cohen die These, dass nicht mehr nur der Straffällige

---

[91] vgl. Norris / Armstrong 1999, S. 24

[92] vgl. Norris / Armstrong 1999, S. 24

[93] siehe Kapitel 2.5

[94] Ericson / Haggerty 1997, S. 450

[95] vgl. Ericson / Haggerty 1997, S. 39f

selbst verfolgt wird, sondern beispielsweise durch Videokameras ganze Menschengruppen und Räume *präventiv* überwacht werden:

> „In this movement technology and resources, particularly at the hard end, are to be directed to surveillance, prevention and control, not ´tracking` the individual adjusticated offender, but preventive surveillance (through closed circuit television, for example) of people and spaces.“[96]

Die Aufgabe des Staates und neue Formen der Machtausübung

In der Risikogesellschaft ist es die Aufgabe der Regierung, Sicherheit herzustellen. Sicherheit ist dabei als Zustand zu betrachten, in dem bestimmten Gefahren entgegengewirkt wird oder diese minimiert werden. Das Bedürfnis nach Sicherheit führt zu einem immer größer werdenden Verlangen nach Wissen über die vorhandenen Risiken. Dabei entsteht das Paradox, dass durch den Versuch, immer mehr Wissen über Risiken zu erhalten, wieder neue Risiken entstehen – beispielsweise das Problem, wer die Kontrolleure kontrolliert.

Die Risikogesellschaft ist von einer negativen Logik geprägt, das Augenmerk wird auf die Gefahren gelegt und auf den Zweifel, dass diesen Gefahren angemessen begegnet werden kann. Vor diesem Hintergrund ist das Ziel, immer bessere Technologien des Risikomanagements zu finden, die helfen, mit Angst und Unsicherheit besser umgehen zu können. Es entstehen neue Formen der Machtausübung. Da die Ausnahmesituation die Norm wird, entwickeln sich Formen der Überwachung, die bisher undenkbar waren. Den Risiken soll mit rationalen Methoden, technischen Lösungen und mit Wissen über sie begegnet werden. Dieses Wissen birgt, wie schon angesprochen, wieder neue Risiken. Der Blick in die Zukunft ist dabei wichtiger als die Vergangenheit oder die Gegenwart. Wir handeln heute, um möglichen Risiken der Zukunft zu begegnen.[97]

2.1.3 Zusammenfassung

Der normative Entwurf der Risikogesellschaft ist die *Sicherheit*. Die *Angst* wird zum verbindenden Element der Risikogesellschaft. Dabei ist der Blick in die Zukunft gerichtet: Es muss Vorsorge getroffen werden für das, was passieren *könnte*. Die Arbeit der Polizei, die Einstellung zum Bürger ändern sich: Der Bürger wird zum *potenziell* Verdächtigen. Das Interesse des Staates oder anderer Institutionen, möglichst viele Daten über seine Bürger zu sammeln, wird so ver-

---

[96] Cohen 1985, S. 127

[97] vgl. Ericson / Haggerty 1997, S. 87

ständlich. Die Risikogesellschaft bedingt automatisch eine Überwachung der Bevölkerung, um potenzielle Risiken bereits im Vorfeld ermitteln zu können.

Diese Zusammenhänge verdeutlichen den Nutzen, den technische Kontroll- und Überwachungssysteme im Rahmen einer Risikogesellschaft haben und erklären, warum sie gerade in den letzten Jahren und stärker auch nach dem 11. September 2001 verstärkt zum Einsatz kommen. Die Transparenz jedes Einzelnen soll die Sicherheit innerhalb der Gesellschaft erhöhen.

Ein interessanter Gesichtspunkt dieses Ansatzes ist, dass Überwachung als Teil eines Risiko-Managements selbst wiederum Risiken hervorbringt. Als Beispiel wäre hier der Eingriff in bürgerliche Grundrechte, beispielsweise in die Informationelle Selbstbestimmung, zu nennen. Für eine pädagogische Diskussion des Themas sei hier ein Hinweis auf die Politische Bildung gegeben, die sich des Themas Demokratie im Spannungsfeld der Überwachung annehmen müsste.

Die Risikogesellschaft befindet sich stets nahe einer Katastrophe. Sie ist eine Gesellschaft, in welcher der Ausnahmezustand zum Normalzustand wird. Der Staat zieht sich – konform mit den derzeit neoliberalen Strömungen - aus vielen gesellschaftlichen Bereichen zurück und legitimiert sich durch die von ihm postulierte Herstellung bzw. Erhaltung der Inneren Sicherheit. Dabei werden vielfach demokratische Grundprinzipien zugunsten der Gefahrenabwehr ausgehebelt. Dieser Umstand muss diskutiert und pädagogisch aufbereitet werden.

2.2 Spannungsfeld der Macht: Das Konzept der Gouvernementalität

Michel Foucault greift innerhalb seiner Machtanalysen ebenfalls den Aspekt der Sicherheit als zentralen Bezugspunkt auf. Seine Analysen werden in der aktuellen Diskussion – ebenso wie die Ulrich Becks - immer wieder aufgegriffen und im folgenden in Bezug auf die Frage, warum die Individuen *selbst* technische Überwachungs- und Kontrollsysteme verwenden und sich vielfach bereitwillig in Überwachungs- und Kontrollsituationen begeben, diskutiert. Wie Foucault in einer seiner Vorlesungen am Collège de France zum Thema „Geschichte der Gouvernementalität“ formulierte:

> „[…] die Analyse dieser Machtbeziehungen kann sich gewiß zu etwas wie einer globalen Analyse der Gesellschaft öffnen, diese in Gang bringen.“[98]

Die Tatsache, dass Foucaults Analysen immer wieder in Theorien und Entwürfen zum Thema Kontrolle und Überwachung aufgegriffen werden, bestätigt Foucaults

[98] Foucault 2004, S. 15

Einschätzung. Dennoch ist eine Auseinandersetzung mit ihm nicht unproblematisch, da er in seinem Werk keine ausgearbeitete Theorie liefert, sondern bestimmte gesellschaftliche Aspekte herausgreift und Werkzeuge zur Analyse dieser Aspekte anbietet. Dabei ist seine Betrachtung nicht stringent und es kommt durchaus vor, dass er sich widerspricht oder Dinge im Nachhinein re-interpretiert. Dies zeigt sich beispielsweise in der Äußerung, dass Inhalt seiner Arbeit nicht die Analyse von Machtphänomenen gewesen sei, sondern dass es ihm darum gegangen sei:

> „eine Geschichte der verschiedenen Verfahren zu entwerfen, durch die in unserer Kultur Menschen zu Subjekten gemacht werden.“[99]

Das Subjekt und nicht die Macht ist nach Foucaults eigenen Angaben das allgemeine Thema seiner Forschung, für ihn wird das Subjekt erst innerhalb komplexer Machtverhältnisse konstituiert. Diese Äußerung Foucaults wird in der Fachliteratur eher kritisch gesehen und als nachträgliche Interpretation gedeutet.[100]

Im folgenden Kapitel wird die Machtanalyse Michel Foucaults im Hinblick auf das Forschungsthema dargestellt. Um den Gedanken Foucaults folgen zu können, wird an dieser Stelle etwas weiter ausgeholt, um mit der Terminologie Foucaults vertraut zu werden und Missverständnisse zu vermeiden. Insbesondere wird hier auf die Begriffe der Souveränitäts-, Disziplinar- und Biomacht eingegangen und Neologismen Foucaults erörtert. Zu Beginn wird eine allgemeine Einführung in seine Machtanalyse vorgenommen.

2.2.1 Die Machtanalyse Foucaults

Ausgangspunkt meiner Betrachtungen der Machtanalyse Foucaults sind die Werke *Überwachen und Strafen* und *Der Wille zum Wissen*, die dann in Vorlesungen[101] weiterentwickelt wurden, die Foucault 1978/79 am Collège de France zur *Gouvernementalität* hielt. Hatte Foucault noch Anfang der 70er Jahre eine zunehmende Disziplinierung der Gesellschaft diagnostiziert, so stellt er in den erwähnten Vorlesungen fest, dass sich die Mechanismen der Macht von den juridischen, also denen mit Rechtsbegriffen wie Gesetz, Verbot, Zwang operie-

---

[99] Foucault 1994b, S. 243

[100] Judith Butler meint beispielsweise dazu: „Nun können wir uns fragen, ob Foucault hier die Wahrheit über das Ziel seiner Arbeit in den vergangenen zwanzig Jahren sagt. Vielleicht scheint es ihm nach diesen zwanzig Jahren von etwa 1961 bis 1981 auch nur so, daß dies immer sein Ziel gewesen sei, und die Eule der Minerva fliegt hier erst in der Dämmerung. Dies nach zwanzig Jahren zu glauben und zu schreiben, ist natürlich nicht ganz dasselbe wie dieses Ziel tatsächlich zwanzig Jahre lang vor Augen gehabt zu haben.“ Butler 2003, S. 59

[101] vgl. Foucault 2004 a und 2004 b

renden, über die Disziplinar- hin zu Sicherheitsmechanismen verschieben. Nach Foucault leben wir heute weniger in einem Rechtsstaat oder einer Disziplinargesellschaft als in einer Sicherheitsgesellschaft, in der juridische und disziplinäre Mechanismen zunehmend durch Dispositive der Sicherheit erschlossen werden.[102] Unter Dispositiven versteht Foucault heterogene Praktiken, die sowohl Diskurse, Institutionen, architektonische Vorrichtungen, Regulierungen, Gesetze, Verwaltungsmaßnahmen oder auch wissenschaftliche Aussagen umfassen. Ausgehend von diesen Bestandteilen versucht Foucault ein Muster flexibler Beziehungen festzulegen und sie in einem einzigen Apparat zu verschmelzen, um ein besonderes, historisches Problem freizulegen. Dieser Apparat verbindet Macht und Wissen in einem spezifischen Analyseraster.

Foucault sieht die Entwicklung nicht als Endpunkt, bei der eine Gesellschaft der Souveränität durch eine Disziplinargesellschaft und diese wiederum durch eine Gesellschaft der Gouvernementalität abgelöst wurde, sondern es handelt sich aus seiner Sicht um das Spannungsfeld: Souveränität - Disziplin - Gouvernementalität, dessen Hauptzielscheibe die Bevölkerung ist und dessen wesentliche Mechanismen die Dispositive der Sicherheit sind.

Im Folgenden werden Foucaults Darstellung der Souveränität, die Disziplinarmacht und im Anschluss den Begriff der Gouvernementalität erörtert.

Souveränitäts-, Disziplinar- und Biomacht

Die Entwicklung von der Souveränitäts- zur Disziplinarmacht ist von Foucault in *Überwachen und Strafen*[103] dargestellt worden. Er führt seine Machtanalyse in dem kurz darauf erscheinenden Werk *Der Wille zum Wissen*[104] weiter, in dem er die Disziplinarmacht in das weiterreichende Konzept der Bio-Macht einordnet.

In der feudalen Gesellschaftsordnung ist der Souverän Herr über den Tod. Er kann seine Macht durch Strafen, Folter oder Hinrichtungen demonstrieren und Menschenleben auslöschen. Diese Demonstration der Macht findet zumeist in der Öffentlichkeit zur Abschreckung statt, sie ist aber gekoppelt an die Verteidigung des Souveräns und seines Überlebens und stellt sich nicht als absolutes und bedingungsloses Recht dar. In der feudalen Gesellschaft drückt der Souverän ferner seine Macht über den Frondienst aus, den die Untertanen leisten müssen. Die politische Struktur ist durch definierte Dienste und Verpflichtungen bestimmt. Sie funktionierte vor allem in der Form der Abschöpfung - dem Entzug von Gütern und Produkten:

---

[102] vgl. Lemke 2003, S. 191

[103] vgl. Foucault 1994a

[104] Foucault 1983

> „Die Macht war vor allem Zugriffsrecht auf die Dinge, die Zeiten, die Körper und schließlich das Leben; sie gipfelte in dem Vorrecht, sich des Lebens zu bemächtigen, um es auszulöschen.“[105]

Foucault stellt im Verlauf seiner Arbeit die Negativität der Souveränitätsmacht der Produktivität der Disziplinarmechanismen gegenüber und beschreibt in diesem Zusammenhang auch eine Veränderung der *Strafe*, von der Marter hin zum Gefängnis, als charakteristisches Merkmal der Disziplinargesellschaft. In diesem Zusammenhang beschreibt Foucault das Modell des Panoptikums von Jeremy Bentham aus dem Jahr 1791.[106] Das Panoptikum ist der Entwurf eines Gefängnisses, in dessen Mitte ein Turm steht, von dem aus ein für die Gefangenen nicht sichtbarer Aufseher seinen Dienst leistet. Die Gefangenen können nicht wissen, wann und ob sie überwacht werden. Konformität ist der einzige Ausweg aus dem Dilemma. Für Foucault ist die Hauptwirkung des Panoptikums folgende:

> „die Schaffung eines bewußten und permanenten Sichtbarkeitszustandes beim Gefangenen, der das automatische Funktionieren der Macht sicherstellt. Die Wirkung der Überwachung ist permanent, auch wenn ihre Durchführung sporadisch ist [...]“[107]

Foucault führt aus, dass, wann immer man es mit einer Vielfalt von Individuen zu tun hat, denen man eine Aufgabe oder ein Verhalten aufzwingen möchte, das panoptische Schema Anwendung finden kann.[108] Auch in der aktuellen Diskussion werden moderne Überwachungssysteme wie die Videoüberwachung mit dem Panoptikum verglichen.

Die Disziplinarmacht entfaltet ihre Wirkung gezielt auf die Individuen und ihre Körper. Anstelle des Prinzips von Gewalt und Beraubung der Souveränitätsmacht setzen die Disziplinen das Prinzip von Milde, Produktion, Profit:

> „Die Disziplinen sind Techniken, die gemäß diesem Prinzip die Vielfältigkeit der Menschen und die Vervielfachung der Produktionsapparate in Übereinstimmung bringen.“[109]

Die Menschen werden in der Disziplinargesellschaft von einem Einschließungsmilieu in das nächste überführt. Als Einschließungsmilieu bezeichnet Foucault beispielsweise Institutionen wie das Militär, die Schule oder die Fabrik. Die Normierung und Normalisierung des Individuums steht dabei im Mittelpunkt. Zent-

---

[105] Foucault 1983, S.162

[106] vgl. Foucault 1994a, S. 256ff

[107] Foucault 1994a, S. 258

[108] vgl. Foucault 1994a S. 264

[109] Foucault 1994a, S. 281

rum der Betrachtung ist der gefügige, disziplinierte und dadurch produktive Körper. Der menschliche Körper geht dabei in eine Machtmaschinerie ein, die ihn durchdringt und arbeiten lässt, wie es gerade benötigt wird. [110]

Ein weiterer interessanter Aspekt ist die Feststellung Foucaults, dass Menschen zum Zwecke ihrer besseren Kontrolle und Beherrschung zu *Subjekten* gemacht werden. Lange Zeit war dies Privileg der Herrschenden, die sich in Chroniken darstellen ließen und die Geschichtsschreibung ihrer Existenz zu den Ritualen der Macht zählten:

> „Betrachtet werden, beobachtet werden, erzählt werden und Tag für Tag aufgezeichnet werden waren Privilegien. Die Chronik eines Menschen, die Erzählung seines Lebens, die Geschichtsschreibung seiner Existenz gehörten zu den Ritualen seiner Macht. Die Disziplinarprozeduren nun kehren dieses Verhältnis um, sie setzen die Schwelle der beschreibbaren Individualität herab und machen aus der Beschreibung ein Mittel der Kontrolle und eine Methode der Beherrschung.“[111]

In *Der Wille zum Wissen* unterscheidet Foucault neben dem Recht des Souveräns und den Mechanismen der Disziplin nun eine dritte Machtform: die der Bio-Macht. Die Disziplin wird nun in diese umfassendere politische Technologie eingeordnet, die sich nicht nur auf die Dressur des Körpers, sondern gleichsam auf eine Kontrolle der Bevölkerung richtet.[112]

Seit dem 17. Jahrhundert kommt es zu einer Verschiebung in der Ausübung der Macht: Die Macht über den *Tod*, ausgeübt durch den Souverän, wird von einer Machtform überlagert, deren Ziel es ist, das *Leben* zu verwalten, zu sichern, zu entwickeln und zu bewirtschaften. Die neue Macht ist dazu bestimmt, Kräfte hervorzubringen, wachsen zu lassen und zu ordnen, anstatt sie zu hemmen oder zu vernichten. Statt Macht über den Tod herrscht die Macht nun über das Leben, sie ist eine *Bio-Macht*. Die Körper werden sorgfältig verwaltet, das Leben rechnerisch geplant, Techniken zur Unterwerfung der Körper und zur Kontrolle der Bevölkerung werden ins Leben gerufen. [113]

Regulierung und Kontrolle sind die hauptsächlichen Instrumente, welche die Bio-Politik zur Anwendung bringt. Es handelt sich nicht um eine Disziplinartechnologie, sondern um eine *Sicherheitstechnologie*, die nach so etwas wie der Sicherheit des Ganzen hinsichtlich der ihm innewohnenden Gefahren strebt und zwar nicht

---

[110] vgl. Foucault 1994a, S. 176

[111] Foucault 1994a S. 246/247

[112] vgl. Lemke 2003, S. 134

[113] Foucault 1983, S. 167

durch Dressuren des Individuums, sondern durch ein allgemeines Gleichgewicht; Ziel ist nicht mehr nur das einzelne Individuum, sondern die *Bevölkerung*.[114]

> „Eine Macht aber, die das Leben zu sichern hat, bedarf fortlaufender, regulierender und korrigierender Mechanismen. Es geht nicht mehr darum, auf dem Feld der Souveränität den Tod auszuspielen, sondern das Lebende in einem Bereich von Wert und Nutzen zu organisieren.“[115]

Auch in der aktuellen politischen Diskussion findet Foucaults Konzept der Biomacht Erwähnung. In dem in 2002 erschienenen[116] und auch in der deutschen Linken lebhaft diskutierten Werk „Empire“ greifen die Autoren Negri und Hardt die Analysen Foucaults auf und diskutieren sie unter der Überschrift von Deleuzes *Kontrollgesellschaft*. An dieser Stelle wird deutlich, dass Begriffe wie Kontroll-, Sicherheits- oder Disziplinargesellschaft nahezu beliebig verwendet und kombiniert werden und keine ausgearbeitete Theorie zugrunde liegt, derer man sich zur Erklärung von Kontrolle und Überwachung bedienen könnte. Auch Foucault bietet diese *eine* Theorie nicht an, sondern widmet sich der Analyse einzelner Phänomene. Negri und Hardt kommen in ihrer Veröffentlichung zu dem Schluss, dass Kriterien der sozialen In- und Exklusion von den Subjekten zunehmend verinnerlicht werden. Die Macht wirkt, nach Negri und Hardt, durch Kommunikations- und Informationssysteme direkt auf die Gehirne. Die Körper werden innerhalb wohlfahrtsstaatlicher Systeme und überwachter Beschäftigung hin zu einem Status der Entfremdung vom Lebenssinn und der Entfremdung vom Wunsch nach Kreativität bewegt. Die Normalisierung als Mittel der Disziplinierung findet immer noch statt, allerdings innerhalb flexibler - und sich ständig verändernder Netzwerke.[117] Das Leben selbst ist Objekt der Macht geworden, es wird verwaltet und kontrolliert. Hardt und Negri sehen den Unterschied zwischen der Disziplinar- und der Kontrollgesellschaft darin, dass in der Disziplinargesellschaft Individuen in Institutionen eingeschlossen wurden; ihre Produktionskraft konnte nicht vollständig abgeschöpft werden. Das Verhältnis zwischen der Macht und dem Individuum blieb statisch. In der von den Autoren beschriebenen Kontrollgesellschaft mit ihren biopolitischen Machtstrukturen sieht das anders aus:

---

[114] vgl. Lemke 2003, S. 136

[115] Foucault 1983, S. 171

[116] Das Erscheinungsjahr der deutschen Übersetzung.

[117] vgl. Hardt / Negri 2000, S. 23

> „[…] when power becomes entirely biopolitical, the whole social body is comprised by power's machine and developed in its virtuality. This relationship is open, qualitative, and affective. Society, subsumed within a power that reaches down to the ganglia of the social structure and its processes of development, reacts like a single body. Power is thus expressed as a control that extends throughout the depths of the consciousnesses and bodies of the population- and at the same time across the entirety of social relations."[118]

Negri und Hardt beschreiben im Prinzip Foucaults Konzept der Biomacht, von der die Disziplinarmacht ein Teil ist. Warum sie das Konzept mit dem von Deleuze geprägten Begriff der Kontrollgesellschaft betiteln, bleibt unklar. Interessant wäre es gewesen, einen Schritt weiter zu gehen und den von Foucault entworfenen Neologismus der Gouvernementalität näher zu betrachten, der weitere Analysen der heutigen Ausübung der Macht zulässt. Dies möchte ich an dieser Stelle tun.

Gouvernementalität

Das 18. Jahrhundert markiert mit dem Auftreten des Liberalismus für Foucault den Beginn des Zeitalters der Gouvernementalität[119], in dem sich der moderne Regierungsstaat formiert und mit ihm ein Machttypus der gouvernementalen Führung, der sich von der Souveränität und der Disziplin unterscheidet.

Das von Foucault entworfene Konzept der Gouvernementalität ist fragmentarisch geblieben. Es geht auf die bereits erwähnten Vorlesungen zurück, die er im Jahr 1978 am Collège de France zu halten begann. Die Reihe, die er zuerst mit „Genealogie des modernen Staates" betitelte, wird von ihm schließlich in „Geschichte der Gouvernementalität" umbenannt. Im Mittelpunkt der Vorlesungsreihe stand die Frage, ob *Regierung* eine allgemeine Machttechnologie repräsentiert, die den Staat so einschließt, wie die Disziplin das Gefängnis einschließt; ob Regierung für den Staat das ist, was die Techniken der Einsperrung, Trennung etc. für die Institution Krankenhaus, Gefängnis etc. sind.[120] Das Konzept der Gouvernementalität wurde vor allem im angloamerikanischen Sprachraum weiterentwickelt, in den letzten Jahren aber auch zunehmend im deutschsprachigen Raum diskutiert. In diesem Zusammenhang ist von der „Ökonomisierung des Sozialen"[121], der „Kriminalität der Gesellschaft"[122] oder der Gouvernementalität als „Sozialwissenschaftliches Konzept"[123] die Rede. Da diese Veröffentlichungen bereits eine

---

[118] vgl. Hardt / Negri 200, S. 24

[119] Foucault 2000, S. 65

[120] vgl. Lemke 2003, S. 146

[121] Bröckling u.a. 2000

[122] Krasmann 2003

[123] Pieper u.a. 2003

Interpretation und Weiterführung Foucaults darstellen, möchte ich mich zu Beginn hauptsächlich auf Foucault selbst beziehen und im Anschluss daran die derzeitige deutschsprachige Diskussion vorstellen. Foucault gebraucht den Begriff der Gouvernementalität in dreierlei Weise:

> „Unter Gouvernementalität verstehe ich die Gesamtheit, gebildet aus den Institutionen, den Verfahren, Analysen und Reflexionen, den Berechnungen und den Taktiken, die es gestatten, diese recht spezifische und doch komplexe Form der Macht auszuüben, die als Hauptzielscheibe die Bevölkerung, als Hauptwissensform die politische Ökonomie und als wesentliches technisches Instrument die Sicherheitsdispositive hat."[124]

Ferner versteht er unter Gouvernementalität die Tendenz, die dem Machttyp der *Regierung* im gesamten Abendland zur Vorrangstellung gegenüber der Souveränität und der Disziplin verholfen hat. Und in seiner dritten Bedeutungsausprägung solle, so Foucault, Gouvernementalität als Ergebnis des Vorgangs betrachtet werden, durch den sich der Gerechtigkeitsstaat des Mittelalters, der sich im 15. und 16. Jahrhundert zum Verwaltungsstaat entwickelte, Schritt für Schritt gouvernementalisiert hat.[125]

Die Gouvernementalität sei das Phänomen gewesen, so meint Foucault, dass es dem Staat ermöglicht hat zu überleben:

> „Denn eben die Taktiken des Regierens gestatten es, zu jedem Zeitpunkt zu bestimmen, was in die Zuständigkeit des Staates gehört und was nicht in die Zuständigkeit des Staates gehört, was öffentlich ist und was privat ist, was staatlich ist und was nicht staatlich ist."[126]

Ein solcher Regierungsstaat, der sich wesentlich auf die Bevölkerung stützt und sich auf die Instrumente des ökonomischen Wissens beruft, entspricht nach Foucault einer durch Sicherheitsdispositive kontrollierten Gesellschaft.[127]

Historisch betrachtet formierte sich der moderne Regierungsstaat mit dem Liberalismus des 18. Jahrhunderts; es kam zu einer Veränderung des Regierungsdenkens: Die *Freiheit* des Individuums nahm einen wichtigen Platz ein, eine komplexe Beziehung zwischen Freiheit und Sicherheit entstand. Die neue Regierungskunst bezog sich nicht mehr ausschließlich auf eine Maximierung der Kräfte des Staates, sondern zielte auf eine ökonomische Regierung. Das Prinzip der Weniger-Regierung ist kein quantitatives Phänomen, sondern deutet auf eine *fundamentale Veränderung* der Machtmechanismen hin. Die neu entstandenen

---

[124] Foucault 2000, S. 64

[125] vgl. Foucault 2000, S. 65

[126] Foucault 2000, S. 66

[127] vgl. Foucault 2000, S. 66

Formen der Macht unterschieden sich sowohl vom Recht der Souveränität als auch von den Disziplinartechnologien. Mit den liberalen Freiheiten etablierten sich auch Dispositive der Sicherheit, die einen bestimmten Gebrauch der Freiheit gewährleisten sollten.

Bei der Disziplinartechnologie wurden hierarchisierende Trennungen installiert, die zwischen Normalem und Anormalem, Geeignetem und Ungeeignetem unterschieden. Dabei wurde ein Optimum entworfen, an dem sich das Individuum auszurichten und anzupassen hatte. Die so genannte Sicherheitstechnologie repräsentiert das Gegenteil des Disziplinarsystems. Statt die Realität an einem Soll auszurichten, nimmt die Sicherheitstechnologie die Realität selbst als Norm und spezifiziert einen Mittelwert innerhalb einer Bandbreite von Variationen.[128]

Die liberale Regierungskunst funktionierte nur über die Garantie der Freiheit, es war allerdings nötig, der Freiheit der Subjekte eine bestimmte Form zu geben. Der Liberalismus organisierte daher die Bedingungen, unter denen die Individuen frei sein konnten, er stellte die Freiheit her. Diese Freiheit war aber fragil und unablässig bedroht und wurde damit zur Grundlage immer neuer Interventionen.[129] Die liberale Freiheit musste daher eingeschränkt werden und wurde unter das Kalkül der Sicherheit gestellt. Das Sicherheitsdispositiv hatte eine entscheidende Rolle, um die kollektive Imagination von Risiken und deren Abwehr zu produzieren.[130]

Dies lässt sich auch auf die heutige, von vielen als *neoliberal* bezeichnete Regierungsform übertragen. Der derzeitige Abbau des Wohlfahrtsstaates lässt sich, so Donzelot[131], nicht als Rückkehr zur frühliberalen Politik deuten, sondern stellt ein Umkodieren der Sicherheitspolitik dar, was die Entwicklung von interventionistischen Technologien ermöglicht, welche Individuen führen und anleiten, ohne für sie verantwortlich zu sein.[132]

---

[128] vgl. Bröckling u.a. 2000, S. 13f

[129] vgl. Lemke 2003, S. 184ff

[130] vgl. Pieper 2003, S. 11/12

[131] vgl. Donzelot 1995, S. 54ff

[132] Das Spannungsverhältnis zwischen dem Sozialen und dem Ökonomischen wird aufgehoben. Im Neoliberalismus werden die Individuen dazu ermutigt, ihrer Existenz eine bestimmte unternehmerische Form zu geben. Der Neoliberalismus reagiert damit auf eine verstärkte Nachfrage nach individuellen Gestaltungsspielräumen und Autonomiebestrebungen mit einem Angebot an Individuen und Kollektive, sich aktiv an der Lösung von bestimmten Problemen zu beteiligen, die bis dahin in die Zuständigkeit von spezialisierten Staatsapparaten fielen. Der Preis ist, dass sie selbst die Verantwortung für ihre Aktivitäten und ihr Scheitern übernehmen müssen. Die Konzeption des *sozialen Risikos* wird somit grundlegend verändert. Sie geht weg von der kollektiven Verantwortung (das alte Versicherungs-Modell) hin zu einer Betonung der bürgerlichen Pflicht des Einzelnen, die Schwere des Risikos, das er für die Gesellschaft darstellt, abzumildern. Das Subjekt ist gehalten, mehr Verantwortung für sich selbst zu übernehmen. Prinzipiell kann alles gesellschaftlich ausgehandelt werden, wenn es sich auf den Boden des Kosten-Nutzen-Kalküls bewegt (vgl. Donzelot 1995, S. 54ff).

Die neoliberalen Freiheiten ermöglichen, konstatiert Robert Castel, neue ökonomische Formen der Kontrolle, die jenseits autoritärer Repression oder wohlfahrtsstaatlicher Integration liegen. Deren Logik war es, mit bürokratischen Mitteln ein Maximum an Menschen zu erreichen, nun steht die Maximierung des Nutzens an erster Stelle. Die unerwünschten Elemente werden so nicht mehr von der Gesellschaft getrennt oder durch korrektive oder therapeutische Eingriffe re-integriert, ihnen werden vielmehr soziale Schicksale zugewiesen, die mit ihrer Fähigkeit im Einklang stehen, den Erfordernissen des Wettbewerbs und des Profits standzuhalten.[133] Diese Feststellungen werden auch im folgenden unter der Überschrift der Kontroll- und Sicherheitsgesellschaft getroffen und im Ansatz der Surveillance und Maximum Surveillance Society in Hinblick auf die Möglichkeiten der Computertechnologie erweitert. Hier wird erneut die Bedeutung von Foucaults Gouvernementalitätsbegriff für die aktuelle Diskussion des Themas deutlich.

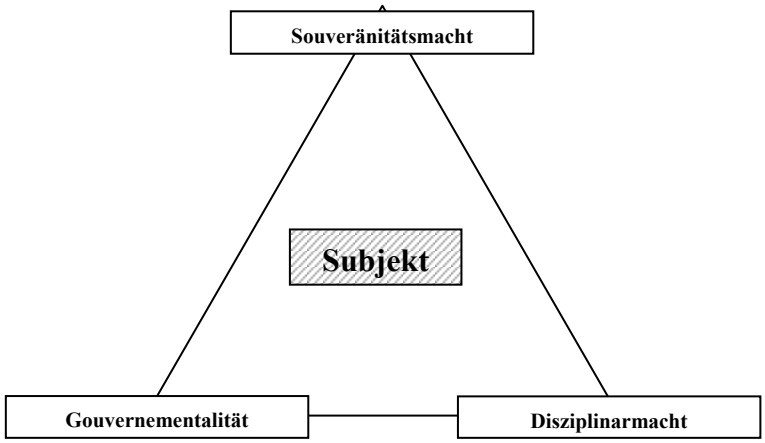
Krasmann fasst die Quintessenz der Gouvernementalität noch einmal treffend zusammen: Gouvernementalität bezeichnet einen Mechanismus des „Regierens aus Distanz“. Unter dem Leitprinzip der *Sicherheit* im Verbund mit Techniken permanenter Überprüfung, Kalkulation und statistischer Berechnung zielt diese Regierungsmentalität einerseits auf Gruppen, auf die Regulation bestimmter Populationen; andererseits auf Individuen, die mittels Techniken der Selbstbefragung und des *Verantwortlichmachens* gelenkt werden, so dass durch Anreiz oder Sorge Aktivität hervorgerufen wird. Beim Einzelnen kann sich dies in einer Besorgnis mit Blick auf eine risikobehaftete Zukunft äußern und in eine daraus hervorgehenden aktiven Selbstsorge münden, die um die Bewältigung entsprechender Unwägbarkeiten bemüht ist.[134]

[133] vgl. Castel 1991, S. 293-296

[134] Krasmann 1999, S. 109

2.2.2 Zusammenfassung

Nach Foucault leben wir in einer Sicherheitsgesellschaft, in der das Subjekt innerhalb komplexer Machtverhältnisse steht. Es befindet sich im Spannungsfeld der Machtformen Souveränitäts-, Disziplinarmacht und Gouvernementalität.



Obwohl Foucault sehr wohl eine historische Betrachtung der Machtformen vornimmt, sieht er die Gouvernementalität nicht als Endpunkt einer Entwicklung, sondern betrachtet das Subjekt im Spannungsfeld der von ihm beschriebenen Machttypen, die auf es mit den Dispositiven der Sicherheit wirken. Die Souveränitätsmacht ist in diesem Zusammenhang natürlich in ihrer aktuellen Form zu betrachten; hier geht es nicht mehr um die Macht des Souveräns über Leben und Tod seiner Untertanen. Aspekte der alten feudalen Macht sind aber dennoch, beispielsweise in der *Abschöpfung*, dem Entzug von Gütern und Produkten durch den „Mächtigeren“ - vielleicht den Arbeitgeber - zu erkennen. Die Disziplinarmacht wird heute beispielsweise innerhalb des Panoptikums deutlich, in dem die Wirkung der Macht permanent ist, auch wenn die Durchführung nur sporadisch ist. Hier wird an vielen Stellen ein Vergleich mit der Videoüberwachung gezogen, die zu Verhaltensanpassungen führen kann, da man ja gefilmt werden *könnte*. Dennoch lässt sich sagen, dass Disziplinartechnologien zunehmend durch Sicherheitstechnologien abgelöst werden, die den Bedingungen der Postmoderne angemessener sind und auch, wie im empirischen Teil der Arbeit deutlich werden wird, innerhalb der Erziehung ihren Platz einnehmen. Hat Krasmann die Gouvernementalität als „Regieren aus Distanz“ [135] bezeichnet, so scheint es auch in der Erziehung einen Trend weg von der Disziplinierung hin zu einem „Erziehen aus Distanz“ - eben mit Hilfe technischer Kontroll- und Überwachungssysteme - zu geben.

[135] vgl. Krasmann 1999, S. 109

Im Hinblick auf den modernen Regierungsstaat lässt sich zusammenfassen, dass dieser höchst flexibel ist, er *führt* die Bevölkerung und beruft sich dabei auf die Instrumente ökonomischen Wissens. Er stellt nach Foucault eine durch „die Sicherheitsdispositive kontrollierte Gesellschaft“[136] dar. Die Flexibilität zeigt sich auch darin, die Zuständigkeiten des Staates flexibel zu interpretieren und zu jedem Zeitpunkt zu bestimmen, was in die Zuständigkeit des Staates gehört, was öffentlich und privat, was staatlich und was nicht staatlich ist. Gerade in Hinblick auf die immer weiter fortschreitende Sammlung von Daten und die Möglichkeit ihrer Vernetzung innerhalb von Großrechnern ist dies ein Aspekt, den man gerade mit Blick auf die Entwicklung der Demokratie nicht aus dem Auge verlieren darf.

Die Sicherheitstechnologien gewinnen an Bedeutung und sind dominanter Mechanismus des Zeitalters der Gouvernementalität. Sie dienen letztlich dazu, die Bevölkerung zu kontrollieren, einen bestimmten Gebrauch von Freiheit zu garantieren und eine kollektive Imagination von Risiken und deren Abwehr zu produzieren. Hier schließt sich der Kreis zu Beck und seiner Analyse der Risikogesellschaft, in der die Sicherheit zum normativen Entwurf der Gesellschaft wird und ein *legitimer Totalitarismus der Gefahrenabwehr* zu entstehen droht. Aus dem Blickwinkel der Gouvernementalität werden unter dem Leitprinzip der Sicherheit im Verbund mit Techniken permanenter Überprüfung, Kalkulation und statistischer Berechnung Subjekte gelenkt und geführt. Das Subjekt *selber* ist angehalten, Verantwortung zu übernehmen und sich selbst an der Produktion von Sicherheit zu beteiligen. In den Wirkweisen der Gouvernementalität ist also *ein* Grund darin zu sehen, warum das Subjekt *selbst* auf technische Kontroll- und Überwachungssysteme zurückgreift.

2.3 Permanente Modulation: Die Kontrollgesellschaft

Beim Ansatz der Kontrollgesellschaft, der auf den französischen Philosophen Gilles Deleuze zurückgeht, handelt es sich um keine vollständige Gesellschaftstheorie, sondern um einen Begriff, der von verschiedenen Autoren aufgegriffen und mit unterschiedlichen Bedeutungen versehen wurde. Auch Aspekte der Risikogesellschaft finden sich in diesem Ansatz wieder. Im Folgenden werden zuerst die Ausführungen von Deleuze vorgestellt, um dann auf weiterführende Darstellungen einzugehen.

[136] Foucault 2000, S. 66

2.3.1 Die Kontrollgesellschaft nach Deleuze

Gilles Deleuze prägte 1990 den Begriff der Kontrollgesellschaft in seinem kurzen Text „Postskriptum über die Kontrollgesellschaften". Deleuze schrieb darin:

> „Wir treten ein in Kontrollgesellschaften, die nicht mehr durch Internierung funktionieren, sondern durch unablässige Kontrolle und unmittelbare Kommunikation."[137]

Die Kontrollgesellschaft löst die von Foucault beschriebene Disziplinargesellschaft ab, die von ca. 1800 bis in das 20. Jahrhundert hinein reicht[138] und in der das Individuum von einem Einschließungsmilieu[139] in das nächste gereicht wurde. Deleuze vergleicht die Einschließungsmilieus der Disziplinargesellschaft mit Gussformen; die Kontrollen bezeichnet er dagegen als Modulationen, die sich von einem Augenblick zum nächsten verändern. *Modulation* ist eigentlich ein Begriff, der aus der Musiktheorie kommt und den Übergang von einer Tonart in eine andere meint. Dabei bleibt die Melodie dieselbe, nur die Tonart ändert sich. Deleuze und andere Autoren haben sich dieses Begriffs bedient, um den Anspruch an den Menschen zu verdeutlichen, sich innerhalb einer Kontrollgesellschaft immer wieder neu und flexibel auf die Anforderungen der jeweiligen Situation und des Raumes einzustellen.[140]

Der *kontrollierte* Mensch ist ein Mensch der Wellenbewegung, der diese ständigen Modulationen vollziehen muss. Die früher so wichtigen Institutionen (Schule, Militär, Fabrik) sind, so Deleuze, in eine Krise gekommen. Eine neue Herrschaftsform bildet sich heraus, in der die Sozialdisziplinierung nicht mehr der dominante Machttyp ist; an ihre Stelle treten *Ausschließungs-* und *Kontrollmechanismen*, die die Kontrollgesellschaften konstituieren. Die Disziplinierung ist dabei nicht verschwunden, sie hat nur einen anderen Stellenwert erhalten und besitzt keine soziale Schlüsselfunktion mehr.

Das Symbol der Kontrollgesellschaft ist die *Zahl*, die als Losungswort gesehen wird, - sie ermöglicht entweder den Zugang zu Informationen oder verweigert ihn.[141] Computer sind daher für Deleuze die dominanten Maschinen der Kontroll-

---

[137] Deleuze 1993, S. 250

[138] vgl. Foucault 1994, S. 15

[139] Mit Einschließungsmilieu meint Foucault, Institutionen, die das Individuum durchlaufen musste (von der Schule zum Militär, vom Militär in die Fabrik). Dabei ging es in erster Linie um eine Normierung und Normalisierung eines jeden Individuums. Zentrum der Betrachtung war der gefügige, disziplinierte Körper. Die Entstehung des Gefängnisses war für Foucault Symbol einer veränderten Machtstruktur und Disziplinierung.

[140] vgl. z.B. auch Linderberg / Schmidt-Semisch 1995, S. 4

[141] vgl. Deleuze 1992, S. 183

gesellschaft, sie ermitteln die zulässige oder unzulässige Position des Einzelnen und bewirken eine allgemeine Modulation.[142]

2.3.2 Räumliche Kontrolle und das Prinzip der Exklusion

Deleuzes Begriff der Kontrollgesellschaft wurde von verschiedenen Autoren aufgegriffen und weiter ausgeführt. Dabei lassen sich einige Begriffe und Merkmale immer wieder finden, die im Folgenden skizziert werden und dazu beitragen sollen, ein dichteres Bild von dem zu erhalten, was unter dem Begriff der Kontrollgesellschaft hier verstanden werden soll.

Veränderte Art der Kontrolle

Ein Aspekt der Kontrollgesellschaft ist in der Literatur eine Veränderung der *Art* der Kontrolle. Die Soziologen und Kriminologen Schmidt-Semisch und Lindenberg konstatieren, dass aufgrund der sich ändernden gesellschaftlichen Strukturen und des wachsenden Pluralismus frühere Formen der Kontrolle und Disziplinierung nicht mehr zeitgemäß sind. Sie beziehen sich dabei auf das Gesellschaftsmodell der Postmoderne. Nach und nach werden bisherige Kontrollstrategien durch andere ersetzt. Die neue Kontrolle bedient sich nicht mehr ausschließlich disziplinierender Kontrollverfahren, sie wendet sich ökonomischeren und rationaleren Mitteln zu und muss sich immer weniger auf moralische Appelle und Legitimationen verlassen. Sie legitimiert sich nicht mehr über Moral, sondern über einen technokratisch aufgefassten Begriff von *Sicherheit*.[143] Die entstehende Kontrollgesellschaft lockert ihren moralisierenden Griff auf den Einzelnen, um ihn in einen räumlich-situativen Kontrollmodus zu überführen, der im Folgenden erläutert wird.

Lindenberg und Schmidt-Semisch schreiben:

> „Die neue Kontrolle trägt den diversifizierten und pluralisierten Lebensweisen Rechnung, indem sie sich weniger über Moral legitimiert, sondern vielmehr über einen technokratisch aufgefaßten Begriff von Sicherheit. Und dieser Sicherheitsbegriff erlaubt es, Phänomene nicht ausrotten zu wollen, sondern sie in bestimmbaren, umgrenzten Räumen zu gewähren.“[144]

---

[142] vgl. Deleuze 1992, S. 185

[143] vgl. Lindenberg / Schmidt-Semisch 1995, S. 3

[144] vgl. Lindenberg / Schmidt-Semisch 1995, S. 3

Die Kontrollräume werden dabei von den Menschen verinnerlicht. Diese Verinnerlichung ist gleichzeitig die Voraussetzung zur Partizipation in diesen Räumen.[145]

Der neue Kontrollanspruch kann sich nicht mehr auf eine einheitliche Moral berufen und sich an das Gewissen des Individuums richten; er bezieht sich nunmehr auf Orte, Plätze und Situationen. Das individuelle Verhalten muss dem Ort und der Zeit angemessen sein.[146] Die Autoren greifen hier auf den schon von Deleuze eingebrachten Begriff der *Modulation* zurück, der eine situationsspezifische Anpassung, in einer Gesellschaft beschreibt, die sich nicht mehr auf einen homogenen Wertekanon berufen kann.

Susanne Krasmann greift ebenfalls die veränderte Art der Kontrolle auf und interpretiert sie aus Foucault`scher Perspektive. Sie führt den Ansatz der Kontrollgesellschaft unter Bezug auf den bereits vorgestellten Gouvernementalitäts-Begriff von Michel Foucault weiter:

> „Unter dem Leitprinzip der Sicherheit im Verbund mit Techniken permanenter Überprüfung, Kalkulation und (statistischer) Berechnung, zielt diese Regierungsmentalität [*gemeint ist hier der Foucault`sche Gouvernementalitäts-Begriff, Anm. C.K]* einerseits auf Gruppen, auf die Regulation aggregierter Populationen. Andererseits werden Individuen mittels Techniken der Selbstbefragung und des Verantwortlichmachens gelenkt, so daß Aktivität hervorgerufen wird durch Anreiz oder Sorge, die sich beim einzelnen in einer Besorgnis mit Blick auf eine risikobehaftete Zukunft äußern kann und in einer daraus hervorgehendenaktiven Selbstsorge, die um die Bewältigung entsprechender Unwägbarkeiten bemüht ist.“[147]

Kontrollgesellschaften sind laut Krasmann nicht durch ein *Mehr* an Kontrolle gekennzeichnet, sondern stellen einfach ein anderes Regime dar, das weder erträglicher noch härter als das vorige ist. Die Formen der Kontrolle sind dagegen subtiler und weniger greifbar geworden.[148]

Das Prinzip der Inklusion und Exklusion

In der Literatur ist ein weiteres Merkmal der Kontrollgesellschaft das bereits erwähnte Prinzip der Inklusion und Exklusion. Die Gesellschaft unterteilt sich demnach in einzelne Kontrollzonen, die eine wachsende Fragmentierung und Desintegration innerhalb der Gesellschaft nach sich ziehen.

Es gibt Gruppen, die *In* sind und Gruppen, die an den Rand gedrängt werden, wo man sie nicht mehr sehen will. Wer sich in der vollkommenen Out-Zone befindet,

---

[145] vgl. Lindenberg / Schmidt-Semisch 1995, S. 6

[146] vgl. Lindenberg / Schmidt-Semisch 1995, S. 10

[147] Krasmann 1999, S. 109

[148] vgl. Krasmann 1999, S. 107

ist aus der Gesellschaft heraus gefallen. Ein Wissen über ihn ist aber dennoch nötig. Flächendeckende Informationen, das Wissen für den jederzeitigen Zugriff sind entscheidend. Nach Scheerer will man „flächendeckende Informationen, weil man alles wissen und auf alles gefasst sein will.“[149]

Die Gesellschaft löst sich allmählich in Gesellschaften auf, unterschiedliche Kontrollzonen mit unterschiedlichen Formen der Machtausübung entstehen.[150] De Marinis sieht es als charakteristisch für die Kontrollgesellschaft an, dass weder die wirtschaftliche Notwendigkeit noch der moralische Druck besteht, die Ausgeschlossenen wieder in eine Gesamtgesellschaft einzugliedern.[151] Diese Tendenz ließ sich bereits in den Ausführungen von Ericson und Haggerty bzw. Norris und Armstrong, die sich in ihren Betrachtungen auf die Risikogesellschaft beziehen, beschreiben. Auch die bereits vorgestellten US-Amerikaner Feely und Simon haben im Rahmen eines Paradigmenwechsel von der *Old Penology* zur *New Penology* ähnliche Tendenzen beschrieben. Die Gesellschaft wird durch diese Einteilung in In- und Out-Zonen fragmentiert, statt einer Integration erfolgt eine Desintegration bestimmter Bevölkerungsgruppen, die jedoch nicht einmal negativ bewertet wird. Das Bild von der Gesellschaft als sozialer Einheit scheint überholt.

2.3.3 Die Kontrollgesellschaft in der Praxis

Die beschriebenen Ansatzpunkte wurden von mehreren Autoren aufgegriffen und zum Teil durch empirische Studien gestützt. Ronneberger, Lanz und Jahn haben beispielsweise die Perspektive einer entstehenden Kontrollgesellschaft auf die *Stadt* als Untersuchungsfeld übertragen. Auch britische Arbeiten schließen hier an und verweisen auf den exkludierenden Charakter *technischer Überwachungssysteme* in Innenstädten, ohne sich aber explizit dem Ansatz der Kontrollgesellschaft anzuschließen. Sie sollen innerhalb dieses Kapitels dennoch vorgestellt werden, da sie den Ansatz der Kontrollgesellschaft im Hinblick auf die Möglichkeiten der technischen Kontrolle erweitern.

Die Stadt als Beute

Ronneberger, Lanz und Jahn konstatieren eine Tendenz zum Umbau der Innenstädte in „Konsum- und Erlebnislandschaften“.[152] Der entstehende metropolitane Raum ist dabei am exklusiven Lebensstil einer globalisierten Arbeitskultur im

---

[149] Scheerer zitiert nach de Marinis 2000, S. 43

[150] vgl. de Marinis 2000, S. 58

[151] vgl. de Marinis 2000, S. 64

[152] vgl. Ronneberger u.a. 1999, S. 9

Bereich der Dienstleistung ausgerichtet. Nachbarschaftlich ausgerichtete Alltagspraktiken der kleinbürgerlichen Quartiersbevölkerung werden dadurch tendenziell verdrängt.[153] Parallel zu diesen Veränderungen weisen die Autoren auf die „Wiederkehr einer gefährlichen Klasse“[154] hin, die im Laufe des 20sten Jahrhunderts zwar zugunsten sozialstaatlicher Normalisierungsstrategien zurückgedrängt wurde, gegenwärtig aber wieder eine Aufwertung erfährt. Zu dieser als Bedrohungsszenario konstruierten gefährlichen Klasse zählen u.a. ausländische Drogendealer, Jugendgangs und Ausländer allgemein. Die Autoren schreiben:

> „Die Polarisierung der Gesellschaft thematisiert man nicht mehr primär unter der Perspektive sozialer Gerechtigkeit, sondern als Problem der öffentlichen Sicherheit und der Standortpflege. Sozialpolitik erscheint nun vor allem als Teil einer präventiven Kriminalpolitik.“[155]

Die Autoren sehen im Rahmen der Durchsetzung neoliberaler Politik einen Trend zur Ausgrenzung bestimmter Gruppen, die nicht mehr dem Wohlfahrtsstaat überantwortet werden, sondern denen mit ordnungspolitischen Mitteln begegnet wird.[156]

Ronneberger et al. verweisen auf die von Gilles Deleuze skizzierte Entstehung der Kontrollgesellschaft, in der es um die entpersonalisierte Regulierung von Orten und prekären Situationen geht. Laut der Autoren operieren die Machtorgane des Neoliberalismus nicht ausschließlich mit dem Zwang zur selbstregulierten Eigenverantwortung und dem Einsatz entmoralisierter Überwachungstechnologien, vielmehr ist auch eine „Rückkehr des strafenden Staates“ mit seinen „Law and Order-Kampagnen“[157] festzustellen, ein Aspekt, den andere Autoren bislang nicht in dieser Form herausgestellt haben und der im Widerspruch zu den anderen Thesen der Kontrollgesellschaft steht.

Die Autoren beschreiben dabei vier unterschiedliche Kontrollszenarien in den Städten:

- Die präventive Abschirmung abgeschlossener Bereiche wie privatwirtschaftliche Bürotürme, Malls oder Einkaufspassagen mit Hilfe technischer Überwachungssysteme und besonderer Raumgestaltung.
- Die Praxis in so genannten umkämpften Territorien wie innerstädtischen Einkaufsmeilen oder Bahnhöfen, in denen mit Hilfe repressiver

[153] vgl. Ronneberger u.a. 1999, S. 51

[154] vgl. Ronneberger u.a. 1999, S. 171ff

[155] Ronneberger u.a. 1999, S. 174

[156] vgl. Ronneberger u.a. 1999, S. 10

[157] vgl. Ronneberger u.a. 1999, S. 198

Verdrängungspraxis eine selektive soziale Homogenität hergestellt werden soll (Hausverbote, Image-Kampagnen).

- Die Bildung von Nachbarschaftshilfen und Bürgerwehren, die eine hohe soziale Kontrolle nach innen und einen Schutz nach außen demonstrieren.
- Die ordnungspolitische Absicherung und Überwachung von Ausschließungs- und Internierungsräumen für die Klasse der Entbehrlichen (Dealer; Junkies; Flüchtlinge).

Es geht hier um einen Macht- und Kontrolltypus, der entweder die dauerhafte Ausschließung bestimmter Menschengruppen aus der Stadt vorsieht oder die Ausschließung mit differenzierten Einschließungs- oder Internierungsmodellen zu kombinieren sucht. Ziel der gegenwärtigen Kontrollpolitik sei es, in zentralen Bereichen der Stadt die Armut unsichtbar zu machen und andererseits einen tief gestaffelten Sicherungsraum gegen Flüchtlinge und Migrationsbewegungen zu installieren.[158] Technische Systeme, wie die Videoüberwachung, tragen dazu bei, diese Ausschließungstendenzen durchzusetzen.[159]

Exklusion durch Technik - das Beispiel Großbritannien

Weitere Beispiele aus der Praxis liegen im Bereich der britischen Forschung vor. Obwohl auch darin der Begriff Kontrollgesellschaft nicht explizit genannt wird[160], werden doch dieselben Phänomene beschrieben, die auch Ronneberger et al. aufzeigte. Das Moment der Videoüberwachung wurde in der britischen Forschung stärker als in der bundesdeutschen aufgegriffen, was nicht zuletzt damit zusammenhängen mag, dass Großbritannien über mehr Kamera-Überwachungssysteme im öffentlichen Raum als jede andere westliche Industrienation verfügt und die öffentliche Diskussion entsprechend weiter fortgeschritten ist.[161] Die Videoüberwachungssysteme (in Großbritannien Closed Circuit Television, abgekürzt CCTV genannt) sollen Verbrechen oder die Angst vor Verbrechen reduzieren, die Innenstädte attraktiver machen und dadurch zum Konsumieren in der Stadt einladen.[162] Bannister et.al. stellen fest:

---

[158] vgl. Ronneberger u.a. 1999, S. 201f

[159] vgl. hierzu auch Ronneberger u.a. 1999, S. 144ff

[160] Es wird in der britischen Literatur eher von „Surveillance“, also von Überwachung, gesprochen. Die beschriebenen Phänomene decken sich aber weitgehend mit denen der deutschen Kollegen; die britischen Autoren gehen aber stärker auf das technische Moment ein.

[161] vgl. Bannister u.a. 1998, S. 21

[162] vgl. Bannister u.a. 1998, S. 22

> „This leads to a consideration of the nature of the urban economic and political processes which have co-joined to promote consumption citizenship, and which in so doing have served to exclude difference. Taken together, these processes may be identified as leading to the privatisation and purification of space in the city-centre.“[163]

Bannister et al. sprechen in ihrem Text von einer Ausschließung des Fremden, von einer Stadt, die zur Festung wird. Diese Tendenz wird durch den Einsatz von Videoüberwachung verstärkt oder erst ermöglicht.[164]

Mc Cahill weist ähnlich wie seine deutschen Kollegen Ronneberger, Lanz und Jahn darauf hin, dass es nach einer Phase des Booms nach dem Zweiten Weltkrieg nun im Rahmen der Globalisierung zu einer Entindustrialisierung der Städte kommt und ein Umbau hin zur Stadt als Ort des störungsfreien Konsums stattfindet.[165] Auf der anderen Seite sieht der Autor eine wachsende Zahl an Armen und Obdachlosen, die verdächtigt werden, das Image der Stadt zu schädigen. Mc Cahill äußert die Besorgnis über eine Erosion des *democratic public space* in Innenstädten in Großbritannien, die zunehmend durch kommerzielle Interessen dominiert werden.[166]

Das Prinzip der Inklusion und Exklusion wird mit Hilfe von Videoüberwachungssystemen durchgesetzt, indem man z.B. für den reinen Konsum bestimmte Orte (Einkaufspassagen etc.) videoüberwacht und somit eine leichtere Kontrolle des Raumes und der nicht erwünschten Personen erhält. Die Innenstadt soll als risikofreier Ort des Konsums konstruiert werden, an welchem der wachsende Einsatz der Kameraüberwachung dazu genutzt werden kann, eine nicht konsumfähige Unterklasse von diesem Ort auszuschließen.[167]

2.3.4 Zusammenfassung

In der Perspektive der Kontrollgesellschaft wird diese als davon gekennzeichnet gesehen, dass die Gesellschaft permanenter Kontrolle ausgesetzt ist. Diese Kontrolle bedient sich nicht mehr ausschließlich disziplinierender Verfahren (wie in der von Foucault beschriebenen Disziplinargesellschaft), sondern nutzt ökonomischere und rationale Mittel. Sie legitimiert sich nicht über die *Moral* sondern, über den Begriff der *Sicherheit*, der auch in der Risikogesellschaft zentral war. Technische Kontroll- und Überwachungssysteme, wie beispielsweise die Videoüberwa-

---

[163] Bannister u.a. 1998, S. 23

[164] vgl. Bannister u.a. 1998, S. 27

[165] vgl. Mc Cahill 1998, S. 48f

[166] vgl. Mc Cahill 1998, S. 52

[167] vgl. Mc Cahill 1998, S. 61

chung, stellen innerhalb dieser veränderten Auffassung von Kontrolle ideale Instrumente des Ausschlusses dar, wie auch die Ausführungen aus Großbritannien verdeutlichen.

Die Kontrolle zielt auf eine Angemessenheit des Verhaltens an bestimmten Orten, Plätzen, Situationen; moralische Appelle sind nicht mehr zeitgemäß. Der Mensch muss zu *Modulationen* fähig sein; er muss sein Verhalten entsprechend dem Ort und der Situation anpassen. Das bedeutet, dass er die unterschiedlichen Kontrollmodalitäten kennen und sie verinnerlicht haben muss, um am sozialen Leben teilnehmen zu können. Wie vermittelt wird, welche Modulation gerade nötig ist, wird in der Literatur allerdings nicht näher beschrieben.[168]

Bestimmte Gruppen und Personen fallen aus dem gesellschaftlichen Raster heraus und werden zu Ausgeschlossenen, die von bestimmten Orten ferngehalten werden sollen; es kommt zu einer Fragmentierung der Gesellschaft in In- und Out-Zonen - Orte, an denen man sich aufhält, wenn man dazu gehört und die Regeln beachtet und Orte, die außerhalb der Gesellschaft stehen, die für die Ausgeschlossenen vorgesehen sind. Die räumliche Exklusion und Inklusion ist laut einiger der vorgestellten Autoren weiteres Merkmal einer entstehenden Kontrollgesellschaft. Gerade technische Überwachungs- und Kontrollsysteme können, wie bereits oben beschrieben, diesen Tendenzen weiteren Vorschub leisten.

Einzig Deleuze hebt in seinen Ausführungen auf die Bedeutung der Computertechnologie ab und bezeichnet Computer als die *dominanten Maschinen* der Kontrollgesellschaft. Computer ermitteln zulässige oder unzulässige Positionen des Einzelnen und berechnen anhand der ihnen zur Verfügung stehenden Daten dessen Standort in der Gesellschaft. Gerade dieser Aspekt erscheint als besonders wichtig für die vorliegende Arbeit. Wie auch die Ausführungen von Susanne Krasmann, die im Ansatz der Kontrollgesellschaft den Einzug eines anderen *Regimes*, einer anderen Form der Machtausübung sieht. Sie bringt an dieser Stelle erneut den Begriff der Gouvernementalität von Foucault in die Diskussion ein.

[168] Weiterführende Gedanken dazu lassen sich bei den Analysen Michel Foucaults in Kapitel 2.5 finden.

2.4 Ständige Kontrolle: Die Sicherheitsgesellschaft

Die *Sicherheitsgesellschaft* stellt ähnlich dem Modell der *Kontrollgesellschaft* keine ausgearbeitete Gesellschaftstheorie dar und wird ähnlich unscharf wie der Begriff der Kontrollgesellschaft verwendet: Bestimmte (teilweise recht unterschiedliche) gesellschaftliche Phänomene werden von einigen Autoren unter dieser Bezeichnung gefasst. Da der Begriff *Sicherheit* spätestens seit dem 11. September in den westlichen Industrienationen ein hochaktuelles Thema ist und auch innerhalb der vorgestellten theoretischen Ansätze immer wieder aufgegriffen wird, wird in diesem Kapitel auch das Spannungsfeld (Innere) Sicherheit – Gesellschaft untersucht. Der Begriff der Sicherheit dient derzeit oftmals als Begründung für vielfältige Gesetzesänderungen und Maßnahmen, die teilweise massive Einschnitte in Bürgerrechte darstellen, und ist damit eine nähere Betrachtung wert.

2.4.1 Die Sicherheitsgesellschaft nach Legnaro und Foucault

Einen direkten Anschluss an den zuvor vorgestellten Ansatz der *Kontrollgesellschaft* bietet Aldo Legnaro in seinem Essay „Konturen der Sicherheitsgesellschaft“.[169] Er sieht in der *Sicherheitsgesellschaft* eine Fortführung der *Kontrollgesellschaft* und weist selbst darauf hin, dass seine Ausführung keine ausformulierte theoretische Einordnung sein will.

Die *Sicherheitsgesellschaft* zeichnet sich laut Legnaro dadurch aus,

> „…daß nicht nur staatliche, sondern allmählich und in stetig zunehmendem Ausmaß auch private Akteure an der Produktion von Sicherheit teilnehmen, daß die Überwachung nicht nur dem Staatsschutz im engeren Sinne gilt, sondern Aktivitätskontrollen von allen Bürgern – tendenziell durch alle Bürger – mit dem Ziel der Risikominimierung für alle angestrebt werden und daß schließlich die Produktion von Sicherheit nicht nur eine staatliche Aufgabe ist, sondern eine permanente gesellschaftliche Anstrengung, ein Régime des täglichen sozialen Lebens.“[170]

Mit diesen Ausführungen greift Legnaro Aspekte der Risikogesellschaft auf, ohne sich jedoch explizit auf diese zu beziehen. Legnaro weist darauf hin, dass soziale und technische Kontrollmechanismen in der Sicherheitsgesellschaft alltäglich geworden sind und nicht nur zur Kontrolle von Devianz genutzt werden – sie werden konstitutives Element zur Herstellung *allgemeiner* Konformität.

---

[169] vgl. Legnaro 1997

[170] Legnaro 1997, S. 271

> „Es geht demnach nicht nur um die Produktion von Sicherheit als Sicherheit vor Funktionsstörungen und Schutz vor devianten Verhaltensweisen, sondern um die Etablierung von innergesellschaftlich wirksamen Mechanismen, die Grenzen von Inklusion und Exklusion herstellen.“[171]

Es kommt zu einer Universalisierung technischer Risken und damit zu einer Universalisierung des Kontrollbedarfs[172], was eine neue Dimension der Überwachung und Kontrolle darstellt. Dies begründet, so Legnaro, die Sicherheitsgesellschaft. Diese Entwicklung wird von einem (vorhandenen oder auch behaupteten) generellen Gefährdungsbewusstsein der Bevölkerung befördert. Die Produktion von Sicherheit gerät zu einer gesellschaftlichen Aufgabe, an der alle mitwirken sollen.[173]

Legnaro sieht drei Elemente, mit denen sich Facetten der Sicherheitsgesellschaft erkennen lassen[174]:

a) Anstelle der Kontrolle von konkreten *Personen* kommt es zu einer Kontrolle des *Raumes*, in dem sich bestimmte Gruppen aufhalten. Sicherheit wird zur Gemeinschaftsaufgabe. Legnaro bezieht sich hier auf die bereits vorgestellten Autoren Feely und Simon[175]: Die gesamte Bevölkerung wird als potenzieller Risikofaktor wahrgenommen, wobei einige Gruppen als gefährlicher wahrgenommen werden als andere. Polizeiarbeit ist nun *proaktiv* nicht mehr *reaktiv*.

b) Es kommt zu einer urbanen Segregation; Sicherheitsstandards werden zu einem neuen Kriterium der sozialen Klassenlage. Wohngegenden der oberen Mittelschicht sind durch Zäune und private Sicherheitsdienste bewacht, während die Polizei in Vierteln der unteren Schichten nur eine notdürftige Präsenz zeigt. Es kommt zu einer Privatisierung des staatlichen Gewaltmonopols. Die zwischen den Extremen liegenden Wohnviertel sind gehalten, sich selbst zu organisieren und unter dem Stichwort Community Policing mit staatlicher Hilfe eigene Sicherheitsnetze aufzubauen. Exklusion erfolgt nicht nur sozial, sondern auch räumlich; gefährliche Klassen, gegen die es sich zu schützen gilt, werden dadurch kreiert.

---

[171] Legnaro 1997, S. 272

[172] An dieser Stelle greift Legnaro erneut die Argumentation Becks bzgl. der Risikogesellschaft auf.

[173] vgl. Legnaro 1997, S. 273

[174] vgl. Legnaro 1997, S. 274ff

[175] vgl. Feely / Simon 1994

c) Sicherheit wird als Bestandteil der Abwicklung des Alltags funktional integriert. In vielen Bereichen kommt es zu einem Rückgang der Anonymität (z.B. durch Kreditkarten oder andere Karten, die Konsum eindeutig zuordnen). Das individuelle Verhalten wird zum Datenprofil[176], innerhalb dessen Jede(r) ständig seine Unschuld nachweisen muss. Was als unschuldig gilt, kann sich, je nach Bedrohungsszenario, ändern.

Legnaro betont, dass die derzeitige soziale Wirklichkeit es nicht rechtfertigt, schon von einer Sicherheitsgesellschaft zu sprechen; dennoch gibt es aus seiner Sicht Entwicklungen, die in diese Richtung weisen.

> „Sicherheitsgesellschaft ist der Versuch, die objektiven Risiken der modernen Industriegesellschaft unter einem bestimmten Aspekt – dem der Überwachung, der sozialen Kontrolle und der Prävention – zu antizipieren und die Eintrittswahrscheinlichkeit bestimmter Ereignisse zu minimieren."[177]

In der Sicherheitsgesellschaft werden objektiv gegebene und subjektiv befürchtete Risiken unter räumlichen, sozialen, ideologischen und technischen Prämissen verknüpft. Mit Hilfe digitaler Verfahren wird versucht, einen Teil der Berechenbarkeit und sozialen Ordnung wieder herzustellen, welche die *alte* Sozialität ausmachte.[178]

Foucaults Skizze der Sicherheitsgesellschaft

Auch innerhalb der bereits vorgestellten Machtanalyse Foucaults findet der Begriff der Sicherheitsgesellschaft Erwähnung. In seiner Arbeit kommt der *Sicherheit* eine entscheidende Rolle in der modernen Ausübung von Macht zu. An dieser Stelle soll ergänzend auf Foucaults Begriff der *Sicherheitsgesellschaft* eingegangen werden.

Foucault hatte noch Anfang der 1970er Jahre eine zunehmende Disziplinierung der Gesellschaft diagnostiziert, in seinen bereits erwähnten Vorlesungen von 1978/79 stellt er dann aber fest, dass sich in der allgemeinen Ökonomie der Macht die Dominanz von den juridischen Mechanismen über die Disziplinar- hin zu Sicherheitsmechanismen verschoben habe. Nach Foucault leben wir heute weniger in einem Rechtsstaat oder einer Disziplinargesellschaft als in einer *Sicher-*

---

[176] Ähnliches meinen auch die Briten Norris und Armstrong: „Everyone is assumed guilty until the risk profile assumes otherwise.", Norris und Armstrong 1999, S. 24.

[177] Legnaro 1997, S. 281

[178] vgl. Legnaro 1997, S. 279f

heitsgesellschaft, in der juridische und disziplinäre Mechanismen zunehmend durch Dispositive der Sicherheit erschlossen werden.[179]

Die Vorlesungen Foucaults standen unter dem Eindruck des linksextremen Terrors in Europa. Die Auseinandersetzung des Staates (hier sowohl der französische als auch der deutsche) mit den Terroristen diente als unfreiwilliges Anschauungsbeispiel für Foucaults Thesen über die Sicherheitsmechanismen.[180] In der Sicherheitsgesellschaft werden in gewissen Grenzen unterschiedliche Handlungsformen akzeptiert und Unsicherheit und soziale Risiken wie Unfälle, Arbeitslosigkeit, Krankheit abgemildert bzw. ausgeschlossen. Um Sicherheit garantieren zu können, muss sich der Staat aber gegen und außerhalb des rechtlichen Rahmens bewegen können.[181]

2.4.2 Auswirkungen auf die Sozialsysteme

Einschnitte in das soziale System

Neben dieser grundsätzlichen Skizzierung einer Sicherheitsgesellschaft, die teils deutliche Anleihen bei der Risikogesellschaft Ulrich Becks macht, interpretieren andere Autoren die Sicherheitsgesellschaft unter dem Aspekt der *sozialen* Sicherheit. Hans-Jürgen Lange wendet sich, ebenfalls unter dem Begriff der Sicherheitsgesellschaft, dem Abbau wohlfahrtsstaatlicher Leistungen während der letzten Jahre zu. Die soziale Sicherheit wird zunehmend in die Verantwortung jedes Einzelnen gegeben, der Wohlfahrtsstaat wird abgebaut und Eigenverantwortlichkeit propagiert. Eine Garantie für soziale Absicherung existiert nicht mehr.[182] Parallel zum Abbau der wohlfahrtsstaatlichen Sicherheit besinnt sich der Staat wieder auf seine (alten) Kompetenzen: der *innenpolitischen* (polizeilichen) und der *außenpolitischen* (militärischen) Sicherung. Der neue Sicherheitsbegriff trennt die soziale Dimension von der polizeilichen und gibt die Verantwortung für die soziale Sicherheit an das Individuum zurück. Wer dieser Aufgabe nicht nachkommt, wird im schlimmsten Fall zum öffentlichen Problem (z.B. durch Nichtsesshaftigkeit), das den verantwortlich handelnden Bürger stört. Lange sieht

---

[179] vgl. Lemke 2003, S. 191

[180] Damit entsteht an dieser Stelle eine interessante Parallele zur heutigen Situation nach dem 11. September.

[181] Ein für Foucault bedeutsames Ereignis war im Rahmen der Terrorismusbekämpfung der 70er Jahre der Fall des RAF-Verteidigers Klaus Croissant, der in der BRD wegen Unterstützung einer kriminellen Vereinigung angeklagt war und nach Frankreich floh um dort politisches Asyl zu beantragen. Entgegen der Bestimmungen des Asylrechts erfolgte die Auslieferung Croissants an die BRD, vgl. Lemke 2003, S. 191

[182] vgl. Lange 2002

hierin die entstehenden Konturen einer *Sicherheitsgesellschaft*, bei welcher der Staat die oben beschriebenen Rahmenbedingungen schafft, gleichzeitig aber seine Bürger zur individuell-sozialen Selbstsicherung verpflichtet und dazu, für den Schutz ihres Eigentums selbst zu sorgen. Fraglich ist, so Lange, ob eine solche Gesellschaft noch mit den Prinzipien einer demokratischen Gesellschaft vereinbar ist und ob der Staat die nun andernorts versprochene Sicherheit überhaupt herstellen kann.[183]

2.4.3 Die Sicherheitsgesellschaft in der Praxis

In einem 2002 gehaltenen Vortrag schließt sich auch Klaus Ronneberger dem Begriff der Sicherheitsgesellschaft an.[184] Dabei erweitert er seine Argumentation, bezieht sich aber teilweise auch auf Merkmale, die er zuvor der Kontrollgesellschaft zugewiesen hat. Dies macht deutlich, dass sich noch kein einheitlicher Gebrauch der hier vorgestellten Begriffe innerhalb der aktuellen Diskussion etablieren konnte. Ronneberger konstatiert eine bereits durch die 1990er Jahre hindurch stattfindende Intensivierung der Sicherheitspolitik, bei der z.B. folgende Punkte eingeführt wurden: die Videoüberwachung von öffentlichen Plätzen, das Verhängen von Aufenthaltsverboten, die Einführung des genetischen Fingerabdrucks, die Einführung der elektronischen Fußfessel für Gefangene und die Schleierfahndung.

Anders als noch in den 1970er und 1980er Jahren, als Bürger aufgrund der damaligen Volkszählung protestierten, löst die derzeitige Verschärfung der Bestimmungen im Bereich Innere Sicherheit keine nennenswerten Proteste bei den Bürgern aus, betont Ronneberger. Heutzutage sei eine wachsende *Strafbereitschaft* in der Bevölkerung festzustellen, deren Gründe in der Erosion des Wohlfahrtsstaates und im Aufkommen neoliberaler Modelle lägen.[185] In den 1990er Jahren, so Ronneberger, sei es zu einem Verschwinden von Millionen von Jobs gekommen, was eine Gruppe von *Überflüssigen* entstehen ließ, die strukturell für den Arbeitsprozess nicht mehr gebraucht werden. Einer neu entstehenden städtischen Armut wird mit ordnungspolitischen Maßnahmen entgegengetreten, die als Leitbild die sichere und saubere Stadt festlegen. Für einkommensstärkere Bevölkerungsgruppen entstehen auf der anderen Seite Konsum- und Erlebnislandschaften, die bestimmte Gesellschaftsmitglieder ausschließen.[186] Diese Entwicklung wurde von Ronneberger, Lanz und Jahn bereits unter der Überschrift der Kon-

[183] vgl. Lange 2002

[184] vgl. Ronneberger 2002

[185] Ronneberger 2002

[186] vgl. Ronneberger 2002, S. 5

trollgesellschaft diskutiert, was deutlich macht, dass die Begriffe noch nicht einheitlich verwendet und relativ beliebig unterschiedlichen gesellschaftlichen Phänomen zugeordnet werden.

Auf technischem Gebiet stellt Ronneberger den Einsatz von Videokameras heraus, die von Behörden immer mehr zur ordnungspolitischen Regulation des städtischen Raumes eingesetzt werden. Er sieht eine potenzielle Wirkung der elektronischen Überwachung darin,

> „Normalitätsnormen auch in solchen Bereichen durchzusetzen, die bislang noch als Refugien für andere Formen von Lebensweisen galten."[187]

Bezogen auf die Zukunft der Stadt sieht Ronneberger eine *ständische Bürgerstadt* entstehen, deren Hierarchie unterschiedlicher Rechts- und Subjektpositionen als legitime Voraussetzung der gesellschaftlichen Ordnung gelten soll.[188]

2.4.4 Exkurs: Sicherheit als gesellschaftlicher Diskurs

Neben den Autoren, die sich begrifflich mit dem Entwurf einer Sicherheitsgesellschaft auseinander gesetzt haben, ist *Sicherheit,* nicht erst seit dem 11. September, Teil des öffentlichen Diskurses. Gerade seit diesem Ereignis ist der Begriff aber vielfach Begründung und Anlass für eine Vielzahl staatlich durchgesetzter Gesetzesänderungen gewesen. Im Kern geht es dabei um die Innere Sicherheit, die gefährdet ist oder gefährdet erscheint.

Die behauptete Gefährdung betrifft dabei - nach Peters und Schetsche - die Funktionsweise staatlicher Instanzen (Korruption oder Unterwanderung durch Verfassungsfeinde); die Abwendung bestimmter Teile der Bevölkerung von der bestehenden Ordnung (Unregierbarkeit der Städte, ziviler Ungehorsam) und die systematische Verletzung des staatlichen Gewaltmonopols (Terrorismus, Organisierte Kriminalität). In demokratischen Staaten sind diese Sicherheitsdiskurse einerseits als Behauptungen der manifest oder potenziellen Störung der Funktionsweise staatlicher Instanzen zu lesen, andererseits als Begründung für Änderungen der inneren Machtverhältnisse zugunsten des Staates / der Exekutive. Hier geht es um die Legitimierung staatlicher Eingriffe in Bürgerrechte, also letztlich auch um die Verschiebung der Grenze zwischen privat und öffentlich, wie die Autoren konstatieren. Vielfach sind es jedoch auch die Bürger selber, die Innere Sicherheit zum Thema machen.[189]

---

[187] vgl. Ronneberger 2002, S. 10

[188] vgl. Ronneberger 2002, S. 12

[189] vgl. Peters / Schetsche 1998, S. 186

Innerhalb der Politik werden die Unsicherheitsgefühle der Bevölkerung aufgegriffen, und es besteht ein Interesse daran, Sicherheitsstrukturen für unvorhersehbare Ereignisse auf Vorrat zu etablieren. Nach Hartmut Aden, der sich mit Polizeikooperationen auf europäischer Ebene auseinandergesetzt hat, liegt die Schattenseite dieser Form von Sicherheitsvorsorge darin, dass die hinter den jeweiligen Sicherheitsproblemen liegenden gesellschaftlichen Probleme ungelöst bleiben.[190]

Im rechtspolitischen Diskurs lässt sich seit längerem eine Verlagerung von einer Täter- zu einer Opferzentrierung feststellen. Der sicherheitspolitische Diskurs dreht sich dabei zunehmend um Sicherheits*gefühle* und subjektive Risikoeinschätzungen, weniger um objektive Zahlen und tatsächliche Bedrohungen, wie Hornbostel[191] feststellt. Dadurch entsteht eine Abkehr vom Prinzip der reinen Gefahrenabwehr, hin zu vor allen Dingen lokal organisierten Präventionsmaßnahmen (z.B. Präventionsräte), die von relativ diffusen Bedrohungsszenarien ausgehen.

2.4.5 Zusammenfassung

Aus dem Ansatz der Sicherheitsgesellschaft und dem damit verknüpften Diskurs um die Innere Sicherheit lassen sich folgende Punkte herausstellen: *Sicherheit* ist ein dominantes Motiv innerhalb der Gesellschaft, ihre Herstellung erfordert permanente Anstrengung von *jedem*, denn die Bedrohung / das Risiko ist universal, die Gefährdung allgegenwärtig - ein Motiv, das bereits in der *Risikogesellschaft* klar herausgestellt wird. Soziale und vor allem auch technische Kontrollsysteme sind in der Sicherheitsgesellschaft alltäglich geworden, sie dienen nicht nur der Verhinderung von Devianz, sondern auch der Herstellung allgemeiner Konformität (als Beispiel wird hier meist die Videoüberwachung herangezogen). Das individuelle Verhalten wird zum Datenprofil, jeder muss seine Unschuld ständig beweisen. Mit Hilfe digitaler Verfahren wird versucht, einen Teil der Berechenbarkeit und sozialen Ordnung wieder herzustellen und Anonymität aufzuheben. Nicht nur staatliche, sondern zunehmend auch private Akteure sind an der Herstellung von Sicherheit beteiligt.

Die Kontrolle zielt nicht mehr auf bestimmte Personen, sondern auf Räume. Jeder ist potenziell verdächtig geworden, was sich in einer proaktiven Polizeiarbeit zeigt, die bereits im Vorfeld agiert und nicht erst reagiert, wenn bereits etwas passiert ist. Innerhalb dieser Kontrolle des Raumes lassen sich räumliche Segregationen feststellen, bei denen bestimmte Personen oder Gruppen unter dem Aspekt

[190] vgl. Aden 1998, S. 76

[191] vgl. Hornbostel 1998, S. 93f

der Sicherheit nicht mehr in bestimmten Räumen (z.B. Innenstädten) erwünscht sind.

In der Literatur wird vielfach der Neoliberalismus und der damit verbundene Rückzug des Staates aus wohlfahrtsstaatlichen Leistungen als Grund für eine Konzentration des Staates auf die Kategorie *Sicherheit* angeführt. Dabei werden soziale Sicherheiten weiter abgebaut und in die Verantwortung des Einzelnen gelegt. Der Staat bezieht sich wieder verstärkt auf seine Kompetenzen der innen- und außenpolitischen Sicherung, um sich selbst zu legitimieren. Foucault hat in seiner Machtanalyse ebenfalls auf die wachsende Bedeutung des Dispositivs der Sicherheit in gegenwärtigen Arten der *Regierung* hingewiesen und festgestellt, dass eine Verschiebung von den juridischen Mechanismen über die Disziplinar- hin zu Sicherheitsmechanismen stattgefunden hat.

Festzustellen ist auch, dass die Grenzen zwischen öffentlich und privat verwischen. Die Privatsphäre wird durch den Diskurs der Inneren Sicherheit zum sicherheitspolitisch relevanten Ort, Privatpersonen werden zu Akteuren der Politik der Inneren Sicherheit. Dabei spielen immer weniger die tatsächlichen Bedrohungen eine Rolle, als vielmehr Gefühle zur Sicherheit und subjektive Risikoeinschätzungen.

2.5 Unaufhaltsamer Informationsfluss: Die Surveillance und Maximum Surveillance Society

Die im angloamerikanischen Sprachraum diskutierten Ansätze der Surveillance und Maximum Surveillance Society fielen im Rahmen der Literaturanalyse besonders auf, da sie stärker als die bisher vorgestellten Perspektiven auf das Moment der *technischen* Überwachung eingehen. Die angloamerikanische Forschung erscheint in diesem Zusammenhang wesentlich strukturierter als die des europäischen Festlands – hier ist das Thema aufgrund der hohen Verbreitung entsprechender Systeme bereits stärker in der wissenschaftlichen Diskussion verankert. Im Folgenden sollen die als dominant erscheinenden Ansätze der Surveillance und Maximum Surveillance Society vorgestellt werden.

2.5.1 Die Surveillance Society nach Marx und Lyon

Der Begriff der Surveillance Society, also der Überwachungsgesellschaft, geht auf den US-amerikanischen Soziologen Gary T. Marx zurück. Auf dem Höhepunkt der Begeisterung für die neuen Informationstechnologien prägte er 1985 den Begriff. Marx sah in diesem Zusammenhang ein Szenario im Stile von George Orwells „1984“ auf die Gesellschaft zukommen. Mit der sich immer weiter verbreitenden Computertechnologie, so mutmaßte er, würden die letzten Barrieren zu einer totalen sozialen Kontrolle fallen.[192]

Ähnlich wie Marx für die USA sah David H. Flaherty 1989 für alle westlichen Industrienationen die Gefahr, durch den wachsenden Einsatz von Informationstechnologien zu Überwachungsgesellschaften zu werden, - wenn sie es nicht schon wären. Obwohl er davon ausgeht, dass bestimmte Überwachungstechniken für eine Demokratie legitim sind, verweist er darauf, dass eine Kumulation solcher Techniken negative Auswirkungen auf die Privatsphäre hat.[193]

Der kanadische Soziologe David Lyon geht in seinem 2001 erschienenen Buch Surveillance Society von einer wachsenden Überwachung der Bevölkerung durch unterschiedliche Stellen aus und definiert *Überwachung* wie folgt:

> „In this context, it is any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered.”

Und weiter:

---

[192] vgl. Marx 1985, S. 21-26

[193] vgl. Flaherty 1989

> "Today the most important means of surveillance reside in computer power, which allows collected data to be stored, matched, retrieved, processed, marketed and circulated. […] It is the massive growth in computer application areas and technical enhancement that makes communication and information technologies central to surveillance."[194]

Es fällt auf, dass hier die Informationstechnologie stärker in den Mittelpunkt gerückt wird, als dies in den vorigen Ansätzen der Fall war. Lyon betont, dass diese Feststellung nichts mit Verschwörungstheorien oder Ähnlichem zu tun hat, sondern die Folge der komplexen Art und Weise ist, wie wir unsere politischen und ökonomischen Beziehungen in einer Gesellschaft strukturieren, die Wert auf Mobilität, Schnelligkeit, Sicherheit und Freiheit des Konsumenten legt.

Lyon sieht mehrere Gründe für die Entstehung einer Überwachungsgesellschaft. Zum einen geht in den heutigen Industriegesellschaften der physische Kontakt der Menschen untereinander zurück. Menschen kommunizieren über weite Entfernungen, ohne sich dabei jemals in die Augen zu schauen. Dies ist überwiegend darin begründet, dass viele Dinge heute über Computer vermittelt werden und sich somit gewohnte Strukturen mehr und mehr verändern. Lyon setzt in diesem Zusammenhang Informationsgesellschaften mit Überwachungsgesellschaften gleich:

> „Surveillance practices are growing at an accelerating rate wherever information infrastructures and knowledge-based economics are established. One intrinsic aspect of all so-called information societies is that they are, by the same token, surveillance societies."[195]

Dies bedeutet allerdings nicht, dass wir es mit einem technischen Determinismus zu tun haben, dem die Gesellschaft ausgeliefert ist. Das technologische Potenzial ist kein soziales Schicksal.

Lyon geht es in seinen Ausführungen nicht um persönliche Überwachung und Kontrolle etwa durch den Vorgesetzten am Arbeitsplatz, sondern um die Möglichkeiten, die sich durch heutige Computertechnik und deren Vernetzung ergeben. Für Lyon entstehen Überwachungsgesellschaften dort, wo direkte Kontakte zwischen Menschen zurückgehen und durch elektronische Medien ersetzt werden. Überwachungstechnik wird dort eingesetzt, wo soziale Beziehungen *entkörperlicht* sind.[196]

---

[194] Lyon 2001, S. 2

[195] Lyon 2001, S. 5

[196] vgl. Lyon 2001, S.26f

> „Surveillance societies exist today because of the need to make visible and coordinate the activities of disappearing bodies “ [197]

Überwachung ist dabei ein generelles soziales Phänomen, das durch unterschiedlichste Institutionen, zu denen auch der Staat gehört, praktiziert wird. Das Konzept der Überwachungsgesellschaft bezeichnet dabei weniger einen festen Status, als vielmehr eine Tendenz im sozialen Bereich, einen *sozialen Trend*.[198] Demnach bezieht sich Lyon hier nicht auf einen Überwachungsstaat, sondern hebt auf eine breitere Verankerung des Überwachungsphänomens innerhalb der gesamten Gesellschaft ab. Daher sind Überwachungsgesellschaften nicht totalitär, auch wenn eine Tendenz dazu nicht mit Sicherheit auszuschließen ist. Die Überwachungsgesellschaft findet sich in allen Informationsgesellschaften und zieht sich durch alle sozialen Bereiche, wobei der Staat nur einen Aspekt innerhalb des Überwachungsszenarios darstellt.[199] Ein wichtiger Punkt in Lyons Argumentation ist die Veränderbarkeit der Ziele der Überwachungstechnologien. Datensätze können immer leichter von unterschiedlichen Stellen genutzt werden, wenn diese sich zu einer Kooperation entschließen.[200]

Einen Grund, warum Überwachung eine stärkere soziale Rolle in unserer Zeit erlangt hat, sieht Lyon darin, dass Überwachung Teil eines Risiko-Managements ist, das selbst wieder Risiken hervorbringt – dabei bezieht er sich auf die Analysen Ulrich Becks.[201]

2.5.2 Die Maximum Surveillance Society nach Norris und Armstrong

Mit dem Begriff der Maximum Surveillance Society beschreiben Norris und Armstrong eine Gesellschaft, in der eine Intensivierung von Überwachung in nahezu allen Lebensbereichen festzustellen ist, wobei die ganze Bandbreite technischer Möglichkeiten ausgeschöpft wird. Die Autoren sehen die wachsende Videoüberwachung im öffentlichen Raum in Großbritannien als *ein* Element in einer hochentwickelten Kombination von Technologien, deren Ziel die Klassifikation, die Aufdeckung von Straftaten und die Herstellung von Konformität ist.[202] Zunehmend werden in Großbritannien auch Computer und Datenbanken eingesetzt, welche die Überwachung der Monitore durch Menschen überflüssig macht

---

[197] Lyon 2001, S. 47

[198] vgl. Lyon 2001, S. 30

[199] vgl. Lyon 2001, S. 35

[200] vgl. Lyon 2001, S. 37

[201] vgl. Lyon 2001, S. 46f

[202] vgl. Norris / Armstrong 1999, S. 20

und die Verdächtige schneller als jeder menschliche Beobachter ermitteln können.[203] Norris und Armstrong weisen darauf hin, dass es auf diese Kombination der Kameras mit anderen Komponenten ankommt:

> „However, while we are all increasingly under the camera`s gaze what this means in practice is that its implications for social control are dependent not so much on the cameras, but on their integration with other technologies, and the organisational environment in which they operate.“[204]

Die Autoren sehen eine Erklärung der wachsenden Verbreitung von technischen Überwachungs- und Kontrollsystemen darin, dass wir in einer Gesellschaft von *Fremden* leben, in der wir uns von traditionellen Familien- und Gemeindestrukturen entfernt haben. Die Frage nach der Identität und der Vertrauenswürdigkeit einer Person kann also nicht mehr durch das unmittelbare Umfeld bestätigt werden und rückt so in das Interesse auch von technischer Überwachung.[205] Mit dieser Interpretation schließen sie sich Lyon an.

Norris und Armstrong stellen heraus, dass die Idee der Überwachung sich durch das ganze 20. Jahrhundert hindurch zieht. Nicht nur im akademischen Diskurs, sondern auch in der Pop-Kultur, in Filmen (z.B. „Das Fenster zum Hof“ von Hitchcock), Büchern (wie z.B. Orwells „1984“) und Songtexten (z.B. „Every Breath you take“ von The Police) ist das Thema vielfältig behandelt worden. Ein grundsätzliches Gefühl des Unbehagens scheint in der Bearbeitung des Themas *Überwachung* stets mitzuschwingen, da Überwachung auch immer tief in die Struktur totalitärer Regime eingebunden ist, auf der anderen Seite aber auch den Schutz und die Fürsorge eines wohlwollenden Wächters verspricht.[206] Überwachung hat somit immer zwei Gesichter. Im akademischen Diskurs wird Überwachung als essenzielle Form der Machtausübung betrachtet, die sich im Rahmen der technischen Entwicklungen immer weiter innerhalb der Gesellschaft ausbreitet. Ein Bild, das dabei häufig Verwendung findet, ist das bereits in Kapitel 2.2.1 beschriebene Panoptikum. Dieses Bild wurde oft auf gesellschaftliche Prozesse, wie z.B. das der technischen Überwachung übertragen. Die Gefahr, die dabei vielfach gesehen wird, liegt in der Zentralisierung der Macht und in der Errichtung eines Totalen Überwachungssystems.

Ein solches System würde, übertragen auf die heutigen technischen Möglichkeiten, nach Dandecker,[207] folgende Merkmale haben:

---

[203] vgl. Norris / Armstrong 1999, S. 56f

[204] Norris / Armstrong 1999, S. 59

[205] vgl. Norris / Armstrong 1999, S. 22

[206] vgl. Norris/Armstrong 1999, S. 3f

[207] Dandecker zitiert nach Norris / Armstrong 1999, S. 7

- eine Verbindung von (beispielsweise) Kamera-Daten mit biographischen Informationen
- eine Zentralisierung dieser Daten (dabei wird es unmöglich, seiner eigenen Biographie zu entgehen, auch nicht, wenn man z.B. in eine andere Stadt zieht)
- eine hohe Geschwindigkeit des Datenaustauschs (z.B. die Datenübertragung via Internet)
- eine große Häufigkeit, mit der das Überwachungssystem auf die zu überwachende Bevölkerung trifft

Bisher war es so, dass es kein Überwachungssystem gab, das von einer einzigen Behörde oder Institution verwaltet wurde. Es bestanden viele kleine „Big Brothers“ mit ganz unterschiedlichen Zielen der Überwachung. Die jüngsten Entwicklungen nach dem 11.September weisen aber in mehreren Staaten in Richtung der Zentralisierung solcher Daten.[208]

2.5.3 Zusammenfassung

Die Perspektiven der Surveillance und Maximum Surveillance Society gehen stärker auf technische Überwachungs- und Kontrollsysteme ein und integrieren auch die Computertechnologie in ihre Analyse. Der kanadische Soziologe Lyon definiert daher Überwachung als „Sammlung und Verarbeitung von persönlichen Daten zum Zwecke der Einflussnahme und der Verwaltung“.[209] Computer spielen dabei eine entscheidende Rolle, da sie die Möglichkeiten bieten, Daten zu verwalten, zu bearbeiten und zu vernetzen. Die heutigen Informationsgesellschaften mit ihrem Rückgang des persönlichen Kontakts zwischen Menschen sind gleichzeitig Überwachungsgesellschaften. Dabei wird das Konzept der Überwachungsgesellschaft nicht als fester Status gesehen, sondern als eine Tendenz im sozialen Bereich, ein sozialer Trend. Sie ist breit in der gesamten Gesellschaft verankert, der Staat bildet nur einen Aspekt innerhalb des Überwachungsszenarios. Gründe für die Entwicklung können in Becks Analyse der Risikogesellschaft gesehen werden, in der Überwachung Teil eines Risikomanagement ist, das selbst wieder Risiken hervorbringt.

Im Ansatz der Maximum Surveillance Society wird ebenfalls eine Intensivierung der Überwachung in nahezu allen Lebensbereichen festgestellt, welche die ganze Bandbreite technischer Möglichkeiten ausschöpft. Die Briten Norris und Arm-

[208] Das in Kapitel 3.2 beschriebene Information Awareness Office der US-Regierung ist ein Beispiel dafür.

[209] vgl. Lyon 2001

strong haben sich in diesem Zusammenhang intensiv mit der Videoüberwachung auseinandergesetzt, weisen jedoch darauf hin, dass es hauptsächlich auf die Integration dieser Technik in andere Systeme und Organisationsstrukturen ankommt. Auch sie sehen den Grund für die steigende Überwachung in den gesellschaftlichen Änderungen der traditionellen Familien- und Gemeindestrukturen und im Rückgang persönlicher Kontakte im Zuge der Nutzung von Informationstechnologien. Es wird immer wichtiger, Orientierungen zu bekommen und sich über die Identität und Absichten eines Anderen Klarheit zu verschaffen. Das Thema Überwachung zieht sich, wie auch schon Lyon argumentierte, durch die gesamte Gesellschaft und zeigt sich in Kunst, Wissenschaft und Politik. Als Metapher für ein totales Überwachungssystem kann Benthams Panoptikum betrachtet werden, ein Gefängnismodell, das seit Foucaults Darstellung in *Überwachen und Strafen* immer wieder als Sinnbild für völlige Konformität auftaucht. Ein totales Überwachungssystem, also die Maximum Surveillance, kann - nach Dandecker - festgestellt werden, wenn z.B. Kamera-Daten (oder andere Informationen des täglichen Lebens) mit biographischen Informationen verknüpft werden, diese Daten zentralisiert werden, eine hohe Geschwindigkeit des Austauschs der Daten zu verzeichnen ist und die Bevölkerung häufig mit Überwachungssystemen konfrontiert wird.

Schwerpunkt des Ansatzes der Maximum Surveillance Society sind die Möglichkeiten, die sich durch die heutige Computertechnik und vor allem deren Vernetzung ergeben. Ziele der Datenerhebung können sich wandeln und Datensätze immer leichter von unterschiedlichen Stellen genutzt werden, die sich zu einer Kooperation entschließen.

2.6 Zwischenfazit

In der gegenwärtigen pluralistischen und hoch differenzierten Gesellschaft der Postmoderne sind auch die Perspektiven auf Kontrolle und Überwachung heterogen und wurden innerhalb des theoretischen Teils der Arbeit vorgestellt. Durch die unterschiedlich betitelten Gesellschaftsbetrachtungen zog sich Ulrich Becks Risikogesellschaft genauso wie die Machtanalysen Foucaults durch. Es kann festgehalten werden, dass innerhalb der vorgestellten Ansätze prinzipiell zwei Erklärungsmuster vorherrschen: Einerseits stellt sich die Situation so dar, dass der Versuch der Herstellung von *Sicherheit* als Handlungsmotiv für die Etablierung von Überwachungs- und Kontrollszenarien gesehen wird. Die Gesellschaft befindet sich in einem permanenten Ausnahmezustand, der die Herstellung von Sicherheit für jeden zur Aufgabe macht. Es zeichnet sich ein verändertes Verhältnis zwischen Staat und Bürger ab, bei dem der Bürger zum Verdächtigen wird und bei dem es zu einer Veränderung des Regimes, der Ausübung von Macht kommt, wie sie von Foucault beschrieben wurde. Laut Foucaults Betrachtung weicht die

Disziplinierung der Bevölkerung immer mehr einer ökonomischeren Methode, die über das Sicherheitsdispositiv wirkt. Die Machtmechanismen regieren weniger über Angst und Schrecken (wie in der Feudalgesellschaft) oder über Einschließungsmilieus wie in der Disziplinargesellschaft (in der es darum ging, den Körper durch Schule, Militär, Fabrik etc. gefügig zu machen), sondern bedienen sich ökonomischeren Methoden, die über das Dispositiv der Sicherheit operieren. Auch für Foucault ist das Motiv der Sicherheit also ein zentrales, das dazu dient, die Bevölkerung zu kontrollieren, einen bestimmten Gebrauch von Freiheit zu garantieren und eine kollektive Imagination von Risiken und deren Abwehr zu produzieren. Die Machtform der Gouvernementalität regiert, wie Krasmann es ausdrückt, aus *Distanz*. Disziplinartechnologien werden durch Sicherheitstechnologien abgelöst, was die Frage aufwirft, ob sich dies auch innerhalb der Erziehung erkennen lässt – in der Praxis vielleicht so etwas wie eine *Erziehung aus Distanz* und unter den Vorzeichen der *Sicherheit* zu finden ist. Im Hinblick auf die beschriebene Flexibilität des Staates in der Interpretation seiner Zuständigkeiten, der Definition was privat und was öffentlich ist, wird es interessant sein zu schauen, ob sich in der Alltagspraxis diese Merkmale der Macht auch zeigen, ob es diese Flexibilität auch im Einsatz technischer Kontroll- und Überwachungssysteme gibt und ob das Subjekt sich tatsächlich dazu angehalten fühlt, sich an der Produktion von Sicherheit zu beteiligen.

Die Risikogesellschaft bedingt automatisch eine Überwachung der Bevölkerung; da potenzielle Risiken bereits im Vorfeld ermittelt werden sollen, ist ein Sammeln von Daten über den Bürger wichtig. Die zu Beginn der Arbeit von Lyotard gestellte Frage „Wer wird wissen?“ ist hier noch einmal interessant, denn es kommt keinesfalls zu einer Demokratisierung des Wissens, sondern das Wissen um das *Risikoprofil* des Einzelnen ist nicht einmal in dessen eigenen Händen, wie es im Rahmen des Rechts auf Informationelle Selbstbestimmung eigentlich sein sollte - es befindet sich in Datenbanken von Wirtschaftsunternehmen und staatlichen Stellen.

Kontrolle und Überwachung stützen sich nicht mehr auf moralische Rechtfertigung, sondern beziehen sich nunmehr auf Räume, aus denen bestimmte Gruppen von Menschen geduldet oder ausgeschlossen werden. In der Innenstadt sind bestimmte Gruppen - beispielsweise Punks und Obdachlose – nicht erwünscht. Sie sollen sich einen anderen Raum suchen; einer möglichen Integration steht ein Ausschluss gegenüber. Technische Kontroll- und Überwachungssysteme sind an dieser Stelle ideale Instrumente innerhalb der beschriebenen Ansätze, denn sie versprechen – auch in der aktuellen Diskussion um Terrorismusbekämpfung – ein Mehr an Sicherheit und machen es leichter, ein In oder Out zu vollziehen. Erst durch den Einsatz von EDV wird es möglich, die Masse an Daten zu verwalten, auszuwerten und Menschen ihren Platz in der Gesellschaft zuzuweisen, wie Deleuze es beschrieben hat. Durch technische Kontroll- und Überwachungssysteme

kann in Verbindung mit Computertechnologie vermeintlich Konformität, Sicherheit und Ordnung hergestellt werden.

Der zweite Erklärungsansatz ergänzt die Betrachtung des Phänomens um die Sichtweise, die Technik nicht nur als *Mittel* zu sehen, um bestimmte Ziele zu erreichen, sondern auch die von den Medien selbst verursachten strukturellen Veränderungen zu berücksichtigen. Technische Kontrolle und Überwachung werden als der Informationsgesellschaft inhärent gesehen, in der immer weniger persönliche Kontakte gepflegt werden und die Frage, mit wem man es eigentlich zu tun hat, eine entscheidende Bedeutung erhält. Hier wird auch der Ansatz der Risikogesellschaft als Erklärung integriert, indem Überwachung als Teil eines Risikomanagements gesehen wird, das selbst wieder Risiken hervorbringt. Überwachung zieht sich als *Trend* durch alle Bereiche der Gesellschaft – der Staat ist *einer* davon. Technische Kontroll- und Überwachungssysteme bieten eine vermeintliche Orientierung und Möglichkeiten, sich über die Intention und Identität des Anderen Klarheit zu verschaffen. In der *Totalen Überwachungsgesellschaft* (also der Maximum Surveillance Society), deren Symbol das Panoptikum ist, sind durch Computernetzwerke alle persönlichen Daten vernetzt – man weiß nicht, in wessen Händen diese Daten sind und zu welchem Zweck sie verwendet werden. Konformität ist der einzige Ausweg aus diesem Dilemma.

Teil II: Zur derzeitigen Anwendung technischer Kontrolle und Überwachung im Alltag

3 Ausgewählte Systeme in der Alltagspraxis

Innerhalb des nun folgenden Kapitels wird ein erster Blick auf die Systeme geworfen, die in den Fallstudien näher untersucht werden. Anhand der Vorstellung soll verdeutlicht werden, in welcher Bandbreite sich technische Kontroll- und Überwachungssysteme bereits in unserem Alltag etabliert haben. Die Auswahl der Techniken verlief nach folgenden Kriterien:

- Zum einen wurde innerhalb der Alltagspraxis der Forscherin geschaut, welche Systeme im Alltag bereits eine feste Größe darstellen. Hier konnte durch Teilnehmende Beobachtung und Auswertung der Tagespresse die Videoüberwachung, die Kundenbonuskarten und das Global Positioning System (GPS) als Systeme ermittelt werden, die sich bereits im Alltag etabliert haben.
- Ein weiteres Kriterium war, Systeme auszuwählen, welche die Menschen *freiwillig* einsetzen oder anscheinend billigend in Kauf nehmen.

Zu den vorgestellten Techniken existiert unterschiedlich viel Material. Die Videoüberwachung beispielsweise stellt, wie bereits verdeutlicht wurde, ein gut erforschtes System dar, während der Kontrollaspekt bei Kundenbonuskarten oder GPS so gut wie nicht erfasst ist. Bei letzteren wurde neben der Beschreibung der Einsatzmöglichkeiten im Alltag daher auch eine Einschätzung des Kontroll- und Überwachungspotenzials gegeben.

3.1 Alles im Blick: Videoüberwachung

Der öffentliche Raum

Abbildung 1: Hinweisschild auf Videoüberwachung in Leipzig.

In Deutschland sind - neben den Verkehrsüberwachungskameras, die es schon seit 1958 gibt – in den letzten Jahren Videokameras im öffentlichen Raum immer häufiger an so genannten Kriminalitätsschwerpunkten von der Polizei eingesetzt worden. In vielen Städten kam es, teilweise nach Änderung der Polizeigesetze, zur Installation von Videoüberwachungsanlagen, wobei eine zuverlässige Angabe über die Zahl der installierten Videokameras derzeit nicht vorliegt. Ziel im städtischen Umfeld ist es, Kriminalitätsschwerpunkte durch die Kameras *sicherer* zu gestalten. Video-

überwachung soll abschreckend auf die Täter wirken und dadurch Verbrechen verhindern. Die Bürger sollen sich durch die Kameras sicherer *fühlen*.

In mehreren Städten sind in den vergangenen Jahren Modellprojekte durchgeführt worden, die erhellen sollten, welche Auswirkungen die Videoüberwachung solcher Kriminalitätsschwerpunkte hat Beispiele sind hier Leipzig, das bundesweit als Pilotprojekt angesehen wird, und Bielefeld, das als Modellprojekt für Nordrhein-Westfalen etabliert wurde.[210] In Leipzig wurden seit 1996 der Bahnhofsvorplatz und andere öffentliche Plätze von der Polizei videoüberwacht. Mit Schildern wird - siehe Abbildung 1 - auf diese Überwachung hingewiesen.

In Bielefeld wurde nach einer Projektphase 2002 die Videoüberwachung des Ravensberger Platzes wieder eingestellt. Das Modellprojekt Bielefeld wurde, trotz Kritik, dass es zu keiner wissenschaftlich fundierten Evaluation des Projektes gekommen war und der Ravensberger Platz mit 6 Delikten im Jahr 2000 nicht wirklich als Kriminalitätsschwerpunkt bezeichnet werden konnte [211], als Erfolg gewertet und im Jahre 2003 daraufhin das Polizeigesetz des Landes Nordrhein-Westfalen in punkto Videoüberwachung verschärft.

Eine Vielzahl an Videokameras lässt sich daneben im privaten und halböffentlichen Bereich, wie z.B. im Bereich der Wahrung des Hausrechts (Bahnhöfe, Einkaufspassagen) lokalisieren. Hier geht es darum, unerwünschte Besucher (Obdachlose, Punks und andere marginalisierte Gruppen) schneller bemerken zu können und sie vom Aufenthalt im Gebäude abzubringen, wie es bereits im Ansatz der Kontrollgesellschaft beschrieben wurde.

Ferner wird oftmals mit dem Aspekt Sicherheit – wie schon bei Legnaro beschrieben - geworben, welche die Videoüberwachung herstellen soll. Im privatwirtschaftlichen Bereich hat Videoüberwachung hauptsächlich den Sinn, den Konsumenten, die Einkaufspassagen oder Kaufhäuser besuchen, ein gutes und sicheres Gefühl zu vermitteln. Einkaufen soll eine angenehme Erfahrung sein, die nicht durch Kriminalität, herumlungernde Jugendliche oder Obdachlose gestört werden soll. Videoüberwachungssysteme sollen eine abschreckende Wirkung haben und im Nachhinein zur Aufklärung von Straftaten beitragen. Vielfach werden sie auch zur Durchsetzung von Hausverboten eingesetzt. Zu diesem Bereich lässt sich auch die Videoüberwachung in öffentlichen Verkehrsmitteln zählen, bei dem ebenso das Argument der Sicherheit der Fahrgäste und des Schutzes gegen Vandalismus vorgebracht wird. Videoüberwachung kann dort aber allenfalls, wie in Fallstudie A am Beispiel der Kölner Verkehrsbetriebe deutlich gemacht werden wird, zur nachträglichen Aufklärung eines Falles beitragen. Die

[210] vgl. z.B. Veil 2001, S. 10f

[211] vgl. z.B. Schulzki-Haddouti 2002 und Foebud 2005

Aufzeichnungen können bei Bekanntwerden eines Vorfalls den Ermittlungsbehörden übergeben werden.

Der private Bereich

Dadurch, dass Videoüberwachungstechnik in den letzten Jahren für viele erschwinglich geworden ist, greifen auch immer mehr Durchschnittsbürger zu diesem Verfahren, um beispielsweise ihre Grundstücke zu überwachen.

Über den Objektschutz hinaus werden auch Systeme angeboten, die unmittelbar in die Kindererziehung hineinspielen und Eltern oder anderen Aufsichtspersonen die Möglichkeit geben, Kinder zu überwachen, sei es per (sichtbarer) Webcam oder versteckter Minikamera. Beim Kaffeeröster Tchibo konnte man vor kurzem beispielsweise eine solche Überwachungstechnik für Kinder (oder auch andere Personen) erwerben: Ein Funk-Überwachungssystem zur kabellosen Farbbild- und Tonüberwachung liefert dank seiner Infrarotbeleuchtung auch Schwarzweißbilder im Nachtsichtmodus. Auch eine Aufzeichnung der Aufnahmen mit dem Videorekorder ist möglich.[212] Das bereits etablierte System der akustischen Überwachung mittels Babyfon wird durch fast schon geheimdienstlich anmutende Systeme mit Nachtsichtmodus ergänzt und einer breiten Zahl von Konsumenten zugänglich gemacht. Ein anderes System ist die so genannte Teddycam, die eine verdeckte Überwachung durch eine in einem Teddy eingebaute Videokamera ermöglicht.

Abbildung 2: Beispiel für ein Kinderüberwachungssystem mit Nachtsichtmodus

Videoüberwachung in öffentlichen Erziehungsräumen

Innerhalb der Aktion Netdays 1998 wurde ein spanisches Projekt mit dem Namen BabyNet von der Europäischen Union gefördert. Hier geht es um ein System, das in Kindergärten und Vorschulen installiert wird, um Videobilder der Kinder in Echtzeit über das Internet an die elterlichen PCs zu übertragen. Dies soll helfen – wie es auf der Webseite heißt - die Eingewöhnungsphase im Hort für die Kinder angenehmer zu gestalten und für die Eltern vertrauenswürdiger erscheinen zu lassen. Eltern sollen so an der Erziehung ihrer Kinder im Kindergarten teilhaben, Kinder sollen „die Hauptdarsteller der neuen Technologie sein“ und die Techno-

[212]Das Angebot stammt vom Februar 2005 und war sowohl online, wie auch in den Tchibo-Filialen für 99,- Euro zu erstehen, vgl. Tchibo 2005

logie soll in einer positiven, erzieherischen und kreativen Art angewendet werden. Die Sorgen der Eltern um ihre Kinder sollen verringert werden und „völliges Vertrauen“ gegenüber den Kindergärten und Vorschulen entstehen.[213] Ähnliche Systeme sind bereits in Ländern wie den USA gängige Praxis in der Vorschulerziehung.[214] In Großbritannien setzt man gar Videoüberwachung auf Schultoiletten ein, um die Jugendlichen am Rauchen zu hindern und auch in Deutschland wurde Videoüberwachung als disziplinierendes Mittel erprobt: Einige Schulbusse im Landkreis Oberhavel sind bereits mit Videoüberwachungskameras ausgestattet worden; es wurden pro Bus vier Videokameras installiert, die das Geschehen in jedem Winkel des Busses aufzeichnen. So soll nach einem Unfall, der durch Rangeleien im Bus ausgelöst wurde, die Disziplin bei der Fahrt verbessert und Streitereien, Mobbing und Schikane unter den Schülern begegnet werden.[215] Auch auf Schulhöfen ist die Videoüberwachung kein Tabuthema mehr, wenn es darum geht, Drogendealer fernzuhalten oder Gewalt einzudämmen.[216]

Forschungsergebnisse aus Großbritannien

Jahrelanger Vorreiter in der Überwachung seiner Bürger war Großbritannien, wo derzeit geschätzte sieben Millionen Kameras im öffentlichen Raum aufgestellt sind[217] und U-Bahnstationen, Busse, Einkaufsstraßen, Parkplätze und zunehmend auch Wohngebiete überwacht werden. Nach den Ereignissen des 11. September hat auch die Überwachung der US-amerikanischen Bürger stark zugenommen, da aktuelle Zahlen zum Stand der Videoüberwachung in den USA nicht vorliegen, darf die Vorreiterstellung Großbritannien in diesem Bereich zumindest in Frage gestellt werden. Es sollen einige wichtige empirische Ergebnisse an dieser Stelle kurz vorgestellt werden.

Eine von der Labour-Regierung in Großbritannien in Auftrag gegebene und 2002 veröffentlichte Studie kommt zu dem Ergebnis, dass in Gegenden mit intensiver Videoüberwachung die Verbrechensquote lediglich um 4% zurückging, auf Straßen, die besser beleuchtet wurden, sank die Quote um 20%. Unterschiede gibt es allerdings bei der Art der Verbrechen. Hier kam es bei der Bekämpfung von Vandalismus und Autodiebstählen zu größeren Erfolgen (Rückgang 41%), im Bereich des Gewaltverbrechens zeigt Videoüberwachung allerdings keine Wirkung.[218] Bei der Sachbeschädigung scheint Videoüberwachung also durchaus eine

---

[213] vgl. BabyNet 2002

[214] vgl. beispielsweise Kindercam 2005 oder Watchmegrow 2005

[215] vgl. Jaeger 2000, S. 142

[216] vgl. Zips 1999, S. 10

[217] vgl. Rötzer 2005

[218] vgl. NTV-Meldung vom 15. August 2002

Wirkung zu zeigen, wobei andere Studien belegen, dass sich die Straftaten nur örtlich verlagern und dann an Stellen begangen werden, an denen es keine Videoüberwachung gibt.[219]

Norris und Armstrong haben die unterschiedlichen Bereiche, in denen Closed Circuit Television (CCTV) eingesetzt wird, zusammengetragen. Zum einen ist dies die Residential Surveillance, also die Überwachung von Wohngebieten durch die Polizei, lokale Verwalter oder Hausmeister, aber auch durch die Bewohner selber, die sich in das CCTV-System einloggen und ihr Wohngebiet überwachen können.[220] Des Weiteren werden in Großbritannien auch Schulen videoüberwacht. 1996 wurden 66 Millionen Pfund für Schulsicherheit bereitgestellt, damit konnten über 100 Schulen mit Videoüberwachungssystemen ausgerüstet werden. Eine Grundschule in Wolverhampton beispielsweise konnte mit Geld aus dem Fonds 16 Kameras installieren. Eine Besonderheit ist, dass über einen Lautsprecher eine mündliche Verwarnung gegeben werden kann, wenn auf dem Überwachungsmonitor ein Verstoß bemerkt wird. Ferner werden in Großbritannien Verkehrsüberwachungen, Parkplatz- und Tankstellenüberwachungen, Telefonzellen- und Geldautomatenüberwachungen durchgeführt. Es werden Eisenbahnstrecken observiert, Geschäfte, Krankenhäuser und Fußballstadien gefilmt.

Abbildung 3: Kleine Decken-Videoüberwachungskamera, aufgenommen in der Neumarkt-Passage in Köln

Beispiele für Kameramodelle im öffentlichen Raum

Videokameras treten im öffentlichen Raum in sehr unterschiedlicher Form in Erscheinung. Einige Beispiele aus der Kölner Innenstadt, aufgenommen in einem U-Bahn-Zugang und einer Einkaufspassage sollen die zurzeit gängigen Modelle darstellen. Teilweise sind die Kameras sehr unauffällig und klein, andernorts, wie links im Bild, deutlich als Überwachungskameras zu erkennen.

[219] Eine gute Übersicht über die Studien aus Großbritannien bietet hier die Arbeit von Veil 2001

[220] Norris / Armstrong 1999, S. 43

Abbildung 4: Beispiel für Standard-Videoüberwachung, aufgenommen im U-Bahn-Zugang am Kölner Neumarkt

Abbildung 5: Beispiel für eine sog. Dome-Kamera an der Decke, aufgenommen in der Neumarkt-Passage in Köln

Ausblick

Die technische Entwicklung schreitet weiter voran, und Softwarefirmen entwickeln Datenbanken, die in der Lage sind, Daten aus verschiedenen Bereichen zusammenzuführen und für die Polizeiarbeit nutzbar zu machen.[221] Damit könnte die Anonymität der Bürger bei der Kameraüberwachung nur noch für einen absehbaren Zeitraum der Status quo sein; in Zukunft wird es auch möglich sein, immer mehr Gesichter aus der Menge mit Datenbanken abzugleichen und zu identifizieren. Norris und Armstrong sehen die Etablierung von Videoüberwachungssystemen in Großbritannien auf uneingeschränkten Vormarsch. Gegenden, die noch keine Videoüberwachung nutzen, werden in einen enormen Zugzwang kommen, diese Systeme ebenfalls einführen, da die Angst besteht, Straftäter oder unerwünschte Personen könnten nun in Bereiche abwandern, die nicht kameraüberwacht sind.[222] Eine Gefahr sehen die Autoren in der Vernetzung verschiedener Systeme aus dem privaten und öffentlichen Bereich, die eine Totalüberwachung und den Weg in die bereits im theoretischen Teil beschriebene Maximum Surveillance Society ankündigt.[223]

Das wahre panoptische Potenzial ist dann erreicht, wenn die Kameradaten einer Masse von Bürgern gesammelt und in Akten aufgenommen werden. Dann wäre es möglich, eine individuelle Datei der Bewegungen und Gewohnheiten einer jeden Person zu erstellen, die mit Polizei und Verwaltungsdaten kombiniert werden könnten.[224]

---

[221] vgl. Norris / Armstrong 1999, S. 201

[222] vgl. Norris / Armstrong 1999, S. 205

[223] vgl. Norris / Armstrong 1999, S. 207

[224] vgl. Norris / Armstrong 1999, S. 210

Ein Augenmerk soll auch auf die in den letzten Jahren in Großbritannien entstandene Konvergenz zwischen Videotechnik und Computer gelegt werden, die auch für Deutschland einen Ausblick geben kann, wohin Entwicklungen gehen können. Immer häufiger werden Daten der Videoüberwachungskameras über Funk oder über Computernetzwerke mit Datenbanken abgeglichen. Beispiel hierfür ist, dass jedes Nummernschild eines in London einfahrenden Autos automatisch mit einer Datenbank abgeglichen wird, die Informationen über gestohlene oder verdächtige Fahrzeuge enthält. Bei Fußballspielen und ähnlichen Großveranstaltungen werden Systeme erprobt, die Gesichter aus einer Datenbank in der Menge wiederfinden können, um so beispielsweise bekannte Unruhestifter ausfindig zu machen. In der Entwicklung stehen des Weiteren Programme, die *verdächtiges* Verhalten von *unverdächtigem* unterscheiden wollen und bereits im Vorfeld durch einen ausgelösten Alarm Straftaten zu verhindern suchen. Entwickelt wurde das System von der University of Leeds gemeinsam mit der University of Reading. Es *lernt* das von einer Videokamera aufgezeichnete *normale* Verhalten auf Parkplätzen oder Supermärkten von *verdächtigem* Verhalten zu unterscheiden und entsprechend mit einem Alarmsignal zu reagieren, wenn jemand sich auffällig verhält.[225]

3.2 Die Kontrolle in der eigenen Tasche: Bonuskarten

Bonuskarten begegnen uns mittlerweile fast ständig bei unseren täglichen Besorgungen. Fast jedes größere Einzelhandelsunternehmen nimmt derzeit an einem so genanten Kundenbonussystem teil, wobei der Markt hauptsächlich vom Marktführer Payback mit Partnern wie Real, dm, Obi und Kaufhof und seinem Konkurrenten Happy Digits mit Beteiligten wie Karstadt, T-Online und Tengelmann dominiert wird. Das, was die Bonuskarten zum technischen Kontroll- und Überwachungssystem werden lässt, liegt eigentlich nicht bei der Karte selbst, deren Speicherkapazität meist nur gering ist, sondern in der Tatsache, dass die auf den Karten gesammelten Informationen eingelesen und weiterverarbeitet werden.

Dazu wird die Bonuskarte von Hand oder maschinell an einem Lesekopf vorbeigezogen, wobei die Daten gelesen und elektronisch gespeichert, weitergeleitet und weiterverarbeitet werden. Im Falle der Payback-Karte, bei der es sich um eine Magnetstreifenkarte handelt, kann es, über die Kundennummer der jeweiligen Karte, zu einer Zusammenführung von persönlichen Daten, wie Name, Adresse und Geburtsdatum mit Daten über den täglichen Konsum kommen, die von den beteiligten Firmen entsprechend ausgewertet werden können. Eine genaue Beschreibung des Verfahrens, welches das Payback-System anwendet, wird innerhalb der Fallstudie B gegeben werden. Anders als bei manchen Formen der

[225] vgl. Rötzer 1998

Videoüberwachung ist die Verwendung von Bonuskarten durchweg freiwillig; niemand wird gezwungen, sich eine solche Kundenkarte zu verschaffen, allerdings kann er so auch unter Umständen gewährte Rabatte nicht in Anspruch nehmen - ein Umstand, der die hohe Verbreitung der Kundenkarten erklärt, den in den Genuss von Rabatten möchten viele gerne kommen. Der Kontroll- und Überwachungseffekt von Kundenkarten ist weitgehend unerforscht. Er wurde lediglich innerhalb der datenschutzrechtlichen Fachdiskussion und in einigen Presseartikeln behandelt.

Technik

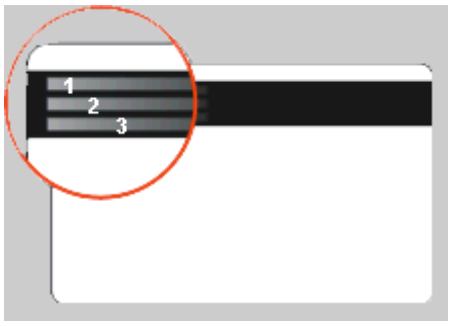


Abbildung 6: Illustration der Funktion einer Magnetstreifenkarte

Hinter den Kundenbonuskarten liegen unterschiedliche technische Systeme. So arbeitet Payback mit einer Magnetstreifenkarte, die in der Herstellung verhältnismäßig günstig ist und somit massenhaft ausgegeben werden kann. Die wichtigsten Daten (z.B. eine Kundennummer oder der Punktestand einer Bonuskarte) lassen sich auf einer Magnetstreifenkarte kodieren.

Einschätzung

Im Falle der Datensammlungen im wirtschaftlichen Bereich ist es so, dass über die Kundenkarten Daten über das Kaufverhalten des Kunden personenbezogen gespeichert werden. Verfahren wie das so genannte Customer Relationship Management (CRM) dienen dazu, aus diesen erhobenen Daten den *Wert eines Kunden* für ein Unternehmen herauszufinden. Ein Zitat aus einem Internet-Fachforum zu diesem Thema illustriert eindrucksvoll, was mit diesen Systemen bezweckt wird:

> „Um zu wissen, in welche Kunden ein Unternehmen investieren sollte, muss gehörige Vorarbeit geleistet werden, angefangen bei einer sauberen Kundendatenbank über die Erfassung der Kundenkontakte und Transaktionen bis hin zur statistischen Auswertung und Segmentierung ist es für die meisten Unternehmen ein langer und beschwerlicher Weg. Aber er lohnt sich, denn bei einer Kundenwertbetrachtung kommen überraschende Ergebnisse heraus – und die Frage: Wie werde ich unrentable Kunden los, wird zwangsläufig aufkommen. Bei den Banken und Telcos hat die Zukunft schon begonnen: Erhöhte Grundgebühren und gestrichene Subventionen nach dem Gießkannenprinzip sind die Realität für Kunden, die nicht genug Geld in den Kassen lassen. „So tragisch das im Einzelfall auch sein mag, diskriminierend ist es nicht, denn nur Gleiches soll Gleich behandelt werden – und Ungleiches ungleich“, sagt Naujoks.“226

Für die Unternehmen bieten Kundenkarten eine ideale Möglichkeit herauszufinden, in welche Kunden es sich lohnt zu investieren und welche Kunden unrentabel sind, dem Unternehmen nicht genug Profit bringen und somit eben weniger Vergünstigungen und Kaufanreize erhalten. Die Kluft zwischen der Behandlung vermögender und weniger betuchter Verbraucher wird mit solchen Systemen verstärkt – es handelt sich also hierbei um eine Art der Diskriminierung. Darauf heben beispielsweise auch Verbraucherschutzministerin Künast und der Bundesdatenschutzbeauftragte Schaar ab, die auf einer gemeinsamen Tagung auf die Gefahren einer Vernetzung und Verknüpfung der gesammelten Daten hinwiesen und sich gegen eine Kundenprofilerstellung aussprachen.[227]

Schleichende Erweiterung der Ziele der eingesetzten Technik

Ein Beispiel für die Möglichkeiten der Erweiterung einmal eingeführter Technik ist der im Februar 2004 bekannt gewordene Fall der Erweiterung der Nutzung von Kundenkarten. In Rheinberg bei Duisburg wurde durch die Metro AG der sogenannte *Futurestore* eingerichtet. Auf der Webseite des Unternehmens heißt es:

> „Gemeinsam mit Intel, SAP und IBM sowie zahlreichen anderen Unternehmen entwickelt die METRO Group im Rahmen der Future Store Initiative den Supermarkt der Zukunft. Als „Zukunftswerkstatt“ dient dabei ein Markt der Vertriebslinie Extra im nordrhein-westfälischen Rheinberg. Dort werden unter realen Bedingungen Einsatz und Akzeptanz von neuen Technologien im Handel getestet. Ziel sind nutzenorientierte Lösungen, die sowohl dem Handel als auch den Kunden Vorteile bringen.“[228]

Zu Protesten kam es, als der Bielefelder Datenschutzverein Foebud e.V. aufdeckte, dass sich in den vom Futurestore herausgegebenen Payback-Kundenkarten der Metro-Group ein Radio Frequency Identification-Chip (RFID-Chip) befindet. RFID-Etiketten sind winzige Computerchips die, mit Miniaturantennen versehen

---

[226] CRM-Forum 2005, Hervorhebung durch die Autorin

[227] vgl. Krempl 2005

[228] Metro 2004

sind und an Objekten (Verpackungen, Kleidung etc.) angebracht werden können. Bei den am meisten beworbenen Anwendungen von RFID enthält der Mikrochip einen elektronischen Produktcode (Electronic Product Code, EPC), der aussagekräftig genug ist, jedes weltweit hergestellte Produkt eindeutig zu identifizieren. Wenn ein RFID-Lesegerät ein Funksignal abgibt, antworten in der Nähe befindliche Chips, indem sie die auf ihnen gespeicherten Daten an das Lesegerät übermitteln. Typischerweise werden die Daten an ein System von vernetzten Computern gesandt, die zum Beispiel im Management von Versorgungsketten oder bei der Inventarkontrolle eines Lagers eingesetzt werden. Dieser Chip war nun ohne Information der Betroffenen auf 10.000 Payback-Karten des Unternehmens aufgebracht worden. Somit waren KartenbesitzerInnen und RFID-markierte Artikel eindeutig einander zuzuordnen und dies, ohne vorige Zustimmung der KarteninhaberInnen. Ein paar Wochen nach Aufdeckung des Vorfalls wurden die Karten von der Metro zurückgezogen.[229]

Ausblick

Der amerikanische Weg: Das Information Awareness Office (IAO)

Abbildung 7: Piktogramm des Information Awareness Office aus der Anfangszeit

Die Vorstellung eines „Big Brother“, der alle überwacht, war bislang eigentlich eine nicht ganz zutreffende Metapher für die zunehmende technische Überwachung und Kontrolle der Bevölkerung. Es gab – und gibt - viele kleine Big Brothers, die nebeneinander wirkten und deren Intentionen meist recht unterschiedlich war. Eine zentrale Speicherung und Zusammenführung der Daten einzelner Individuen war bisher nicht denkbar. Ende 2002 jedoch gab es erste Pressemeldungen, in denen die Gründung des Information Awareness Office (IAO) kommentiert wurde. Hinter diesem Begriff, der sich mit „Büro für Informationsbewusstsein“ übersetzen lässt, verbirgt sich ein möglichst lückenloses und flächendeckendes Personen-Überwachungssystem der US-Regierung, das den gesamten Erdball umspannen soll.

Das mit einem Budget von 200 Millionen US-Dollar ausgestattete Büro[230] hatte den Auftrag, ein Computersystem zu schaffen, das weltweite Datenströme auf

[229] vgl. Foebud 2004

[230] vgl. Illinger 2002 und Streck 2002

Hinweise zu geplanten Verbrechen überprüft. Dabei standen nicht nur die Datenströme des Internet im Fokus, sondern alle staatlichen, kommerziellen und privaten Daten, die Menschen in der digitalisierten Welt hinterlassen (Daten von Flugzeugpassagieren, Rabattkarten, Arzneibestellungen etc.). Als Symbol hatte sich das Büro das schon vom Dollar-Schein bekannte Auge über der Pyramide ausgewählt, der Slogan war „Scientia est potentia“: Wissen ist Macht. Die US-Regierung plante, aus der Fülle privater, behördlicher und geschäftlicher Daten Hinweise für Terroranschläge zu erhalten. Im Januar 2003 bekam diese Idee allerdings Gegenwind vom US-Senat, der eine Umsetzung, wenn überhaupt, nur unter strengen Auflagen bewilligen wollte. Der Senat folgte damit einem Gesetzentwurf eines demokratischen Senators, wonach genaue Pläne zu Umfang, Zielen und Kosten des Programms, sowie über Erfolgsaussichten und potenzielle Einschnitte in die Privatsphäre amerikanischer Bürger vorgelegt werden müssten. Das Pentagon hat allerdings erneut unterstrichen, wie wichtig das Programm und die Entwicklung neuer Informationstechnologie-Werkzeuge für die Bekämpfung des internationalen Terrorismus seien.[231] Wie sich das Projekt weiterentwickelt, bleibt abzuwarten.

Ein weiteres Beispiel für Data-Mining

Ein weiterer Schritt in Richtung transparenter Bürger ist die im Januar 2004 von Deutschlands größter Krankenkasse, der Barmer Ersatzkasse, eingeführte Idee der so genannten Barmer-Service-Apotheke. Hierbei handelt es sich um ein Konzept, dass es Barmer-Versicherten ermöglicht, „künftig eine individuelle pharmazeutische Betreuung“[232] in Anspruch zu nehmen.

> „Vorausgesetzt, der Versicherte entscheidet sich für eine bestimmte Service-Apotheke und erklärt sich damit einverstanden, dass dort alles seine medikationsbezogene Daten (eingeschlossen der Selbstmedikation) gespeichert werden dürfen.“[233]

Der Versicherte muss also zustimmen, dass seine individuellen medizinischen Daten zentral gespeichert werden. Als Gegenleistung führt die Barmer an, dass es nun möglich sei, die komplette Medikation eines Patienten via EDV abzurufen und auf eventuelle Wechsel- oder Nebenwirkungen aufmerksam zu machen. Ferner bietet die Barmer-Service-Apotheke an, gegen eine geringe Schutzgebühr Blutdruck, Cholesterinwerte oder Ähnliches zu ermitteln.

---

[231] vgl. Siegle 2003

[232] Barmer 2004, S. 24

[233] Barmer 2004, S. 24

Einschätzung

Der Versicherte stimmt zu, sämtliche seiner Medikamente, seien es Anti-Depressiva, Schlafmittel oder Viagra zentral speichern zu lassen. Als Gegenleistung erhält er eigentlich nichts, das nicht jetzt schon nahezu jede Apotheke anbietet, beziehungsweise, Dienstleistungen, die bei jedem Hausarzt kostenlos erhältlich sind. Die Frage ist, was sich die Krankenkasse von der Einführung eines solchen Systems verspricht. Um einen bloßen Gefallen am Kunden kann es dabei kaum gehen. Die Missbrauchsmöglichkeiten solcher Datensammlungen dagegen sind immens. Kommen die Daten in falsche Hände kann, das für den Einzelnen schwerwiegende Folgen haben (beispielsweise in Berufs- oder Privatleben, bei Versicherungen etc.).

3.3 Auf der Spur: Ortungstechniken (GPS und GSM)

Das Global Positioning System

Die am meisten bekannte Einsatzmöglichkeit des Global Positioning Systems dürfte der Einsatz innerhalb von Navigationssystemen im Auto sein. Fahrtziele können in das Gerät eingegeben werden, und mit Hilfe der Satellitentechnik wird der Fahrer oder die Fahrerin, meist über eine Ansage, zum gewünschten Ziel geleitet.

Neben Anwendungsmöglichkeiten im Bereich Verkehr kann GPS auch im Bereich der Personensicherheit verwendet werden. Menschen, die Angst vor Gewaltverbrechen oder Entführung haben, können sich dieser Technik bedienen. Immer wieder berichtet die Presse auch über die Möglichkeit, Kinder mit dieser Technik auszustatten, um sie besser vor Verbrechen zu schützen. Die Firma Philips hat beispielsweise im Jahr 2002 einen Kinderanorak auf den Markt gebracht, der mit einer Mini-Videokamera und einem Empfänger für das Global Positioning System ausgestattet ist. Eltern sollen so ihre Sprösslinge immer im Blick haben und über ihren genauen Aufenthaltsort informiert sein.[234] Eine andere Möglichkeit bietet ein Modell der Firma Wherify: Der GPS Personal Locator for Children, der wie eine Armbanduhr am Arm des Kindes befestigt ist (siehe Abbildung 8) und mit einer speziellen Sperre ausgestattet ist, damit er sich nicht ohne weiteres lösen lässt. Über eine Telefonnummer oder via Internet können die Eltern dann den Aufenthaltsort ihrer Sprösslinge metergenau ermitteln.[235] Die sicherlich drastischste Form, dieses System zum Einsatz zu bringen, sind GPS-Chips, die direkt

[234] mobil 2002, S. 33f.

[235] vgl. Wherify 2002

unter die Haut eingesetzt werden. Es gab in Amerika bereits vor Jahren einige Produkte (z.B. Kidbug[236]), die jetzt aber auch langsam in Europa an Beliebtheit gewinnen. Eine Familie aus Reading in England hat ihrer, zu diesem Zeitpunkt elfjährigen Tochter einen solchen Chip einsetzen lassen und der Entwickler dieser Technologie, Professor Kevin Warwick vom Cybernetics Department at Reading University, sieht darin eine Chance für Eltern, ihre Kinder im Falle eines Verbrechens lebend zu finden. Prof. Warwick fordert eine dringende Debatte der Britischen Regierung zu diesem Thema und vertritt die Ansicht, dass über Implantate für alle Kinder nachgedacht werden sollte.[237] Jede Bewegung des Kindes wäre somit rund um die Uhr nachvollziehbar.

Abbildung 8: GPS-Armbanduhr der Firma Wherify

Das Global System for Mobile Communications

Für ein deutsches Produkt der Siemens-Tochter Mobile Family Services wurde als Prototyp ein Teddybär gewählt, der mit einem Mobiltelefon und einem GPS-Empfänger ausgestattet ist. Die Kombination aus dem Global System for Mobile Communications (GSM) und GPS ermöglicht, den Standort des Kindes bis auf wenige Meter genau zu bestimmen.

Ein deutscher Provider bietet beispielsweise seinen Kunden an, über einen passwortgeschützten Zugang über das Internet den Standort des Handys zu ermitteln.[238] Ist es gerade ausgeschaltet oder wurde es einfach einer anderen Person übergeben, ist die Ermittlung des Aufenthaltsortes einer bestimmten Person allerdings nicht möglich. Hier bietet sich, wie bereits vorgestellt, GPS – oder wie beim Siemens-Produkt- eine Kombination aus beiden Systemen an.

Der GSM-Standard wird auch bei einem weiteren deutschen Produkt mit dem Namen Trackyourkid verwendet. Technisch funktioniert das Ganze so, dass jedes eingeschaltete Handy in mehreren Stationen eingebucht ist und darauf wartet, angerufen zu werden. Unter Zuhilfenahme der Location Based Services (LBS) wird der Standort des Handys nach der Signallaufzeit zu den einzelnen Stationen

[236] Rötzer 2002

[237] vgl. Wilson 2002

[238] vgl. O2 2004

berechnet und so der Standpunkt ermittelt. Über einen Internet-Zugang kann mal sich dann diesen Standpunkt auf einer Karte anzeigen lassen. Ferner kann man sich den Aufenthaltsort des Kindes auch per SMS auf das eigene Handy schicken lassen.

Einschätzung

Über den Mobilfunkstandard GSM ist für jeden Handy-Besitzer heraus zu bekommen, in welcher Funkzelle er oder sie sich gerade befindet. Bei einigen Providern ist es auch möglich, sich den Standort des Handys im Internet anzeigen zu lassen. Ob dies von den Kunden wirklich nur genutzt wird, um das Handy bei einem Verlust wieder zu finden, ist ungewiss, bietet diese Option doch auch eine bequeme Möglichkeit zu erfahren, ob der Partner sich wirklich noch im Büro aufhält, oder seine Funkzelle eventuell doch schon gewechselt hat. Bereits diese Technik bietet also schon ein hohes Maß an Möglichkeiten, Menschen zu überwachen. Die Freiheit des Handy-Trägers besteht allerdings auch darin, das Handy schlicht auszustellen, es einer anderen Person anzuvertrauen oder es einfach an einem Ort liegen zu lassen. Insbesondere bei der Verwendung des Handys als Überwachungstechnik für Kinder fehlen bislang Untersuchungen, wie sich eine solche Kontrolle auf das Vertrauensverhältnis zwischen Eltern und Kindern auswirkt, welche pädagogischen Konsequenzen daraus erwachsen und ob dieses Verfahren überhaupt funktioniert oder nicht vom Kind oder Jugendlichen schlicht umgangen wird. Durch Verwendung einer solchen Technik ändert sich in jedem Fall etwas in der Qualität des menschlichen Umgangs und der Erziehung, das es näher zu untersuchen gilt.

Das GPS-System arbeitet noch genauer und lässt eine Ortung bis auf wenige Meter genau zu. Hier haben sich mit Systemen wie Armbanduhren, die man nicht alleine entfernen kann oder Chips, die implantiert werden, Techniken etabliert, die an die Grenzen der Selbstbestimmung stoßen und an die Elektronische Fußfessel bei Straftätern erinnern. Unter dem Aspekt der *Sicherheit* des Kindes wird dies aber in Kauf genommen. Bei den Erwachsenen kann man beobachten, dass GPS-Empfänger in Autos eingebaut werden, ohne dass ein Bewusstsein darüber vorhanden ist, dass man im Gegenzug auch überall aufspürbar ist. Nicht ohne Grund hat sich die Bundesregierung für ein Mautsystem entschieden, dass über GPS funktioniert und einfachere Lösungen, wie beispielsweise die Vignette ausgeschlagen. GPS bietet viele verlockende Möglichkeiten, den Verkehrsstrom zu überwachen oder einzelne Fahrzeuge zu verfolgen, die man eventuell in Zukunft ausbauen kann.

3.4 Zusammenfassung

Die technischen Möglichkeiten der Kontrolle und Überwachung haben sich in den vergangenen Jahren immer mehr erweitert. Deutlich wurde anhand der Beispiele, dass Verfahren, die vor einigen Jahren noch geheimdienstlich anmuteten, mittlerweile auch von Privatpersonen genutzt werden. Der implantierte Ortungschip oder die Infrarot-Minikamera sind bei den ersten Privatanwendern angekommen.

Deutlich wurde in den Beispielen, dass die Zielsetzung der technischen Systeme sich wandeln kann. Einmal etabliert, bieten sie eine Vielzahl von Verwendungszwecken, die teilweise von ihrer ursprünglichen Zielsetzung abweichen, wie unter anderem die Beispiele aus dem Bereich Videoüberwachung und GPS illustrieren. Vor diesem Hintergrund zeichnen sich vielfältige gesellschaftliche Veränderungen ab, die sich in nahezu allen Bereichen vollziehen. Das Beispiel des Information Awareness Office zeigt, wie weit die Begehrlichkeiten des Staates gehen und zu welchen Profilen vermeintlich harmlose Informationen über Einzelne zusammengefasst werden können. Hier entstehen Datensammlungen über Bürger, die so in ein Raster geraten können, das sich gänzlich ihren Einflüssen entzieht, da einmal ausgegebene Daten nicht mehr rückholbar sind.

4 Fallstudien zur technischen Kontrolle und Überwachung

Das folgende Kapitel stellt die ausgewählten Fallstudien zu Techniken der Kontrolle und Überwachung im Alltag vor. Um einen Einstieg in die empirische Untersuchung zu erhalten, wurde ein Expertinneninterview mit der Datenschutzbeauftragten des Landes Nordrhein-Westfalen geführt. Hier interessierte – auch im Rückbezug auf Lyotard und die Frage „Wer wird wissen?“[239] – die Einschätzung der Datenschutzbeauftragten zur wachsenden Verbreitung technischer Kontroll- und Überwachungssysteme und den damit verbundenen Datensammlungen.

Die Datensammlungen haben das Ziel, die unterschiedlichen gesellschaftliche Bereichen - das öffentliche Leben, der Konsumalltag, und der private Familienalltag - mit beispielhaft ausgewählten technischen Systemen abzubilden. Die Fallstudie ist eine qualitative Methode der empirischen Sozialforschung, die sich vor allem für die Beobachtung zeitgenössischer Phänomene eignet. Unter Berücksichtigung unterschiedlicher Zugänge und Quellen ist diese Methode besonders geeignet, Beschreibungen empirischer Phänomene zu liefern oder für weitere Forschungsarbeiten als explorativer Einstieg in ein neues Forschungsfeld zu dienen.[240] Da die Verwendung technischer Kontroll- und Überwachungssysteme in der Praxis noch weitgehend unerforscht ist, eignen sich Fallstudien besonders zu einer ersten Exploration, wie sich dieses Phänomen im Alltag darstellt. Dabei sind die Fälle so aufgebaut, dass sie jeweils innerhalb der Ethnographie den Blickwinkel der Forscherin und innerhalb der Interviews den des Betreibers und der von der Überwachung Betroffenen zeigen. Der Rolle der Forscherin kommt dabei eine besondere Bedeutung zu, sie geht nie unvoreingenommen in das Feld, ihr Vorwissen strukturiert ihre Wahrnehmung und die Interpretation des Alltags. Es wurde daher bereits zu Beginn der Arbeit, das Vorwissen offengelegt, um den weiteren Forschungsprozess transparent zu machen. Für das folgende Kapitel stellen sich folgende Fragen:

[239] Im Hinblick auf das Forschungsthema wird Lyotard so gelesen, dass die Frage nach den Auswirkungen postmoderner Wissensstrukturen auf demokratische Grundrechte, wie beispielsweise das Recht auf Informationelle Selbstbestimmung, gestellt wird und die Bedingungen, unter denen Informationen über Personen gesammelt werden, im Alltag untersucht werden.

[240] vgl. Mayring 1996, S. 29f

- Wie stellt sich die jeweilige Technik im Alltag des Durchschnittsbürgers dar?
- Was versprechen sich diejenigen, die diese Technik einsetzen von diesen Systemen, und welche Ziele verfolgen sie?
- Welche Einstellungen haben die Adressaten der technischen Systeme? Aus welchen Gründen nutzen *sie selbst* die Technik?

Methodik

Innerhalb der Fallstudien wurde das methodische Ideal der Triangulation verfolgt. Die grundlegenden Techniken bestehen darin, wie Hitzler es formuliert, das Geschehen zu beobachten, sich Dokumente zu beschaffen und auszuwerten und mit beteiligten Personen zu sprechen.[241] Die Ethnographie, die Auswertung von Informationsmaterial, das Experteninterview und die Befragung von NutzerInnen der Systeme innerhalb Problemzentrierter Interviews stellen die in den Fallstudien verwendeten Methoden dar. In der Mehrheit handelt es sich bei der Untersuchung um qualitative Forschung, die aber an Stellen, an denen dies sinnvoll war, durch quantitative Daten ergänzt wurde.

In Anlehnung an Mayring erfolgt nach Erhebung des Materials die *Fallzusammenfassung*, bei der die wichtigsten Eckpunkte übersichtlich dargestellt werden und die *Fallstrukturierung*, in der das Material in Abhängigkeit von Fragestellung und Theorie gegliedert wird und versucht wird, das Fallmaterial in einzelne Kategorien zu ordnen. Diese beiden Verfahren bilden die Grundlage der Fallinterpretation und ermöglichen, schrittweise Erklärungen aus dem Material zu gewinnen. Schließlich wird der einzelne Fall mit anderen Fällen verglichen, um die Gültigkeit der Ergebnisse abschätzen zu können.[242]

Bei der Fallstudie zum Global Positioning System konnte aufgrund der noch geringen Verbreitung des Systeme keine Befragung der NutzerInnen erfolgen, denn dies hätte einen unverhältnismäßig hohen Aufwand, kombiniert mit datenschutzrechtlichen Problemen[243] dargestellt. Stattdessen wurde eine Radio-Diskussion zu diesem Thema mitgeschnitten, bei der sich Eltern zum Einsatz solcher Systeme äußerten. Diese wurde transkribiert und ausgewertet.

---

[241] vgl. Hitzler / Honer 1997, S. 13

[242] vgl. Mayring 1996, S. 29f

[243] Da die Betreiberfirma ihre Kundendaten nicht weitergeben darf, hätte der Kontakt direkt über eine Anfrage der Firma bei ihren Kunden laufen müssen. Dies wäre innerhalb des gesetzten Zeitrahmens nicht zu realisieren gewesen.

Auswahl der Fälle

Die einzelnen Fallstudien wurden auf das Ziel hin ausgewählt, verschiedene Bereiche des Alltagslebens zu erfassen. Diese sind: der Bereich des öffentlichen Lebens, der Konsumalltag und der private Familienalltag.

Der öffentliche Bereich wird über eine Fallstudie zur Videoüberwachung in den Fahrzeugen und Gebäuden der Kölner Verkehrsbetriebe (KVB) abgedeckt. Dieser Sonderfall der Videoüberwachung wurde ausgewählt, da von ihm weitere Erkenntnisse zu Effekten der Videoüberwachung erwartet wurden, welche über die im Theorieteil der Arbeit dargestellte Exklusion von Menschen hinausgeht. Ein weiterer Aspekt war, dass die KVB zum Zeitpunkt der Untersuchung der größte Betreiber von Videoüberwachungssystemen in Köln war. Die Videokameras sind sowohl in den Fahrzeugen der Verkehrsbetriebe, an den meisten Haltestellen, sowie in Passagen und Durchgängen zu KVB-Haltestellen zu finden. Sie stellen also für den öffentlichen Raum eine wichtige Größe dar. In Köln sind Videokameras auch an anderen öffentlichen Plätzen, Passagen und in Fußgängerzonen installiert; die Betreiber sind hier jedoch zumeist Einzelhandelsunternehmen oder Institutionen, wie z.B. die Polizei Köln, die einzelne Kameras betreiben. Die KVB stellte aufgrund der hohen Anzahl der Videokameras im öffentlichen bzw. halböffentlichen Raum, ein ideales Untersuchungsfeld dar.

Technische Kontroll- und Überwachungssysteme wurden durch die Untersuchung des Payback-Systems - einem Bonuskarten-Programm, bei dem die Einkaufsgewohnheiten der TeilnehmerInnen erfasst und Kundenprofile erstellt werden – für den Bereich des privaten Konsums erschlossen. Das seit dem Jahr 2000 existierende Payback-System ist mit über 27 Millionen[244] eingesetzten Karten das führende Bonusprogramm in Deutschland, es stellt damit die bislang größte zusammenhängende Erhebung des Kaufverhaltens der Bürger dar.

Im privaten Familienalltag wurden Kindersicherungssysteme unter Einsatz des Global Positioning Systems und der Mobilfunktechnik untersucht. Diese technischen Kontroll- und Überwachungssysteme sind relativ neu auf dem Markt und haben daher noch keine weite Verbreitung gefunden. Sie wurden in letzter Zeit aber häufiger in den Medien diskutiert und stellen einen Bereich der Kontrolle und Überwachung dar, der sich im Privaten abspielt - und dabei auf das sensible Thema der Sicherheit der eigenen Kinder abzielt. Dieser weitgehend unerforschte Bereich soll durch die Fallstudien weiter erschlossen werden. Dabei tritt im Rahmen dieser Fallstudie der pädagogische Aspekt am deutlichsten zu Tage.

[244] Stand: Januar 2005, vgl. Loyalty Partner 2005

4.1 Erhebung und Auswertung

Im Folgenden werden die Methoden, die innerhalb der Fallstudien benutzt wurden, vorgestellt. Der Zugang zu den einzelnen Untersuchungsfeldern wird innerhalb jeder Fallstudie zu Beginn beschrieben.

4.1.1 Die Ethnographie

Diese Methode wurde im deutschsprachigen Raum unter dem Begriff Teilnehmende Beobachtung beschrieben und ist in neuerer Zeit unter dem Einfluss der englischen und amerikanischen Diskussion und damit verbundenen konzeptionellen Veränderungen vornehmlich unter dem Begriff der Ethnographie diskutiert worden. Innerhalb der Ethnographie werden Beobachtung und Teilnahme mit anderen Verfahren verwoben. Die Ethnographie sucht nach Mitteln und Wegen, an der zu untersuchenden Alltagspraxis möglichst lange teilzunehmen und aus dieser Perspektive heraus Erkenntnisse zu gewinnen. Dabei wird versucht, möglichst viel an Daten über das Untersuchungsfeld zusammen zu tragen. Innerhalb der Fallstudien gehören dazu das Erstellen von Fotos, das Zusammentragen von Informationsmaterial, die Beobachtung und das Führen von Interviews. Die Fotos geben dabei einen Eindruck, wie sich die technischen Kontroll- und Überwachungssysteme vor Ort darstellen und wie sie aussehen. Dieser banal anmutende Aspekt zeigt sich in der Praxis als hilfreich, da bestimmte Kontroll- und Überwachungssysteme (z.B. Minikameras) für den Laien oft gar nicht zu erkennen sind.

Zugang zum Feld

Der Zugang zum Feld war durch die tägliche Alltagspraxis der Forscherin gegeben; hier wurde die Nutzung öffentlicher Verkehrsmittel oder der Einkauf im Supermarkt zur Teilnehmenden Beobachtung. Der Zugang war also problemlos und musste nicht durch das Einholen von Erlaubnissen legitimiert werden. Um Eindrücke festzuhalten, wurden Feldnotizen erstellt, bei denen alltägliche Situationen protokolliert wurden.

4.1.2 Das Experteninterview

Im Rahmen der durchgeführten Fallstudien wurden Experteninterviews mit Vertretern der Institutionen bzw. Firmen geführt, die technische Kontroll- und Überwachungssysteme betreiben. Der Expertenbegriff lehnt sich dabei an die

Ausführungen von Hitzler[245] an, nach dem ein Experte oder eine Expertin als eine Person gilt, von der man begründet annimmt, dass sie über ein Wissen verfügt, das nicht jedermann / jederfrau in dem interessierenden Handlungsfeld zugänglich ist. Auf diesen *Wissensvorsprung* zielen die Experteninterviews innerhalb der Fallstudien ab. Als Experte/in kommt also in Betracht, wer sich durch eine „institutionalisierte Kompetenz zur Konstruktion von Wirklichkeit“[246] auszeichnet, wie Hitzler u.a. betonen. Damit ist eine Sichtweise ausgeschlossen, die jede/n zur Experte/in macht (des eigenen Lebens etc.).[247] Hitzler grenzt den Experten weiter vom Spezialisten ab. Der Experte arbeitet relativ autonom, während das Arbeitsgebiet des Spezialisten von einem Vorgesetzten oder Auftraggeber relativ genau umrissen ist und deren Tätigkeit Kontrollen unterliegt.[248] Der Experte ist dabei immer im Rahmen seiner Funktion in der jeweiligen Institution zu sehen, seine persönliche Einstellung ist nicht relevant, es geht ausschließlich um das *Wissen*, das er oder sie weitergeben kann.

Zur Erhebung der Experteninterviews wurde, wie in der Literatur weitgehend übereinstimmend vorgeschlagen, ein flexibel gehandhabter Leitfaden erstellt.[249] Dieser ist wichtig, um das Thema einzugrenzen und dem / der Interviewten als kompetenter Gesprächspartner gegenübertreten zu können. Eine gründliche Vor-ab-Recherche ist dabei unerlässlich.

Als Einstieg in den empirischen Teil wurde ein Expertinneninterview mit der Datenschutzbeauftragten des Landes Nordrhein-Westfalen geführt. Dies sollte die Sicht einer Expertin deutlich machen, die mehrfach in ihren Veröffentlichungen auf die wachsende Verbreitung technischer Kontroll- und Überwachungssysteme in unserer Gesellschaft hingewiesen hat.[250] Das Interview sollte dazu dienen, weiteres Hintergrundwissen und Einschätzungen zu einer späteren Analyse des in den Fallstudien zusammengetragenen Materials zu erhalten.

Innerhalb den anschließenden Fallstudien wurden Vertreter der Betreiber des jeweils untersuchten technischen Kontroll- und Überwachungssystems als Experten befragt. Diese Interviews dienten dazu, aus Sicht der Betreiber zu erfahren, aus welchem Grund das System eingesetzt wird, was sich die Betreiber davon versprechen und wie die Betreiber selbst ihr System sehen. Dabei wurde auch die Frage nach potenziellen Vor- und Nachteilen des Systems gestellt.

---

[245] vgl. Hitzler 1994, S. 271

[246] Hitzler/Honer/Maeder 1994, dies ist der Untertitel des Buches.

[247] Diese Daten lassen sich beispielsweise im Rahmen des Narrativen Interviews erfassen.

[248] vgl. Hitzler 1994, S. 25ff.

[249] vgl. Meuser/Nagel 2003,S. 481

[250] vgl. z.B. Datenschutzbericht 2003

Die Experteninterviews wurden mit einem Mini-Disc-Recorder bzw. einem Kassettenrekorder aufgenommen. Eine Ausnahme bilden die beiden Interviews zur Fallstudie *Ortungssysteme im privaten Raum*, denen Protokolle der Telefoninterviews zur Auswertung zugrunde lagen.

Die InterviewpartnerInnen

An dieser Stelle werden die interviewten ExpertInnen und deren Positionen in den jeweiligen Institutionen oder Unternehmen vorgestellt.

Bettina Sokol, Landesbeauftragte für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen, Interviewpartnerin in der Basiserhebung

Frau Sokol ist seit 1996 Datenschutzbeauftragte des Landes und wurde 2004 für weitere acht Jahre wiedergewählt. Vor dieser Tätigkeit arbeitete Frau Sokol als Richterin am Verwaltungsgericht in Bremen, von 1993 bis 1996 war sie als wissenschaftliche Mitarbeiterin beim Bundesverfassungsgericht tätig.

Ihre Aufgabe ist es, darüber zu wachen, dass datenschutzrechtliche Vorschriften - sowohl im öffentlichen wie auch im privaten Bereich - eingehalten werden und BürgerInnen ihr Recht auf Informationsfreiheit wahrnehmen können. Jährlich wird von ihrer Dienststelle der „Datenschutzbericht“ herausgegeben, der über die Lage des Datenschutzes im Land Nordrhein-Westfalen Auskunft gibt.

Der Kontakt zu Frau Sokol wurde über eine E-Mail-Anfrage hergestellt, der eine weitere Korrespondenz mit der Referentin für Presse- und Öffentlichkeitsarbeit, Frau Bettina Gayk folgte, innerhalb der dann ein Termin für ein persönliches Gespräch in den Räumen der Landesdatenschutzbeauftragten vereinbart wurde.

Joachim Berger, Pressesprecher der Kölner Verkehrsbetriebe (KVB), Interviewpartner in der Fallstudie A: Videoüberwachung und technische Sicherungssysteme im öffentlichen Raum – das Beispiel der Kölner Verkehrsbetriebe

Herr Berger ist seit 1985 Pressesprecher der Kölner Verkehrsbetriebe und mit sämtlichen öffentlichkeitsrelevanten Themen befasst, was auch das Thema Sicherheit und somit auch Sicherheit durch technische Systeme mit einschließt.[251] Er repräsentiert das Unternehmen in der Öffentlichkeit und ist auch für die Herausgabe von Informationsschriften verantwortlich. Der Kontakt zu Herrn Berger wurde über eine E-Mail-Anfrage hergestellt, bei der ein Termin für ein persönliches Gespräch vereinbart wurde.

[251] vgl. Berger 2003, Antwort 4

Jürgen Weber, stellvertretender Konzerndatenschutzbeauftragter der Deutschen Lufthansa AG, Interviewpartner in der Fallstudie B: Magnetstreifenkarten im Konsumalltag – Datensammlungen mit dem Payback-System

Herr Weber ist in seiner Position als stellvertretender Konzerndatenschutzbeauftragter der Lufthansa AG, die mit 51% an der Firma Loyalty Partner, der Betreiberin des Payback-Systems beteiligt ist, interviewt worden. Da beim Thema Payback hauptsächlich der Aspekt der Datenverarbeitung und –nutzung interessierte, wurde Herr Weber als Experte zu diesem Thema befragt. Die Lufthansa hatte sich entschieden, aufgrund der Mehrheitsbeteiligung bei Loyalty Partner den Datenschutz, wie bei allen Konzerngesellschaften, vom Konzerndatenschutzbeauftragten wahrnehmen zu lassen. Insgesamt werden von den Konzerndatenschutzbeauftragten 35 Firmen betreut, dabei werden im Datenschutzteam Schwerpunkte festgelegt. Herr Weber ist dabei für die Betreuung der Firma Loyalty Partner zuständig. Der Kontakt zu Herrn Weber wurde über eine E-Mail-Anfrage hergestellt, dem ein Telefonat folgte, bei dem ein Termin für ein persönliches Gespräch vereinbart wurde.

Susanne Müller-Zantop, Vice President und Leiterin Investor and Analyst Relations bei Siemens Mobile, Interviewpartnerin in der Fallstudie C: Ortungstechniken im privaten Familienalltag – das Beispiel der Kindersicherungen Leonie und Trackyourkid

Frau Müller-Zantop ist in ihrer Funktion als ehemalige Projektmanagerin von Leonie, einem Teddybären, der mit einem Mobiltelefon und einem GPS-Empfänger ausgestattet ist, interviewt worden. Sie war selbst die Ideengeberin zu Leonie und hat das Projekt von Anfang an betreut. Frau Müller-Zantop war daher die ideale Ansprechpartnerin für alle Fragen zum System Leonie. Der Kontakt zu Frau Müller-Zantop wurde über eine E-Mail-Anfrage hergestellt, der ein fernmündliches Interview folgte.

Dirk Teubner, Geschäftsführer der Firma ARMEX, Betreiberin von Trackyourkid, Interviewpartner in der Fallstudie C: Ortungstechniken im privaten Familienalltag – das Beispiel der Kindersicherungen Leonie und Trackyourkid

Herr Teubner ist in seiner Funktion als Geschäftsführer der Firma ARMEX und Beteiligter an der Entwicklung des Produktes Trackyourkid interviewt worden. Er hat die Produktentwicklung von Trackyourkid von der ersten Idee bis zur Markteinführung im Oktober 2003 verfolgt und war somit kompetenter Ansprechpartner zu allen Fragen, die das Produkt betreffen. Auch hier wurde der Anfangskontakt über eine E-Mail-Anfrage hergestellt, in der ein Termin für ein fernmündliches Interview vereinbart wurde, welches kurz darauf geführt wurde.

Auswertungsstrategie

Im Folgenden werden zuerst die Schritte bei der Auswertung der mit einem Aufzeichnungsgerät geführten Interviews vorgestellt. Dies wurde in Anlehnung an die von Meuser und Nagel[252] vorgeschlagene Auswertungsstrategie für ExpertInneninterviews durchgeführt. Das Vorgehen wird im Folgenden beschrieben.

Transkription der Interviews

Die aufgenommenen Interviews müssen im Anschluss verschriftlicht werden. Die Besonderheit beim Experteninterview besteht darin, dass es nicht um die *Person* des Experten geht, sondern um das *Wissen* über das er oder sie verfügt. Aufwendige Notationssysteme, der Vermerk von Pausen oder sonstige parasprachliche oder nonverbale Elemente werden nicht zum Gegenstand der Interpretation gemacht, wie dies z.B. bei narrativen Interviews der Fall ist.[253] Zur Diskussion steht in der Literatur, ob es nötig sei, dass gesamte Interview zu transkribieren, oder nur Äußerungen, die zur Sache gehören. Meuser und Nagel weisen darauf hin, dass bei gelungenen Diskursverläufen auch vollständige Transkriptionen sinnvoll sein können.[254] Im Rahmen der vorliegenden Fallstudien wurden die aufgezeichneten Interviews vollständig transkribiert, um ein „Verschenken von Wirklichkeit“[255] zu vermeiden. Bei der Transkription wurde eine Verschriftlichung in Standardorthographie und eine Orientierung an den Normen der geschriebenen Sprache gewählt. Der dabei entstehende Nachteil, die Besonderheiten der gesprochenen Sprache (wie Elisionen etc.) nicht erfassen zu können, wurde aufgrund der Wahl der Methode des Experteninterviews in Kauf genommen, da er für die weitergehende Analyse irrelevant ist.[256] Dauer von Sprechpausen oder Betonungen einzelner Silben waren im Rahmen meines Forschungsinteresses nicht relevant.

Die erstellte Transkription der Interviews wurde auf Wunsch an die Interviewpartner zur Durchsicht übersandt. Dieses Angebot wurde vom stellvertretenden Konzerndatenschutzbeauftragten der Deutschen Lufthansa AG, Herrn Jürgen Weber in Anspruch genommen. Herr Weber hat dabei im Transkript missverständliche Formulierungen oder falsch verstandene Namen korrigiert und formale Änderungen vorgenommen. Der ursprünglichen Inhalte des Interviews blieb dabei unverfälscht.

---

[252] vgl. Meuser/Nagel 2002

[253] vgl. Meuser/Nagel 2002, S. 83

[254] vgl. Meuser/Nagel 2002, S. 83

[255] vgl. Meuser/Nagel 2002, S. 83

[256] vgl. auch Kowal / O´Connell 2000, S. 439

Paraphrase

In einem weiteren Schritt zur Verdichtung des Materials wurde eine Paraphrase der Interviews erstellt, die der Chronologie des Gesprächsverlaufs folgt und wiedergibt, was der Experte insgesamt geäußert hat. Mit dieser Vorgehensweise soll dem Zirkelproblem entgegengetreten werden: Man versichert sich des Expertenwissens, indem man textgetreu mit eigenen Worten, wiedergibt, was gesagt wurde. Es wurde darauf geachtet, in Bezug auf die angesprochenen Themen und Inhalte nicht zu selektieren und nichts hinzuzufügen, zu verzerren oder zu unterschlagen. Ziel der Paraphrase ist es, erste Trennlinien zwischen Themen zu verdeutlichen und Argumentationsmuster erkennbar zu machen.

Überschriften und Hauptüberschriften

Nächster Schritt zur Verdichtung des Materials ist es, die paraphrasierten Passagen mit Überschriften zu versehen. Dabei wird textnah vorgegangen und die Terminologie der Interviewten aufgegriffen. Ob einer Passage eine oder mehrere Überschriften zugeordnet werden hängt davon ab wie viele Themen jeweils angesprochen werden. Die Reihenfolge des Textes, auch innerhalb der Passagen, aufzubrechen, ist erlaubt und notwendig. Passagen, in denen gleiche oder ähnliche Themen behandelt werden, werden zusammengestellt und eine Hauptüberschrift, die den Inhalt sämtlicher subsumierter Passagen abdeckt, wird formuliert. Dabei wird eine Übersicht über den Text erzielt, die sich auf Themen und Informationen, nicht aber auf eine Falldarstellung bezieht.

Thematischer Vergleich

Erst an dieser Stelle geht die Auswertung über die einzelne Texteinheit hinaus. Es wird jetzt nach thematisch vergleichbaren Textpassagen aus verschiedenen Interviews *gefahndet*. Bei den vorliegenden Fallstudien erfolgt der thematische Vergleich zwischen den Aussagen der Experten und den Ergebnissen aus den Problemzentrierten Interviews mit den Nutzern der Systeme bzw. der davon Betroffenen innerhalb des jeweiligen Falls. Passagen aus den verschiedenen Interviews, in denen gleiche oder ähnliche Themen behandelt wurden, wurden zusammengestellt und die Überschriften vereinheitlicht. Es wurde weiterhin eine textnahe Kategorienbildung verfolgt und auf eine soziologische Terminologie an dieser Stelle noch verzichtet. Die Resultate des thematischen Vergleichs wurden kontinuierlich an den Passagen der Interviews auf Vollständigkeit und Validität hin geprüft. Fragen an dieser Stelle waren: Wo gibt es Übereinstimmungen zwischen den Aussagen der Experten und der Nutzer, bzw. Betroffenen und wo lassen sich Unterschiede feststellen? Zu welchen Themen äußern sich die Experten, welche werden auf Nutzerseite angesprochen? Was sind das für Themen, zu denen nur in einem Text etwas zu finden ist?

4.1.3 Das Problemzentrierte Interview

Unter dem Begriff des Problemzentrierten Interviews werden alle Formen der offenen, halbstrukturierten Befragungen zusammengefasst. Diese Methode bietet sich dort an, wo bereits Wissen über den Forschungsgegenstand gewonnen wurde und spezifische, also keine rein explorativen Fragen im Vordergrund stehen. Bei den vorliegenden Fallstudien wurden im Vorfeld bereits die ethnographischen Verfahren und die Experteninterviews durchgeführt. Bei den Problemzentrierten Interviews kommt der Befragte möglichst frei zu Wort, um der Situation eines offenen Gesprächs nahe zu kommen. Das Gespräch ist dabei auf eine bestimmte Problemstellung zentriert, die von der Interviewerin eingeführt wird und auf die sie auch immer zurück kommt. Die Forschung setzt dabei an konkreten gesellschaftlichen Problemen an. Bestimmte, interessierende Aspekte werden danach innerhalb eines Interviewleitfadens zusammengestellt. Die Interviewten werden durch den Interviewleitfaden auf bestimmte Fragestellungen hingelenkt, antworten aber offen und ohne Antwortvorgaben. Ein Vorteil der teilweisen Standardisierung durch den Leitfaden ist, dass es so leichter fällt, mehrere Interviews miteinander zu vergleichen.[257] Die Aufzeichnung der Interviews erfolgte im Falle der vorliegenden Fallstudien durch ein schriftliches Protokoll.

Auswertungsstrategie

Bei der Auswertung der Problemzentrierten Interviews wurden die halbstandardisierten Interviews in Tabellenform aufbereitet um, in grafischer Form, eine bessere Übersicht über die jeweils zehn bis zwölf geführten Interviews zu ermöglichen. Parallel dazu wurden die Interviews nach der im folgenden Kapitel beschriebenen Methode der Qualitativen Inhaltsanalyse, ausgewertet.

4.1.4 Die Qualitative Inhaltsanalyse

Neben den Experteninterviews werden innerhalb der Fallstudien weitere Texte analysiert. Dabei handelt es sich um Broschüren, Webseiten, Feldnotizen und Transkripte von Interviews und in einem Fall einer Radiosendung. Diese wurden nach der Methode der Qualitativen Inhaltsanalyse ausgewertet. Durch inhaltsanalytische Zusammenfassung wurde eine induktive Kategorienbildung gewährleistet. Hier wird der Text im Hinblick auf ein vorher definiertes Ziel, also einer Grundfrage im Hinterkopf, in Kategorien unterteilt, die möglichst nahe am Mate-

[257] vgl. Mayring 1996, S. 50ff

rial formuliert werden. Das gesamte Kategoriensystem kann danach in Bezug auf die Fragestellung interpretiert werden.[258]

4.2 Basiserhebung: Die Perspektive der Bürgerrechte. Interview mit der Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen

Als Grundlage für das Expertinneninterview mit der Datenschutzbeauftragten Frau Sokol diente der jährlich veröffentlichte Datenschutzbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit. Frau Sokol zeigte sich von Anfang an trotz ihres dichten Terminkalenders sehr entgegenkommend und offen. Das einstündige Gespräch verlief in entspannter Atmosphäre unter Beteiligung der Referentin für Presse- und Öffentlichkeitsarbeit, Frau Bettina Gayk.

Expertinneninterview mit Bettina Sokol

Frau Bettina Sokol ist in ihrer Position sowohl für Datenschutzfragen im öffentlichen Bereich (z.B. Verwaltung, Polizei, Verfassungsschutz), als auch seit dem Jahr 2000 für den privaten Bereich zuständig.[259] Durch das Interview mit der Datenschutzbeauftragten sollte die wachsende Verbreitung technischer Kontroll- und Überwachungssysteme im Alltag aus Sicht einer Expertin betrachtet werden, die sich qua ihres Amtes mit der Verbreitung solcher Systeme und ihre Einflüsse auf Bürgerrechte auseinandersetzt. Es war also davon auszugehen, dass Frau Sokol einen guten Überblick über das Thema geben kann. Dabei interessierten folgende Fragen:

- Welche Meinung vertritt die Datenschützerin zur wachsenden Verbreitung von Videokameras im öffentlichen Raum?
- Welche Meinung besteht zum Thema Bonuskarten und Datensammlungen?
- Welche Bedeutung sollen Persönlichkeitsrechte und Privatheit innerhalb einer Demokratie haben?
- Wie stellt sich die Situation aus Sicht des Datenschutzes gesamtgesellschaftlich dar?

---

[258] vgl. Mayring 1996

[259] Diese Möglichkeit besteht innerhalb des Bundesdatenschutzgesetzes und wurde in Nordrhein-Westfalen mittels einer Gesetzgebungsnovelle im Jahr 2000 so beschlossen, dass der oder die Landesdatenschutzbeauftragte sowohl für den öffentlichen als auch den privaten Bereich zuständig ist.

Auswertung des Interviews

Videoüberwachung

Das Gespräch wurde im Hinblick auf die Fallstudie zur Videoüberwachung in den Kölner Verkehrsbetrieben auf den speziellen Fall der Videoüberwachung in öffentlichen Verkehrsmitteln gelenkt. Es habe, so erklärt Frau Sokol, den Wunsch der Verkehrsbetriebe gegeben, in Straßenbahnen und Bussen Videokameras zum Schutz der Fahrgäste, und des Eigentums der Betriebe einsetzen zu können. Es seien dann mit allen Beteiligten Anforderungen erarbeitet worden, die beim Einsatz solcher Systeme beachtet werden müssen. Beispielsweise sei in jedem Einzelfall zu prüfen, ob es auf einer bestimmten Straßenbahnlinie und zu einer bestimmten Tages- oder Nachtzeit *unbedingt erforderlich* ist, eine Kamera einzusetzen. Diese Erforderlichkeit sei, so Bettina Sokol, streng zu prüfen und nur da, wo sie zu bejahen ist, könne ein Kameraeinsatz in Frage kommen.[260] Ferner wurden Anforderungen technischer Natur gestellt, wie zum Beispiel Vorgaben, um sicher zu stellen, dass möglichst kein Missbrauch mit den Kameraaufzeichnungen betrieben werden kann. So müssen Aufzeichnungen, wenn sie überhaupt gemacht werden müssen, binnen kurzer Fristen wieder gelöscht werden und dürfen nur von bestimmten befugten Personen eingesehen werden. Auf die Videoüberwachung muss klar erkennbar und deutlich hingewiesen werden. Frau Sokol verweist für weitere Informationen auf den Datenschutzbericht 2003, aus dem folgende Passage stammt:

> „Die Videoüberwachung darf nicht der Regelfall sein, sondern nur stattfinden, wenn sie notwendig ist. [...] ... es darf keine automatische Ausstattung aller Verkehrsmittel mit Videokameras stattfinden.“[261]

Die erarbeiteten Anforderungen seien, so Sokol, durch den Verband der Verkehrsbetriebe, den Aufsichtbehörden im nicht-öffentlichen Bereich, dem so genannten Düsseldorfer Kreis und durch die Landesbeauftragten für den Datenschutz erarbeitet worden und können somit als eine Art Handreichung zum Verständnis und zu den Anforderungen der Videoüberwachung gelten.[262] Videoüberwachung im öffentlichen Bereich des Personennahverkehrs ist also, aus Sicht des Datenschutzes, strengen Regeln unterworfen und kann nicht per se in jedem Wagen und in beliebiger Art und Weise eingesetzt werden.

Abgesehen von dieser speziellen Form der Videoüberwachung weist Frau Sokol darauf hin, dass Videokameras mittlerweile von vielen unterschiedlichen Betrei-

---

[260] vgl. Sokol 2003, Antwort 1

[261] Datenschutzbericht 2003, S. 209

[262] vgl. Sokol 2003, Antwort 1

bern betrieben würde. Aus Sicht der Bürger sei es erst einmal relativ egal, wer die Kameras betreibe, die Gefahr läge darin, dass es bei den Bürgern zu Verhaltensanpassungen kommen könne:

> „Aber die Tatsache, sich nicht mehr unbeobachtet bewegen zu können, kann etwas sein, was sich langfristig auf die Verhaltensweisen der Personen auswirkt, indem sie etwa in dem Bewusstsein, nicht unbeobachtet zu sein, ihre Unbefangenheit verlieren und sich in einem Maße kontrollieren, das zu Verhaltensanpassungen führt."[263]

Hier spricht die Datenschutzbeauftragte mögliche Folgen der sich immer stärker verbreitenden Videoüberwachung an. Sie weist dabei auf die Möglichkeit hin, seine Unbefangenheit zu verlieren und sein Verhalten an vermeintliche Normen anzupassen, da man sich ständig beobachtet wähnt - eine Form von Selbstkontrolle also, die an das im Theorieteil vorgestellte Modell des Panoptikums von Foucault anschließt. Wenn die wachsende Verbreitung von Videoüberwachung dazu führe, dass sich Personen in einer Art und Weise verhielten, die nicht normabweichend ist, um nicht vor einer Kamera auffällig zu werden, dann habe dies Auswirkungen auf die Grundrechte und mittelbar auch auf die Demokratie, erklärt die Datenschutzbeauftragte. Sie konstatiert, dass man ein Grundrecht darauf habe, sich frei und unbeobachtet bewegen zu können.[264]

Neben den privatwirtschaftlichen Betreibern, die in Passagen, Einkaufszentren oder eben in Straßenbahnen Kameras installieren, weitet sich die Videoüberwachung immer stärker auch innerhalb der Polizeiarbeit aus. Diese ist ebenfalls daran interessiert, die Technik für ihre Arbeit zu nutzen. Es stand daher zum Zeitpunkt des Interviews die Änderung des NRW-Polizeigesetzes zur Diskussion, bei der die Befugnisse ausgeweitet werden sollten. Dabei war geplant, den Einsatz von Videokameras für die Polizei erheblich zu erleichtern und nicht mehr nur bei Straftaten von erheblicher Bedeutung zuzulassen.[265] Frau Sokol kritisiert im Hinblick auf den derzeitigen Erkenntnisstand über den Nutzen von Videoüberwachung den Wunsch nach der Änderung des Polizeigesetzes von NRW. Es gäbe keine Rechtfertigung für diese Gesetzesänderung. Bisher sei auch noch nicht geklärt, ob es durch Videoüberwachung überhaupt zu einer Verhinderung von Straftaten kommen könne, oder diese nur verlagert würden. Auch das einzige Pilotprojekt in Bielefeld (Ravensberger Park) sei nicht wissenschaftlich fundiert untersucht worden. Es sei noch nirgendwo richtig nachgewiesen worden, dass Videoüberwachung eine Straftatenreduzierung bewirken könne. Selbst in Groß-

---

[263] Sokol 2003, Antwort 1

[264] vgl. Sokol 2003, Antwort 1

[265] Anm. der Verf.: Das Polizeigesetz von NRW wurde am 26.6.2003 geändert. Die Polizei darf künftig *alle* Straftaten aufzeichnen, bisher war dies nur bei Delikten von erheblicher Bedeutung möglich.

britannien, dem Mutterland der Überwachungskameras, seien Untersuchungen zu sehr unterschiedlichen Ergebnissen gekommen. Man könne daraus schlussfolgern, dass Diebstähle o.ä. etwas weniger im Blickfeld einer Kamera zu verzeichnen sind, dafür aber unter Umständen einige Meter weiter. Für Gewalttaten gelte, dass diese eher nicht verhindert würden, zumal dann nicht, wenn sie im Affekt begangen würden.[266] Die Geschichte zeigt, dass die Bedenken der Datenschutzbeauftragten und anderer Kritiker nicht verhindern konnten, dass das Gesetz im Juni desselben Jahres noch geändert wurde und die Befugnisse der Polizei, Videoüberwachung einzusetzen, erheblich erweitert wurden. Eine Tatsache, welche die Frage aufwirft, warum es zu einer Gesetzesänderung kommen konnte, wenn es keinen Nachweis für die Wirksamkeit von Videoüberwachung gibt und erhebliche datenschutzrechtliche Bedenken bestanden. Denn schließlich äußert Frau Sokol:

> „Es ist überhaupt nicht ersichtlich, warum man ohne Not jetzt hier eine Erleichterung für den Videoeinsatz schaffen will. Es gibt also keine Rechtfertigung für diese Gesetzesänderung. Und schließlich werden die Menschen mit der Videoüberwachung zunehmend stärker behelligt, das kann auch langfristig entsprechende Auswirkungen auf Verhaltensanpassungen und damit die Ausübung von Grundrechten haben.“[267]

Für den Gesetzgeber waren augenscheinlich andere Argumente gewichtiger und führten zu einer Änderung des Polizeigesetzes von Nordrhein-Westfalen noch im selben Jahr.

Datensammlungen

Eine Sammlung von Daten über Personen fände, so Sokol, an verschiedensten Stellen, aber auch insbesondere in der Privatwirtschaft statt. Dies sei ein eigener Geschäftszweig geworden. Heutzutage meine man, sich nicht mehr auf die eigene Menschenkenntnis oder die Angaben, welche die Person selber macht, verlassen zu können und bedürfe anscheinend der Auskünfte Dritter.[268] Hier haben sich Auskunfteien gegründet, die Daten des Einzelnen je nach Bedarf zusammenstellen und auswerten. Der Handel mit Daten hat sich als Geschäftsidee etabliert. Je mehr technische Möglichkeiten es gäbe, Daten in großer Menge zu sammeln, zu speichern und thematisch zu sortieren, desto reizvoller würde es für Menschen, damit Geld zu verdienen. Im Internet gäbe es Anreize für Menschen, ihre persönlichen Daten preiszugeben, ohne dass in jedem Fall klar wäre, dass die Auswertung der Daten eigentlich dazu dient, Geld damit zu verdienen, kritisiert Sokol.[269] Diese

---

[266] vgl. Sokol 2003, Antwort 13

[267] Sokol 2003, Antwort 14

[268] vgl. Sokol 2003, Antwort 15

[269] vgl. Sokol 2003, Antwort 16

Datensammlungen können von der Sammlung über Vorlieben bei Büchern bis hin zur Erfassung des Kaufverhaltens und der Einschätzung der Kreditwürdigkeit gehen.[270]

Frau Sokol weist in diesem Zusammenhang ergänzend auf die Möglichkeit hin, Menschen aufgrund von gesammelten Informationen zu manipulieren:

> „Natürlich, je mehr Daten ich über jemanden habe, umso leichter ist es mir möglich, zu wissen an welcher Stelle ich diesen Menschen packen kann, um ihn in eine bestimmte Richtung zu lenken. Je gläserner jemand wird, desto leichter ist es für mich doch zu sagen: Jetzt manipulier ich dich mal in die und die Richtung.“ [271]

Datensammlungen, zu welchem Zweck auch immer, stellen also aus Sicht des Datenschutzes ein erhebliches Risiko dar, dass es zu vermeiden gilt, will man die Grundrechte des Bürgers nicht gefährden.

Datenmissbrauch

Die Sammlung unterschiedlicher Daten über den einzelnen Bürger eröffnet Möglichkeiten des Missbrauchs. Am Beispiel biometrischer Verfahren verdeutlicht Frau Sokol die Gefahr der Entstehung so genannter Überschussinformationen, also Informationen, die über das eigentliche Ziel der Erfassung hinaus entstehen und bei denen bei einigen Systemen noch gar nicht klar ist, welche weiteren Informationen entstehen können. Es gäbe Leute, die vertreten, dass man aus den Fingerabdrucksmerkmalen, der Iris-Struktur oder erst recht aus dem Augenhintergrund auch mehr als nur die Identifikation herauslesen könne.

> „Gleichwohl ist natürlich immer zu bedenken, dass beim fortschreitenden Stand von Wissenschaft und Technik und in besonderen Situationen und Lebenslagen, Informationen, die bis zu einem gewissen Zeitpunkt als nicht relevant erachtet wurden, plötzlich eine Bedeutung gewinnen können und zu einem anderen Zweck verwandt werden sollen, als zu dem, zu dem sie ursprünglich erhoben wurden.“[272]

Die erhobenen Daten befinden sich also nicht in einem neutralen Raum, sondern sind gesellschaftlichen Veränderungen unterworfen. Aufgrund von neuen wissenschaftlichen Erkenntnissen könnte es möglich werden, aus den einmal erhobenen Daten plötzlich etwas ganz anderes herauszulesen, als zum Zeitpunkt der Erhebung. Dies trifft vor allem für biometrische Daten, wie Fingerabdrücke oder Ab-

---

[270] Dieses Verfahren nennt sich Scoring. Bei ihm werden z.B. Daten über die Wohnlage (arme oder reiche Wohngegend) und je nach Verfahren weitere Daten wie Kaufverhalten etc. ausgewertet, um den Kunden einen bestimmten *Wert* oder auch ein Risiko für ein Unternehmen zuzuordnen. Es wird in der Fallstudie B zu den Payback-Karten noch einmal erläutert.

[271] Sokol 2003, Antwort 25

[272] Sokol 2003, Antwort 8

bildungen des Augenhintergrundes zu, - hier können heute schon Krankheiten aus den biometrischen Daten herausgelesen werden. Als Gegenstrategie weist Frau Sokol etwas später auf den Grundsatz der Datensparsamkeit und Datenvermeidung hin, mit dem erreicht werden soll, dass technische Systeme bereits in einer Art und Weise entwickelt werden, die möglichst wenig personenbezogene Daten verwenden.[273] Für diejenigen, die nicht alles in die Öffentlichkeit tragen wollten, müsse die Möglichkeit bleiben, dies auch zu tun. Im Zusammenhang mit biometrischen Daten weist Frau Sokol ferner auf die Gefahr der Auswahl und Diskriminierung hin, die aufgrund erhobener biometrischer Daten möglich wäre.[274] Filme wie „Gattaca", „Minority Report" oder Huxleys „Brave New World" geben eine Vorstellung, wie eine Welt aussehen könnte, in welcher der Lebensweg von Menschen schon bei der Geburt aufgrund ihres genetischen Materials vorbestimmt ist und die Biometrie über das In und Out in der Gesellschaft bestimmt.

Neben den Möglichkeiten, die sich bei der Auswertung der Daten erweitern können, kann sich auch schlicht, wie bereits erwähnt, der Zweck, zu dem die Daten erhoben wurden, ändern. Als Beispiel führt Frau Gayk an, dass bereits heute Passagierdaten, welche die Lufthansa nur zur Abwicklung einer Reise erhoben hat, an US-amerikanische Behörden weitergegeben werden. Aus Daten, welche die Fluggesellschaften alleine zur Abwicklung der Reise erhoben habe, sei ein riesiger Datenpool entstanden, der jetzt auch von anderen Bedarfsträgern eingesehen werden könne. Etwas Vergleichbares könne natürlich auch passieren, wenn man zum Beispiel biometrische Daten nicht datenschutzgerecht auf einer Karte bei der einzelnen Person speicherte, sondern auf einem zentralen Rechner. Dann hätte man einen Datenpool auf den, obwohl heute noch keiner darüber nachdenken würde, in der Zukunft jemand zu einem völlig anderen Zweck zugreifen könnte.[275] Daten, die zentral und über längere Zeit gespeichert werden, bieten also immer auch die Möglichkeit des Missbrauchs. Sie sind Veränderungen in den politischen Verhältnissen und neuen wissenschaftlichen Erkenntnissen unterworfen.

Grundrechte des Bürgers

Trotz der immer stärkeren Verbreitung von Überwachungssystemen und Datensammlungen betont Frau Sokol das Grundrecht auf Informationelle Selbstbestimmung, wonach man zumindest gegenüber dem Staat in der Rechtsposition sei, dass dieser begründen müsse, wenn er Informationen über einen Bürger haben möchte. Dies dürfe nur zu einem bestimmten Zweck und unter dem Grundsatz der

[273] vgl. Sokol 2003, Antwort 21

[274] vgl. Sokol 2003, Antwort 10

[275] vgl. Gayk 2003, Antwort 3

Verhältnismäßigkeit erfolgen, der in der Verfassung verankert ist. Nur also, wenn es für die staatliche Aufgabenerfüllung zu einem bestimmten Zweck nötig sei, dürfe kontrolliert werden.[276] Frau Sokol streicht an dieser Stelle heraus, dass es ein Grundrecht des Bürgers gegenüber dem Staat ist, über seine Daten selbst zu bestimmen und es recht enge Regeln gibt, wann der Staat das Recht erhält, in die Privatsphäre seiner Bürger einzugreifen.

Im privaten Bereich gelte, so Sokol, das Grundrecht auf Informationelle Selbstbestimmung zwar nicht unmittelbar, die Grundrechte hätten aber auch eine Ausstrahlungswirkung auf das Zivilrecht. Nach dem Kunsturhebergesetz sei es beispielsweise nicht erlaubt, ein Bild einer Person ohne deren Einwilligung einfach so zu veröffentlichen. Für den Bereich der Videokameras sei inzwischen eine eigene Norm in das Bundesdatenschutzgesetz aufgenommen worden, wann Unternehmen oder Privatleute Videokameras zu welchem Zweck und in welchem Umfang betreiben dürfen.

Frau Sokol räumt dem Grundrecht auf Informationelle Selbstbestimmung einen sehr hohen Stellenwert ein:

> „Ja, das Grundrecht auf Informationelle Selbstbestimmung gehört zu den Grundrechten, die in unserem Grundgesetz stehen und die die fundamentalen Menschenrechte beschreiben und garantieren sollen."[277]

Sie führt weiter aus, dass das Bundesverfassungsgericht es als eine elementare Funktionsbedingung der Demokratie angesehen hat, dass die Menschen ihre Grundrechte ausüben können, dass sie daran nicht gehindert werden und einen Freiraum haben, selbstbestimmt zu leben.

> „Es geht um die Garantien, die da anfangen mit dem Recht auf Leben und körperliche Integrität, etwa Folterverbot, über eben das Recht auf Informationelle Selbstbestimmung, das Recht auf politische Meinungsbildung und Meinungsäußerung bis zur Demonstrationsfreiheit und beispielsweise dem Recht, sich grundsätzlich selber den Beruf wählen zu können, den man gerne ausüben möchte. [...] Dieser ganze Kanon ist das Fundament unserer Demokratie."

Für Frau Sokol gehört also das Recht auf Informationelle Selbstbestimmung zum Fundament der Demokratie, an dem demnach gerüttelt wird, wenn man die Bürger immer mehr überwacht. Dies beobachtet auch die Datenschutzbeauftragte, wenn sie den Abbau der Grundrechte nach den Ereignissen des 11. September beurteilt. Es habe danach im Bereich der Inneren Sicherheit einen Abbau der Grundrechte gegeben. Dort sei bei einigen Änderungen zumindest aber eine Evaluation der Gesetzesänderungen vorgeschrieben, ob die erweiterten Befugnisse beibehalten

---

[276] vgl. Sokol 2003, Antwort 1

[277] Sokol 2003, Antwort 20

oder wieder abgeschafft werden sollten. Bei der Novelle des Bundesdatenschutzgesetzes habe es dagegen bei der Anpassung an europäische Richtlinien einige positive Ansätze gegeben, beispielsweise im Umgang von nicht-öffentlichen Stellen mit Daten. Dort gäbe es nun vermehrt Hinweispflichten und mehr Rechte für die Betroffenen.[278] Frau Gayk ergänzt, dass die von Frau Sokol genannten Grundrechte auch als Garantie dafür zu sehen sind, dass man sich eine politische Meinung bilden kann. Ideal sei in einer Demokratie die Möglichkeit, dass sich eine Minderheitenmeinung zu einer Mehrheitsmeinung fortbilden könne. Wenn aber über die Verhaltensweisen von Menschen Rückschlüsse auf das, was sie dort tun, möglich sind, habe eine politische Mehrheit, die auf solche Informationen Zugriff hat, ihrerseits Möglichkeiten, solche Meinungen erst gar nicht wachsen zu lassen. Von daher stelle sich auch die Notwendigkeit, immer wieder zu hinterfragen, ob vor allem der Staat Informationen in diesem Umfang über seine Bürgerinnen und Bürger brauche.[279]

Privatheit

Neben dem wachsenden Interesse verschiedener Stellen, möglichst viel über den Einzelnen zu erfahren, scheint es auch eine erhöhte Bereitschaft bei vielen zu geben, Informationen über sich mitzuteilen. Dies ließ die Frage aufkommen, ob sich das Bewusstsein für Privatheit in den letzten Jahren innerhalb der Bevölkerung gewandelt hätte. Frau Sokol erklärt, sie könne dazu nur Spekulationen anstellen, und führt aus, dass sich das Verständnis von Privatheit in gewisser Weise gewandelt habe und die Leute sich gerne präsentieren und stärker selbstdarstellerisch tätig seien als früher. Gleichzeitig gäbe es aber auch eine Gegentendenz. Frau Sokol macht dies an den Anfragen, die an ihre Dienststelle gestellt werden fest, die sich mehr als verdoppelt hätten. Dies könne allerdings die unterschiedlichsten Gründe haben, beispielsweise, dass die Dienststelle bekannter geworden sei oder die Leute eine höhere Sensibilität für den Datenschutz entwickelt hätten oder aber auch, dass mehr Verstöße gegen den Datenschutz stattfinden. Frau Sokol glaubt, dass in bestimmten Bereichen wie dem Internet oder bei der Werbung das Bewusstsein eher wächst und dort viele Menschen empört sind und sich beschweren würden. Gleichzeitig würden auch Teile der Wirtschaft dies erkennen und Datenschutz als Qualitätsmerkmal für sich erkennen und damit werben.[280] Es ist also differenziert zu betrachten, ob der Sinn für das Private wirklich zurückgegangen ist und müsste durch weitere Studien untersucht werden, um zu einem

[278] vgl. Sokol 2003, Antwort 27

[279] vgl. Gayk 2003, Antworten 5 und 6

[280] vgl. Sokol 2003, Antwort 26

aussagekräftigen Ergebnis zu kommen. Zur Bedeutung von Privatsphäre in einer Demokratie äußert die Datenschutzbeauftragte:

> „Also Privatsphäre ist etwas, was den Menschen sicherlich unmittelbar ausmacht: Selber darüber entscheiden zu können, was ich von mir bekannt geben möchte und was nicht. Das Bundesverfassungsgericht hat es auch mal so ausgedrückt, dass es einen Raum geben muss, in dem die Bürgerinnen und Bürger vom Staat in Ruhe gelassen werden, in den sie sich zurückziehen können, um eben auch sagen zu können: Ich will meine Ruhe haben!“[281]

Bei aller Toleranz denjenigen gegenüber, die freiwillig auf ihre Privatsphäre verzichteten (z.B. im Big Brother Container), müsse für die anderen, die das nicht wollten, umso strikter gewährleistet werden, dass das Grundbedürfnis nach Privatheit auch realisiert werden könne. Wer behaupte, „er habe nichts zu verbergen“, würde meist sofort bei irgendeinem kleinen Beispiel, das ihm persönlich am Herzen liegt, einknicken. Denn auch da seien die Einstellungen der Leute unterschiedlich. Wenn jemand etwa in eine Selbsthilfegruppe von Betroffenen einer bestimmten Krankheit ginge, dann sei er natürlich daran interessiert, sich mit den anderen Gruppenmitgliedern auch über Details auszutauschen. Er müsse aber überhaupt nicht daran interessiert sein, dass das sein Arbeitgeber, sein Nachbar oder gar die Polizei erfährt. Deswegen mache es Sinn, zu sagen, dass es allen Personen grundsätzlich möglich sein muss, selbst darüber zu entscheiden, was sie von sich preisgeben. Außerdem müsste man auch eine Art Überblick behalten können, wer was über einen selbst wisse.[282] Dafür muss man Informationelle Selbstbestimmung ausüben können.

Verhältnis Staat / Bürger

Frau Sokol führt aus, dass in einem Rechtsstaat der Staat einen Anlass haben müsse, um seine BürgerInnen zu überwachen und in deren Rechte einzugreifen, ansonsten gelte zuerst einmal die Unschuldsvermutung. In der bundesweiten Gesetzgebung sei aber eine Tendenz zu sehen, immer mehr polizeiliche Möglichkeiten zu schaffen, *ohne* den zuvor beschriebenen Anlass zu haben. Gemeint sei zum Beispiel die Schleierfahndung, die Personenkontrollen ermögliche, bloß weil sich jemand an einen bestimmten Ort aufhielte. Dies sei etwas, was sich von dem ursprünglichen Verständnis entferne, so dass Frau Sokol im Datenschutzbericht 2003[283] überspitzt formuliert habe, dass der Staat den Bürgerinnen und Bürgern

---

[281] Sokol 2003, Antwort 19

[282] Sokol 2003, Antwort 22

[283] Im Datenschutzbericht 2003, S. 5, weist Frau Sokol auf ein gewandeltes Grundverständnis zwischen Staat und Bürger hin und darauf, dass die Bürger nicht mehr als *unverdächtig*, sondern nur noch *nicht verdächtig* betrachtet würden. Auch von einer entstehenden *Kultur des Misstrauens* ist die Rede.

nicht als Personen, die grundsätzlich unverdächtig seien gegenübertrete, sondern ihnen mittlerweile in vielerlei Hinsicht so begegne, dass sie als *noch nicht verdächtig* gelten. Die polizeilichen Befugnisse hätten in den letzten Jahren, wenn man auch die bundesweite Situation berücksichtige, enorm zugenommen.[284] Die Datenschutzbeauftragte weist hier auf eine grundlegende Änderung im Verhältnis Staat / Bürger hin, der im theoretischen Teil, vor allem bei der Beschreibung der New Penology, zum Tragen kam. Auch in Deutschland lässt sich also diese Tendenz erkennen, erst einmal mehr über den Einzelnen zu erfahren, der irgendwann ja zu einem Verdächtigen werden könnte. Frau Sokol sieht insgesamt in der Gesellschaft eine *Kultur des Misstrauens* entstehen.[285]

Die Rolle der Politik

Der Datenschutz ist letztendlich eine politische Entscheidung. Frau Sokol beurteilt die Situation in der Politik so, dass es von mehreren Komponenten abhänge, wie Entscheidungen über den Datenschutz zustande kommen.

> „Es mag da Naivität geben, das will ich nicht ausschließen. Es mag sicherlich auch Einzelne geben, die das Ausmaß dessen absehen und es gleichwohl forcieren, im Wissen um die Folgen für die Demokratie. Und es mag sicherlich eine große Zahl von Leuten geben, die bestimmte Befürchtungen hegen, bestimmte Erkenntnisse und Vermutungen darüber besitzen, wie sich etwas langfristig auswirken wird und gleichwohl im politischen Geschäft möglicherweise auch unter einem bestimmten Druck stehen, Anforderungen zu erfüllen, die von den verschiedensten gesellschaftlichen Kräften gestellt werden.“[286]

Die so genannte Sicherheitsgesetzgebung sei auch bei ihrer Entstehung durchaus politisch umstritten gewesen. Bestimmten Kräften sei sie nicht weit genug gegangen, anderen Kräften zu weit. Es würden dort dann Kompromisse ausgehandelt.[287] Es lasse sich auf staatlicher Seite eine Eigendynamik beobachten, dass wenn technische Möglichkeiten da sind, diese auch gerne genutzt würden. Daher sei es wichtig, bereits bei der Entwicklung der technischen Möglichkeiten darauf zu achten, dass diese nur in einer für den Menschen nützlichen Form eingesetzt werden könnten. Als Beispiel für diese Eigendynamik führt Frau Sokol die Einrichtung der DNA-Analysedatei an. Hier hätten die Datenschützerinnen und Datenschützer durchaus vor diesem qualitativ neuen Schritt gewarnt. Dennoch sei die Datei zu einem gesetzlich fixierten Zweck und mit einer bestimmten Beschränkung auf Straftaten von erheblicher Bedeutung eingerichtet worden, und

---

[284] Sokol 2003, Antwort 15

[285] vgl. Sokol 2003, Antwort 15

[286] Sokol 2003, Antwort 28

[287] Sokol 2003, Antwort 28

nun solle auch hier, wie damals leider schon befürchtet, eine weitere Öffnung stattfinden. Die politischen Vorstellungen dahingehend seien von unterschiedlicher Intensität und reichten von einer schrittweiten Ausweitung dieser Datei bis zu der Forderung, alle Straftäterinnen und Straftäter dort mit dem Ergebnis ihrer DNA-Analyse registrieren zu lassen.[288] Alles, was technisch möglich sei, würde auch gemacht werden, es sei denn, es werde politisch entschieden, das zu begrenzen. Dies sei eines der wichtigsten Elemente in einer Demokratie, dass man in einem demokratischen Verfahren entscheide, was für Verhältnisse man in der Gesellschaft haben wolle und wo Grenzen gezogen werden müssten. Vielfach hinke der Gesetzgeber den technischen Entwicklungen aber hinterher.

Zusammenfassung

Frau Sokol beurteilt die wachsende staatliche und privatwirtschaftliche Überwachung äußerst kritisch. Bei der Einführung technischer Systeme ist daher, nach ihren Angaben, eine strenge Überprüfung nötig, da die Gefahr bestehe, dass es bei den Bürgern zu Verhaltensanpassungen kommt, wenn kein unbeobachtetes Bewegen mehr möglich ist.

Der Handel mit Daten hat sich nach Frau Sokol zur Geschäftsidee entwickelt, mit der man Geld verdienen kann. Es besteht hier die Gefahr, dass Menschen aufgrund der gesammelten Daten manipuliert werden können. Der Zweck, zu dem Daten erhoben werden, kann sich ändern und Daten, die zentral und über längere Zeit gespeichert werden, bieten Möglichkeiten des Missbrauchs.

Das Grundrecht auf Informationelle Selbstbestimmung ist nach Sokol ein fundamentales Menschenrecht und ein Fundament der Demokratie, das es zu bewahren gilt. Hier kam es insbesondere nach dem 11. September im Bereich der Inneren Sicherheit zu einem Grundrechteabbau. Diese Grundrechte sind aber eine Garantie dafür, dass man eine politische Meinung bilden kann – es sei immer wieder zu hinterfragen, ob der Staat Informationen über seine Bürger in diesem Umfang brauche. Trotz datenschutzrechtlicher Bedenken sind viele Gesetze, wie zuvor dargestellt, in letzter Zeit aber geändert worden - ein Hinweis darauf, dass die Datenschutzbeauftragten in Deutschland nicht die Einflussmöglichkeiten haben, die aus der Perspektive der Bürgerrechte sinnvoll wären. Die von Frau Sokol angeführte Änderung des Polizeigesetzes in NRW bezüglich der Videoüberwachung oder die Einführung einer DNA-Datenbank trotz Warnung von Seiten der Datenschützer verdeutlicht des Weiteren die beschränkte Macht dieser Behörde. Politiker sehen die Datenschützer wohl eher als *Störenfriede*, wie der aktuelle Konflikt zwischen Bundesinnenminister Schily und dem Bundesdatenschutzbeauftragten Peter Schaar verdeutlicht: Die Kritik Schaars an den Plänen für die

[288] Sokol 2003, Antwort 17

Einführung neuer Pässe mit biometrischen Daten wies Schily scharf zurück und warf Schaar Kompetenzüberschreitung vor.[289]

Das Verhältnis der Bürger zu ihrer Privatsphäre und ihren eigenen Daten schätzt Frau Sokol als ambivalent ein: Zum einen präsentieren die Menschen sich immer mehr und sind stärker selbstdarstellerisch tätig, zum anderen sind aber auch die Anfragen an ihre Dienststelle stark gestiegen. In bestimmten Bereichen wie Internet und Werbung sei das Bewusstsein für den Datenschutz gestiegen, in anderen eher zurück gegangen.

Die Datenschutzbeauftragte betont, dass der Staat einen Anlass haben muss, um seine Bürger zu überwachen und in ihre Rechte einzugreifen, ansonsten bestehe erst einmal eine Unschuldsvermutung. Hier stellt Frau Sokol aber eine Änderung fest, indem der Staat den Bürgern zunehmend so gegenüber treten würde, als ob sie *nur noch nicht verdächtig* wären. Sokol sieht hier eine Kultur des Misstrauens entstehen. Sie beobachtet eine Eigendynamik in der Techniknutzung - wenn Möglichkeiten da seien, würden diese auch gerne genutzt. Alles, was möglich ist, würde auch gemacht, es sei denn, es würde politisch begrenzt.

4.3 Fallstudie A: Videoüberwachung und technische Sicherungssysteme im öffentlichen Raum – das Beispiel der Kölner Verkehrsbetriebe (KVB)

Die Kölner Verkehrsbetriebe stellen, wie bereits zuvor beschrieben, innerhalb der Stadt den größten Betreiber von Videoüberwachungssystemen dar. Für die KVB ist die Videoüberwachung *ein* Mittel, um Sicherheit zu gewährleisten. Auch andere Hilfsmittel, wie z.B. Notsprechanlagen oder besondere Mechanismen in den Türen, die ein Einklemmen verhindern sollen, sind Teil des Sicherheitskonzepts. Diese sind aber innerhalb der Fallstudie nicht von Bedeutung, da bei ihnen der Aspekt der Überwachung nicht gegeben ist.

Während der gesamten empirischen Phase, die ca. ein Jahr dauerte, wurde Material über die technischen Sicherungssysteme gesammelt, inhaltsanalytisch ausgewertet und als Hintergrundinformation aufbereitet. Fotos wurden erstellt und Interviews geführt. Im Rahmen der Teilnehmenden Beobachtung wurde ein Forschungstagebuch geführt und diente als Grundlage der Beurteilung des Einsatzes dieser Systeme im Alltag. Der Zugang zum Feld gestaltete sich unproblematisch, da die Forscherin selbst Kundin der KVB ist und diese nahezu täglich nutzt.

Als Ansprechpartner für ein Experteninterview wurde Herr Joachim Berger, der Pressesprecher der KVB ermittelt, der das Unternehmen nach außen hin vertritt

[289] vgl. Tagesschau 2005

und zu Fragen der Installation von technischen Sicherungssystemen als kompetenter Ansprechpartner zur Verfügung stand. Der Kontakt war von Anfang an durch große Offenheit und Entgegenkommen seitens Herrn Bergers gekennzeichnet, der auch noch nach dem Interview für Rückfragen zur Verfügung stand. Da ein Ziel der Studie war, den Fall aus verschiedenen Perspektiven zu betrachten, wurde neben der Ebene *Forscherin* und *Betreiber* auch die Perspektive der *Kunden* als Adressaten der Videoüberwachung durch Interviews mit einer Stichprobe von Fahrgästen abgedeckt.

4.3.1 Hintergrund-Informationen

Wirkweise und Nutzen der Videoüberwachung in Köln

Die Ausweitung der Videoüberwachung an öffentlichen Plätzen wird auch in Köln diskutiert.[290] Innerhalb dieser Diskussion wurde eine Bürgerbefragung der Kölner Polizei veröffentlicht, die sich unter anderem mit dem Sicherheitsgefühl der Bürger an unterschiedlichen Kölner Plätzen beschäftigt und diese mit den Daten der Kölner Kriminalitätsstatistik in Verbindung bringt. Eine Frage, der nachgegangen wird ist: Wo *fühlen* sich die Kölner unsicher, wo finden *tatsächlich* die meisten Straftaten statt und welche Rolle spielt die Videoüberwachung an dieser Stelle? Hier geht es insbesondere um eine Einschätzung des Einsatzes von Videokameras im öffentlichen oder halböffentlichen Raum, wie er nachfolgend in der Fallstudie zur Videoüberwachung innerhalb der Kölner Verkehrsbetriebe (KVB) untersucht wird. Ergänzend sollen Ergebnisse der Studie daher an dieser Stelle vorgestellt werden.

Allgemeine Bürgerbefragung durch die Polizei Köln und Einschätzungen der Polizeiinspektion Mitte zur Videoüberwachung

Bei der im Jahr 2003 von der Polizei Köln durchgeführte Bürgerbefragung wurden laut Angaben der Polizei Köln 9.159 Fragebögen verschickt, die innerhalb des Erhebungszeitraumes von einem Monat eine Rücklaufquote von 30,5 % hatten.[291] Innerhalb der Bürgerbefragung wurde neben der Zufriedenheit der Bürger mit der

[290] Dazu gab es beispielsweise am 14.06.2004 ein öffentliches Hearing, bei dem die Datenschutzbeauftragte des Landes NRW, Frau Sokol und jeweils ein Vertreter der Firma Siemens, des Verbandes der Elektrotechnik, der Polizeigewerkschaft und Vertreter der Politik und der Kölner Polizei kontrovers diskutierten. Innerhalb dieser Diskussion wurde auf das im Anschluss vorgestellte Papier (die Allgemeine Bürgerbefragung) verwiesen.

[291] Die Daten der Bürgerbefragung und die interne Einschätzung zur Bewertung von Örtlichkeiten für die Installation von Videoüberwachungsanlagen wurden mir durch die Abteilung für Öffentlichkeitsarbeit der Polizei freundlicherweise zur Verfügung gestellt.

Polizei auch abgefragt, an welchen Orten sich die Bürger besonders unwohl und unsicher fühlten. Diese Orte wurden als potenzielle *Angsträume* interpretiert. Im Einzelnen sind dies Plätze in der Kölner Innenstadt, wie die Domplatte (Nennung an erster Stelle), der Ebertplatz (zweite Stelle), der Neumarkt und schließlich der Bahnhofsvorplatz. Interessant ist dabei, dass der Neumarkt, ein zentraler Verkehrsknotenpunkt der Kölner Innenstadt, mit 1.934 Delikten im Jahr 2003 der am stärksten von Kriminalität belastete Platz ist. 1.372 Fälle waren einfacher Diebstahl, davon waren 929 Taschendiebstähle. Ferner fanden 35 Raub- und 58 Körperverletzungsdelikte, sowie 48 Rauschgiftdelikte statt. Die Bürger liegen in ihrer Einschätzung, sich dort unsicher zu fühlen, also nicht falsch. Gerade dieser Bereich wird aber auch von den Kölner Verkehrsbetrieben videoüberwacht. Herr Udo Behrendes, Polizeidirektor der Polizeiinspektion Köln Mitte, stellt in einem internen Papier, das durch die Pressestelle der Polizei Köln zur Verfügung gestellt wurde, fest:

> „Wie [...] dargelegt, werden die meisten Taschendiebstahlsdelikte in den U-Bahnbereichen der KVB verübt. Nutzer des ÖPNV werden dort im dichten Gedränge bestohlen. Trotz bereits vorhandener, gut sichtbarer Video-Überwachungsanlagen ist keine Reduzierung der Fallzahlen in den betroffenen Bereichen feststellbar. Eine abschreckende Wirkung bereits vorhandener Kameras ist daher nicht eingetreten.“[292]

Auch beim Bahnhofsvorplatz wird dieses Ergebnis bestätigt: Hier kam es trotz Videoüberwachung und deren Auswertung in der so genannten 3-S-Zentrale[293] der Bahn im Jahr 2003 zu einer Erhöhung der Fallzahlen um ca. 100 Delikte. Die Polizei in Köln setzt daher auf den Einsatz so genannter City-Streifen, einer Erhöhung der Personalpräsenz also, und sieht Videoüberwachung derzeit nicht als geeignetes Mittel zur Bekämpfung der Kriminalität in Köln.

4.3.2 Die Videoüberwachung vor Ort

Verbreitung der Videoüberwachung innerhalb der KVB

Videoüberwachungssysteme wurden in den Fahrzeugen der KVB am 1. Juli 1999 in Betrieb genommen, bis Jahresende waren rund 70 Bahnen ausgerüstet. Im Verlauf des Jahres 2000 stieg die Zahl auf 120 Fahrzeuge mit Videoüberwachung. Mit einer neuen Fahrzeugserie, die ab Ende 2000 ausgeliefert wurde, stieg die Zahl bis Ende 2002 auf 183 Fahrzeuge. Insgesamt liegt die Zahl der KVB-

[292] Behrendes 2003, S. 3

[293] Die drei „S“ stehen für Service, Sicherheit und Sauberkeit und sind eine Image-Kampagne der Deutschen Bahn AG, in der es darum geht, die Bahnhöfe von ihrem *Schmuddel-Image* weg zu bringen.

Fahrzeuge bei rund 360, es waren also 2002 50% der Fahrzeuge mit Videokameras ausgestattet. Ab Herbst 2005 wird eine weitere Serie von Fahrzeugen ausgeliefert, die ebenfalls alle mit Videoüberwachung ausgerüstet sind. Bis Ende 2006 wird sich die Zahl der ausgerüsteten Fahrzeuge auf über 250 erhöhen, was dann 70% des Fahrzeug-Bestandes ausmacht.

In den U-Bahn-Stationen werden Videokameras zur Überwachung des Betriebsablaufes seit 1982 eingesetzt. In diesem Jahr wurde auch die zentrale Leitstelle der KVB in Betrieb genommen. Die Zahl der im U-Bahnbereich installierten Kameras liegt bei ca. 180.[294]

Funktionsweise der Kameras

1999 führten die Kölner Verkehrsbetriebe, erstmals in diesem Umfang in Europa, Videoüberwachung in den Fahrzeugen ein, bei welcher der gesamte Innenraum per Videokamera überwacht wird.[295] Dabei werden alle zwei Sekunden vier Aufnahmen durch die Kameras erstellt. Pro Kamera macht das *ein* Bild alle 2 Sekunden[296], das digital auf einer Festplatte, die sich vorne beim Fahrer befindet, gespeichert wird. Die Festplatte verfügt über einen Speicher, der 24 Stunden aufzeichnen kann und wird nach Ablauf dieser Zeit wieder überschrieben. Dies hat unter anderem datenschutzrechtliche Gründe, die Daten werden nicht aufbewahrt. Nur wenn innerhalb von 24 Stunden Hinweise auf eine Straftat eingehen, kann der Datenträger dem Fahrzeug entnommen und die Daten ausgewertet werden. Diese gehen zur Auswertung ausschließlich an Strafverfolgungs- und Ordnungsbehörden und dürfen von der KVB nicht genutzt werden.[297]

[294] vgl. Berger 2005

[295] vgl. Berger 2003, Antwort 6

[296] vgl. Berger 2003, Antwort 9-12

[297] vgl. Berger 2003, Antwort 7

Kameras in den Fahrzeugen

In den meisten Bahnen der KVB befinden sich mittlerweile Videokameras. Pro Fahrzeugwagen sind vier Kameras angebracht, deren Linsen so angeordnet sind, dass jede Hälfte des Wagens vollständig erfasst wird. Es handelt sich bei den Kameras um kleine, so genannte Dome-Kameras, die an der Fahrzeugdecke angebracht sind, und sehr unauffällig sind. Sie haben die Form von kleinen Halbkreisen, deren Durchmesser in etwa 10 cm beträgt. An einer Seite ist ein kleiner schwarzer Punkt zu sehen, bei dem es sich bei näherem Hinsehen um die Linse der Kamera handelt. Betritt man ein Fahrzeug der Kölner Verkehrsbetriebe fällt einem nicht auf Anhieb auf, dass Videokameras installiert sind.

Abbildung 9: Dome-Kameras an den Decken der KVB-Fahrzeuge, aufgenommen in der Linie 12

Abbildung 10: Nahaufnahme einer Dome-Kamera an der Decke

Abbildung 11: Nahaufnahme eines Hinweisaufklebers

Die Aufkleber, die auf die Videoüberwachung in den Fahrzeugen hinweisen sollen, sind in den älteren Wagen, also die, die vor 2002 ausgestattet wurden, ganz hinten im Fahrzeug angebracht. Sie sind, geht man nicht nach ganz hinten durch, nicht zu entdecken. Es handelt sich hierbei um rechteckige Aufkleber, die den Text: „Videoüberwachung in den Bahnen: Zu Ihrer Sicherheit und gegen Vandalismus“ tragen.

Bei den neueren Bahnmodellen sind die Aufkleber besser sichtbar in der Nähe der Türen angebracht.

Abbildung 12: Anbringung der Hinweisaufkleber in älteren Bahnmodellen

Abbildung 13: Anbringung der Hinwesaufkleber in neueren Bahnmodellen

Videokameras auf den Bahnsteigen

Auf den meisten Bahnsteigen hat die KVB ebenfalls Videokameras installiert. Hierbei handelt es sich um größere Modelle der Firma Grundig. Die Kameras sind in der Regel am Ende des Bahnsteigs, seitlich des Treppenaufgangs, installiert, so dass sie den Bahnsteig komplett im Blick haben. Normalerweise befinden sich zwei Kameras auf einem Bahnsteig (die eine am rechten, die andere am linken Aufgang), es gibt aber auch Haltestellen, an denen eine weitere Kamera in der Mitte des Bahnsteiges installiert ist. Die Kameras auf den Bahnsteigen werden nicht durch ein Hinweisschild kommentiert, was den von Frau Sokol beschriebenen Anforderungen an die Videoüberwachung in öffentlichen Verkehrsmitteln deutlich widerspricht.

Abbildung 14: Videoüberwachung auf den Bahnsteigen der KVB

Alltäglichkeit der Videoüberwachung

Abbildung 15: Detail der Videoüberwachung auf den Bahnsteigen der KVB

Die Videoüberwachung wird in der Regel bei der täglichen Nutzung der KVB nicht zum Thema. Während der gesamten Teilnehmenden Beobachtung tritt die Videoüberwachung nie aus ihrem Schattendasein heraus. Die Kameras existieren zwar, sie werden aber, so könnte man mutmaßen, entweder gar nicht wahrgenommen oder schlicht ignoriert. Es konnte zu keiner Zeit beobachtet werden, dass Menschen sich z.B. von einer Kamera wegsetzten, oder ihren Blick zu den Kameras schweifen ließen. Auch eine Kenntnisnahme der Hinweisschilder wurde nicht beobachtet. Innerhalb der Ethnographie wurde also zum einen die Frage aufgeworfen, welche Ziele die KVB mit der Installation der zumeist unauffälligen Kameras verfolgt und zum anderen, wie die KundInnen der KVB die Kameras wahrnehmen und interpretieren. Die anschließenden Interviews mit dem Pressesprecher der KVB und mit Fahrgästen sollen darüber Aufschluss geben.

4.3.3 Die Videoüberwachung aus Sicht der Kölner Verkehrsbetriebe

Der Interviewpartner Herr Berger ist seit 1985 Pressesprecher der Kölner Verkehrsbetriebe (KVB) und mit sämtlichen öffentlichkeitsrelevanten Themen befasst, was auch das Thema Sicherheit und somit auch Sicherheit durch technische Systeme mit einschließt.[298] Durch das Experteninterview mit dem Pressesprecher der Kölner Verkehrsbetriebe sollten die Motive der KVB ermittelt werden, warum Videokameras installiert werden und welche sonstigen technischen Kontroll- und Überwachungs- bzw. Sicherheitssysteme innerhalb der KVB in Gebrauch sind. Ermittelt werden sollte:

- Was verspricht sich die KVB vom Einsatz solcher Systeme?
- Gibt es Beispiele aus der Praxis, in denen technische Sicherheitssysteme besonders positiv bzw. negativ aufgefallen sind?

[298] vgl. Berger 2003, Antwort 4

- Welche Vor- und Nachteile werden in den Systemen von Seiten des Betreibers gesehen?
- Welche Meinung herrscht dazu, wie die Systeme von den Kunden angenommen werden und gibt es dazu Untersuchungen seitens der KVB?
- Gibt es weitere Pläne, die technische Überwachung und Kontrolle auszuweiten und wird das Personal speziell geschult, mit der Technik umzugehen?

Auswertung des Interviews

Sicherheit

Für Herrn Berger stellt die Videoüberwachung und andere technische Systeme, welche die KVB einsetzt – wie z.B. Notsprechstellen oder Notbremsen in den Fahrzeugen – ein Mittel dar, um Sicherheit herzustellen. Gleich zu Beginn des Interviews weist Herr Berger auf die Rücknahme der personellen Präsenz in den Fahrzeugen und Anlagen in den letzten 30 bis 40 Jahren hin. Damit sei im subjektiven Empfinden der Fahrgäste auch ein Verlust von Sicherheit einhergegangen, da Ansprechpartner fehlten. Die Entwicklung im technischen Bereich hätte es aber ermöglicht, technische Maßnahmen an die Stelle menschlicher Sicherheitsüberprüfungen zu setzen. Zu diesen Sicherheitstechniken gehört auch die Videoüberwachung, die von der KVB im Jahre 1999 erstmals in Europa in diesem Umfang realisiert wurde.

Herr Berger führt aus, dass im vergangenen Jahrzehnt

> „das Bedürfnis nach Sicherheit in der Öffentlichkeit und vor allem im öffentlichen Raum immer größer wurde , dass das aber von den Ordnungs- und Polizeibehörden nicht mehr in genügendem Maße geleistet werden konnte.“[299]

Sicherheit ist ein Thema, das in der Öffentlichkeit hoch im Kurs steht, es hat also auch letztlich etwas mit dem Image der KVB in der Öffentlichkeit zu tun, wenn das Verkehrsunternehmen verstärkt das Thema Sicherheit aufgreift und hohe Summen in die Installation von technischen Überwachungssystemen steckt. Dies wird auch in der folgenden Äußerung von Herrn Berger deutlich:

[299] Berger 2003, Antwort 7

> „Die Medien arbeiten vor allem mit unsicheren Situationen. Sie kennen die Vorfälle auf Friedhöfen, in Parkhäusern, in dunklen U-Bahnschächten. Das sind alles, wenn es dort Vorkommnisse gibt, Themen für die Medien und sie erzeugen in der Berichterstattung auch gleichzeitig immer die Reaktion auf der anderen Seite, das heißt, die Frage nach mehr Sicherheit und von daher kann man nicht sagen, dass wir zu einem bestimmten Zeitpunkt die Forderung aus unserer Kundschaft gehabt hätten: das müsst ihr jetzt machen, sondern es ist eine laufende Entwicklung, die überall in der Gesellschaft stattfindet, nicht nur bei uns im Nahverkehr."[300]

Die KVB orientiert sich stark an der öffentlichen Berichterstattung und ist logischerweise daran interessiert, als *sicheres* Unternehmen, das sich um die potenziellen Sicherheitsbedürfnisse der Kunden kümmert, wahrgenommen zu werden. In diesem Sinne bedeutet die Installation von Videokameras – und das noch dazu, wie bereits erwähnt, als erstes Nahverkehrsunternehmen in ganz Europa - erst einmal einen Imagegewinn für das Unternehmen. Wie Herr Berger ausführt, ist von Seiten der Kundschaft selbst keine Forderung nach mehr Kontrolle oder Überwachung geäußert worden, das Unternehmen richtet sich hier stark nach der Presse. Befragungen oder Untersuchungen zum Bedürfnis nach Sicherheit hat die KVB nur in solchen Fällen unternommen, wo es beispielsweise um die Anzahl der zu installierenden Notsprechanlagen oder der Videokameras in den Fahrzeugen ging. Diese Untersuchungen standen aber nicht mehr zur Auswertung zur Verfügung, da sie laut Herrn Berger nicht aufbewahrt wurden.[301] Auch innerhalb der folgenden Ausführung wird deutlich, dass das Image der KVB von großer Bedeutung ist und zu dem Entschluss geführt hat, Videoüberwachung nach und nach in jedem Fahrzeug zu installieren:

> „[...] denn, das hat sich auch gezeigt, wiederum in Reaktionen der Öffentlichkeit, wenn irgendwo etwas passiert und es ist dann ein Fahrzeug, was keine Videoüberwachung hat, dann wirkt das kontraproduktiv. Dann wird sofort gesagt: Warum da nicht?"

Um sich also in punkto Berichterstattung auf der sicheren Seite zu befinden, erscheint es für die KVB als sinnvoll, die Zahl der mit Videoüberwachung ausgerüsteten Fahrzeuge zu erhöhen.

Neben den technischen Installationen betont Herr Berger aber auch gleich zu Beginn des Interviews, das diese alleine nicht ausreichen, um bei den Fahrgästen ein Sicherheitsgefühl herzustellen:

---

[300] Berger 2003, Antwort 13

[301] vgl. Berger 2003, Antwort 14

> „Zur Herstellung des Sicherheitsgefühls benötigen wir heute aber auch die personelle Präsenz, um dem Fahrgast einfach mental den Eindruck zu vermitteln, dass er nicht alleine ist, und das es in jeder Situation für ihn Hilfe gibt.“[302]

Daher wurde, parallel zur Einführung technischer Sicherheitssysteme, auch das Personal wieder aufgestockt und eine Sicherheits- und Serviceabteilung eingerichtet. Herr Berger begründet dies damit, dass Sicherheit vor allem ein subjektives Empfinden sei und die technischen Einrichtungen alleine nicht in der Lage seien, beim Fahrgast ein subjektives Sicherheitsgefühl in ausreichendem Maße herzustellen.[303] Die Videoüberwachung bewertet Herr Berger aber dennoch positiv und dies unabhängig davon, ob tatsächlich mehr Sicherheit erreicht wird:

> „[...] Unabhängig davon, ob objektiv tatsächlich mehr Sicherheit erreicht wird, aber subjektiv ist auf jeden Fall dieser Effekt vorhanden und das betrifft eigentlich auch den wesentlichen Teil, denn die Frage, ob Sicherheit vorhanden ist oder nicht, ist immer relativ.“[304]

Die Frage sei, ob man als Unternehmen im öffentlichen Raum durch technische Einrichtungen auf das Sicherheitsgefühl Einfluss nehmen könne. Die KVB sei davon überzeugt, dass, wenn man dem Kunden das Bewusstsein oder die Information gäbe, dass eine Videoüberwachung stattfindet, liefere man ihm damit auf jeden Fall ein zusätzliches Stück an *subjektiver Einstimmung für mehr Sicherheit*.[305] Ob es wirklich zu einem Mehr an Sicherheit kommt, ist also in der Praxis gar nicht entscheidend. Es geht, wie schon oben, darum, ein positives Image aufzubauen und den Fahrgästen ein *gutes Gefühl* zu vermitteln. Dass diese Haltung trügerisch ist, wurde schon in Kapitel 4.3.1 deutlich, in dem die Ergebnisse der „Allgemeinen Bürgerbefragung“ der Polizei Köln vorgestellt wurden, bei der herauskam, dass gerade an den Orten, wo Videokameras installiert sind und man sich eigentlich sicher fühlt, die Kriminalität am höchsten ist.[306] Entscheidend ist nicht die tatsächliche, sondern die subjektive Sicherheit, oder besser: das bereits viel zitierte *subjektive Sicherheitsgefühl.* Gefühle scheinen in der Diskussion um Sicherheit mehr zu gelten als Fakten.

---

[302] vgl. Berger 2003, Antwort 7

[303] vgl. Berger 2003, Antwort 7

[304] Berger 2003, Antwort 20

[305] vgl. Berger 2003, Antwort 20

[306] Dies ist in der Passage der KVB am Kölner Neumarkt der Fall, die komplett videoüberwacht ist und die höchste Rate an Handtaschendiebstählen aufweist, vgl. Behrendes 2003

Beurteilung des Nutzens der Videoüberwachung

Entgegen der positiven Bewertung, die Herr Berger der Videoüberwachung bei der Entstehung eines guten Sicherheitsgefühls zukommen lässt, sieht die Einschätzung, die er dem tatsächlichen Nutzen der Kameras entgegenbringt, z.B. bei der Verhinderung von Straftaten, sehr nüchtern aus. So führt er aus, dass man Sicherheit nicht vorsorglich herstellen, sondern immer nur die Folgen beeinflussen könne, die ein Vorfall hervorruft.[307]

> „In dem Moment, wo etwas passiert, können Sie den Vorgang selbst nie verhindern. Man kann durch Sicherheitseinrichtungen eigentlich immer nur die Folgen beeinflussen. Es ist ein weit reichender Irrtum, dass man meint, man könnte Sicherheit vorsorglich herstellen. Das können Sie in keinem Fall.“[308]

Im Falle der Videoüberwachung könne aber im Nachhinein die Strafverfolgung beschleunigt werden, wenn es denn innerhalb von 24 Stunden zu einer Anzeige gekommen ist. Ansonsten ist das aufgenommene Videomaterial der KVB nämlich schon wieder gelöscht worden. Hier kann Herr Berger auch von einem Fall berichten, in dem Videoüberwachung in der KVB zur Aufklärung einer Straftat beigetragen hat. Neben dieser aufklärerischen Wirkung der Videoüberwachung rechnet sich die KVB auch eine abschreckende Wirkung aus:

> „Allein durch das Vorhandensein dieser Einrichtung in den Fahrzeugen, davon gehen wir jedenfalls aus, wird ein Großteil der Taten und Vorkommnisse verhindert, die sonst möglicherweise stattfinden würden.“[309]

Wie schon bei dem zuvor behandelten *Sicherheitsgefühl* der Fahrgäste geht die Aussage Bergers in Richtung von Mutmaßungen über Wirkungen, die man der Videoüberwachung unterstellt. Die bereits zitierte Polizeistatistik der Stadt Köln zeigt aber, dass sich bestimmte Straftäter durch Videoüberwachung keinesfalls von ihrem Vorhaben abhalten lassen. Dies sieht auch Herr Berger und betont mehrmals, dass man die Tat als solche nie verhindern könne und ein hoher Prozentsatz der Vorfälle in den Fahrzeugen spontan passiere. Selbst wenn eine zeitgleiche Videoüberwachung mit Personal, welches die Aufnahmen direkt ansieht, passiert, ist dieser spontane Faktor nicht aus der Welt zu schaffen. Wer eine Tat verüben möchte, den hält auch die Videoüberwachung nicht auf:

---

[307] vgl. Berger 2003, Antwort 8

[308] Berger 2003, Antwort 8

[309] Berger 2003, Antwort 8

> „Genauso ist das auch mit der Videoüberwachung. Auch durch eine, ja zeitgleiche Videobeobachtung, beispielsweise durch menschliches Personal können Sie nicht verhindern, dass eine Handtasche geklaut wird, oder dass irgendwo ein Graffiti gemalt wird."[310]

Herr Berger bewertet es aber dennoch als positiv, überhaupt etwas tun zu können, auch wenn sich dies nur auf eine spätere Strafverfolgung bezieht. Der Nutzen der Kameras für Opfer einer kriminellen Handlung besteht also, wenn überhaupt, darin bei der späteren Täterverfolgung hilfreich zu sein. In andere Fahrgäste, welche die Straftat eventuell mitverfolgen, setzt Berger dabei wenig Vertrauen: „[...] wir haben ja heute die Problematik, dass alle Leute weggucken, wenn irgendwo was passiert."[311] Videokameras werden also zu *Hinguckern*, die sich 24 Stunden merken, was passiert ist und ihr Wissen gegebenenfalls den Strafverfolgungsbehörden zur Verfügung stellen.

Genaue Zahlen über Aufklärungserfolge der Videoüberwachung liegen Herrn Berger nicht vor, da das Kameramaterial, sollte es überhaupt dazu kommen, direkt an die Strafverfolgungsbehörden weiter gegeben werden, und für die KVB nicht mehr nachvollziehbar ist, welcher Effekt entsteht. Herr Berger geht davon aus, dass viele Fälle aufgrund von fehlendem Verhandlungserfolg eingestellt werden und etwa 10 bis 20 Fälle pro Jahr existieren, bei denen das Kameramaterial der KVB tatsächlich bei der Strafverfolgung hilfreich ist.[312] Auch an dieser Stelle zeigt sich, dass die Effizienz und der Nutzen der Videokamera nicht mit realen Zahlen oder Fällen belegt werden kann, sondern Annahmen bestehen, dass es eine gewisse Anzahl an aufgeklärten Fällen gibt. Die Videoüberwachung lebt also von ihrem positiven Image, vom Mythos der Sicherheit, der um sie erbaut wurde und der durch keinerlei Zahlen belegt wird. Dies wird aber in der Regel ignoriert. Der Image-Gewinn, dem die Installation solcher Kameras zugerechnet wird, wiegt höher.

Kooperation der KVB mit Polizei und Ordnungsbehörden

Ein interessanter Aspekt im Sicherheitskonzept der Kölner Verkehrsbetriebe ist die Ordnungspartnerschaft mit den Polizei- und Ordnungsbehörden in Köln, sowie dem Bundesgrenzschutz. Diese Kooperation ergibt sich dort, wo die KVB und die Deutsche Bahn gemeinsame betriebliche Bereiche unterhalten, wie es beispielsweise am Kölner Hauptbahnhof oder in Köln-Chorweiler der Fall ist. Dort laufen S-Bahnen, U-Bahnen oder auch Züge der Deutschen Bahn im glei-

---

[310] Berger 2003, Antwort 8

[311] Berger 2003, Antwort 22

[312] vgl. Berger 2003, Antwort 19

chen Gebäude zusammen und führen zu einer ordnungspolitischen Zusammenarbeit, wie Berger es ausdrückt.[313]

Brisant wird das Thema an der Stelle, an der es zu Synergien zwischen Unternehmen wie der KVB, den Polizei- und Ordnungsbehörden und dem Bundesgrenzschutz kommt, d.h. an der Stelle, an der unterschiedliche Begehrlichkeiten zusammentreffen und auch zusammenarbeiten.

Beurteilung der Kundenseite / Informationspolitik der KVB

Herr Berger erklärt, dass die KVB zur Information der Kunden sämtliche möglichen Informationsmedien heranzieht. Auf die Frage nach den relativ unauffällig, am Ende des Wagens angebrachten Hinweisaufkleber zur Videoüberwachung, erklärt Berger, dass möglicherweise einfach keine geeigneten anderen Flächen mehr zu Verfügung standen. Es gäbe eine Reihe von Pflichthinweisen (z.B. die bzgl. dem erhöhten Beförderungsentgelt oder der Türöffnung im Notfall) und in Zusammenhang damit müsse man sich überlegen, wo man überhaupt noch einen Hinweis anbringen könne, der wahrgenommen werde. Ob die Hinweisaufkleber allerdings ganz hinten am Ende des Wagens wahrgenommen werden, bleibt fragwürdig. Wie Herr Berger bemerkt, ist Aufmerksamkeit immer von Interesse geleitet - jemand, der sehr unsicher ist, würde solche Hinweise auch an unauffälligen oder versteckten Stellen finden. Herr Berger erklärt, dass bei der Einführung neuer Systeme auch die Medien, vor allem die Presse, das Radio, sowie Broschüren, Flyer und Schilder genutzt würden. Ferner behandelt die KVB in eigenen Publikationen, wie einer Kundenzeitung, die an alle Kölner Haushalte verteilt wird, Schwerpunktthemen wie beispielsweise die Bedienung einer Notbremse. Die Hinwendung der Kunden zu solchen Themen seien jedoch immer interessegeleitet:

> „Wenn irgendwo heute ein Verbrechen geschieht, dann sind alle Leute auf einmal elektrisiert und sensibilisiert, nach einem halben Jahr ist das wieder weg. Genauso ist das auch bei uns, wenn etwas passiert, dann gucken alle und fragen: wo sind die Kameras, aber nach drei, vier Monaten ist das wieder vorbei.“[314]

[313] vgl. Berger 2003, Antwort 17

[314] Berger 2003, Antwort 22

Zusammenfassung

Auffällig innerhalb des Interviews mit Herrn Berger ist der häufige Bezug auf Gefühle der Fahrgäste und Mutmaßungen über die Wirkung der Kameraüberwachung. Fazit des Experteninterviews ist, dass es für die KVB einen Imagegewinn gegenüber der Öffentlichkeit, vertreten durch die Presse, bedeutet, solche Systeme zu installieren. Dabei folgt die Aufrüstung der Fahrzeuge der Berichterstattung über Vorfälle und „unsichere Situationen". Da man negative Presse fürchtet, wenn etwas in einer Bahn passiert, die nicht über Videoüberwachung verfügt, besteht die Tendenz möglichst viele Bahnen mit Videoüberwachung auszustatten. Die Äußerungen Bergers stehen hier denen der Datenschutzbeauftragten Frau Sokol gegenüber, die darauf hinwies, dass die Installation von Videokameras in jedem Einzelfall streng zu prüfen sei. Herrn Bergers Äußerungen lassen eher auf ein Gießkannenprinzip schließen, das eher eine Bahn mehr als eine zuwenig mit Videoüberwachung ausgestattet werden sollen. Auch mit den Hinweisschildern auf die Überwachung sieht es die KVB nicht so streng wie die Datenschützerin. Ein klar erkennbarer und deutlicher Hinweis, wie in erarbeiteten Anforderungen festgelegt[315], fehlt in den älteren Bahnmodellen, die einen Hinweisaufkleber in der hintersten Ecke des Waggons angebracht haben, und an den Bahnsteigen.

Der tatsächliche Nutzen der Kameras ist lediglich dann festzustellen, wie auch Herr Berger feststellt, wenn es um eine potenzielle Strafverfolgung geht und wenn es innerhalb der 24 Stunden Aufzeichnungszeit der Kameras zu einer Anzeige kommt. In der konkreten Notsituation hilft eine Kamera dem Opfer gar nichts und wiegt es unter Umständen sogar in einer falschen Sicherheit. Kameras sind in der Wahrnehmung der KVB mit einem *Gefühl von Sicherheit* verbunden, nicht mit einer tatsächlichen. Sie werden, obwohl ihr Nutzen begrenzt ist und auch objektive Zahlen, wie z.B. die der Kölner Polizei, darlegen, dass sie zu keiner Minderung von Straftaten führen, aufgrund des positiven Images gerne eingesetzt.

Sicherheit wird, das hat Herr Berger selbst mehrfach betont, mit den technischen Systemen nicht hergestellt. Es wird aber versucht, ein Gefühl hervorzurufen, nämlich das der subjektiven Sicherheit. Das Wort *subjektiv* zeigt, dass es sich um eine sehr individuelle, schwer fassbare, fast schon nebulöse Formulierung handelt. Auch in anderen Zusammenhängen wird der Begriff der subjektiven Sicherheit herangezogen, wenn es um die Errichtung von Videoüberwachung auf öffentlichen Plätzen oder ähnliche Themen geht. Deutlich wird, dass das Thema Sicherheit höchst aktuell ist, unabhängig davon, ob die Kriminalitätszahlen steigen oder sinken, ist es für ein öffentliches Transportunternehmen wichtig, sich dieses Themas anzunehmen.

---

[315] siehe Kapitel 4.2

4.3.4 Die Videoüberwachung aus Sicht der Fahrgäste

Die Fahrgäste sollten in den Fahrzeugen zur Videoüberwachung der KVB befragt werden, um Fragen wie „Wie finden Sie die Videoüberwachung in den Fahrzeugen?“ zu vermeiden. Die KundInnen sollten vor Ort eine Einschätzung der Installation und ihre Interpretation geben, ohne bereits im Vorfeld zu wissen, dass es sich um das Thema Videoüberwachung handelt. Es wurde angenommen, dass viele Fahrgäste gar nicht wissen, dass es sich bei den Installationen in den Bahnen um Videoüberwachungssysteme handelt.

Bei den Interviews musste der besonderen Situation der Bahnfahrt Rechnung getragen werden. Diese stellte sich so dar, dass die InterviewpartnerInnen nur eine begrenzte Zeitspanne zur Verfügung standen, bis sie die Bahn wieder verließen. Die Interviews dauerten im Schnitt fünf bis zehn Minuten und wurden in Form eines halbstandardisierten Interviewverfahrens mit offen gestellten Fragen konzipiert, um die benötigten Informationen abzufragen. Die Antworten wurden schriftlich protokolliert.

Die Befragung erhebt keinen Anspruch auf Repräsentativität, sie soll der Illustration dienen und Tendenzen innerhalb der Stichprobe anzeigen.

Die Befragung wurde vormittags in der Linie eins der Kölner Verkehrsbetriebe (KVB) auf der Fahrt vom Rudolfplatz in der Kölner Innenstadt bis Köln-Weiden und in entgegengesetzter Richtung durchgeführt.

Die InterviewpartnerInnen

Die Stichprobe besteht aus 12 zufällig ausgewählten Personen, die, was ihr Alter angeht, möglichst unterschiedlich sein sollten. Dabei reicht die Spannbreite des Alters von 20 bis 70 Jahren. Es wurde angestrebt, eine möglichst gleiche Anzahl von Männern und Frauen zu befragen, allerdings waren die männlichen Fahrgäste weniger bereit, Antwort zu geben und gaben das Wort in einigen Fällen an ihre jeweilige weibliche Begleitung ab. Somit kam es zu einem Verteilungsverhältnis von vier Männern zu acht Frauen. Neun der zwölf Personen fahren regelmäßig mit der KVB, drei nur alle paar Wochen oder Monate.

Tabelle 1: Übersicht der befragten KVB-Kunden

	Geschlecht	Alter	Beruf
Person A	weiblich	63	Fotografin im Ruhestand
Person B	weiblich	56	Sparkassen-Angestellte
Person C	männlich	31	Lehrer
Person D	weiblich	71	Rentnerin
Person E	weiblich	20	Teilnehmerin an einem Förderlehrgang
Person F	männlich	25	Student
Person G	männlich	28	Küchenhilfe
Person H	weiblich	70	Hausfrau
Person I	weiblich	26	Sprachschülerin
Person J	weiblich	63	Rentnerin
Person K	weiblich	62	Rentnerin
Person L	männlich	66	Rentner
Gesamtzahl			**12**

Fragestellung der Interviews

Beim Interview wurden halboffene Fragen gestellt, die einen Vergleich zwischen den Antworten ermöglichen, gleichzeitig aber auch Raum für individuelle Äußerungen geben sollten. Zu Beginn des Interviews wurden die Befragten über den Zweck der Befragung informiert und gefragt, ob sie regelmäßige Nutzer der KVB seien. Im Anschluss daran wurde die Frage gestellt, ob den Fahrgästen die weißen Halbkugeln[316], die an der Decke der KVB-Wagen installiert sind schon einmal aufgefallen sind, dabei wurde auf die Halbkugeln gedeutet. Im Anschluss wurde die Frage gestellt, ob die Interviewten wissen, worum es sich dabei handelt. Falls diese Frage bejaht wurde, wurden sie gefragt, ob sie wissen, wie dieses System funktioniert; falls sie es nicht wussten, wurde erklärt, dass es sich um Videokameras handelt, die den Innenraum der Bahn filmen. Die Befragten wurden dann aufgefordert, Ideen zu entwickeln, wie so ein System funktionieren *könnte.* Im Anschluss wurde die Frage gestellt, ob die Fahrgäste sich seit der Einführung der Videoüberwachung im Jahr 1999 sicherer fühlen als vorher. Die nächste Frage zielte darauf, ob die Interviewten sich gut über die Überwachung in den Bahnen informiert fühlen. Abschließend wurde die grundsätzliche Meinung zum Thema Videoüberwachung abgefragt und zum Schluss noch Alter und Beruf der Fahrgäste erhoben.

[316] siehe Abbildung 10, Kapitel 4.3.2

Auswertung

Die Mehrheit der Befragten fährt regelmäßig - also täglich oder mehrmals wöchentlich - mit der KVB, es ist also davon auszugehen, dass sie ausreichend Zeit hatten, sich ein Bild über die Ausstattung der Bahnen zu machen und sich gegebenenfalls auch über diese zu informieren.

In der Auswertung der Interviews wurde eine grafische Darstellung der Befragungsergebnisse gewählt, die im Anschluss weiter erläutern werden. Die Darstellung folgt der Reihenfolge der oben formulierten Fragstellungen.

Tabelle 2

Bemerken der Installation der weißen Halbkugeln an der Decke	
Ja	6
Nein	6
Gesamtzahl	**12**

Die Hälfte der Befragten hat schon einmal Notiz von den weißen Halbkugeln[317] genommen. Der anderen Hälfte sind diese Installationen bislang noch nicht aufgefallen, darunter sind auch die 3 Personen, die weniger häufig mit der KVB fahren. Dies deutet darauf hin, dass die Kameras recht unauffällig angebracht sind und nicht von jedem auf Anhieb wahrgenommen werden können. Sie fügen sich so unscheinbar in die Innenausstattung der Bahn ein, dass nur 50% der Befragten sie überhaupt jemals wahrgenommen haben.

Nachdem die Befragten auf die Installation aufmerksam wurden, wurden sie im Anschluss befragt, ob sie eine Idee hätten, worum es sich bei den „weißen Halbkugeln“ handele. Dabei wurden keine Vorgaben durch die Interviewerin gemacht, sondern die Äußerungen der Fahrgäste dokumentiert.

Tabelle 3

Wissen darum, was das sein könnte	
Feuermelder/Sprinkleranlage	2
Kamera	6
Beleuchtung	1
Keine Kenntnis	3
Gesamtzahl	**12**

[317] siehe Abbildung 10, Kapitel 4.3.2

Die Hälfte der Befragten konnte dabei richtig äußern, dass es sich um eine Videokamera handelt. Zwei Personen hielten die Halbkugeln für eine Sprinkleranlage bzw. einen Feuermelder, eine Person dachte, dass es sich dabei um Beleuchtung handelt. Drei Personen hatten keine Idee, was es mit den Halbkugeln auf sich haben könnte. Die meisten Befragten (5 Personen), welche die Installation schon einmal bemerkt hatten, konnten auch angeben, dass es sich dabei um ein Videoüberwachungssystem handelt, - nur eine Person hielt die Halbkugeln für Beleuchtung. Eine Person, welche die Halbkugeln zuvor noch nicht bemerkt hatte, riet, dass es sich dabei um eine Kamera handeln könnte. Wenn man die Halbkugeln also erst einmal bemerkt hat, ist der Schluss auf Videoüberwachung bei den meisten naheliegend. Spontan sind die Geräte aber anscheinend nicht sofort als Videokameras zu identifizieren, denn immerhin können 50% der Befragten den Halbkugeln gar keine oder nur eine falsche Funktion zuordnen. Es scheint also, dass das Design eher so gewählt wurde, dass man

a) die Kameras nicht auf Anhieb bemerkt und

b) sie nicht auf Anhieb als Videokameras identifizieren kann.

Die Befragten, die nicht wussten, dass es sich um Videoüberwachungskameras handelt, wurden anschließend über die tatsächliche Funktion der Halbkugeln aufgeklärt und gebeten, zu mutmaßen, wie so ein Videoüberwachungssystem funktionieren könnte. Diese Frage hatte das Ziel, herauszufinden, welche Vorstellungen über Videoüberwachung bei den Fahrgästen der KVB verbreitet sind und wie viele davon mit der tatsächlichen Praxis der Videoüberwachung übereinstimmen. Die Beteiligten hatten die Möglichkeit, unterschiedliche Vorstellungen zu äußern.

Tabelle 4

Mögliche Funktionsweise des Systems (Mehrfachnennungen möglich)	
Fahrer kann Fahrzeuge überwachen	2
Videorekorderaufzeichnung	1
Direktübertragung in Zentrale	2
Film/Mikrofilmaufzeichnung	1
Keine Vorstellung	2
Aufzeichnung und Löschung der Aufnahmen	1
Kamera mit Computer verbunden	1
Wie ein Türspion/Videoüberwachung am Haus	3
Gesamtzahl	**13**

Dreimal verglichen die Interviewten die Funktionsweise der Kameras mit elektronischen Türspionen, also einer Videoüberwachung am Haus, bei der man durch eine Kameraübertragung sieht, was sich vor der Haustür abspielt. *Wer* dort überwacht oder wohin die Bilder übermittelt werden könnten, wurde nicht thematisiert, deutlich wurde aber, dass erwartet wird, *dass* jemand überwacht.

Zweimal wurde die Angabe gemacht, der Fahrer könne mit den Kameras die Innenräume der Bahnen überwachen. Die Vermutung, die Kamerabilder würden direkt in die Zentrale der KVB weitergeleitet werden, wurde ebenfalls zweimal geäußert. Ein Befragter meinte, die Aufnahmen würden auf Film oder Mikrofiche aufgezeichnet werden; ein anderer äußerte, dass es zu einer Videoaufzeichnung der Aufnahmen komme. Ein weiterer Befragter wusste, das es zu einer Aufzeichnung und späteren Löschung kommt, und eine Nennung bezog sich darauf, dass die Kamera mit einem Computer verbunden sei. Zwei Interviewpartner hatte keine Ideen, wie die Videoüberwachung in den Bahnen in der Praxis funktionieren könnte.

Deutlich wird, dass die Mehrheit der Befragten (7 von 12) sich die Videoüberwachung *aktiv* vorstellen, das heißt, sie gehen davon aus, dass der Fahrer, die Leitstelle der KVB oder andere Personen aktiv die Innenräume der Bahnen überwachen. Es wird deutlich, dass die meisten Befragten eine Vorstellung davon haben, wie eine Videoüberwachung der Straßenbahnen funktionieren könnte. Dabei wird klar, dass die Mehrheit der Befragten erwartet, eine Person (also z.B. der Fahrer oder jemand in der Leitstelle der KVB) beobachte über einen Monitor das Geschehen in der Bahn. Die Erwartung geht also deutlich in Richtung dahin, dass Angestellte der KVB im Notfall intervenieren, was in der Realität aber nicht der Fall ist, da das Geschehen in der Bahn aufgezeichnet wird und es nur im Nachhinein, bei Erstatten einer Anzeige innerhalb von 24 Stunden, zu einer Auswertung der Kameradaten kommt. Hier stehen die Erwartungen der Fahrgäste in Kontrast zur wirklichen Praxis der KVB.

Tabelle 5: Steigerung des Sicherheitsgefühls durch Videoüberwachung

Steigerung des Sicherheitsgefühls durch Videoüberwachung	
Steigerung	2
Keine Steigerung	6
Auch vorher schon sicher gefühlt	2
Keine/unklare Nennung	2
Gesamtzahl	**12**

Tabelle 5 gibt Auskunft über die Steigerung des Sicherheitsgefühls nach Einführung der Videoüberwachung in den Wagen der KVB im Jahr 1999. Zwei der Befragten äußern, dass sie sich durch die Videokameras sicherer fühlen, zwei weitere, dass sie sich auch schon vorher, ohne die Videoüberwachung, sicher gefühlt haben. Sechs Befragte verneinen, dass sie sich durch die Videokameras sicherer fühlen, und zwei äußern sich unklar oder wollen sich dazu nicht äußern. Ein Kommentar innerhalb der Antworten war, dass die Videokameras auch nicht helfen, wenn man tatsächlich angegriffen wird, diese würden dann nur bei der Aufklärung nützlich sein. Ein anderer Fahrgast bemerkt, dass sich sein persönliches Sicherheitsempfinden durch die Kameras nicht verbessert hat, er aber den Sinn der Videoüberwachung für ältere Fahrgäste oder bei Fahrten in der Nacht sieht.

Die beiden Fahrgäste, die sich durch Videoüberwachung sicherer fühlen, gehören paradoxerweise zu denen, welche die Halbkugeln an der Decke noch gar nicht bemerkt hatten und auch nicht wussten, worum es sich handelt. Ihre Aussagen, sich durch die Installation sicherer zu fühlen, ist also in Frage zu stellen, wenn sie vorher gar nichts von der Überwachung wussten, eventuell war ihr Wissen um die Videoüberwachung aber medial vermittelt. Zusammenfassend bedeutet dies, dass mindestens zwei Drittel der Befragten keine Steigerung ihres Sicherheitsgefühls durch die installierten Videokameras empfinden. Das Ziel der KVB, das Sicherheitsgefühl ihrer Fahrgäste durch die Videokameras zu erhöhen, ist also innerhalb dieser Stichprobe nicht erreicht worden.

Tabelle 6

Zufriedenheit mit der Information über die Systeme	
Zufrieden	2
Unzufrieden	7
Keine/unklare Nennung	3
Gesamtzahl	**12**

Nur zwei der Befragten sind zufrieden mit der Information über die Systeme, welche die KVB an ihre Kunden ausgibt; diese beiden erkannten auch die Halbkugeln als Kameras und wussten über die Funktionsweise relativ gut Bescheid, sie scheinen sich also entsprechend informiert zu haben. Sieben Personen erklären sich unzufrieden über die Information, die über die Überwachung in den Bahnen ausgegeben wird; eine davon entdeckte während des Interviews das erste Mal einen Aufkleber, der auf die Videoüberwachung hinweist und ganz am Ende des Wagens angebracht ist. Die Mehrheit der Stichprobe sieht sich also nicht gut informiert, was sich auch mit den unterschiedlichen Interpretationen der Kameras deckt.

Tabelle 7

Grundsätzliche Meinung zur Videoüberwachung (Mehrfachnennungen möglich)	
Grundsätzlich ablehnend	1
Grundsätzlich positiv	8
Furcht vor Missbrauch + Überwachungsstaat	3
Unklar	1
Gesamtzahl	**13**

Die Mehrheit der Befragten äußert sich grundsätzlich positiv über Videoüberwachung. Eine Person findet sie gut, weil damit „die Anonymität aufhört", ein anderer hält sie für eine sinnvolle Idee, um den Vandalismus einzudämmen; er selber fühlt sich davon eher nicht betroffen, da er „ja nichts Schlimmes anstellt". Ein Befragter steht der Videoüberwachung grundsätzlich ablehnend gegenüber, findet sie aber in der Bahn sinnvoll, da dies ein öffentlicher Ort sei und es dann „o.k. sei, wenn die Leute sich dann besser fühlen". Ein Fahrgast bemerkt, dass es gut ist, wenn etwas „Schlimmes passiert", meistens merke man aber gar nichts von der Videoüberwachung, da „meistens nichts passiert". Eine Befragte äußert sich, dass sie Kameraüberwachung gut findet, sie sich aber „durch Wachpersonal in den Bahnen oder auf den Bahnsteigen eher sicherer fühlt als durch Kameras".

Lediglich drei Befragte äußern sich besorgt über den Einsatz von Videoüberwachung, einer äußert, dass „man gläsern wird" und dass das „wie Big Brother" sei. Dennoch findet er die Überwachung in bestimmten Bereichen in Ordnung, wenn man es nicht übertreibe. Ein anderer Fahrgast äußert sich ähnlich und verweist auf George Orwells „1984" und einen „überwachten Staat", innerhalb der Bahn wird die Videoüberwachung aber auch hier als sinnvoll erachtet – gerade für ältere Menschen. Die dritte Person hält Videoüberwachung grundsätzlich für „gut und sinnvoll", fürchtet aber den Missbrauch der Informationen. Dieser muss, so der Befragte, ausgeschlossen werden. Videoüberwachung hat unter den Befragten eine recht hohe Akzeptanz. Obwohl es auch Bedenken gibt, die den Datenschutz betreffen, oder in Richtung „Überwachungsstaat" gehen, stehen die meisten Fahrgäste Videoüberwachung positiv gegenüber. Sie erwähnen Vorteile bei der Eindämmung von Vandalismus, „im Notfall" und für „ältere Leute". Diese Ergebnisse decken sich mit denen, die beim Interview mit Herrn Berger ebenfalls zutage traten: Videoüberwachung hat innerhalb der Stichprobe eine recht hohe Akzeptanz und ein mehrheitlich gutes Image, auch wenn man gar nicht so genau weiß, wie diese Dinge funktionieren und sich selbst nicht per se sicherer fühlt.

4.3.5 Fallinterpretation

Es lässt sich feststellen, dass die Videoüberwachung innerhalb der KVB seit ihrer Einführung im Jahr 1999 immer mehr ausgeweitet wurde. Ziel ist es, bis zum Jahr 2006 70% der Fahrzeuge mit Videokameras auszustatten.

Wie Herr Berger ausführte, ist von Seiten der Fahrgäste selbst keine Forderung nach mehr Kontrolle oder einer Videoüberwachung geäußert worden, das Unternehmen orientiert sich hier stark an der Diskussion des Themas in der Öffentlichkeit, denn es würde einen Imageverlust für das Unternehmen bedeuten, wenn etwas *da* passiert, wo noch keine Kamera installiert ist. Dies führt, aus Sicht der KVB, zu einer Art Zugzwang, alle Fahrzeuge mit Kameras auszustatten.

Das Thema *Sicherheit* steht in der Öffentlichkeit hoch im Kurs, es hat also auch letztlich etwas mit dem Image der KVB in der Öffentlichkeit zu tun, wenn sich das Verkehrsunternehmen verstärkt dieses Themas annimmt und augenscheinlich etwas für die Sicherheit seiner Fahrgäste tut. Videokameras bedeuten daher zunächst einen Imagegewinn für das Unternehmen. Die KVB bemüht sich daher auch um so genannte Ordnungspartnerschaften mit den Polizei- und Ordnungsbehörden in Köln, sowie dem Bundesgrenzschutz an den Stellen, wo Deutsche Bundesbahn und Kölner Verkehrsbetriebe zusammenlaufen. Diese Kooperation ist Teil des Sicherheitskonzeptes der KVB, die über die Videoüberwachung hinausgehen und teilweise zu einer gemeinsamen Nutzung der Sicherheitstechnik oder einem Austausch von Informationen führt.

Dass die Bürger sich an manchen Orten in Köln nicht sicher fühlen, bestätigt die Allgemeine Bürgerbefragung der Kölner Polizei, die den Neumarkt, einen zentralen Umsteigepunkt der KVB, als Platz mit der höchsten Zahl an Straftaten ausweist. Wie bereits erwähnt, wird dieser Platz aber zum Zeitpunkt der Erhebung durch die KVB komplett videoüberwacht. Ein Zeichen dafür, dass Videoüberwachung nicht immer die Erwartungen erfüllt, die an sie gestellt werden.

Nach eigenen Angaben stellt die Videoüberwachung aus Sicht der KVB *ein* Mittel[318] dar, um Sicherheit herzustellen. Herr Berger führt aber innerhalb des Interviews selbst an, dass man *Sicherheit in keinem Fall herstellen* kann. Lediglich bei der Aufklärung einer bereits begangenen Straftat könne Videoüberwachung hilfreich sein, sofern es innerhalb von 24 Stunden zu einer Anzeige gekommen ist.

Die KVB setzt bei der Installation der Videoüberwachung auf drei Dinge: zum einen auf den abschreckenden Effekt, den die Videoüberwachung haben könnte, zum anderen auf eine Steigerung des Sicherheits*gefühls* der Fahrgäste und zum

[318] Wie bereits innerhalb der Fallstudie dargestellt, gehören Notrufstellen, die Ordnungspartnerschaften oder das Einsetzen von Sicherheits- und Servicepersonal ebenfalls zum Sicherheitskonzept der KVB.

dritten auf einen Imagegewinn, den sie durch die Installation der Technik in der öffentlichen Diskussion erhält. Das *Gefühl* der Fahrgäste ist dabei das entscheidende Moment, denn es geht der KVB gar nicht um konkrete Aufklärungszahlen – die kann Herr Berger im Interview auch nicht genau nennen – sondern, wie er es formuliert, um ein zusätzliches Stück an *subjektiver Einstimmung für mehr Sicherheit*.[319] Videokameras bieten also die Illusion von Sicherheit, wie schon am Beispiel des Neumarktes deutlich gemacht wurde. Videokameras scheinen auch die Illusion zu vermitteln, dass *da schon jemand ist*, der alles sieht und eingreift. Herr Berger bemängelt im Interview, dass heutzutage alle weggeguckten, wenn etwas passiere. Videokameras werden hier zu idealen Hinguckern, die 24 Stunden das Geschehene aufzeichnen und bei Bedarf wiedergeben. Leider verhindern sie aber keine Straftaten, sie können sie lediglich dokumentieren. An dieser Stelle wäre eine (sozial-) pädagogische Intervention, die einen Umgang mit Konflikt- und Notsituationen thematisiert, besser geeignet, um eine wirkliche Hilfe für das Opfer zu gewährleisten.

Im Alltag der Menschen scheinen die Kameras keine große Bedeutung zu haben. Eine bemerkbare Kenntnisnahme der Kameras durch die Fahrgäste ist innerhalb der Teilnehmenden Beobachtung nicht zu verzeichnen. Im Interview hat nur die Hälfte der Stichprobe die Kameras je bemerkt, von denen, welche die unscheinbare Installation an der Decke schon einmal wahrgenommen hat, weiß die Mehrheit, dass es sich dabei um Überwachungskameras handelt. Die Mehrheit der Befragten stellt sich die Funktionsweise der Kameras aktiv vor, sie gehen davon aus, dass der Fahrer, die Leitstelle der KVB oder andere Personen die Innenräume der Bahnen über einen Monitor überwachen. Es wird also von der Videoüberwachung eine Intervention von KVB-Personal im Notfall erwartet.

Zum Ziel der KVB, das Sicherheitsgefühl der Fahrgäste zu steigern, kann man konstatieren, dass dies innerhalb der Stichprobe nicht gelungen ist; hier empfanden zwei Drittel der Befragten keine Steigerung ihres eigenen Sicherheitsgefühls durch die installierten Videokameras, fühlten sich aber zum Teil auch vorher nicht unsicher. Einige unterstellten aber, dass andere – beispielsweise ältere Menschen – sich durch die Videokameras sicherer fühlten.

Videoüberwachung hat unter den Befragten eine recht hohe Akzeptanz. Obwohl es auch Bedenken gibt, die den Datenschutz betreffen oder in Richtung Überwachungsstaat gehen, stehen die meisten Fahrgäste Videoüberwachung positiv gegenüber. Sie erwähnen Vorteile bei der Eindämmung von Vandalismus, im Notfall und für ältere Leute. Diese Ergebnisse decken sich mit denen, die beim Interview mit Herrn Berger ebenfalls zutage traten: Videoüberwachung hat ein

[319] Berger 2003, Antwort 20

mehrheitlich gutes Image, auch wenn man gar nicht so genau weiß, wie sie konkret funktioniert.

Innerhalb der Fallzusammenfassung und der Fallstrukturierung wurde deutlich, dass sich der innerhalb des Theorieteils erarbeitete Aspekt der *Sicherheit* für die Videoüberwachung der KVB wiederfinden lässt. Die Herstellung von Sicherheit ist eine Hauptlegitimation zur Installation der Videoüberwachung, Sicherheit wird aber, wie wir erfahren konnten, durch die Videoüberwachung gar nicht hergestellt, lediglich spätere Aufklärungsarbeit kann unter Umständen unterstützt werden.

Sicherheit kann durch technische Systeme nicht hergestellt werden und Technik kann mithin soziale Probleme nicht lösen. Hier ist ein Eingreifen (Zivilcourage) nötig. Pädagogische Maßnahmen könnten hier ermutigen und zum Eingreifen erziehen. Die Einmischung und die Solidarität von Bürgern kann eine Kamera nicht liefern.

4.4 Fallstudie B: Magnetstreifenkarten im Konsumalltag – Datensammlungen mit dem Payback-System

Payback ist das in Deutschland meist verbreitete Bonusprogramm und wurde daher als Beispiel einer großen Datensammlung über privates Konsumverhalten exemplarisch ausgewählt. Innerhalb der empirischen Phase wurde Material über Payback gesammelt, inhaltsanalytisch ausgewertet und als Hintergrundinformation aufbereitet. Im Rahmen der Teilnehmenden Beobachtung wurde ebenfalls ein Forschungstagebuch geführt und zur Beurteilung des Einsatzes im Alltag herangezogen. Es wurden ferner Interviews geführt und da, wo es sinnvoll erschien, Fotos erstellt.

Der Zugang zum Feld gestaltete sich, was die Teilnehmende Beobachtung angeht, wiederum unproblematisch, da das Payback-System so verbreitet ist, dass man bei nahezu jedem Einkauf in den angeschlossenen Ladenketten Beobachtungen anstellen kann. Als Ansprechpartner für ein Experteninterview wurde Herr Jürgen Weber ermittelt, der innerhalb des Datenschutzteams der Lufthansa für das Payback-System zuständig ist. Wie bereits erwähnt ist die Lufthansa Mehrheitsbeteiligte des Betreiberunternehmens von Payback und hat einen ihrer Datenschutzbeauftragten für die Betreuung von Payback eingesetzt. Herr Weber stand der Anfrage von Anfang an sehr offen gegenüber und zeigte großes Entgegenkommen bei der Vereinbarung eines Gesprächstermins. Auch nach dem Interview stand Herr Weber für Rückfragen zur Verfügung. Zur Ermittlung der Kundenmeinung wurden Interviews mit Payback-Nutzern geführt.

4.4.1 Hintergrund-Informationen

Rabattsysteme gibt es nicht erst seit heute. Um Kunden zu binden, gab es schon in der Vergangenheit Rabattmarken und dazugehörige Hefte, in denen man diese Marken einkleben konnte und bei Erreichen einer bestimmten Anzahl ein Präsent oder Bargeld bekam. Dabei blieb man weitgehend anonym, es sei denn, der Verkäufer oder die Verkäuferin des Geschäftes kannte den Kunden persönlich. Das Payback-System, das es seit März 2000 gibt, bezeichnet sich selbst als „Bonusprogramm“ und ist mit über 27 Millionen[320] eingesetzten Karten das führende Bonusprogramm in Deutschland. Es wird von der Münchner Loyalty Partner GmbH unterhalten. Dieses rund 180 Mitarbeiter zählende Unternehmen ist in der Mehrheit in Besitz der Lufthansa Commercial Holding GmbH, einer Tochtergesellschaft der Deutschen Lufthansa, 25% hält die Metro AG, den Rest teilen sich ein Geschäftsführer und eine weitere Person. Am Payback-System sind derzeit 12 größere Wirtschaftsunternehmen beteiligt, z.B. die Obi-Baumärkte, die dm-Drogeriemärkte, AOL oder Galeria Kaufhof. Die beteiligten Unternehmen sind Partner der Loyalty Partner GmbH, die für sie quasi die Verwaltung der Payback-Punkte, deren Abrechnung und die Verteilung der Prämien etc. übernimmt.

Wie funktioniert Payback für den Verbraucher?

Um am Bonusprogramm teilnehmen zu können, muss der Verbraucher sich entweder direkt bei Loyalty Partner oder bei einem Partnerunternehmen anmelden. Dabei werden persönliche Daten von ihm erhoben, von denen einige freiwillig, andere zwingend sind. Daten wie vollständiger Name, Geburtsdatum und Adresse sind zwingend, andere wie Familienstand, monatliches Einkommen, Anzahl und Geburtsjahr der Kinder freiwillig. Mit seiner Unterschrift erklärt man sich unter anderem damit einverstanden, dass die Daten zur Erstellung von Informationen per Post sowie zu Zwecken der Marktforschung von den Partnerunternehmen und der Loyalty Partner GmbH genutzt werden. Es ist aber auch möglich, dem zu widersprechen oder dies noch im Nachhinein zu tun. Nach Ausfüllen der Anmeldung erhält man per Post eine so genannte Payback-Karte, die das Format einer EC-Karte hat. Bei Einkauf bei einem Payback-Partner kann man die Karte vorzeigen und erhält je nach Partner eine unterschiedliche Anzahl von Punkten gut geschrieben (beim Drogeriemarkt dm ist es beispielsweise ein Punkt pro vollem Euro, bei der Tankstellenkette DEA ist es ein Punkt für zwei Liter Benzin). Bei dieser Gutschrift werden die gekauften Waren oder Dienstleistungen, der Preis, der Rabattbetrag, sowie der Ort und das Datum des Vorganges an die Loyalty Partner GmbH übermittelt. Ein Payback-Punkt hat dabei den Gegenwert von einen Euro-Cent, ab einer Punktemenge von 1500 Punkten kann man sich das

[320] Stand: Januar 2005, vgl. Loyalty Partner 2005

Geld (also 15 Euro) entweder auszahlen lassen, an Unicef spenden oder eine Prämie erhalten. Es besteht weiterhin die Möglichkeit, zu der Hauptkarte eine Zweitkarte zu beantragen, die man dann einer weiteren Person geben kann, welche dann für die Hauptkarte mitsammelt.

Was passiert mit den Daten?

Die Kundendaten werden von Loyalty Partner gesammelt und, falls kein Einspruch erfolgt ist, zu Zwecken der Marktforschung sowie zur individuellen Erstellung und Versendung ausgewählter Informationen per Post oder, sofern man dazu Angaben gemacht hat, per SMS oder E-Mail genutzt. Das Partnerunternehmen, von dem man die Payback-Karte erhalten hat, kann die Basisdaten (also Adresse, Geburtsdatum etc.), die freiwilligen Angaben und die anfallenden Rabattdaten (also die gekauften Waren oder Dienstleistungen, der Preis, der Rabattbetrag, sowie der Ort und das Datum des Vorganges) zu eigenen Zwecken der Marktforschung und für die Versendung von Werbung nutzen. Loyalty Partner weist darauf hin, dass zur Versendung von Postwerbung, des Newsletters und der SMS-Werbung die notwendigen Basisdaten fallweise durch beauftragte Dienstleistungsunternehmen verarbeitet werden. Diese werden als Auftragsdatenverarbeiter bezeichnet, und es wird zugesichert, dass die jeweiligen Kundendaten nach Durchführung der Aktion gelöscht werden sowie eine Identifikation des Kunden durch Partnerunternehmen oder Dritte ausgeschlossen sei.

4.4.2 Die Payback-Karte vor Ort

Abbildung 16: Payback-Karte der Drogeriemarktkette dm

Die Untersuchung zum Thema Payback-Karte fand über mehrere Monate in einem dm-Drogeriemarkt in Köln-Nippes statt. Beobachtet wurde bei ca. zwei Besuchen pro Woche, wie der Umgang mit der Payback-Karte im Alltag verläuft.

Es fiel auf, dass bereits viele KundInnen des Marktes über eine solche Payback-Karte verfügen und diese von alleine bei ihrem Einkauf vorzeigten. Geschah dies nicht, so wurden sie von der KassiererIn gefragt, ob sie über eine Payback-Karte verfügten. Die Personen, die eine solche besaßen, fingen dann meist an, diese aus einer Fülle von anderen Plastikkarten

heraus zu sortieren. Es entstand der Eindruck, dass es ihnen unangenehm war, nicht selbst daran gedacht zu haben und somit eine Verzögerung hervorzurufen.

Die KundInnen, die nicht über eine Payback-Karte verfügten, antworteten auf die Frage danach sehr knapp mit „Nein“ oder machten in seltenen Fällen den Eindruck, dass sie das wiederholte Nachfragen als störend empfinden. Die Kassiererin fragte bei diesen Personen in keinem Fall nach, ob Interesse an der Payback-Karte bestünde, sondern kassierte nach einmaliger Nachfrage weiter.

Abbildung 17: Werbebroschüre für die dm-Paybackkarte

Im dm-Drogerie-Markt wird massiv Werbung für die Payback- und seit kurzem auch für die „dmPayback Visa Karte“ gemacht. Unter dem Motto: “Mehr Spaß beim Einkaufen für Sie“ liegen Broschüren an den Kassen aus und an mehreren Stellen im Markt hängen Plakate aus. Payback scheint bei den meisten KundInnen zum Einkauf dazu zu gehören: Ganz selbstverständlich wird die Karte vorgezeigt oder auf Anfrage, hervorgeholt. Bei der Beobachtung stellte sich die Frage, welche Intentionen die Betreiber von Payback mit ihrem System verfolgen und wie die KundInnen selbst die Bonuskarte beurteilen. Diese Fragen werden in den folgenden Interviews geklärt werden.

4.4.3 Payback aus Sicht des zuständigen Konzerndatenschutzbeauftragten der Lufthansa AG

Herr Weber ist stellvertretender Konzerndatenschutzbeauftragter der Lufthansa AG. Insgesamt werden von den Konzerndatenschutzbeauftragten 35 Firmen betreut, dabei werden im Datenschutzteam Schwerpunkte festgelegt. Herr Weber ist für die Betreuung der Firma Loyalty Partner zuständig, die Betreiberin des Payback-Systems ist.

Fragestellungen des Interviews

Innerhalb des Interviews sollte geklärt werden, wie sich das Payback-System von Seiten der Betreiber her darstellt. Dabei interessierten insbesondere folgende Punkte:

- Aus welchem Grund hat sich die Lufthansa AG an einem System wie Payback beteiligt?
- Worin werden die Unterschiede zwischen Payback und dem alten Rabattsystem (z.B. mit Marken) gesehen?
- Woher kommt das Bedürfnis der Firmen, so viel über ihre Kunden zu erfahren?
- Wie gestaltet sich der Datenschutz und wie kann Datenmissbrauch verhindert werden?

Auswertung des Interviews

Beteiligung der Lufthansa

Herr Weber bezeichnet das Interesse der Lufthansa AG, sich an einem System wie Payback zu beteiligen, als rein zufällig. Die Kapitalbeteiligung der Lufthansa AG liege bei 51 Prozent und wurde unter anderem durch persönliche Beziehungen des Geschäftsführers von Loyalty Partner mit dem Vorstand der Lufthansa AG ermöglicht. Der weitere Partner ist Roland Berger, der eine große Unternehmensberatung betreibt. Eine strategische Bedeutung gibt es, so Weber, eigentlich nicht. Da die Lufthansa aber mit Payback in Verbindung gebracht wird, hat sich das Untenehmen aufgrund des sensiblen Themas entschieden, den Datenschutz, wie bei allen Konzerngesellschaften, vom Konzerndatenschutzbeauftragten wahrnehmen zu lassen. Es scheint also hauptsächlich über persönliche Kontakte zu einer Beteiligung der Lufthansa an Loyalty Partner gekommen zu sein.

Sinn und Zweck von Payback

Nach Aussage von Herrn Weber stellt Payback in erster Linie ein Mittel zur Kundenbindung dar. Er vergleicht dies mit den Rabattmarken im Tante-Emma-Laden, die in entsprechende Hefte eingeklebt werden mussten. Die gewährten Rabatte seien wichtig, um den Kunden an das Unternehmen zu binden. Die Kunden würden dort einkaufen, wo es Rabatte gäbe. Auch wenn Herr Weber den Vergleich zu den traditionellen Rabattmarken trifft, unterscheidet sich Payback hier ganz entscheidend von diesen. Es handelt sich hierbei nicht um eine Marke, die man anonym in ein Heft klebt, sondern um eine Magnetstreifenkarte, auf der Daten gespeichert werden und hinter der leistungsstarke Datenbanken stecken, welche die gewonnenen Informationen aus unterschiedlichen Einkäufen zusammenführen

und auswerten. Dies spricht auch Herr Weber an, wenn er deutlich macht, dass es auch darum geht, zu ermitteln *wer* die Kunden sind und *was* diese Kunden wollen.[321] Die Marketingleute wollten dieses Prinzip für einen Großkonzern nutzbar machen, um zu erfahren, welche Interessen und Schwerpunkte die Kunden haben und welche Produkte diese kaufen, damit das Sortiment daran ausgerichtet werden kann, führt Weber aus.[322]

> „[...] es geht tatsächlich auch um Differenzierung des Angebots, das man sagt: Also Sie kriegen einen höheren Rabatt, nicht nur Punkte, sondern was weiß ich, eine... für Sie haben wir diesen Artikel um dreißig Prozent heruntergesetzt und für den normalen Kunden nur um zwanzig Prozent. Tatsächlich um den Kunden an das Unternehmen zu binden.“[323]

Dieses von Herrn Weber beschriebene Vorgehen der Wirtschaft wird mit dem Fachbegriff Customer Relationship Management (CRM) belegt und wurde bereits in Kapitel 3.2 beschrieben. Für die Unternehmen bietet ein System wie Payback eine ideale Möglichkeit, herauszufinden, in welche Kunden es sich lohnt zu investieren und welche Kunden unrentabel sind. Die Kluft zwischen vermögenden und weniger Umsatz bringenden Verbrauchern kann und soll mit solchen Systemen verstärkt werden.

Die Unternehmen wollen ihre Kunden *kennen*. Sie wollen wissen, was sie konsumieren, wo sie dies tun und wie oft. In Verbindung mit den erhobenen Stammdaten ergeben sich Möglichkeiten, noch *viel mehr* über den Kunden herauszubekommen, als dies auf den ersten Blick scheint. Mittlerweile existieren Datenbanken, die genaueste Aufstellungen darüber liefern, wie die Einkommensstruktur in Viertel X aussieht oder wie sich die soziale Lage in Viertel Y darstellt. Ein solches Verfahren nennt sich *Scoring*, und Payback liefert einen weiteren Baustein auf dem Weg zum Gläsernen Kunden, der dann seinem Profil entsprechend behandelt wird. Dass durchaus auch Regierungen Interesse an diesen Daten haben können, wurde in der Vorstellung des Information Awareness Office deutlich und wurde auch von Herrn Weber innerhalb des Interviews thematisiert.

Anonymität des Kunden

Die Frage danach, warum man die Payback-Karte nicht auch anonym nutzen kann, wenn es doch nur um die Kundenbindung ginge, beantwortet Herr Weber zuerst ausweichend, kommt aber im Laufe des Gesprächs mehrmals auf das Thema zurück und erklärt beispielsweise:

---

[321] vgl. Weber 2003, Antwort 9

[322] vgl. Weber 2003, Antwort 9

[323] Weber 2003, Antwort 13

> „Der Kunde kann übrigens auch die Payback-Karte jahrelang völlig anonym benutzen. Er kann sie einfach einsetzen, sammelt seine Punkte, einfach unter der Nummer, Payback wird das alles registrieren, wie quasi in einem Nummern-Konto, völlig anonym. Erst wenn Sie tatsächlich eine Prämie ausgezahlt haben wollen, dann müssen Sie zumindest ihre Bankverbindung angeben... ja, und Ihren Namen. Sie können Payback unter Umständen auch im Unklaren lassen, oder können eine falsche Adresse angeben, wenn Sie das nun wirklich wollen.“ [324]

In der Realität wird dieser Fall allerdings vermutlich selten vorkommen, da man sich die Payback-Karte in der Regel zuschicken lässt und dazu schon ein Anmeldeformular mit entsprechenden Angaben ausgefüllt haben muss. Es stimmt zwar, dass vereinzelt auch Payback-Karten in den Geschäften ausliegen; der Großteil muss aber bestellt werden. Zur Anonymität bemerkt Herr Weber weiterhin, dass es eine Anonymität gegenüber den Partnerfirmen von Loyalty Partner gibt, wenn man eine Payback-Karte direkt bei Loyalty Partner bestellen würde.

> „Wenn Sie so eine Karte haben, die Sie zum Beispiel übers Internet sich bestellen können, dann kennt nur Loyalty Partner Sie. Die einzelnen Partnergesellschaften wissen nicht, wer steht jetzt hier unter dieser Mitgliedsnummer, die hier steht.“[325]

Egal, was registriert würde, die beteiligten Partnerfirmen könnten den Personenbezug nicht herstellen. Dies gelte auch, wenn man z.B. eine Payback-Karte von Real hätte; die Stammdaten der Karte seien nur Real selber und Loyalty Partner bekannt, ein andere Partner, könne diese nicht einsehen. Diese Äußerungen stellen eigentlich nur noch einmal klar, dass alle Daten bei Loyalty Partner zusammenlaufen und Loyalty Partner aufgrund dieser Tatsache Dienstleistungen anbieten kann: Geht es z.B. darum, eine Werbeaktion zu starten, muss sich das entsprechende Unternehmen an Loyalty Partner wenden, die alle Daten zentral verwalten und die Werbeaktion (z.B. ein Mailing) dann in Auftrag geben. Eine Anonymität kann also maximal gegenüber einem Partnerunternehmen bestehen, sie existiert in der Regel nicht gegenüber Loyalty Partner, denn dort laufen alle Daten zusammen, werden ausgewertet und auf unbestimmte Zeit gespeichert. Es liegt nicht im Interesse von Payback, es mit anonymen Kunden zu tun zu haben, daher wird diese Möglichkeit der Payback-Nutzung auch nicht propagiert.

Umgang mit den Daten

Herr Weber betont, dass Loyalty Partner keine Daten an die Partnerfirmen übermittelt, sondern diese, wie bereits erwähnt, zentral beim Unternehmen gespeichert werden. Teilweise werden die Daten dabei an Dritte zur Weiterverarbeitung gegeben, was aber keine Übermittlung von Daten im Sinne des Bundesdatenschutzge-

---

[324] Weber 2003, Antwort 23

[325] Weber 2003, Antwort 23

setzes darstelle, sondern quasi wie eine Abteilung von Loyalty Partner zu betrachten sei.[326] Herr Weber unterstreicht, dass kein Datenaustausch zwischen den Partnern stattfindet, sondern jeder Kunde einem bestimmten Partner oder direkt der Firma Loyalty Partner zugeordnet ist. Was explizit gekauft wird, wird nicht an Loyalty Partner übermittelt – dort gehen, laut Weber, maximal Informationen zu den Artikelgruppen ein.[327] Was allerdings die einzelnen Partner selbst noch zusätzlich über ihre Kunden erheben, kann Herr Weber nicht genau sagen:

> „Die Partner an sich sind natürlich in der Lage und das machen die ja vielleicht auch, sogar artikelbezogen die Daten für sich zu registrieren. Also man muss schon unterscheiden zwischen den Datenbanken, die die Partner selber haben durch so eine Karte und dem, was in diesem Gesamtverbund aller Partner gespeichert wird. Das ist eben genau das, was ich eben gesagt habe. Das geht maximal auf die Artikelgruppenebene.“[328]

Loyalty Partner kann somit also nur erfahren, dass etwas im Bereich Kosmetik oder Computer gekauft wurde, nicht aber welches Produkt.

Was den Datenschutz angeht, stellt Herr Weber fest, dass es für betriebliche Datenschutzbeauftragte keine Sanktionsmöglichkeiten gäbe. Was man nur machen könnte, seien Empfehlungen zu geben und zu versuchen, auf die Kollegen einzuwirken:

> „[...] und denen predigen wir immer zwei ganz wichtige Sachen: Transparenz, am besten dreimal Transparenz, Transparenz, Transparenz, also sagt dem Kunden, was Ihr mit seinen Daten macht und ich meine also Loyalty Partner hat das gemacht und dann sagt er in diese komplexen Dinge, also die Bildung von Profilen, die Bildung von, ja also die Marketingaktionen und so was, dafür braucht Ihr eigentlich die Einwilligung des Kunden. Macht nichts ohne die Einwilligung des Kunden und ich bin eigentlich zumindest in unserem Bereich den wir zu vertreten haben, und das ist auch Loyalty Partner und ist aber genauso gut das Marketing der Deutschen Lufthansa, haben wir die Leute davon überzeugt, dass man das so machen muss.“[329]

Auch wenn Herr Weber keine direkten Einwirkmöglichkeiten hat, versucht er, seine Kollegen davon zu überzeugen Vorgänge transparenter zu machen; umgesetzt werden muss so etwas nicht, und die Marketingabteilung wird sich überlegen, wie viel sie preisgibt, solange alles noch innerhalb des gesetzlichen Rahmens liegt.

---

[326] vgl. Weber 2003, Antwort 31, dies bezieht sich z.B. auf Werbebriefe, die von anderen Firmen im Auftrag von Loyalty Partner verschickt werden.

[327] vgl. Weber 2003, Antworten 25 - 29

[328] Weber 2003, Antwort 20

[329] Weber 2003, Antwort 42

Selbstverständlich besteht, das räumt auch Herr Weber ein, die Möglichkeit des Datenmissbrauchs. Angesprochen auf die Miles-and-More-Affäre - bei der bekannt wurde, dass Politiker ihre beruflich angesparten Bonusmeilen auch privat genutzt hatten - bemerkt Herr Weber, dass jeder Mitarbeiter, der Zugriffsrechte hat, diese auch missbrauchen könne. Bei Loyalty Partner sei so etwas aber noch nicht vorgekommen, so Weber.[330] Der entsprechenden Mitarbeiterin bei der Miles-and-More-Affäre sei natürlich sofort gekündigt worden. Weber kritisiert, dass es der Staatsanwaltschaft trotz Bereitstellung genauer und lückenloser Nachweise über die Identität der entsprechenden Mitarbeiterin nicht gelungen sei, innerhalb eines Dreivierteljahres eine Anklage zu formulieren. Weber führt an, dass das Datenschutzrecht auch für die Strafverfolgungsbehörden eine schwierige Materie sei und er es gerne gesehen hätte, wenn wirklich einmal jemand wegen Verstoß gegen das Datenschutzgesetz ins Gefängnis gekommen wäre. Ihm ist nicht bekannt, dass der Fall bislang zu einem Abschluss gekommen sei, obwohl die Lufthansa AG alle Möglichkeiten zur Verfügung gestellt habe.[331]

Der Gläserne Bürger

Angesprochen auf den Vorwurf, dass durch die Payback-Karte der Gläserne Konsument, bzw. der Gläserne Bürger geschaffen wird, erwidert Herr Weber, dass sein Unternehmen sicherlich nicht den Gläsernen Bürger schaffe. Stattdessen hätte er aber immer mehr den Eindruck, dass der Staat heute den Gläsernen Bürger schaffe. Weber führt das Beispiel an, dass die Lufthansa seit kurzem verpflichtet ist, zum Beispiel an die amerikanischen Behörden Reservierungsdaten weiterzugeben. Die deutschen Behörden würden jetzt plötzlich aufwachen und diese Daten ebenfalls haben wollen, obwohl die deutschen Gesetze so etwas natürlich überhaupt nicht vorsähen.[332]

> „Das ist egal, ob wir nun viel oder wenig Daten speichern, wenn wir dem Staat erlauben diese Daten, auch die kleinen Datenmengen zu sammeln, dann entsteht dort die Möglichkeit, die Möglichkeit wirklich den Gläsernen Bürger zu haben und ich bin sicher, dass es einige, dass es Politiker auch in Deutschland gibt, die so was gerne hätten.“[333]

Und weiter:

---

[330] vgl. Weber 2003, Antwort 32, 33

[331] vgl. Weber 2003, Antwort 34, 35

[332] Weber 2003, Antwort 37

[333] Weber 2003, Antwort 40

> „Also wir schaffen sicherlich nicht den Gläsernen Bürger. Wir haben immer mehr den Eindruck, dass der Staat heute den Gläsernen Bürger schafft. [...] Also der Staat ist schon sehr daran interessiert tatsächlich den Gläsernen Bürger zu schaffen und die Argumente der Terrorismusbekämpfung sind jetzt ideale Argumente für Strafverfolgungsbehörden, für die Dienste und so weiter.“[334]

Herr Weber gibt den Schwarzen Peter weiter an staatliche Stellen und Behörden, denen er unterstellt, den Gläsernen Bürger schaffen zu wollen. Den eigenen Anteil an einer fortschreitenden Transparenz der Bevölkerung spielt er dabei herunter, räumt allerdings ein, dass durch Systeme wie Payback der Kunde „natürlich ein bisschen gläserner gemacht“[335] wird. Dieser sei in einem Kaufhaus nicht mehr so anonym, wie er es vielleicht noch vor fünf Jahren gewesen sei. Im Tante-Emma-Laden sei der Kunde aber wesentlich transparenter gewesen, jetzt sei alles nur moderner.[336] Diese Behauptung gründet Herr Weber darauf, dass man den Kunden im Tante-Emma-Laden persönlich kannte und daher viel mehr über ihn wusste als dies heutzutage der Fall sei. Angesichts der enormen Möglichkeiten, welche die moderne Datenbanktechnik, kombiniert mit den Methoden des Customer Relationship Managements bietet, ist dies eine Haltung, die an der Realität des Datamining völlig vorbei läuft und seine Möglichkeiten unangemessen herunterspielt.

Im Bezug auf zukünftige Entwicklungen verweist Weber auf *ubiquitous computing*, Computersysteme, die z.B. an der Jacke getragen werden oder unter die Haut implantiert werden und die mit ihrer Umwelt kommunizieren und dadurch überall Datenspuren des Trägers hinterlassen. Herr Weber führt das Beispiel der Firma REAL an, die in Süddeutschland eine Filiale aufgebaut hat, in der elektronische Einkaufswagen zum Einsatz kommen. Die Ware sei dabei mit billig herstellbaren Plastikchips ausgestattet, der zu zahlende Preis würde automatisch ermittelt und mache eine Kassiererin unnötig. Da diese Chips – hier ist von den bereits in Kapitel 3.2 beschriebenen RFID-Chips die Rede - alle kleine Sender seien, sei es möglich nachzuvollziehen, wohin die Ware gelange. Es sei mit einem entsprechenden Kühlschrank denkbar, dass die mit intelligenten Chips ausgestatteten Produkte sich meldeten, wenn es Zeit sei, Nachschub über das Internet zu bestellen.

Herr Weber sieht eine Technik in der Entwicklung, die mehr und mehr das Verhalten von Menschen nachvollziehbar mache.[337] Er führt an, dass sein Unternehmen engen Kontakt zur Technischen Universität Dresden hat, an der versucht

---

[334] Weber 2003, Antwort 37

[335] Weber 2003, Antwort 38

[336] vgl. Weber 2003, Antwort 37

[337] Weber 2003, Antwort 38

wird, Geräte so zu entwickeln, dass sie datenschutzgerecht sind. Die Industrie sei eher nur an ihren Produkten, aber weniger am Datenschutz interessiert.

Jürgen Weber hebt noch einmal das aktuelle Beispiel mit deutschen Flugreservierungsdaten hervor, die im Rahmen der US-amerikanischen Terrorismusbekämpfung nun an den US-Zoll weitergeleitet werden müssen, und äußert, dass gerade dies ein ganz typisches Beispiel dafür sei, dass egal, was das Unternehmen mache, die Gefahr, dass der Staat die Daten sammelt, überhaupt nicht vermeidbar sei. Nur die Politiker könnten entscheiden welchen Wert dem Datenschutz beigemessen werden sollte. Die Frage sei, ob wir uns wirklich davon überzeugen ließen, dass Terrorismusbekämpfung wichtiger als Persönlichkeitsrechte unbescholtener Bürger sei.[338]

Die Reservierungsdaten an sich seien erst einmal nur die Information über eine einzelne Reise des Kunden. Weber ist sich allerdings sicher, dass diese Einzelreisen der Kunden in den amerikanischen Systemen über mehrere Jahre hinaus gespeichert und aus der Summe der Informationen Schlüsse gezogen würden. Es sei egal, ob die Unternehmen nun viele oder wenige Daten speicherten, denn wenn es dem Staat erlaubt würde diese Daten, auch in kleinen Datenmengen zu sammeln, dann entstünde die Möglichkeit wirklich den Gläsernen Bürger zu schaffen. Herr Weber ist sich sicher, dass es Politiker in Deutschland gibt, die so etwas gern sähen.[339]

Herr Weber beschreibt, dass die Lufthansa AG sich im Falle der Weitergabe von Buchungsdaten an den US-amerikanischen Zoll an den Bundesbeauftragten für den Datenschutz und auch an die Landesbeauftragte von Nordrhein-Westfalen, Frau Sokol, gewandt habe. Dies sei bereits vor anderthalb Jahren (also Anfang 2002, Anm. d. Verf.) geschehen und es habe Verhandlungen gegeben, die dann bis hinauf auf die EU-Ebene gebracht worden seien. Da die Bitte der Amerikaner um Weiterleitung der Daten nicht mit EU-Datenschutzrecht vereinbar ist, wurde eine Klärung der Situation von Seiten der EU-Gremien erbeten. Während des Irak-Krieges sei die EU auf die Idee gekommen, dass dies eigentlich nicht schlimm sei und die Airlines das „mal ruhig machen sollten".[340] Herr Weber stellt fest, dass sein Unternehmen keine andere Möglichkeit mehr gehabt habe, als die Buchungsdaten weiter zu geben. Er verweist weiter auf ein Gespräch mit Mitarbeitern der Landesbeauftragten für den Datenschutz, das am Morgen des Interviewtages[341] stattgefunden hat und in dem von Seiten der Lufthansa die Bitte vorgetragen wurde, Verhandlungen darüber zu führen, was aus den Buchungsda-

[338] Weber 2003, Antwort 39

[339] Weber 2003, Antwort 41

[340] Weber 2003, Antwort 41

[341] Dies war der 28.05.2003

ten herausgefiltert werden könne, damit nicht alles an die US-Behörden ginge. In den Buchungsdaten befänden sich laut Weber auch sehr sensible Informationen. Die deutschen Beamten würden dazu sagen, dass sie eigentlich gerne sehr viel rausfiltern würden, sie dies aber gegenüber den US-Behörden wahrscheinlich nicht durchsetzen könnten.[342]

Weber meint mit diesen Beamten zum einen die Landesbeauftragte für den Datenschutz in Nordrhein-Westfalen, Mitarbeiter des Regierungspräsidiums in Darmstadt und den Bundesbeauftragten für den Datenschutz. Er kritisiert, dass keine der drei Institutionen die Initiative ergriffen habe und deutsche Rechte gegenüber der EU durchsetze, sondern alle nur zögerten und bezweifeln würden, überhaupt etwas ausrichten zu können.[343]

Herr Weber weist darauf hin, dass die betrieblichen Datenschutzbeauftragten selber keine Sanktionsmöglichkeiten besäßen, sondern lediglich Empfehlungen aussprechen und Überzeugungsarbeit leisten könnten. Sanktionen könnten nur von behördlichen Datenschutzbeauftragten verhängt werden. Im betrieblichen Bereich bestehe lediglich die Möglichkeit, die Kollegen auf die Wichtigkeit von Transparenz für den Kunden hinzuweisen und darauf, dass die Einwilligung des Kunden einzuholen sei, wenn es um Marketingaktionen und die Bildung von Kunden-Profilen geht. Weber betont, dass es für den Bereich, den er betreut, geglückt sei, die Kollegen von der Wichtigkeit dieser beiden Forderungen zu überzeugen.[344] Weber betont weiter, dass Loyalty Partner keine Daten an Dritte weitergäbe und dass die Praxis, die Daten der Kunden nicht als beliebiges Gut zu betrachten, auch langsam Konsens bei anderen Großfirmen würde. Man werde sich einig darüber, dass man die Kunden auch ernst nehmen und auch ihre Rechte, wie das auf Informationelle Selbstbestimmung wahren müsse.[345]

Befragt nach einem Schlusswort, erklärt Herr Weber, dass er gerade im staatlichen Bereich, zu dem sehr viele Kontakte bestünden, wirklich ganz große Befürchtungen habe, dass da in Zukunft einiges laufen werde, was uns allen nicht gefallen werde.[346]

Weber betont weiter, dass man die moderne Technik in den Griff bekommen müsse. Die Lufthansa beteilige sich in diesem Rahmen an einem Projekt der TU Dresden, bei dem sie sich als Anwenderin zur Verfügung stelle und bei dem es um die Nutzung von Systemen durch Pseudonymisierung geht. Weber betont,

---

[342] Weber 2003, Antwort 41

[343] vgl. Weber 2003, Antwort 42

[344] vgl. Weber 2003, Antwort 43

[345] vgl. Weber 2003, Antwort 46

[346] Weber 2003, Antwort 47

dass insbesondere die technische Umsetzung des Datenschutzes in Zukunft von Bedeutung sein wird. Er äußert, dass technischer Datenschutz die einzige Lösung sein wird, den anderen technischen Systemen zu begegnen. Es gäbe einen großen Bedarf in diesem Bereich, in dem bisher noch relativ wenig gearbeitet wurde. Weber verweist auf Herrn Prof. Pfitzmann von der TU Dresden, der an Systemen arbeitet, um beispielsweise Flugbuchungen unter einem Pseudonym vorzunehmen. Gerade den Kunden, die ihre Daten nicht preisgeben wollten, müssten Angebote gemacht werden und die entsprechende Technik müsse entwickelt werden.[347]

4.4.4 Payback aus Sicht der Nutzer

Die Interviews mit den Nutzern der Payback-Karte sollten zuerst in den jeweiligen Geschäften durchgeführt werden, die das Payback-System anbieten. Schon bei der Teilnehmenden Beobachtung fiel aber auf, dass die meisten Kunden wenig Zeit mitbringen und die hektische Atmosphäre im Kassenbereich der Geschäfte nicht geeignet ist, Interviews zu führen. Außerdem hätte eine Einwilligung der Geschäftsführung eingeholt werden müssen.

Daher wurde ein anderer Weg gewählt, um an eine zufällige und heterogene Stichprobe von Payback-NutzerInnen zu kommen. Auf mehreren Mailinglisten von Vereinen und Projekten, auf denen die Autorin Mitglied ist, wurde per E-Mail die Frage gestellt, ob jemand in seinem Bekanntenkreis Menschen kennt, die NutzerIn des Payback-Systems sind. Durch diese Anfrage wurden die Telefonnummern einer Stichprobe von 10 Personen ermittelt, die sowohl in Hinblick auf ihr Alter als auch auf ihre Berufe recht heterogen waren. Die TeilnehmerInnen wurden zuvor durch die Kontaktpersonen der Mailingliste über die bevorstehende Kontaktaufnahme informiert.

Die Interviews wurden Ende 2003 telefonisch durchgeführt und die Antworten der Interviewten wurden in einem Gesprächsprotokoll festgehalten. Die InterviewpartnerInnen wurden über die Anonymisierung ihrer Daten und die Verwendung ihrer Aussagen innerhalb der vorliegenden Arbeit informiert. Die Ergebnisse der Befragung erheben keinen Anspruch auf Repräsentativität, sondern dienen dazu, den Gebrauch von Payback in der Alltagspraxis zu illustrieren und Tendenzen innerhalb der Stichprobe heraus zu arbeiten.

---

[347] vgl. Weber 2003 Antwort 47

Die InterviewpartnerInnen

Die Stichprobe besteht aus 10 Personen, die, wie oben beschrieben, ausgewählt wurden. Das Alter reicht von 20 bis 60 Jahren, wobei Personen im Alter von ca. 50 Jahren stärker vertreten sind. Durch die zufällige Auswahl der Interviewpersonen kam es zu einer Verteilung von sieben Frauen zu drei Männern, dieser Umstand ist allerdings im Rahmen des Forschungsinteresses unerheblich.

Tabelle 8: Übersicht der befragten PayBack-Kunden

	Geschlecht	**Alter**	**Beruf**
Person A	weiblich	26	Dipl. Sozialpädagogin
Person B	männlich	44	Verkaufsleiter
Person C	männlich	50	Arzt
Person D	weiblich	32	Diplom-Sozialpädagogin
Person E	weiblich	61	Beamtin im Ruhestand
Person F	weiblich	53	Buchhalterin
Person G	weiblich	20	Studentin
Person H	männlich	52	Pfarrer
Person I	weiblich	49	Diplom-Pädagogin
Person J	weiblich	33	Optikerin
Gesamtzahl			**10**

Fragestellung der Interviews

Die halboffenen Fragen der Interviews ermöglichten einerseits einen Vergleich zwischen den Antworten und boten andererseits den Befragten die Möglichkeit, individuelle Äußerungen einzubringen.

Zu Anfang wurden die Interviewten über den Zweck der Befragung informiert und ermittelt, wie lange sie bereits das Payback-System nutzen. Im Anschluss wurden die Fragen gestellt, auf welche Weise sie Zugang zu diesem System gefunden haben und was sie von einer Teilnahme erwarten. Ferner interessierte, ob sie bereits persönlich von ihrer Teilnahme profitiert haben. Ob die Befragten Dinge im Zusammenhang mit Payback kritisieren, sollte innerhalb der nächsten Frage herausgefunden und im Anschluss geklärt werden, ob die InterviewpartnerInnen bei der Anmeldung ihre Zustimmung zu einer Datenverwertung zum Zwecke der Werbung gemacht haben. Die nächste Frage zielte darauf ab, herauszufinden, wie gut die Befragten über die Art der Daten, die Payback erhebt, informiert sind, wobei Mehrfachnennungen möglich waren. Zuletzt wurde erho-

ben, ob die Personen Gefahren oder Nachteile in der Nutzung des Payback-Systems sehen und ihr Alter und ihr Beruf ermittelt.

Auswertung

Die meisten der befragten Payback-NutzerInnen haben schon mehrere Jahre Erfahrung mit dem System und somit Zeit gehabt, sich mit den Vor- und Nachteilen auseinander zu setzen. Die Ergebnisse der Interviews wurden grafisch dargestellt und im Anschluss weiter erläutert. Die Darstellung folgt der Reihenfolge der bereits formulierten Fragstellungen.

Tabelle 9

Dauer der Payback-Nutzung	
< 1 Jahr	2
1-2 Jahre	3
2-3 Jahre	2
3-4 Jahre	3
Gesamtzahl	**10**

Die beteiligten Personen nutzen die Payback-Karte bereits unterschiedlich lange. Zwei Befragte haben sie vor weniger als einem Jahr erhalten, drei Personen sind dagegen schon seit Beginn der Aktion dabei und konnten über mehrere Jahre Erfahrungen sammeln. Die Hälfte der NutzerInnen hat die Karte seit 1-3 Jahren. Die Stichprobe enthält somit sowohl NutzerInnen, welche die Karte schon fast seit Beginn der Aktion nutzen, als auch Neuzugänge, die noch nicht so lange Erfahrung mit dem System haben.

Tabelle 10

Art des Zugangs zu Payback: durch	
Freunde/Bekannte	1
Werbung im Geschäft	6
Direkte Ansprache im Geschäft	2
Zusendung der Karte über einen Stromanbieter	1
Gesamtzahl	**10**

Die meisten der Payback-NutzerInnen sind durch Werbung im Geschäft auf die Karte aufmerksam geworden, einige davon wurden auch direkt im Geschäft durch Personal auf die Payback-Karte angesprochen. Dies deckt sich auch mit meinen eigenen teilnehmenden Beobachtungen, bei denen die Werbung für Payback in den Geschäften sehr ins Auge fiel und man bei nahezu jedem Einkauf auf den potenziellen Besitz einer Payback-Karte angesprochen wurde. Nur einer Person ist das Payback-System von einem Bekannten empfohlen worden, und ein Befragter bekam die Karte im Rahmen einer Aktion zur Einführung des Systems direkt durch seinen Stromanbieter zugeschickt. Die Werbeaktionen in den Geschäften und die direkte Ansprache der Befragten scheint also eine erfolgreiche Methode zu sein, um Kunden für das Payback-System zu gewinnen, dagegen wurde Payback im Rahmen der Stichprobe aber nur ein einziges Mal von Freunden weiterempfohlen.

Tabelle 11

Erwartungen an die Teilnahme bei Payback	
Prämie erhalten	5
Geld sparen	5
Gesamtzahl	**10**

Die Äußerungen, warum die Beteiligten bei Payback mitmachen sind in zwei Kategorien zu unterteilen. Einer Hälfte der Befragten geht es darum, eines der von Payback angebotenen Präsente zu erhalten, die vom Schneebesen bis hin zu hochwertigeren Produkten bei entsprechend hoher Punktzahl reichen können. Eine Interviewpartnerin gibt an, sie wolle „etwas Praktisches erhalten“. Ebenso hoch ist aber auch der Anteil, der als Hauptgrund die Hoffnung angibt, mit Payback Geld zu sparen und in den Genuss von speziellen Rabatten zu kommen. Ein Befragter vergleicht das System mit Rabattmarken, die er noch aus seiner Jugend kennt. Eine andere bemerkt, sie wolle „ein bisschen sparen“, im Laufe des Jahres käme etwas zusammen.

Tabelle 12

Angaben über die Art des persönlichen Profits bei Payback	
Keiner	3
Rabatte erhalten	2
Erhalt von Bargeld	5
Gesamtzahl	**10**

Die Hälfte der Befragten hat bereits durch Auszahlung von Bargeld von der Teilnahme an Payback profitiert. Dabei handelt es sich um Summen von 17 Euro bei einer Person, die seit 1,5 bis 2 Jahren teilnimmt, bis hin zu 80 Euro bei einer Befragten, die bereits seit Beginn der Aktion teilnimmt. Diese relativ hohe Summe erklärt sich daraus, dass am Anfang drei Paypack-Punkte pro Euro vergeben wurden; die Punkte-Vergabe wurde dann später auf einen Punkt pro Euro reduziert. Zwei Personen geben an, bereits einmal durch spezielle Rabatt-Gutscheine profitiert zu haben, die einen Rabatt von 10% bis 20% einräumen. Bei den drei Befragten, die noch nicht von der Teilnahme profitiert haben, handelt es sich um Personen, die etwas weniger als ein Jahr oder gerade ein knappes Jahr bei der Aktion mitmachen. Einen materiellen Nutzen für den Verbraucher hat das System also erst nach längerer Teilnahme und einem entsprechend hohen Umsatz. Einlösen kann man die Punkte erst ab 1.500 Punkten, das heißt man muss im Schnitt 1.000 Euro umgesetzt haben, um eine Prämie oder eine Auszahlung zu erhalten. Zur Illustration sei an dieser Stelle angemerkt, dass es für 1.000 gesammelte Bonuspunkte beispielsweise einen Korkenzieher, eine Taschenlampe oder einen Pizzaschneider gibt - Artikel, die eher im Niedrigpreisbereich angesiedelt sind. Höherwertige Warenprämien sind meist mit erheblichen Zuzahlungen verbunden.[348] Die Teilnahme ist also im Schnitt für den Verbraucher wenig lohnenswert, jedenfalls gemessen an dem Nutzen, den die teilnehmenden Unternehmen durch die zunehmende Transparenz ihrer Kunden von der Payback-Aktion haben. Eventuell werden durch die vermeintlichen Rabatte auch Käufe getätigt, die vielleicht sonst nicht in Betrachte gezogen worden wären - ein weiterer Vorteil für die Unternehmen.

[348] vgl. Payback 2005

Tabelle 13

Kritik an Payback	
Nein	5
„*Noch* eine Plastikkarte im Portemonnaie“	1
Zuviel Versand von Werbung	2
Lieber direkt Rabatt auf die Ware	1
Keine Meinung	1
Gesamtzahl	**10**

Die Kritik am Payback-System ist eher gering. Ein Befragter äußert sich unzufrieden mit der Chipkarten-Form und wünscht sich eine andere Art der Rabatt-Vergabe, da er bereits viele Plastikkarten in seinem Portemonnaie mit sich führt. Eine weitere Person äußert, dass sie eigentlich lieber direkt auf die Ware Rabatte hätte, die Firmen wollten eine Kundenbindung und „Kunden fangen“, die gewährten Rabatte würden vermutlich ohnehin wieder auf die Ware aufgeschlagen werden. Eine Interviewte hat keine Meinung zu diesem Thema, da sie erst seit kurzer Zeit an der Aktion teilnimmt. Zwei Personen beklagen sich über die übermäßige Zusendung von Werbung, zu viele „Heftchen, Kataloge, Extras“ würden zugeschickt, im Grunde, so mutmaßt sie, soll der gewährte Rabatt direkt wieder in den Geschäften umgesetzt werden. Die Hälfte der Befragten äußert dagegen keine Kritik an Payback, eine davon bemängelt nur, dass es lästig sei, die Chipkarte immer heraus zu holen.

Tabelle 14

Zustimmung zur „Datenverwertung zu Werbezwecken“	
Ja	2
Nein	7
Unwissen	1
Gesamtzahl	**10**

Beim Ausfüllen des Antrages auf eine Payback-Karte hat man die Möglichkeit, der Verwertung der persönlichen Daten zu Werbezwecken zu widersprechen. Die meisten der befragten Personen haben diese Möglichkeit für sich in Anspruch genommen. Zwei Personen haben der Verwertung ihrer Daten zu Werbezwecken zugestimmt. Ein Befragter kann sich nicht mehr erinnern, welche Angaben er gemacht hat.

Erstaunlicherweise stimmen die Personen, die sich in der vorangegangenen Frage über die übermäßige Zusendung von Werbung beschwert haben, aber nicht mit

denen überein, die auch der Verwertung ihrer Daten zu Werbezwecken zugestimmt haben. Diese Personen scheinen also trotz ihres Widerspruchs Werbematerial zugesandt zu bekommen. Dies bestätig auch eine weitere Person, die nicht zugestimmt hat, aber dennoch Informationen zu Payback zusammen mit ihrem Payback-Kontoauszug geschickt bekommt. Eine andere Person, die der Verwertung nicht zugestimmt hat, bekommt dagegen auch wirklich keine Informationen per Post. Es scheint also je nach Payback-Partner unterschiedliche Arten des Umgangs mit den eingelegten Widersprüchen zu geben. Die Mehrheit der Paback-NutzerInnen haben kein Interesse an der Zusendung von Werbematerial und sich bewusst dagegen entschieden.

Tabelle 15

Angaben über die Art der Datenerhebung (Mehrfachnennungen möglich)	
Einkaufsverhalten	4
Persönliche Daten (Adresse, Alter etc.)	6
Es wird ein Profil erstellt	1
Orte, wo man eingekauft hat	2
Welche Warengruppen gekauft werden	1
Unwissen / keine genaue Kenntnis	2
Gesamtzahl	**16**

Die Antworten auf diese Frage waren sehr heterogen, Mehrfachnennungen waren möglich. Vier Personen gaben an, dass ihr Kaufverhalten erhoben wird. Dabei führte eine Person weiter aus, dass erhoben werde, ob man teuere oder billige Produkte und ob man Sonderangebote kaufe. Eine Befragte wusste, dass die gekauften Warengruppen erhoben werden. Zwei Befragte gaben an, dass erfasst wird, was man wo kaufe. Ein Interviewter äußerte, dass das Einkaufsverhalten erfasst und ein Profil erstellt werde. Etwas mehr als die Hälfte gaben an, dass ihre persönlichen Daten, wie Alter, Name, Adresse, Anzahl der Kinder erhoben werde. Zwei davon wussten darüber hinaus keine weiteren erhobenen Daten, und zwei weitere Befragte hatten keine, bzw. keine genauen Kenntnisse, welche Daten bei der Teilnahme am Payback-System erhoben werden. Anhand dieser Daten lässt sich erkennen, dass gut die Hälfte weiß, dass ihr Einkaufsverhalten in irgendeiner Form erfasst wird. Einige können dies recht genau formulieren („Es wird ein Profil erstellt“), andere etwas allgemeiner. Zwei der Befragten sind entweder gar nicht oder sehr ungenau informiert, was für Daten anfallen oder wissen nur, dass ihre persönlichen Daten gespeichert werden.

Tabelle 16

Gefahren oder Nachteile des Payback-Systems? (Mehrfachnennungen möglich)	
„Transparenter Kunde“	4
Datenmissbrauch	3
Nein	5
Künstliches Wecken von Bedürfnissen über Rabatte (Schuldenfalle)	1
Datensammlung / Big Brother	1
Gesamtzahl	**14**

Vier der Befragten sehen, bei möglichen Mehrfachnennungen, als Nachteil beim Payback-System, „dass man als Kunde transparent wird“. Einer dieser Gruppe äußert, dass Verbrauchergewohnheiten ausspioniert würden, erklärt aber, das mache nichts, da man ja überall überwacht werde. Ähnlich resignativ äußert sich ein Interviewter, der feststellt, die Datensammlungen wären „Big Brother in Vollendung“ und dass mittlerweile „so viele Querverbindungen über alle möglichen Karten“ hergestellt werden könnten. Dieselbe Person äußert auch, dass durch die Rabattaktionen Kaufbedürfnisse künstlich geweckt werden könnten und Verbraucher dadurch in eine Schuldenfalle gelangen könnten; für sich selber sieht er allerdings keine direkten Nachteile. Eine andere Befragte sieht ebenfalls die Gefahr des Gläsernen Kunden, vertraut aber dem Datenschutz und dass die Daten nicht für andere Dinge missbraucht werden. Drei Befragte können sich dagegen vorstellen, dass ihre Daten in irgendeiner Form, beispielsweise für Werbesendungen, missbraucht werden.

Die Hälfte der befragten Payback-NutzerInnen gibt an, keine Gefahren oder Nachteile in dem System zu sehen. Eine Person weiß zwar um die Datensammlungen, misst aber den Informationen über die eigene Person keine Bedeutung bei. So äußert sich auch eine weitere Interview-Partnerin, die sagt „Man ist ja nur einer unter Millionen, das wird schon nichts machen!“ Ferner gibt sie an, dass man ohnehin schon überall überwacht werden würde. Eine weitere Befragte bemerkt, dass sie keine Nachteile in Payback sieht, da die erhobenen Daten ja nicht öffentlich gemacht werden (z.B. im Internet); sie sieht es stattdessen als Vorteil für den Verbraucher, wenn Angebote besser auf diesen abgestimmt werden können. Ein anderer Payback-Nutzer sieht für sich persönlich keine Nachteile, verweist aber auf Nachteile für Personen, die durch künstliches Wecken von Bedürfnissen in eine Schuldenfalle manövriert würden.

4.4.5 Fallinterpretation

Payback stellt die am meisten verbreitete Kundenbonuskarte Deutschlands dar. Dies implizierte bereits im Vorfeld der empirischen Studie, dass eine Fülle von Daten über privaten Konsum zentral bei einer Firma zusammenlaufen, Payback also als Beispiel für groß angelegtes Datamining fungieren kann. Kunden werden durch Payback in ihrem Kaufverhalten *überwacht*, die Daten bieten den angeschlossenen Firmen Möglichkeiten, ihr Marketing anzupassen; aber auch weitere Verwendungsmöglichkeiten sind denkbar. Wie genau die Verbraucher über die Verwendung ihrer Daten Bescheid wissen und welche Möglichkeiten sich über eine Nutzung der Daten im Bereich des Marketing hinaus noch eröffnen, sollte innerhalb der Fallstudie herausgefunden werden.

Auf Anbieterseite sollte ermittelt werden, was das Unternehmen sich vom Einsatz des Systems erhofft und welche Bedeutung es grundsätzlich im wirtschaftlichen Bereich hat. Dabei wurde der Marktführer Payback als *ein* Beispiel für Datamining herausgegriffen um dessen Möglichkeiten zu illustrieren. Es sollte ferner die Präsenz des Systems im Alltag des Durchschnittsbürgers untersucht und seine Einstellungen zum System herausgearbeitet werden.

Mit 27 Millionen Karten ist Payback Marktführer der Bonuskarten in Deutschland. Dies bedeutet 27 Millionen Kundenprofile und das Wissen darüber, wer, wann, welche Art von Produkt wo gekauft hat. Hier können unter anderem Vorlieben, Preisbewusstsein und Umsatz des Kunden ermittelt werden und – das Einverständnis der Kunden vorausgesetzt – in persönliche Werbesendungen an den Kunden münden. Doch nicht nur die besser an den Interessen des Einzelnen angepasste Werbung ist interessant für ein Unternehmen – am Beispiel des Customer Relationship Managements wurde deutlich, wie entsprechende Datensätze auch diskriminierenden Charakter haben können. Das längere Warten bei einer Hotline, das Vorenthalten von Extra-Leistungen oder das Verweigern eines Kredites sind Folgen umfangreicher Kundendatenbanken, die zunehmend zusammengeführt und ausgewertet werden.[349] Es soll an dieser Stelle Payback nicht unterstellt werden, dass es erhobene Daten seiner Kunden weiterverkauft und mit anderen Datenbanken zusammenführt, sondern deutlich gemacht werden, dass Datensammlungen – und hier stellt Payback quasi den Prototyp dar – weiter reichende Folgen haben können, als man dies gemeinhin annimmt.

Interessant sind bei Payback auch die wirtschaftlichen Verflechtungen: Mehrheitseigner ist die Lufthansa AG, die sich aufgrund von persönlichen Kontakten des Geschäftsführers von Loyalty Partner mit dem Vorstand der Lufthansa erge-

[349] Das Thema wurde auch unlängst von der Verbraucherschutzministerin Künast aufgegriffen, Künast 2005.

ben hat. Eine der größten Unternehmensberatungen Deutschlands, Roland Berger, ist ebenfalls beteiligt. Der Datenschutz wird von der Lufthansa AG wahrgenommen, die nach eigenen Angaben dieses Thema als wichtig ansieht. Allein die Tatsache dieser Beteiligungen zeigt schon die Verflechtung, die sich bereits heute im Bereich der Datensammlungen ergeben. Durch Fusionen von Unternehmen oder Wechsel der Partnerfirmen können persönliche Konsumdaten letztlich ganz woanders hingelangen und eventuell auch auf dem internationalen Markt, der teilweise nicht über entsprechende Datenschutzgesetze verfügt, verbreitet werden.

Herr Weber vergleicht die Payback-Karte im Interview mehrmals mit den Rabattmarken im Tante-Emma-Laden, wo es darum ging, Kunden zu binden. Der Vergleich zu den Rabattmarken hinkt allerdings, da diese anonym zu nutzen waren und auch nicht festgehalten wurde, was wann gekauft wurde. Der Vergleich zu den Rabattmarkenheften erscheint als Verharmlosung der Möglichkeiten des Dataminings und dem bereits erwähnten Customer Relationship Management. Den Unternehmen geht es darum zu erfahren, welche Interessen und Schwerpunkte die Kunden haben und welche Produkte diese kaufen. Und zwar zum einen, um Sortiment und Werbung darauf abzustimmen, zum anderen, um für das Unternehmen umsatzstarke Kunden zu binden und andere abzustoßen. Anonymität ist prinzipiell zwar während des Punktesammelns möglich, muss aber spätestens beim Wunsch nach Erhalt einer Prämie aufgegeben werden. Auch gegenüber den Partnerunternehmen besteht Anonymität, allerdings laufen alle Daten bei der Betreiberfirma Loyalty Partner zusammen, welche die Daten zentral verwaltet und Werbesendungen etc. für die Partnerfirmen organisiert und damit letztlich ihr Geld verdient.

Aus den Äußerungen von Herrn Weber lässt sich erkennen, dass es innerhalb des Unternehmens nicht ganz einfach ist, den Gedanken des Datenschutzes zu vertreten. Herr Weber beklagt auch an dieser Stelle die fehlenden Sanktionsmöglichkeiten für ihn als Datenschutzbeauftragten. Er könne immer nur „Transparenz predigen“ und hoffen, dass seine Ratschläge angenommen werden. Es würde sich aber innerhalb einer Reihe von Großkonzernen zunehmend die Einsicht durchsetzen, dass die Daten der Kunden nicht als beliebiges Gut zu betrachten seien. Es handelt sich hier also um einen Prozess, der noch nicht abgeschlossen ist und somit den Rückschluss zulässt, dass Kundendaten – vermutlich in den meisten Fällen im gesetzlichen Rahmen – nach den Bedürfnissen des Unternehmens ausgewertet werden und man versucht, so viel als möglich zusammen zu tragen. Datenschutz ist demnach für die Wirtschaft nicht sonderlich attraktiv, und den Missbrauch von Daten kann man nicht verhindern.

Für die Zukunft sieht Herr Weber die Tendenz, das menschliche Verhalten immer nachvollziehbarer machen zu wollen. Dem könne nur mit technischem Datenschutz begegnet werden, indem man entsprechende Geräte entwickelt, die daten-

schutzgerecht sind und Missbrauch schon auf Geräteseite eindämme. Es entsteht der Eindruck, dass dem Datenschutz nicht die Bedeutung zukommt, die Herr Weber als Datenschutzbeauftragter sich wünscht. Zum einen wird dies in seiner Beschreibung der mangelnden Sanktionsmöglichkeiten innerhalb des Unternehmens deutlich, zum anderen in der Beschreibung der Situation des Datenschutzes bei anderen Großkonzernen. Auch Kritik an den für den Datenschutz zuständigen Landes- und Bundesbehörden äußert Weber – diese würden sich z.B. im Falle der Weitergabe von Flugreservierungsdaten nicht ausreichend für die Belange des Datenschutzes einsetzen. Der Schwarze Peter wird hier zwischen Staat und Unternehmen hin und her geschoben – je nach Perspektive sind es entweder die Unternehmen, die zunehmend und nahezu ungebremst Daten der Kunden sammeln oder eben der Staat, der, wie Weber es formuliert, ein Interesse daran hat, den Gläsernen Bürger zu schaffen. Herr Weber zeigt sich an dieser Stelle stark besorgt und macht den Zugriff des Staates auf Firmendaten am genannten Beispiel der Übermittlung von deutschen Flugreservierungsdaten an die USA deutlich. Hier seien die Argumente der Terrorismusbekämpfung ideal, um den Gläsernen Bürger entstehen zu lassen, äußert Weber. Egal, was das Unternehmen mache, ob es viele oder wenige Daten sammele, die Gefahr, dass der Staat auf die Daten zugreife, sei nicht vermeidbar. An dieser Stelle wird zum einen deutlich, dass sowohl der Staat als auch das Unternehmen gleichermaßen ein Interesse an der Transparenz der Bürger haben. Der Staat kann in der heutigen Zeit, nach dem 11. September, immer die Argumente der Sicherheit und Terrorismusbekämpfung anführen, um auf Datensammlungen, wie sie letztlich auch durch Payback entstehen, zuzugreifen. Durch die Verknüpfung mit anderen Datenbanken kann so ein immer detaillierteres Bild des Einzelnen entstehen, dass das Recht auf Informationelle Selbstbestimmung ad absurdum führt. Die USA hat mit dem bereits vorgestellten Information Awareness Office gezeigt, wohin die Entwicklung geht. Datensammlungen, wie sie auch durch Payback entstehen, sind also keinesfalls so harmlos, wie man auf den ersten Blick vermuten könnte. Neben dem Diskriminierungspotenzial finanziell schwächerer Kunden, wie es anhand des Customer Relationship Management beschrieben wurde, bieten sie auch dem Staat Möglichkeiten, ein immer detaillierteres Bild seiner Bürger zu erhalten. Wie Frau Sokol es formulierte dreht sich die grundsätzliche Unschuldsvermutung gegenüber dem Bürger ins Gegenteil: Jeder ist nur *noch nicht* verdächtig.

Wie Herr Weber es ausdrückte, ist es eine politische Entscheidung, welchen Wert dem Datenschutz beigemessen werden solle und ob Terrorismusbekämpfung wichtiger als die Wahrung der Persönlichkeitsrechte unbescholtener Bürger sei.

Im Alltag spielen solche Überlegungen keine Rolle. Die Payback-Karte hat sich durchgesetzt und wird beim Einkauf wie selbstverständlich vorgezeigt und auch in den Geschäften aktiv nachgefragt („Haben Sie eine Payback-Karte?“). Die meisten der befragten Payback-NutzerInnen sind auf diese Weise auch auf das

System aufmerksam geworden. Sie versprechen sich von der Teilnahme Bargeld oder eine Ersparnis. Die Hälfte der Befragten hat auch schon einmal tatsächlich eine Prämie erhalten, dies allerdings erst nach mehrjähriger Teilnahme und entsprechend hohem Umsatz. Was die Menschen am meisten stört ist das Versenden von Werbebriefen durch Payback, das auch stattfindet, wenn die NutzerInnen der Zusendung von Werbung, nach eigenen Angaben, nicht zugestimmt haben.

Gut die Hälfte der Befragten weiß, dass ihr Einkaufsverhalten in irgendeiner Form erhoben wird. Auch wenn diese Datenerhebung klar ist, wird den eigenen Daten nicht allzu viel Wert beigemessen. Äußerungen wie: man sei ja nur einer unter „Millionen von Beteiligten“ illustrieren, warum die Hälfte der Befragten keine Gefahren und Nachteile in der Teilnahme an Payback sehen. Selbst solche Befragten, die das System als „Big Brother in Vollendung“ bezeichnen, nehmen eine resignative Haltung ein und äußern, dass man ohnehin schon überall überwacht würde, da mache die Teilnahme an diesem System auch nichts mehr aus. Obwohl einigen Menschen bewusst ist, das Kundenprofile erstellt werden und die Daten beispielsweise für Marketingaktionen gebraucht werden, ziehen sie nicht die Konsequenz daraus, an dem System nicht teil zu nehmen. Vielmehr „fügen sie sich in ihr Schicksal“, erklären sich selbst als unbedeutend in einer Menge von Teilnehmern und sehen, wenn überhaupt, direkte Nachteile für andere, die in eine Schuldenfalle geraten könnten oder sich von vermeintlichen Sonderangeboten locken lassen.

Aufgabe der Politischen Bildung und der Medienpädagogik muss es hier sein, einen kritischen Umgang mit den eigenen Daten zu vermitteln und die Tragweite der wachsenden Verbreitung von Datensammlungen aufzuzeigen - der Wert privater Daten für die Demokratie müsste stärker betont und eine kritische Öffentlichkeit für das Problem geschaffen werden.

4.5 Fallstudie C: Ortungstechniken im privaten Familienalltag – das Beispiel der Kindersicherungen Leonie und Trackyourkid

Ortungstechniken wie das Global Positioning System oder die Möglichkeiten, die der Mobilfunkstandard GSM bietet, werden im privaten Bereich zunehmend in der Erziehung eingesetzt. So ist es möglich, sein Kind mit einem GPS-Empfänger auszustatten – sei es, wie schon in Großbritannien und den USA geschehen, als Implantat, oder wie hierzulande im Handy des Kindes integriert. Bei der Recherche für diese Fallstudie wurden für den deutschen Markt das von Siemens entwickelte GPS-System Leonie und das System Trackyourkid der Firma Armex ermittelt, welches auf Basis des Mobilfunkstandards GSM arbeitet. Dass das Mobiltelefon von vielen Eltern als *unsichtbare Nabelschnur* genutzt wird, ist

nichts neues. Schon seit längerem nutzen Eltern das Handy, um zum einen für den Nachwuchs erreichbar zu sein, zum anderen durch eigene Anrufe eine Kontrolle ausüben zu können. Neu ist bei den vorgestellten Systemen allerdings die Tatsache, dass Eltern über eine Hotline oder auch einer Karte im Internet fast metergenau Gewissheit über den Aufenthaltsort des Kindes erhalten können - eine ganz andere Qualität der Kontrolle.

Der Zugang zum Feld gestaltete sich problematischer als bei den anderen Fallstudien. Im Verlauf der Recherche stellte sich heraus, dass das System Leonie von Siemens nicht weiter verfolgt und schließlich eingestellt wurde. Trotz dieser Tatsache wird das System in der folgenden Studie kurz vorgestellt, da es einen Prototyp für den deutschen Markt darstellt. Innerhalb der Fallstudie wurde von Siemens zur Verfügung gestelltes Material inhaltsanalytisch ausgewertet und ein kurzes Expertinneninterview mit Frau Müller-Zantop, der ehemaligen Projektleiterin von Leonie, geführt. Das Protokoll des Interviews wurde Frau Müller-Zantop zur Durchsicht übersandt und dabei am Telefon missverstandene Fachbegriffe durch sie ergänzt. Der Kontakt war von Interesse am Forschungsvorhaben geprägt, wobei aber auch deutlich wurde, dass Frau Müller-Zantop nicht bereit war, Details zur Einstellung ihres Projektes preiszugeben. Es wurde aber Informationsmaterial und eine Studie zur Akzeptanz des Produktes zur Verfügung gestellt. Aus datenschutzrechtlichen Gründen war es nicht möglich, selbst Kontakt zu den damals beteiligten Eltern aufzunehmen.

Bei Trackyourkid handelt es sich um ein System, das seit 2003 auf dem Markt ist und bereits, anders als Leonie, Anwender gefunden hat. Innerhalb der Fallstudie wurde die Webseite des Unternehmens inhaltsanalytisch ausgewertet und ein Experteninterview mit Herrn Teubner, dem Geschäftsführer der Betreiberfirma von Trackyourkid geführt. Auch hier wurde das Protokoll Herrn Teubner zur Durchsicht geschickt. Der Kontakt war durch große Offenheit und Entgegenkommen gekennzeichnet.

Aus datenschutzrechtlichen und zeitlichen Gründen war es nicht möglich, die bereits vorhandenen KundInnen solcher Systeme zu ermitteln und mit ihnen in Kontakt zu treten. Die Systeme waren aber zum Zeitpunkt der empirischen Untersuchung Thema einer Radiodiskussion des Senders WDR 5 mit dem Titel „Überwachung mit dem Teddybär: Wenn Eltern ihre Kinder mit dem Minisender orten lassen“.[350] Diese Diskussion gab einen guten Einblick in die Meinung von Erziehungsberechtigten zu solchen Überwachungssystemen und wurde daher in die Fallstudie aufgenommen. Sie wurde per Tonband aufgezeichnet, transkribiert und ausgewertet.

[350] Die Diskussion fand im Rahmen der Sendung “Das Tagesgespräch” des Radiosenders WDR 5 am 6.11.2003 statt.

4.5.1 Das System Leonie

Was ist Leonie?

Leonie ist eine Entwicklung der Siemens-Tochter Mobile Family Services unter Verwendung einiger Komponenten der Gap AG, die im Bereich der Entwicklung flexibler Plattformen für Telematik und Telemetrieanwendungen angesiedelt ist. Wie sich bei der Recherche zu diesem System herausstellte wurde das Projekt 2001 durch Siemens aus firmeninternen Gründen eingestellt. Bei Leonie handelt es sich beim Prototypen um einen Teddybären, der mit einem Mobiltelefon und einem GPS-Empfänger ausgestattet ist.

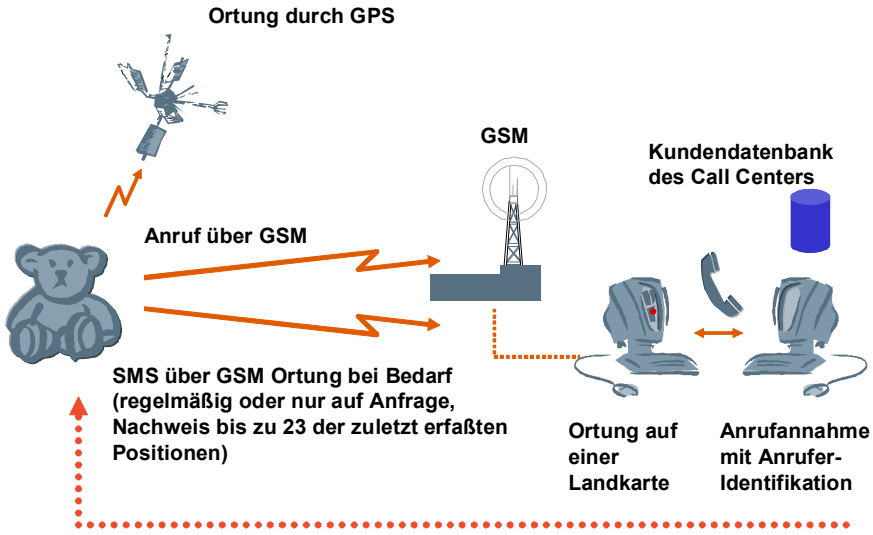


Abbildung 18: Bildquelle: Müller-Zantop, Teleshoppingpräsentation, 2001

Wie funktioniert Leonie?

Die Kombination aus GSM und GPS ermöglicht, den Standort des Kindes bis auf wenige Meter genau zu bestimmen. Die Daten werden ständig an ein so genanntes Kinder-Call-Center übermittelt. Dort verfügen Mitarbeiter über eine Datenbank, in der neben medizinischen Daten, Informationen über Freunde, Verwandte und Lehrer, aber auch persönliche Informationen wie z.B. das Lieblingsgericht des Kindes gespeichert sind. Dieses Call-Center übernimmt auch die Vermittlung

aller Gespräche, die von Leonie abgehen oder zu dem System gelangen sollen. Eltern können, nach erfolgter Identifikation, die Position ihres Kindes im Call-Center abfragen. Es besteht auch die Möglichkeit, das Kind direkt auf dem Handy anzurufen. Das Kind selbst kann durch einen Knopfdruck jederzeit mit einem Mitarbeiter des Call-Centers sprechen und wird dann entweder mit einer Person, deren Nummer im Call-Center hinterlegt wurde, verbunden oder direkt vom Mitarbeiter betreut. Es ist für das Kind nicht möglich, Personen direkt anzurufen, sondern es muss immer über das Call-Center verbunden werden. Bei Verdacht auf eine Gefahrensituation kann das Call-Center mittels Handy in die jeweilige Situation *hineinhorchen* und gegebenenfalls die Polizei alarmieren. Die Hersteller bezeichnen das in einer Information für die Fachpresse als Listen-In-Funktion, die in der Praxis juristisch auf Durchführbarkeit abzuprüfen gewesen wäre.[351] Konzipiert wurde Leonie für Kinder von drei bis elf Jahren.

Expertinneninterview mit der ehemaligen Projektmanagerin von Leonie

Motivation, Leonie einzuführen

Frau Müller-Zantop erklärt die Motivation zur Entwicklung eines Systems wie Leonie aus ihrer eigenen Situation als berufstätige, allein erziehende Mutter heraus. Sie könne daher die Bedürfnisse von Eltern gut nachvollziehen und es sei ihr aus diesem Grund die Idee für ein solches Projekt im Sommer 1999 nach einem Besuch bei Technologie-Spezialisten in den USA gekommen.

Einstellung des Projektes

Frau Müller-Zantop hat die Entwicklung von Leonie auch gegen Widerstände im Unternehmen vorangetrieben. Das Projekt wurde allerdings dann aufgrund firmeninterner Gründe im Jahr 2001 auf Eis gelegt (gleichzeitig geschah dies mit vier anderen Siemens-internen Projekten zu weiteren Mobilapplikationen); die Außenwirkung des Produktes oder etwaige kritische Pressestimmen hätten dabei, so Müller-Zantop, keinen Einfluss auf die Einstellung des Projektes gehabt.

4.5.2 Das System Trackyourkid

Was ist Trackyourkid?

Trackyourkid ist eigentlich nichts anderes als eine Zusatznutzung eines bereits vorhandenen Handys. Dabei kann das Handy ein Vertragshandy sein oder aber auch eines mit Prepaid-Karte. Derzeit kann jedes freigeschaltete Handy der gän-

[351] vgl. Mobile Family Services 2000

gigen Provider, innerhalb von Deutschland bis auf 250 Meter genau geortet werden. Das System bietet also den Service, zu ermitteln, wo sich das nachgefragte Handy – soweit eingeschaltet - gerade befindet. Die Information darüber kann entweder über das Internet auf einer Karte angezeigt oder auf das Elternhandy per SMS geschickt werden. Für diesen Service wird eine jährliche Gebühr gezahlt.

Wie funktioniert Trackyourkid?

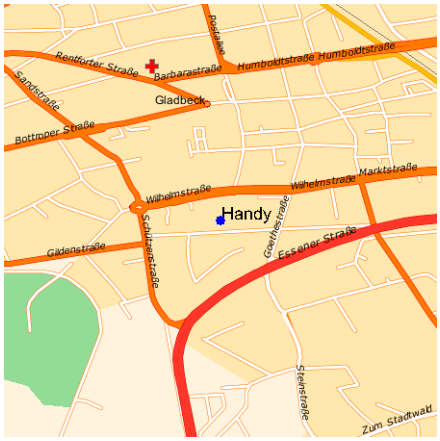


Abbildung 19: Demo-Karte einer Trackyourkid Suchanfrage

Das System arbeitet nicht mit GPS, wie es bei Leonie der Fall war, sondern nutzt die Tatsache, dass jedes eingeschaltete Handy stetigen Funkaustausch mit der jeweils nächsten Basisstation einer Funkzelle hält. Der Standort kann so auf eine Zelle hin – und damit auf mehrere 100 Meter ermittelt werden.

Die Webseiten von Trackyourkid

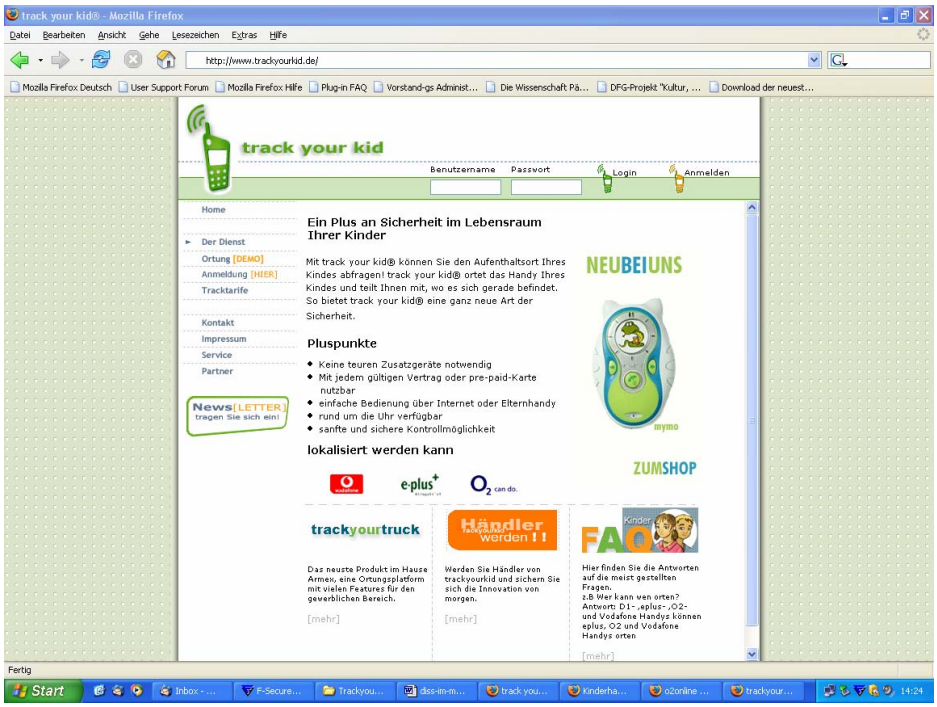


Abbildung 20: Screenshot der Homepage

Bei der Auswertung der Webseiten von Trackyourkid sollte darauf geachtet werden, wie das Unternehmen ihr Produkt darstellt und welche Punkte dabei besonders im Vordergrund stehen. Dazu wurden aus den Webseiten heraus Kategorien gebildet und ausgewertet.

Sicherheit

Abbildung 21: Werbegrafik von Trackyourkid

Mit dem Slogan „Ein Plus an Sicherheit im Lebensraum ihrer Kinder“ wendet sich der Anbieter auf seiner Startseite an potenzielle Kunden. Dadurch, dass Trackyourkid es ermöglicht, den Aufenthaltsort des Kindes abzufragen, indem es das Handy des Kindes ortet, wird laut der Betreiberfirma „eine ganz neue Art der Sicherheit“[352] geboten. Als Pluspunkte des Produktes werden unter anderem der Wegfall von teuren Zusatzgerä-

[352] vgl. Trackyourkid 2004a

ten, die einfache Bedienung über Internet oder Elternhandy, sowie der Umstand, dass es sich um eine „sanfte und sichere Kontrollmöglichkeit“[353] handele, angeführt.

Unter dem Link „Der Dienst“ wird erneut der Begriff der Sicherheit aufgegriffen: „Unser Produkt – für die Sicherheit ihrer Kinder entwickelt“. Es wird darauf verwiesen, dass die Eltern durch die Nutzung von Trackyourkid wissen würden, dass das Kind sich in einer sicheren Umgebung befindet.

Sicherheit hat aber auch noch eine andere Bedeutung, indem es bei der auf den Webseiten gegebenen „Sicherheitsgarantie“ nicht mehr um die Sicherheit des Kindes geht, sondern um die sichere Übertragung von Daten. Hier lautet der Slogan: „Auf dem neuesten Stand. Mit Sicherheit!“[354] Auch auf die Überprüfung der Richtigkeit der Angaben, die zur Nutzung des Dienstes nötig sind, wird hingewiesen (das zu ortende Handy muss im Besitz des Nutzers sein), die Firma wirbt mit den Worten „Sie sehen, Sicherheit wird bei uns groß geschrieben.“[355]

Vertrauen

Eine weitere Kategorie, die mehrmals auftaucht, ist die des Vertrauens. Der Betreiber empfiehlt, die Nutzung von Trackyourkid mit dem Kind durchzusprechen, das schaffe „notwendiges gegenseitiges Vertrauen“[356] Gleichzeitig wird die relative Ungenauigkeit des Dienstes (eine Ortung ist bis auf ca. 250 Meter genau möglich), als *nachhaltig wichtiger* Aspekt gesehen.

> „Wir meinen, gerade in punkto Vertrauen sollten Sie Ihrem Kind einen wichtigen Bonus einbauen und unseren Dienst verantwortlich nutzen.“[357]

Trackyourkid sei nicht entwickelt worden, das Kind ständig auf allen Wegen zu kontrollieren; der mit 250 Metern relativ große Radius, in dem das Kind sich aufhalten kann, wird also als Bonus in Richtung Vertrauen in das Kind interpretiert. Es reicht also demnach, wenn das Kind *so ungefähr* da ist, wo es sein soll. Nach dem Motto *Vertrauen ist gut, Kontrolle ist besser* dient Trackyourkid, laut der Betreiber dazu, den Kindern Stück für Stück dem „Kind Vertrauen [zu] schenken, welches es auch verdient“.[358] Gegenseitiges Vertrauen soll also unter Zuhilfenahme technischer Kontrollsysteme hergestellt werden.

---

[353] vgl. Trackyourkid 2004b

[354] vgl. Trackyourkid 2005b

[355] vgl. Trackyourkid 2005b

[356] vgl. Trackyourkid 2005b

[357] vgl. Trackyourkid 2005c

[358] vgl. Trackyourkid 2005d

Ängste

Das Produkt hebt auf die Ängste der Eltern ab, ihrem Kind könnte etwas zustoßen und verspricht durch eine Ortung des Kindes, diese zu beseitigen. Ferner ist Trackyourkid laut der Betreiber ein ideales Mittel, um Streit zwischen Eltern und Kindern zu vermeiden.

> „Meistens sind Ihre Ängste unbegründet und aus kindlicher Sicht kaum nachvollziehbar. Später stellen Sie Ihr Kind zur Rede. Das Fazit: Streit kommt auf, weil Ihr Kind sich zu sehr kontrolliert fühlt und mehr Freiräume für sich verlangt."[359]

Statt mit dem Kind direkt zu sprechen soll die Auseinandersetzung um Grenzen vermieden werden und die Eltern durch das Produkt auch so an die Informationen kommen, die sie brauchen, um keine Angst mehr zu haben. Trackyourkid wird von den Betreibern daher als „zeitgemäße und aus pädagogischer Sicht sanfte Kontrollmöglichkeit" gesehen. Was genau unter dem Begriff *sanft* verstanden wird, wird nicht näher erläutert: Eventuell eben eine Kontrolle, die vom Kind gar nicht bemerkt wird und Diskussionen um den Aufenthaltsort umgeht.

Experteninterview mit dem Geschäftsführer von Trackyourkid

Das Experteninterview mit Herrn Teubner, dem Geschäftsführer der Betreiberfirma von Trackyourkid, wurde im Sommer 2004, also circa ein halbes Jahr, nachdem der Dienst eingeführt wurde, fernmündlich geführt. Es wurde ein Protokoll erstellt, das Herrn Teubner zur Durchsicht zugesandt wurde. Innerhalb des Interviews sollte ermittelt werden, welche Motive es gab, ein System wie Trackyourkid einzuführen und welche Erfahrungen bislang damit gesammelt werden konnten. Ermittelt werden sollte:

- Was hat Firma dazu bewogen, ein solches Produkt auf den Markt zu bringen?
- Worin liegen aus Sicht des Geschäftsführers die Vor- und Nachteile des Einsatzes von Trackyourkid?
- Wie wird das Produkt derzeit von den Verbrauchern angenommen und welche Reaktionen kommen aus der Praxis?
- Hat es Kritik an Trackyourkid in der Öffentlichkeit gegeben?
- Welche Entwicklungen werden für die Zukunft gesehen?

[359] vgl. Trackyourkid 2005d

Auswertung des Interviews

Entstehung der Idee

Trackyourkid ist seit Oktober 2003 online. Die Idee kam laut Herrn Teubner in Verbindung mit einem anderen Produkt der Firma Armex auf, das „Schul-SMS" heißt. Dabei geht es nach Aussage Herrn Teubners darum, die Kommunikationswege zwischen Schule und Elternhaus zu verkürzen und Schulschwänzer schneller zu melden.

> „Daraus kam die Idee, zu ermitteln, wo ist das Kind denn dann? Welche Möglichkeiten gibt uns der Markt?"[360]

Teubner berichtet, dass zur Einführung des Produktes keine Marktforschung betrieben wurde, sondern im Kontaktfeld anderer Produkte (wie z.B. Schul-SMS) und im Bekanntenkreis Befragungen durchgeführt wurden. Es wurden dazu ca. 1000 Personen befragt, aber keine Repräsentativumfrage durchgeführt. Die Firma beschäftigte sich also schon vor Einführung von Trackyourkid mit Systemen, die dazu dienen, Kinder und Jugendliche mit Hilfe der Mobilfunktechnik zu kontrollieren. Durch Schul-SMS kann die am System beteiligte Schule den Eltern direkt per SMS mitteilen, wenn ihr Kind nicht in der Schule erschienen ist. Ein nächster Schritt sei es dann gewesen, zu ermitteln, wo genau das Kind sich aufhält.

Nachfrage nach dem Produkt

Die Nachfrage nach Trackyourkid ist aus Sicht des Geschäftsführers gut. Seit Einführung im Oktober 2003 hätten sich 7000 KundInnen angemeldet. Dies ist eine beachtliche Zahl innerhalb eines halben Jahres, die darauf schließen lässt, dass es auf Seiten der Eltern ein hohes Bedürfnis gibt zu wissen, wo genau sich ihr Kind aufhält. Das Produkt scheint also bei den teilnehmenden Eltern den *richtigen Nerv* getroffen zu haben. Laut Herrn Teubner gibt es derzeit keine vergleichbaren Produkte auf dem Markt; ein ähnliches Siemens-Produkt sei aus Kostengründen eingestellt worden, womit er das bereits beschriebene System Leonie anspricht.

Die Eltern

Herr Teubner erklärt, dass bei den Eltern und Erziehungsberechtigten eine Sorge bestehe, wo sich ihr Kind gerade aufhält. Kinder seien in heutiger Zeit früher selbständig und bewegten sich in viel größerem Radius, als dies noch vor einigen Jahren der Fall war. Durch die Überwachung mit dem Produkt soll den Eltern die

[360] vgl. Teubner 2004, Antwort 1

Möglichkeit gegeben werden, zu erfahren, wo sich ihr Kind, oder zumindest das Handy des Kindes, gerade befindet. Wie schon auf der Webseite zu lesen war, soll so ein unnötiges zur-Rede-Stellen des Kindes vermieden werden, das in einen Streit zwischen Eltern und Kind münden könnte. Durch Trackyourkid können die Eltern vermeintliche Auseinandersetzungen vermeiden und erfahren trotzdem, was sie wissen wollen, nämlich ob das Kind wirklich da ist, wo es sein soll. Herr Teubner unterstreicht dies mit der Formulierung:

> „Die Frage, ´verhält sich das Kind so, wie ich es möchte`, kann so beantwortet werden“

Es bleibt den Eltern überlassen, ob sie ihrem Kind per SMS mitteilen, dass sie es geortet haben; eine verdeckte Überwachung ist also möglich und wirft die Frage nach dem Vertrauensverhältnis zwischen Eltern und Kind auf. Man wisse durch das Produkt, ob das Kind in einem Feld ist, wo es o.k. ist, formuliert Teubner. Auch bei schwierigen Schulwegen könnten die Eltern so erfahren, ob das Kind in der Schule angekommen sei. Direkte Rückmeldungen, wie die Nutzung des Produktes in der Praxis aussieht, gäbe es allerdings selten, meist seien es Supportfragen, die gestellt werden würden. Trackyourkid setzt also darauf, dass die Eltern vermeiden wollen, ihr Kind direkt anzusprechen, wo es denn gewesen sei oder es durch Anrufe auf dem Handy zu *nerven*. Statt dessen können Eltern ihrer Sorge dadurch begegnen, das Kind über ein technisches System - wahlweise unbemerkt – zu überwachen. Dies ist ein Umstand, der tief in das Vertrauensverhältnis zwischen Eltern und Kind eingreift und versucht, Probleme in der Kommunikation und Erziehung mit technischen Mitteln zu lösen.

Sicherheit

Trackyourkid sei ein „relativ sicherer“ Kontrollmechanismus über das Kind, erläutert Teubner. Er äußert, dass das Produkt für das „Gefühl der Sicherheit“ bei den Eltern gut sei. Auch innerhalb der Webseiten spielt der Begriff der Sicherheit, wie bereits gezeigt, eine große Rolle und ist im Prinzip Hauptverkaufsargument. Wie auch schon bei anderen technischen Systemen wie der Videoüberwachung der Kölner Verkehrsbetriebe, wird hier auf das „Gefühl der Sicherheit“ abgehoben. Genau betrachtet kann das Produkt in keinerlei Weise eine Sicherheit für das Kind oder die Eltern darstellen. Auf Seiten des Kindes stellt sich nicht mehr Sicherheit ein, wenn es ein Handy bei sich trägt, dass die Eltern genau orten können. Vielmehr wird dem Kind das Gefühl vermittelt: meine Eltern vertrauen mir nicht oder ich brauche ja nicht selber acht zu geben, da meine Eltern ja sowieso immer wissen, wo ich bin. Einen Beitrag zur Selbstständigkeit und zu einer vertrauensvollen Beziehung wäre das Produkt demnach nicht. Die Eltern wähnen sich auf der anderen Seite in einer *Schein-Sicherheit*, wenn sie sich auf ein technisches Produkt verlassen, das Erziehung nicht ersetzen kann. Das Handy kann beispiels-

weise einfach ausgeschaltet, weggeworfen oder einem Freund oder Freundin mitgegeben werden, und schon ist das System ausgehebelt. Transportiert wird aber mit diesen Systemen viel mehr: nämlich das Gefühl des Kindes, ständig kontrolliert zu sein und sich konform und wie die Eltern es gerne möchten verhalten zu müssen. Von Kindesbeinen an entsteht so ein Gefühl, sich in gewünschter Art und Weise verhalten zu müssen, da eine übermächtige Technik einen sowieso *überführen* kann. Dies stellt einen massiven Eingriff in Kinderrechte dar.

Missbrauch des Systems

Herr Teubner sieht es als Nachteil an, wenn das Produkt missbräuchlich eingesetzt wird; er lehnt eine Beobachtung des Kindes auf Schritt und Tritt ab. Dann stimme, so der Geschäftsführer, aber etwas im Verhältnis zwischen Eltern und Kind nicht, dies deute auf schlechte Familienverhältnisse hin. Dennoch liege es im Ermessen der Eltern, wie sie das System einsetzten. Ein Gespräch mit dem Kind wäre sinnvoll, Tipps würden auf der Webseite gegeben. Bis zum Zeitpunkt des Interviews im Sommer 2004 seien aber laut Herrn Teubner keine Fälle von Missbrauch des Systems bekannt geworden. Auch wenn Herr Teubner eine ständige Überwachung des Kindes durch die Eltern ablehnt, ist er in erster Linie daran interessiert, sein Produkt zu verkaufen. Seine Firma bietet keine pädagogische Beratung an und sie gibt keine Hilfe für eine Lösung im zwischenmenschlichen Bereich, sondern sie verkauft technische Systeme, die etwaige Kommunikations- und Vertrauensprobleme umgehen sollen oder den Eltern ein *Gefühl von Sicherheit* verkaufen.

Soziale Probleme der Nutzer

Teilweise bekomme man aber durch die Anrufe der Kunden bemerkenswerte soziale Probleme mit, erklärt Herr Teubner. Er berichtet von einer Frau, die bei der Hotline anrief und das Produkt haben wollte, da ihr Mann damit drohte, das gemeinsame Kind zu entführen. Es riefen auch besorgte Eltern an, weil das Kind nicht nach Hause gekommen sei. Hier wird deutlich, dass die Technik etwas lösen soll, dass eigentlich einer pädagogischen Intervention bedürfte. Die zugrunde liegenden familiären Probleme, die eine drohende Entführung durch den Vater nach sich ziehen, können nicht durch das Mitgeben eines ortungsfähigen Handys gelöst werden. Auch der zweite Fall zeigt, dass das Produkt keine Probleme lösen kann, sondern nur neue produziert. Die Sorgen werden sich nicht verringern, wenn das Kind nicht nach Hause kommt, das Handy womöglich ausgeschaltet hat oder die Ortung einen Umkreis von 250 Metern zum Ergebnis hatte. Das Problem bleibt ein erzieherisches und ist auch nur auf dieser Ebene zu lösen.

Reaktionen auf das Produkt

In den Medien habe es ein „super Medien-Echo“ gegeben, so Teubner. Die Reaktionen seien überwiegend positiv gewesen. Es hätte aber auch einen „Aufschrei der Datenschützer“ in Richtung Gläserner Mensch und Überwachungsstaat gegeben. Herr Teubner räumt ein:

> „Aus Sicht der Datenschützer ist das wirklich so. Das ist aber der Lauf der Technik: man wird immer gläserner.“[361]

Der eigene Umgang mit der Technik sei wichtig, auf den Webseiten der Firma würden Hinweise und Informationen dazu gegeben. Herr Teubner räumt einerseits ein, dass sein Produkt aus datenschutzrechtlicher Sicht nicht wünschenswert ist, begibt sich auf der anderen Seite aber in eine technikdeterministische Haltung, in dem er es so darstellt, als sei man der Technik ausgeliefert. Mit dem Ausspruch, der Lauf der Technik bedinge, dass man immer „gläserner“ wird, stellt er Technik wie einen Selbstläufer dar, dem man sich nicht entziehen kann. Die Firma Armex ist aber letztendlich Produzentin dieser Technik und trägt aktiv dazu bei, dass das Leben von Menschen immer stärker überwacht und kontrolliert wird.

Zukunftspläne

Für die Zukunft plant die Firma einen so genannten Notfallserver, bei dem Eltern ihre Telefonnummern, unter denen sie zu erreichen sind, hinterlegen können. Das Kind kann dann beim Notfallserver anrufen und wird automatisch an die angegebenen Nummern weitergeleitet. Diese Idee stellt im Prinzip eine etwas weniger aufwendige Variation des Call-Centers bei Leonie dar. Hier sind aber keine Menschen im Call-Center, die den Anruf des Kindes entgegennehmen und mit ihm sprechen oder in einer wirklichen Notsituation erste Hilfeangebote machen können, sondern das System ist ganz in die Hände der Technik gelegt. Ansprechpartner für das Kind ist im Notfall also ein Computer.

4.5.3 Ortungssysteme für Kinder aus Sicht von Eltern

Aus bereits genannten Gründen war es nicht möglich, eigene Interviews mit Eltern zu führen. An dieser Stelle sollen daher Meinungen, die innerhalb einer Radiodiskussion von anrufenden Eltern vertreten wurden, wiedergegeben werden. Beteiligt waren dabei sechs Hörerinnen und drei Hörer des Senders WDR 5, die sich zum Thema „Überwachung mit dem Teddybär: Wenn Eltern ihre Kinder mit dem Minisender orten lassen“ äußerten. Sechs der HörerInnen sprachen sich

[361] vgl. Teubner 2004, Antwort 8

gegen die Systeme aus, drei HörerInnen befürworteten den Einsatz solcher Systeme. Die Diskussion wurde transkribiert und im Anschluss inhaltsanalytisch ausgewertet.

Tabelle 17: GesprächsteilnehmerInnen Radiosendung

	Geschlecht	**selbst Elternteil**
Person A	weiblich	unbekannt
Person B	weiblich	ja
Person C	männlich	ja
Person D	männlich	ja
Person E	weiblich	ja
Person F	weiblich	ja
Person G	weiblich	ja
Person H	weiblich	ja
Person I	männlich	unbekannt
Gesamtzahl		**9**

Auswertung

Zweifel am Nutzen

Zwei HörerInnen bemerken, dass das System hauptsächlich dazu da wäre, den Eltern die Angst zu nehmen. Kinder seien nicht hundertprozentig zu schützen. Ein Vater bemerkt:

> „[...] ich glaube, dass das mehr zur Beruhigung der Eltern beiträgt, abgesehen davon, dass die Industrie sich wieder ein neues Marktsegment erschlossen hat, um da eine Menge Geld mit zu machen, denn heute ist ja kein Quatsch dumm genug, dass man den nicht zumindest mal ausprobiert, weil es ja vielleicht Geld damit zu verdienen gibt. Ich halte das für eine sehr schlechte Geschichte."

Ein anderer Hörer bemerkt, dass man das Handy auch wegschmeißen könne oder der Akku leer gehen könne, somit wäre der Nutzen in Frage gestellt. Aus Sicht dieser Beteiligten besteht der Nutzen allenfalls in der Beruhigung der Eltern und darin, der Industrie eine neue Möglichkeit des Verdienstes mit den Sorgen der Eltern zu erschließen.

Erziehungsauftrag der Eltern

Eine Hörerin betont, es sei wichtig, die Balance zwischen Schutz und völliger Kontrolle zu finden, das Kind müsse gefördert werden, selbständig zu werden. Ein Vater führt aus, dass man sich auf sein Gefühl verlassen müsse und nicht versuchen sollte, alles zu kontrollieren. Mit Überwachung, so eine Hörerin, fände kein Lernen statt.

Gesellschaftliche Aspekte

Eine Hörerin bemerkt, dass es wichtig sei, dass das Kind *in der Gesellschaft* aufgehoben sei und nicht in einem Überwachungsapparat. Wichtig sei es, dass die Menschen sich austauschten und gemeinsam schauten, wo die Kinder sind. Der Aspekt, dass das Umfeld sich stärker verantwortlich zeigen sollte – und dies auch tut -, wird von einigen Hörerinnen und Hörern vertreten, die menschliche Intervention und ein „Achten aufeinander" den technischen Lösungen vorziehen. Eine Hörerin berichtet in diesem Zusammenhang von ihren positiven Erfahrungen in südlichen Ländern, in denen die Erwachsenen ganz selbstverständlich auf andere Kinder mit aufpassen würden.

Ein Vater sieht das System als *weiteren Schritt in den Überwachungsstaat* und die Unselbständigkeit der Kinder:

> „Was ich schaffe damit sind eigentlich, ich sag mal, Opfertypen, die permanent überwacht werden, permanent anrufen können: Mama ich bin jetzt aus der Straßenbahn ausgestiegen und Mama, die Straßenbahn macht jetzt ihre Türen zu und zwei Minuten später Mama, die ist jetzt abgefahren die Straßenbahn, das heißt die Kinder werden absolut unselbständig und das ist etwas, was wir eigentlich in dieser Welt überhaupt nicht gebrauchen können."

Die Überbetonung technischer Möglichkeiten, um jeden kleinsten Schritt des Kindes nachvollziehen zu können, wird hier abgelehnt und als gesamtgesellschaftlich kontraproduktiv interpretiert. Eine weitere Hörerin stellt in diesem Zusammenhang die Frage danach, welche Generation da entstehe, wenn sie in einer *totalen Überwachung* groß werden würde. Ein Gesprächsteilnehmer spricht sich dagegen provokativ für die Überwachung aller durch alle aus. Jeder sollte jeden überwachen können, dann wäre es gerecht.

Seite der Kinder

Ein Vater vertritt die Ansicht, dass Kinder immer eine Möglichkeit finden würden, die elterlichen Kontrollversuche zu umgehen, sei es, indem sie das Handy einem Freund mitgeben, oder indem sie behaupteten, sie seien in einem Funkloch gewesen. Eine Hörerin spricht sich grundsätzlich gegen technische Überwachung aus, denn auch Kinder hätten Menschenrechte, die es zu respektieren gälte.

Eine grundsätzlich positive Haltung vertritt dagegen ein Vater, der sich als ängstlich bezeichnet und für sich folgende Position gefunden hat:

> „Man muss es den Kindern ja nicht erzählen. Sie brauchen es ja gar nicht zu wissen. Es ist für mich aber als Vater beruhigend, beide Elternteile sind am Arbeiten und sie kommt von der Schule, wird von der Oma abgeholt oder... wo sind sie? Einfach für mich mal am Arbeitsplatz, übers Internet zu schauen, wo sind sie denn gerade, was machen sie gerade?“

Für diesen Vater ist es eine bequeme Art, seinen Sorgen um den Aufenthaltsort seiner Tochter durch einen Blick ins Internet zu begegnen. Er habe dabei keine Bedenken, die Überwachung vor seiner Tochter zu verheimlichen.

Zustimmung aufgrund besonderer Situationen

Zwei der HörerInnen befürworten das System, da ihre Kinder an chronischen Krankheiten leiden, bzw. eine Behinderung haben und für sie das ortungsfähige Handy zu einer „langen Leine“ werden könnte, mit der sie schrittweise ihren Kindern mehr Freiheiten gewähren möchten.

Sicherheit

Eine Mutter betont, dass es völlige Sicherheit und Kontrolle nicht geben könne und dass man es als Elternteil aushalten und lernen müsse, loszulassen:

> „Ich denke, das Wichtigste ist zu lernen einzuschätzen, was das Kind schon leisten kann und es auch in dem zu fördern, Eigenleistungen zu bringen, auch die, die die persönliche Sicherheit betreffen und nicht nur schulische Leistungen.“

Es ist nach Ansicht dieser Mutter also auch für die Eltern wichtig, nicht alles „kontrollieren“ zu können, sondern zu lernen, dem Kind Stück für Stück Eigenverantwortung beizubringen. Dies würde durch den Einsatz des technischen Kontrollsystems unterwandert. Ein Vater beurteilt das anders und sieht die Sicherheit seiner Tochter, gerade im Hinblick auf Straftaten, durch den Einsatz des Ortungssystems verbessert:

> „Dann die andere Sache ist zum Beispiel das Thema der Sicherheit, das heißt, weil ich ein etwas ängstlicherer Vater bin, sehe jetzt die ganzen Kindermisshandlungen, Kindermissbräuche, wenn meine Tochter das gar nicht weiß, dass man ihr Handy orten kann, dann habe ich die Möglichkeit, zu schauen: wo ist sie denn gerade und auch in so einem Fall, in einem extremeren Fall, was Kriminelle angeht, habe ich die Möglichkeit mein Kind zu orten.“

Kinder hätten nach seiner Ansicht gerettet werden können, hätten sie ein entsprechendes Gerät bei sich gehabt.

4.5.4 Fallinterpretation

Innerhalb der Fallstudie zu Ortungstechniken im privaten Bereich sollten anhand der beiden Kindersicherungssysteme Leonie und Trackyourkid zwei Systeme vorgestellt werden, die in Deutschland entwickelt wurden und sich teilweise bereits etabliert haben. Da Leonie vom Hersteller nicht weiter verfolgt wurde, liegt der Hauptaugenmerk auf Trackyourkid, das seit 2003 auf dem Markt ist. Die Auswahl der Ortungssysteme spielt stark in den erzieherischen Bereich hinein. Es sollte hier ermittelt werden, wie sich die Technik im Alltag darstellt, welchen Nutzen die Betreiber der Systeme in ihren Produkten sehen und wie sich das System aus deren Sicht in der Praxis zeigt. Ferner sollte untersucht werden, welche Positionen die potenziellen NutzerInnen solcher Systeme einnehmen.

Das von der Siemens Tochter Mobile Family Services entwickelte Produkt Leonie wurde bereits in der Erprobungsphase wieder eingestellt, die genauen Gründe dafür waren nicht zu ermitteln, außer dass es firmeninterne waren und zur selben Zeit auch noch andere Projekte eingestellt wurden. Das Besondere an Leonie war zum einen die Kombination von GPS und GSM und der Einsatz eines so genannten Kinder-Call-Centers. Dort verfügten Mitarbeiter über eine Datenbank, in der neben medizinischen Daten, Informationen über Freunde, Verwandte und Lehrer auch persönliche Informationen wie z.B. das Lieblingsgericht des Kindes gespeichert waren. Es handelte sich hierbei also nicht um ein reines Ortungssystem, sondern eher um so etwas wie ein virtueller Babysitter, den die Kinder anrufen können, wenn irgendetwas passiert ist. Eine direkte Kommunikation des Kindes mit der gewünschten Person war nämlich nicht im Konzept vorgesehen. Bemerkenswert ist in diesem Zusammenhang, ähnlich wie bei Payback, die Sammlung von Daten – hier schon von frühester Kindheit an. Die am Pilotprojekt teilnehmenden Eltern hatten anscheinend kein Problem damit, die Vorlieben ihres Kindes, etwaige Krankheiten und sein soziales Umfeld einer Datenbank anzuvertrauen. Etablierten sich solche Systeme, würden bereits von Kindesbeinen an Profile möglich sein. Deutlich wird hier erneut, dass Privatsphäre und der Schutz persönlicher Daten für viele Menschen keinen Wert mehr haben und diese unbekümmert weitergegeben werden. Im Dienste der Sicherheit war im Konzept von Leonie auch eine so genannte Listen-In-Funktion vorgesehen, die es dem Call-Center bei Verdacht auf eine Gefahrensituation ermöglichte, mittels Handy in die jeweilige Situation *hineinzuhorchen* und gegebenenfalls die Polizei zu alarmieren. Ob dies juristisch möglich gewesen wäre, hätte laut Müller-Zantop noch geprüft werden müssen. Es wird an dieser Stelle aber deutlich, dass Persönlichkeitsrechte – noch dazu von Kindern, die diese noch nicht selbst verteidigen können – gerne zugunsten eines vermeintlichen Zugewinns an Sicherheit preisgegeben werden.

An dieser Stelle wird klar, was das Produkt leisten soll: Es wird versucht, soziale Probleme – wie eine mangelnde gesellschaftliche Solidarität von Eltern, ein Fehlen von adäquaten Betreuungsmöglichkeiten – durch Technik zu kompensieren und den Eltern das Gefühl zu geben: Es kann ja nichts passieren, Leonie passt schon auf mein Kind auf. Es scheint also für einige Eltern nicht mehr möglich zu sein, Kinderbetreuung durch andere Mittel im nötigen Maßstab zu gewährleisten.

Das zweite System, Trackyourkid ist seit Oktober 2003 online und kann bereits innerhalb des ersten halben Jahres des Betriebs 7000 KundInnen verzeichnen. Eine Zahl, die darauf schließen lässt, dass es auf Seiten der Eltern einen großen Bedarf gibt.

Das System verzichtet auf den Einsatz von GPS und eines Call-Centers. Das bedeutet, dass das System ungenauer ist als Leonie und sich ausschließlich auf die Standortermittlung des Handys und dessen Darstellung auf einer Karte spezialisiert hat. Daten über das Kind werden an dieser Stelle nicht gesammelt, ein Ansprechpartner für das Kind in einem Call-Center steht nicht zur Verfügung. Dieser Umstand hat nicht zuletzt damit zu tun, dass es sich – im Gegensatz zu den Siemens Mobile Family Services – um ein mittelständisches Unternehmen handelt, dem vermutlich schlicht die Mittel zur Etablierung einer solchen Infrastruktur fehlen. Im Prinzip bietet Trackyourkid daher nichts anderes als der Mobilfunkanbieter O2 schon seit Jahren anbietet: Die Darstellung des Handy-Standortes auf einer Karte, die über das Internet abgerufen werden kann. Die Ungenauigkeit des Dienstes, nämlich bis auf 250 Meter genau, wird als Vertrauensbonus an das Kind gewertet, da das System nicht entwickelt worden sei, das Kind ständig auf allen Wegen zu kontrollieren. Das Wissen darum, wo das Kind *so ungefähr* ist, soll dazu dienen, dem Kind Stück für Stück „Vertrauen [zu] schenken, welches es auch verdient".[362] Gegenseitiges Vertrauen soll also unter Zuhilfenahme technischer Kontrollsysteme hergestellt werden. Es muss erst verdient werden, indem überprüft werden kann, ob man auch wirklich da ist, wo man sein soll. Mit Vertrauen hat das nicht mehr viel zu tun.

Das System soll ferner den Eltern die Möglichkeit geben, Konflikten aus dem Weg zu gehen, wenn sie das Kind *schon wieder zur Rede stellen*, wo es denn gewesen sei. Diese Frage muss man – laut Trackyourkid – nicht mehr stellen, da man ja immer nachsehen kann, wo das Kind sich ungefähr aufhält und somit unangenehmen Diskussionen aus dem Weg geht. Wie schon bei Leonie soll das System soziale Probleme lösen. Der Fokus wird aber hier nicht darauf gelegt, dass ein Ansprechpartner (also das Call-Center) da ist, der quasi auf das Kind aufpasst, sondern dass direkt erzieherische Konfliktbereiche, wie gegenseitiges Vertrauen oder das Treffen und Einhalten von Absprachen, durch das System elegant um-

[362] vgl. Trackyourkid 2005d

schifft werden sollen. Dies ist ein Konzept, das aus pädagogischer Sicht als ausgesprochen kontraproduktiv beurteilt werden muss.

In der Vermarktung des Produktes steht die *Sicherheit* im Vordergrund. Trackyourkid bedeutet hier: „Ein Plus an Sicherheit im Lebensraum ihrer Kinder“ oder „Eine ganz neue Art der Sicherheit“. Es ist eine „sanfte und sichere Kontrollmöglichkeit“. Hier hebt das Produkt auf die Ängste der Eltern ab, ihrem Kind könnte etwas zustoßen und verspricht durch Ortung des Kindes, diese Ängste gar nicht erst aufkommen zu lassen. Aus Sicht des Geschäftsführers der Betreiberfirma dient das Produkt dazu, den Eltern die Sorge darüber zu nehmen, wo sich ihr Kind gerade befindet und ihnen ein Gefühl der Sicherheit zu vermitteln. Diese Formulierung tauchte bereits in der Fallstudie zur Videoüberwachung in der KVB auf, in der bereits deutlich wurde, dass Sicherheit im Vorfeld nie herzustellen ist. Ähnlich verhält es sich auch mit dem Einsatz des Handys zur Ortung eines Kindes. Sicherheit für das Kind kann so nicht geschaffen werden. Eventuell dient das System dazu, ein Kind, das vermisst wird, zu finden. Es hilft ihm aber nicht, mit gefährlichen Situationen fertig zu werden und sich richtig zu verhalten. Dies kann nur eine entsprechende Erziehung leisten.

Das System soll den Eltern Informationen darüber liefern, wie Teubner es formuliert, ob das Kind sich so verhält, wie die Eltern dies möchten. Statt auf Kommunikation wird hier auf Technik gesetzt, die tief in das Vertrauensverhältnis zwischen Eltern und Kind eingreift. Es bleibt, laut Teubner, den Eltern überlassen, ob sie ihrem Kind per SMS mitteilen, dass sie es geortet haben, eine *verdeckte* Überwachung ist also auch möglich. Ein bisschen erinnert diese Vorgehensweise an das Foucault`sche Panoptikum – aufgrund der Tatsache, dass man weiß, dass man jederzeit überwacht werden *könnte*, verhält man sich konform. Pädagogisch fragwürdig ist an dieser Stelle, was für Auswirkungen dies auf die Persönlichkeitsentwicklung eines Menschen haben kann.

Herr Teubners eigene Erfahrungen mit der Praxis zeigen die Grenzen des Systems sehr deutlich auf und sind gleichzeitig ein Spiegel, welche Hoffnungen und Erwartungen die Eltern in die Nutzung des Systems setzen. Bei der Technik-Hotline meldeten sich beispielsweise Eltern, die besorgt sind, weil ihr Kind nicht nach Hause kam oder eine Mutter, die Angst vor einer drohenden Kindesentführung durch den Vater hatte und sich in Trackyourkid eine Lösung ihres Problems erhoffte. Hier wird deutlich, dass die geweckten Erwartungen nicht erfüllt werden können; statt Sorgen zu nehmen, werden neue geschaffen, wenn das Kind nicht nach Hause kommt, in einem Bereich geortet wird, wo es eben *nicht* sein sollte oder das Handy schlicht ausgeschaltet hat. Sicherheit kann das System nicht herstellen, wie auch die Videoüberwachung in der KVB dies nicht vermag. Die Probleme bleiben erzieherische und sind auch nur auf dieser Ebene zu lösen.

Aus Sicht von Herrn Teubner ist die Kritik der Datenschützer in Richtung Gläserner Mensch und Überwachungsstaat durchaus berechtigt. Nicht nur Bürgerrechte sind hier tangiert, sondern auch Kinderrechte, denen ein besonderer Schutz zuerkannt werden muss. Herrn Teubners Bemerkung, dies sei der Lauf der Technik, man werde immer gläserner, schließt an die Theorie der Surveillance und Maximum Surveillance Society an, in denen die Überwachung quasi als *natürliche* Folge der Informationsgesellschaft gesehen wird. Dieser Umstand macht ein weiteres Mal auf die Dringlichkeit einer Auseinandersetzung mit dem Thema innerhalb der Pädagogik aufmerksam.

Die potenziellen Adressaten der Technik haben recht unterschiedliche Ansichten, in der Mehrheit lehnen sie ein System wie Trackyourkid aber ab. Sie stellen beispielsweise heraus, dass es keine hundertprozentige Sicherheit geben könne und das Produkt ein Versuch sei, mit der Sorge der Eltern Geschäfte zu machen. Ferner betonen einige die Verantwortung der Gesellschaft und lehnen eine Abgabe der Verantwortung an Überwachungsapparate ab. In der Mehrheit setzen die Gesprächsteilnehmer auf erzieherische Lösungen und gesellschaftliche Solidarität bei der Kindererziehung. Mit Hilfe der technischen Systeme würden Opfertypen geschaffen, die permanent überwacht werden und somit nicht selbständig werden können, auch der Überwachungsstaat wird als Bild entworfen. Eine Mutter betont, dass es auch für die Eltern wichtig sei, nicht alles kontrollieren zu können, sondern zu lernen, dem Kind Stück für Stück Eigenverantwortung beizubringen. Dies würde durch den Einsatz des technischen Kontrollsystems unterwandert.

Die Minderheit, die sich für einen Einsatz des Systems ausspricht, sieht zum einen eine bequeme Art der Kontrolle darin, die man dem Kind ja gar nicht mitteilen müsse, die einem selbst aber die Sorge um das Kind nehmen könnte. Bedenken, eine Überwachung zu verheimlichen, bestehen hier nicht. Kinder hätten nach Ansicht eines Vaters in Zusammenhang mit Straftaten gerettet werden können, hätten sie ein entsprechendes Gerät bei sich gehabt.

Vorteile des Systems werden zum anderen bei chronisch Kranken oder behinderten Kindern gesehen, denen durch die Mitgabe eines solchen Überwachungsgerätes mehr Autonomie zugesprochen werden könnte.

Die Mehrheit der potenziellen Adressaten setzt auf Lösungen, die sich im zwischenmenschlichen und erzieherischen Bereich bewegen. Technische Systeme werden hier als Scheinlösungen abgetan und als der Erziehung abträglich interpretiert. Es gibt aber auch Stimmen, die sich eine Verringerung ihrer Ängste erhoffen und keinerlei Bedenken beim Einsatz haben. Die bereits zum Zeitpunkt des Interviews mit Herrn Teubner recht hohe Zahl an KundInnen des Systems zeigt aber, dass das Produkt seine Abnehmer findet und technische Lösungen dankbar als Ersatz oder Ergänzung für Erziehung gesehen werden. Dass diese Lösungen aber

nur Scheinlösungen darstellen und eine pädagogische Intervention nicht ersetzen können, wurde gezeigt.

4.6 Zusammenfassende Einschätzung der Fallstudien

Bereits durch die Basiserhebung mit der Datenschutzbeauftragten Frau Sokol wurden Eckpunkte der Interpretation der Fallstudien gelegt. Da es *ein* Ziel der Arbeit ist, Konsequenzen für eine Pädagogik zu erarbeiten, die sich einer freiheitlich-demokratischen Grundordnung verpflichtet fühlt, schien es geboten, die Perspektive der Grund- und Bürgerrechte in dieser Form in die Arbeit mit aufzunehmen.

Das Thema *Sicherheit* konnte in allen Fallstudien in der einen oder anderen Form angetroffen werden. Der Versuch der Herstellung von Sicherheit – und damit aktuell zusammenhängend die Terrorismusbekämpfung - ist aus der Sicht der Datenschutzbeauftragten ein Anlass für den Abbau von Grundrechten, die das Fundament unserer Demokratie bilden. Dabei spielen die Möglichkeiten technischer Kontroll- und Überwachungssysteme eine immer größer werdende Rolle. Frau Sokol plädiert hier für ein Hinterfragen der Notwendigkeiten eines Grundrechteabbaus.

Im Falle der Kölner Verkehrsbetriebe ist das Thema Sicherheit ebenfalls Motivation zur Einführung der Videoüberwachung in den Fahrzeugen der KVB. Hier wurde innerhalb der Fallstudie deutlich, dass Sicherheit durch die Installation der Videoüberwachung nicht hergestellt werden kann. Die Kameras vermitteln ein *Gefühl von Sicherheit*, können das Image der KVB in der Öffentlichkeit verbessern und eventuell eine abschreckende Wirkung haben. Sicherheit kann aber, so betont auch Herr Berger, in keinem Fall durch die Kameras hergestellt werden. Dennoch ist das Argument der Sicherheit ein so wirkungsvolles, dass die Überwachung bei den Fahrgästen in der Mehrheit eine hohe Akzeptanz findet, auch wenn die Funktionsweise der Kameras in den meisten Fällen falsch eingeschätzt wird.

Im Falle Payback ist das Thema Sicherheit erst auf dem zweiten Blick zu finden; es zeigt sich im Interesse z.B. zum Zwecke der Terrorismusbekämpfung Daten über Bürger zu sammeln und auszuwerten – hier wurde das Information Awareness Office der US-Regierung vorgestellt. Die Daten harmloser Konsumenten können so in die Maschinerie der internationalen Terrorismusbekämpfung geraten, wie Herr Weber es schon bei der Weitergabe der deutschen Flugdaten an US-amerikanische Behörden, bemängelte. Der von Frau Sokol gebrachte Hinweis, dass Ziele sich ändern können und Datensammlungen in großer Masse und über einen längeren Zeitraum immer auch Möglichkeiten des Missbrauchs in sich bergen, nimmt hier Gestalt an.

Bei den Ortungssystemen für Kinder tritt das Thema *Sicherheit* wieder ganz offenkundig zu Tage, denn hier ist die vermeintliche Sicherheit des Kindes das Hauptverkaufsargument. Ähnlich wie in der KVB-Fallstudie scheint es hier aber auch eher um ein Gefühl der Sicherheit zu gehen denn um eine tatsächliche Sicherheit für das Kind. In einer Gefahrensituation bieten die Systeme keinerlei Sicherheit, ein Auffinden des Kindes in einer Notsituation scheint zwar möglich, ist bei der Ungenauigkeit des derzeit auf dem Markt erhältlichen Systems Trackyourkid aber auch kritisch zu betrachten. Sorgen und Ängste der Eltern werden in der Praxis eher noch verstärkt, wenn das Kind sich nicht dort aufhält, wo es sein sollte oder das Handy schlicht ausgeschaltet ist.

Ein weiteres Ergebnis, das sich innerhalb der Fallstudien zeigt, ist die relativ hohe *Akzeptanz der Kontroll- und Überwachungssysteme*, die sich nahezu selbstverständlich im Alltag etablieren konnten. Außer bei den Kinderortungssystemen, die noch keine hohe Verbreitung gefunden haben und relativ neu auf dem Markt sind, werden die Systeme von den Adressaten entweder recht positiv bewertet oder es wird die Meinung vertreten, dass es ohnehin egal sei, da man sowieso überall überwacht werde. Der Wert der persönlichen Daten wird allgemein gering geschätzt - man ist ja nur eine/r unter Millionen – zugunsten eines vermeintlichen Zugewinns an Sicherheit werden persönliche Daten der eigenen Person oder die der Kinder herausgegeben.

Die Entstehung des *Gläsernen Bürgers* lässt sich daher innerhalb der Fallstudien durchaus erkennen. Frau Sokol formulierte bereits, dass der Staat die Unschuldsvermutung gegen seine Bürger mittlerweile modifiziere, indem er möglichst viele Daten zu sammeln versucht, als sei jede und jeder eben *nur noch nicht verdächtig*. Die *Kultur des Misstrauens*, die sie beschreibt, birgt den Wunsch, jeden und jede möglichst transparent zu machen und möglichst viele Informationen über die einzelne Person zu sammeln. Dazu trägt letztlich auch die Videoüberwachung bei, die in Ländern wie Großbritannien dazu genutzt werden kann, einzelne Personen auf ihren Weg durch eine Innenstadt zu verfolgen und so Gewohnheiten und Verhaltensmuster auszuwerten. Mit Payback wird das Konsumverhalten der Bürger gläsern und auswertbar. Wann hat eine Person was zu welchem Preis gekauft? Ist sie interessant für ein Unternehmen und *lohnt* sich dieser Kunde überhaupt? Welches Marketing muss bei dieser Person angewendet werden, um sie zu einer Kaufentscheidung zu bewegen? Eventuell können auch Aufschlüsse über verdächtiges Verhalten aus den Konsumdaten gezogen werden. Wieso kaufte Person X zehn identische Aluminiumkoffer? Plant er oder sie eventuell einen Anschlag?

Auch bei den Kindersicherungssystemen wird der Mensch immer gläserner. Beim Produkt Leonie konnten Angaben über soziales Umfeld, Krankheiten und Lieblingsessen dem Call-Center anvertraut werden. Auch wenn dies beim derzeit auf

dem Markt erhältlichen Produkt Trackyourkid nicht im System integriert ist, ist doch schon von Kindesbeinen an klar: Meine Wege sind nachvollziehbar, ich kann mich nicht unkontrolliert bewegen: Ein Foucault`sches Panoptikum von Kindesbeinen an, das Kinderrechte völlig mißachtet.

Für die Fallstudien über die KVB und die Kinderortung lässt sich ferner sagen, dass hier soziale Probleme durch technische Kontroll- und Überwachungssysteme gelöst werden sollen. In den Fahrzeugen der Kölner Verkehrsbetriebe ist es das von Herrn Berger beschriebene *Weggucken* der Menschen bei Straftaten oder Vandalismus, dem die Videokameras als allzeit bereite *Hingucker* entgegengesetzt werden. Die Kinderortungssysteme dienen dagegen zum einen als Beruhigung für die Eltern, die nun immer sehen können, wo ihr Kind sich befindet, zum anderen als Lösung bei Erziehungsproblemen. So wurde das Produkt als Möglichkeit zur Umgehung von Konflikten mit dem Kind angepriesen, wenn dieses sich durch ständiges Nachfragen der Eltern, wo es denn gewesen sei, mal wieder *genervt* fühlt. Ferner soll das Produkt dazu dienen, Vertrauen zu gewähren, welches auch verdient ist. Die Eltern können also über das technische Gerät erst einmal überprüfen, ob das Kind ihr Vertrauen verdient hat. Die ist eine aus pädagogischer Sicht fragwürdige Methode der Vertrauensbildung.

Teil III: Ergebnisse und Folgerungen der Arbeit

5 Resümee und Ausblick

Die vorliegende Arbeit hat die wachsende Verbreitung technischer Kontroll- und Überwachungssysteme in unserem Alltag analysiert und vorhandene gesellschaftstheoretische Modelle vorgestellt, die Ansätze zu ihrer Erklärung bereitstellen. Insbesondere der Aspekt der *freiwilligen* Nutzung solcher Systeme durch die Bürger wurde berücksichtigt.

In der Praxis ging es darum zu schauen, welche Aufgaben die technischen Kontroll- und Überwachungssysteme bereits übernehmen. Außerdem wurde ein Augenmerk darauf gelegt, welche Konsequenzen sich daraus für die Erziehungswissenschaft ergeben.

Aufgrund der Vielschichtigkeit des Themas lässt sich nicht die *eine* Antwort geben. Die Arbeit hatte das Ziel, gerade die Vielfalt darzustellen in der uns technische Kontrolle und Überwachung entgegentritt. Sie stellt eine erste Auseinandersetzung mit dem Thema dar: Sie gibt einen Überblick, der angesichts der Allgegenwart der technischen Kontrolle mehr als angebracht ist, sie stellt derzeit international diskutierte Theorien zu Kontrolle und Überwachung ebenso vor wie exemplarische Praxisfelder und unternimmt den Versuch, eine Erklärung für das Phänomen zu finden. Dabei zeigt sie Bereiche auf, in denen eine Pädagogik eingreifen muss, die den Anschluss an die sich verändernde, zunehmend technisierte Gesellschaft nicht verpassen will.

Die theoretischen Ergebnisse der Arbeit bewegen sich zwischen den Gedankengebäuden Ulrich Becks und Michel Foucaults, auf die auch die derzeit diskutierten Ansätze zu Kontrolle und Überwachung rekurrieren.[363] Anhand der Analyse Becks konnte deutlich gemacht werden, warum sich technische Kontroll- und Überwachungssysteme immer mehr in der Gesellschaft verbreiten: Die Risikogesellschaft und ihr normativer Entwurf der Sicherheit bedarf eines Risikomanagements – z.B. in Form technischer Kontroll- und Überwachungstechnik -, das allerdings selbst wieder Risiken hervorbringt. Die Analyse Foucaults zeigte auf, warum das Individuum von sich aus diese Systeme einsetzt: Es hat sein Verhalten an die Gouvernementalisierung der Gesellschaft angepasst und wird dazu angehalten, sich selbst an der Produktion von Sicherheit zu beteiligen.

Innerhalb der theoretischen Betrachtung des Themas wurde deutlich, dass sich die westlichen Gesellschaften, nicht zuletzt nach dem 11. September 2001 in einem

[363] In den folgenden Ausführungen wird deutlich werden, dass innerhalb der Arbeit keiner der vorgestellten Gesellschaftsbezeichnungen ein Vorzug gegeben wird. Aus Sicht der Autorin existieren Merkmale der Risiko-, Kontroll-, Sicherheits- und Maximum Surveillance Society nebeneinander. Ein allumfassendes Gesellschaftsmodell wird innerhalb einer postmodernen Gesellschaft in Zweifel gezogen.

permanenten Ausnahmezustand befinden. Die Herstellung von Sicherheit ist hier dominantes Motiv einer Risikogesellschaft, hinter dem auch Grundrechte des Bürgers zurückstehen. Das Verhältnis Staat / Bürger wandelt sich. Wie die nordrhein-westfälische Datenschutzbeauftragte Bettina Sokol es formuliert hat: Jede/r ist nur noch nicht verdächtig. Auch das Private wird Ort sicherheitspolitischer Intervention. Sicherheit wird zum Ziel einer Gesellschaft, die sich nicht mehr auf ein gemeinsames Wertedach stützen kann und in welcher der Staat sich aus einem wohlfahrtsstaatlichen Engagement zurückzieht und seine Kernkompetenz im Schaffen von Sicherheit etabliert. Dabei sind frühere Formen der Disziplinierung und Kontrolle nicht mehr zeitgemäß und werden schrittweise durch neue, eben auch technische, ersetzt.

Auch ureigenste pädagogische Themen, wie z.B. Fragen der Disziplinierung, sind davon, wie im empirischen Teil deutlich wurde, berührt. Die (sozial-) pädagogische Intervention geht zurück, wenn in einem sich verändernden Strafrecht nicht mehr versucht wird, Delinquente zu re-integrieren, sondern Kriminalität als dazugehörend akzeptiert wird und – wie de Marinis[364] es formulierte – In- und Out-Zonen geschaffen werden, in denen bestimmte Dinge geduldet oder eben nicht geduldet werden. Es besteht weder die wirtschaftliche Notwendigkeit noch der moralische Druck, die Ausgeschlossenen wieder in die Gesellschaft zu integrieren, wie es der Ansatz der Kontrollgesellschaft zeigt. Durch die dort beschriebene Fragmentierung der Gesellschaft in In- und Out-Zonen ist eine Integration bestimmter Bevölkerungsgruppen nicht mehr nötig. Sie fallen schlicht aus der Gesellschaft heraus, denn technische Kontroll- und Überwachungssysteme können hier in Verbindung mit Computertechnologie vermeintlich Konformität, Sicherheit und Ordnung herstellen. Es wäre wichtig, gerade diesen Aspekt auch innerhalb der Sozialpädagogik stärker zu berücksichtigen.

Wissen über den Einzelnen wird innerhalb eines solchen Regimes elementar. Technische Kontroll- und Überwachungssysteme tragen dazu bei, Informationen zu sammeln, und sie dringen dabei – wie empirisch belegt wurde – in vielfältige Bereiche des Lebens ein, was die Privatsphäre nicht unberührt lässt. Das Wissen über den Einzelnen führt zu einem Konformitätsdruck, wie er bereits in Foucaults Panoptikum beschrieben wurde. Der Konformitätsdruck wird immer größer, je mehr Daten über eine Person aus unterschiedlichsten Bereichen gesammelt wurden. Wie Frau Sokol es befürchtet, kann es so zu Verhaltensanpassungen kommen, die letztlich das Grundrecht auf Informationelle Selbstbestimmung und somit die Grundpfeiler der Demokratie unterwandern.

Parallel dazu weisen einige Autoren darauf hin, dass auch die Medien von sich aus Veränderungen bewirken und somit innerhalb der bestehenden Informations-

[364] siehe Kapitel 2.2.2

gesellschaft mit ihren globalisierten und entpersonalisierten Kontakten ein gewisses Maß an Überwachung mit sich bringen. Die Frage, mit wem man es eigentlich genau zu tun hat, wird bei weltweiten Datenströmen, wirtschaftlicher und politischer Verflechtungen und (Reise-) Freizügigkeiten der Bürger fast automatisch zu einer bedeutenden, die man mit Hilfe wachsender Datensammlungen zu beantworten sucht. Technik existiert allerdings niemals im luftleeren Raum – sie wird von Menschen entwickelt und genutzt, um eine bestimmte Intention zu verfolgen – man ist ihr also nicht hilflos ausgeliefert. Diese Hintergründe aufzudecken und kritisch zu diskutieren, ist nicht zuletzt Aufgabe einer Pädagogik, die sich den Herausforderungen der technisierten Gesellschaft stellt. Hier wird auch die Frage interessant, in wessen Händen die Datensammlungen liegen und welche Machtmechanismen in der heutigen Gesellschaft wirken.

Wie Foucault zeigte, bewirkte der Wechsel in das Zeitalter der Gouvernementalität, dass Sicherheitstechnologien an Bedeutung gewinnen und als dominanter Mechanismus der Regierung zu identifizieren sind. Sie dienen letztlich dazu, die Bevölkerung zu kontrollieren, einen bestimmten Gebrauch von Freiheit zu garantieren und eine kollektive Imagination von Risiken und deren Abwehr zu produzieren. Das Subjekt selbst ist angehalten, Verantwortung zu übernehmen und sich an der Produktion von Sicherheit zu beteiligen. Der Sicherheitsdiskurs beherrscht die Gesellschaft und führt auch bei jedem Einzelnen zum Bemühen, Sicherheit herzustellen.

Zusammenfassend kann also für den theoretischen Teil erklärt werden, dass technische Kontroll- und Überwachungssysteme sich vermutlich aufgrund der Bedingungen einer Risikogesellschaft und den damit zu verhindernden Risiken immer stärker etablieren, da schlicht *Angst*[365] die Gesellschaft durchzieht. Gleichzeitig kommt es unter den Bedingungen einer Informationsgesellschaft zu einem fast automatischen Bedürfnis, zu wissen, mit wem man es zu tun hat. Aufgrund der sich weltweit ändernden Regierungsformen kommt es zu einer Gouvernementalisierung, einer Ökonomisierung des Sozialen und im Rahmen neoliberaler Strömungen zu einer wachsenden Verantwortung des Einzelnen. Dieser ist somit auch am obersten Ziel der Gesellschaft - Sicherheit herzustellen – aktiv beteiligt und versucht auf seine Weise, den Risiken zu begegnen.

Im empirischen Teil der Arbeit ging es darum, explorativ zu erkunden, welche Bereiche des täglichen Lebens bereits vom Einsatz der technischen Kontroll- und Überwachungssysteme durchdrungen sind und wo diese vom Individuum freiwil-

[365] Ob es sich dabei um eine tatsächlich begründete oder eine (medial) vermittelte Angst handelt sei dahingestellt.

lig eingesetzt werden. Dabei konnten mehrere Aspekte des theoretischen Teils bestätigt werden:

Die Videoüberwachung hat im Laufe der letzten Jahrzehnte ihre Einsatzbereiche zunehmend erweitert. War sie in den 50er Jahren erstmals in der Verkehrsüberwachung zu finden, kam in den darauf folgenden Jahrzehnten die Überwachung von so genannten *Kriminalitätsschwerpunkten* und *Angsträumen* hinzu. In heutiger Zeit wird sie auch in Schulbussen, auf Schulhöfen oder im Kinderzimmer eingesetzt. Auch bei den Ortungstechniken kann man eine Entwicklung von der Verwendung als Navigationssystem im Auto oder bei der Erhebung der LKW-Maut in Deutschland bis hin zur Verwendung in Kinderortungssystemen, die sogar implantiert werden können, beobachten. Kundenbonuskarten haben sich seit ihrer Einführung Anfang 2000 rasant verbreitet, und der Marktführer Payback ist nach eigenen Angaben derzeit in 27 Millionen Kundenportemonnaies vertreten. Die Kundenbonuskarten scheinen auf dem ersten Blick keine Verbindung zum Thema Sicherheit zu haben. Bei näherem Hinsehen fällt allerdings auf, dass sie einen Baustein in der wachsenden Transparenz des Bürgers darstellen, dessen persönliche Daten mittlerweile in unzähligen Datenbanken weltweit auftauchen können. Daten über den Konsum von Menschen können nämlich, wie am Beispiel des Information Awareness Office gezeigt wurde, sehr wohl interessant im internationalen Bemühen um Sicherheit und Terrorismusbekämpfung sein.

Es lässt sich also festhalten, dass technische Kontroll- und Überwachungssysteme derzeit in nahezu allen Bereichen des täglichen Lebens – im öffentlichen Leben, im Konsumalltag, wie im privaten Familienalltag – vorkommen. Der freiwillige Einsatz erfolgt hier, wie es auch in der Theorie bereits herausgestellt wurde, unter dem Vorzeichen der Sicherheit oder, wie bei Payback, aus der Motivation heraus, Geld sparen oder eine Prämie erhalten zu wollen.

Bei der genaueren Betrachtung des Einsatzes der Systeme vor Ort konnte bei der Fallstudie zur Videoüberwachung innerhalb der Kölner Verkehrsbetriebe herausgefunden werden, dass die Installation der Videokameras die Aufgabe hat, Sicherheitsgefühle zu vermitteln, die nicht unbedingt etwas mit der tatsächlichen Sicherheitslage zu tun haben müssen, wie die vorgestellte Studie der Kölner Polizei illustrierte.[366] Von Seiten des Unternehmens bedeutet die Installation von Videokameras in erster Linie einen Imagegewinn, da das Thema Sicherheit stark im Fokus der öffentlichen Wahrnehmung steht.

Von einer strengen Prüfung, ob die Videoüberwachung unbedingt erforderlich ist, wie sie Frau Sokol erwähnte, war in der Praxis eher wenig zu spüren. Hier machte

[366] siehe Kapitel 4.3.1

es eher den Anschein, Ziel sei es, möglichst viele Fahrzeuge der KVB mit Videoüberwachung auszustatten.

In der Praxis sollen Videokameras die Illusion von Sicherheit vermitteln und eben auch das Gefühl, dass jemand da ist, wenn etwas passiert. Leider ist die Videoüberwachung nicht in der Lage, eine wirkliche Hilfestellung bei einem Verbrechen zu sein. Sie kann nur dokumentieren was passiert, nicht aber in der konkreten Situation Hilfe leisten. Somit hält die untersuchte KVB-Überwachung nicht, was sie verspricht, denn die tatsächliche Sicherheit der Fahrgäste kann durch sie nicht erhöht werden. Sicherheit lässt sich, wie auch Herr Berger – der Pressesprecher des Unternehmens - es formuliert, in keinem Fall herstellen.[367] Ein anderer Punkt ist die von Herrn Berger bemängelte Zivilcourage der Fahrgäste – hier werden die Videokameras zu Hinguckern, wo Menschen wegschauen. Eigentlich hat man es im Falle der KVB also mit einem sozialen Problem zu tun, das auch auf dieser Ebene gelöst werden müsste; stattdessen versucht man es mit technischen Mitteln, die aber den Kern des Problems nicht berühren.

Die falschen Erwartungen an die Videoüberwachung werden auch in der Befragung der Fahrgäste deutlich: Die Mehrheit erwartet hier eine Intervention durch Personal, im Falle eines Vorfalls, sie vermutet, dass der Fahrer oder die Leitstelle der KVB die Videoaufzeichnungen direkt auswerten. Für sich selbst stellen die befragten Personen keine Steigerung ihres Sicherheitsgefühls fest, bewerten aber Videoüberwachung gerade für ältere Menschen oder in Notsituationen als positiv. Das potenzielle Risiko reicht hier aus, um eine Kameraüberwachung zu befürworten; wenn man nicht an das eigene Risiko für sich selbst denkt, dann hat man immerhin noch das seines Nächsten im Blick. Die Kameras werden über das Argument eines Zugewinns an Sicherheit in den Bahnen installiert und von den Kunden aufgrund des Risikos, dass etwas passieren könnte, akzeptiert. Um den vorhandenen Problemen wirklich begegnen zu können, sollte man die Kameras aber als das sehen, was sie sind: Dokumentarsysteme von Ereignissen, die nur durch menschliches Eingreifen verhindert werden könnten. Dies gilt es klarzustellen, um eine wirkliche Verbesserung der Sicherheitslage zu erreichen. Ein falsches Verständnis von Sicherheit hilft hier keinem.

Im Falle der Kundenbonuskarten wird deutlich, dass hinter dem vermeintlich harmlosen Rabattpunkte sammeln mehr stehen kann, als man zu Anfang vermutet. Das anhand des Payback-Systems vorgestellte Datamining macht es möglich, den Kunden in seinem Kaufverhalten für das Unternehmen transparent zu machen. So kann, wie im Falle Payback, genau erfasst werden, mit wem man es zu tun hat und das Marketing und das Sortiment an den Kunden angepasst werden. Das auch von anderen Firmen verfolgte Datamining kann aber, das hat das Beispiel des Custo-

[367] siehe Kapitel 4.3.3

mer Relationship Managements[368] gezeigt, auch zu Diskriminierungen führen, die weniger umsatzstarke Konsumenten entsprechend klassifizieren und diese bei bestimmten Serviceleistungen, Angeboten etc. entsprechend hinten anzustellen. Interesse des Unternehmens ist natürlich, konsumstarke Kunden zu binden und andere abzustoßen. Datamining kann so Informationen zusammentragen, die zum einen etwas über die Vorlieben des Kunden aussagen, aber auch bis zur Einschätzung der Kreditwürdigkeit einer Person aufgrund ihres Profils gehen. Hier betonte bereits Frau Sokol die Tendenz in der Gesellschaft, sich nicht mehr auf die Angaben des Einzelnen zu verlassen und immer mehr auf die gesammelten Informationen Dritte zurückzugreifen; sie fasste dies unter dem Begriff der „Kultur des Misstrauens“ zusammen.

Nach Einschätzung der Datenschutzbeauftragten bergen Datensammlungen die Gefahr, dass Menschen aufgrund der über sie gesammelten Daten manipulierbar werden. Die hohe Verbreitung, beispielsweise des Payback-Systems mit 27 Millionen Karten, verdeutlicht, dass sich eine wachsende Zahl von Menschen des Wertes ihrer Daten nicht mehr bewusst sind und viele das System positiv bewerten. Reg Whitaker, ein kanadischer Politologe vermerkt dazu, dass das Verbraucherpanoptikum seine Teilnehmer belohnt[369] und ihnen das Leben angenehmer zu machen scheint. Die Befragung der Payback-Kunden zeigte auch eine grundsätzliche Zufriedenheit mit dem System. Auch wenn fast die Hälfte der NutzerInnen als Nachteil die Entstehung des „Transparenten Kunden“ angaben, wurde dies nicht zum Anlass genommen, nicht am System teilzunehmen, sondern es wurde mehrmals eine resignative Haltung eingenommen, indem formuliert wurde, dass man ohnehin schon überall überwacht würde.

Durch die zentrale Sammlung von Daten und deren langfristige Speicherung ergibt sich die Gefahr, dass die Datensammlungen im Laufe der Zeit anderen Zielen untergeordnet werden, als denen, denen sie zu Anfang zugeordnet waren. Ein Beispiel ist hier das US-amerikanische Information Awareness Office, dessen Ziel es ist, ein Computersystem zu entwickeln, dass beispielsweise auch kommerzielle Transaktionen nach Mustern durchsuchen soll, die auf terroristische Aktivitäten hindeuten. In diesem Falle wären alle unter einen Generalverdacht gestellt, wie es bereits durch Feely und Simon[370] im Theorieteil der Arbeit dargestellt wurde. Unter der Prämisse der Sicherheit werden hier auch private Konsumdaten oder, wie Herr Weber es als Beispiel anführte, Passagierflugdaten interessant.

Der Einsatz von Ortungssystemen im familiären erzieherischen Bereich macht die beschriebenen Veränderungen innerhalb der Gesellschaft und ihre Auswirkungen

---

[368] siehe Kapitel 3.2

[369] vgl. Whitaker 1999, S. 179

[370] siehe Kapitel 1.4.3

auf die Erziehung besonders deutlich. Hier lässt sich erkennen, wie der Sicherheitsdiskurs sich auch innerhalb des Privaten etabliert und bereits direkte Auswirkungen auf erzieherische Prozesse genommen hat. Das Produkt Leonie stellte dabei auf berufstätige Eltern ab, denen mit dem System eine Art technisierter Babysitter zur Verfügung gestellt werden sollte.

Die Kopplung aus der Ortung des Kindes und dem Call-Center, bei dem das Kind anrufen kann, wenn es ein Problem hat, ging über die bloße Standortermittlung des Kindes hinaus. Hier wurde neben dem Wissen über den Aufenthaltsort des Nachwuchses auch die Möglichkeit bereitgestellt, einen Ansprechpartner für es zu haben, wenn die Eltern dies z.B. aufgrund ihrer beruflichen Situation nicht mehr selbst sein können. Dem Call-Center wurden von den Eltern persönliche Daten ihres Kindes wie die Namen der Freunde, das Lieblingsessen oder etwaige Krankheiten zur Verfügung gestellt und in einer Datenbank gespeichert. Zugunsten eines versprochenen Zugewinns an Sicherheit waren die Eltern bereit, sehr persönliche Daten ihrer Kinder preiszugeben und einem Konzern anzuvertrauen.

Sicherheit ist also auch hier wieder das Motiv, das Menschen dazu bewegt, ihre Daten und auch die ihrer Kinder preiszugeben. So gelangen schon in frühesten Jahren Informationen in zentrale Datenbanken, die dort eigentlich nicht hingehören und zur Erstellung von Profilen des Individuums führen. Bedenklich ist hier auch die frühe Gewöhnung des Kindes an Überwachungssysteme, die unter der Prämisse der Sicherheit vermarktet werden und somit zu einer leichteren Akzeptanz führen, als wenn sie unter anderen Vorzeichen eingesetzt würden. Selbst die Möglichkeit, das Kind über das Call-Center zu belauschen – vom Hersteller als Listen-In-Funktion vermarktet – ist kein Tabu mehr, wenn es um eine vermeintliche Erhöhung der Sicherheit des Nachwuchses geht. Vom Hersteller wird versucht, eine technische Lösung für soziale Probleme zur Verfügung zu stellen, ein Motiv, das auch schon beim Einsatz der Videoüberwachung zum Tragen kam, und auch im vorliegenden Fall kritisch - möglicherweise sogar noch kritischer, weil es in den ureigensten privaten Bereich, den von Familie und Kindeserziehung, hineinreicht - gesehen werden muss.

Die bereits ein halbes Jahr nach dem Verkaufsstart recht hohe Anzahl der NutzerInnen[371] des zweiten Systems mit Namen Trackyourkid verdeutlicht, dass es anscheinend einen hohen Bedarf an einer solchen Art der Kontrolle gibt.

Anders als das System Leonie verzichtet Trackyourkid auf den Einsatz von GPS und stellt die daraus resultierende Ungenauigkeit des Systems als „Vertrauensbonus an das Kind“ dar. Die Sicherheit des Kindes ist auch hier Verkaufsargument Nummer eins und unterstreicht noch einmal, dass der Sicherheitsdiskurs im Priva-

[371] nach Angaben des Herstellers 7000 Personen

ten angekommen ist. Aus der Perspektive des Kindes entsteht hier so etwas wie ein Foucault`sches Panoptikum, denn das Kind muss sich immer darüber im Klaren sein, dass Abweichungen vom erwünschten Verhalten über das technische System bemerkt werden und den Eltern nicht verborgen bleiben. Vertrauen soll – so wurde es vom Hersteller formuliert – Stück für Stück da geschenkt werden, wo es auch verdient wurde.

Die Pädagogik muss hier erst recht Stellung beziehen, denn im Falle von Leonie und Trackyourkid geht es um den Kernkompetenzbereich der Pädagogik: die Erziehung. Der durch diese Systeme entstehende Konformitätsdruck ist nicht mehr moralisch legitimiert, sondern schlicht wird über das Vorhandensein technischer Kontrollsysteme vermittelt. Dieses Phänomen wurde bereits innerhalb des theoretischen Teils formuliert: Die Kontrolle legitimierte sich z.B. im Ansatz der Kontrollgesellschaft nicht mehr über die Moral, sondern über die Sicherheit, ein Trend, der sich im familiären Umfeld ebenso wie in anderen gesellschaftlichen Bereichen zeigt. Die technischen Kontrollsysteme ermöglichen nicht nur diese andere Art der Kontrolle, sie setzen vielmehr Erziehungswerte, indem sie als neuer Erziehungsmaßstab fungieren und die totale Kontrolle propagieren.

Aus den Berichten des Geschäftsführers von Trackyourkid, Herrn Teubner, wurde jedoch abermals deutlich, dass die bestehenden Probleme mit dem System nicht gelöst werden können und stattdessen neue entstehen. Soziale Probleme können auch nur auf sozialer Ebene gelöst werden und Erziehung kann und darf nicht durch Technik ersetzt werden. Dieser Meinung schloss sich auch die Mehrheit der TeilnehmerInnen der ausgewerteten Radiodiskussion zu diesem Thema an. Anscheinend gibt es aber eine nicht unerhebliche Anzahl von Leuten, die sich technischer Systeme bedient, um lästigen Erziehungskonflikten auszuweichen. Hier zeigt sich noch einmal die Wichtigkeit einer pädagogischen Intervention.

Am Beispiel der vorgestellten Kinderortungssysteme tritt die wachsende freiwillige Nutzung technischer Kontroll- und Überwachungssysteme durch den einzelnen Bürger besonders markant hervor. Selbst geheimdienstlich anmutende Systeme, wie z.B. mit Nachtsichtmodus ausgestattete Mini-Kameras für das Kinderzimmer,[372] etablieren sich zunehmend im familiären Rahmen, deren hohe Akzeptanz allein durch die Tatsache, dass dieses System bereits beim Kaffee-Röster Tchibo erhältlich ist, deutlich wird. Dieser Trend wurde bislang innerhalb der Erziehungswissenschaft nicht reflektiert und bedarf dringend einer Stellungnahme über den pädagogischen Nutzen oder die Gefahren dieser Technik. Vor allem werden hier Kinderrechte durch die technischen Systeme beschnitten. Die Dringlichkeit, mit der das Thema in die pädagogische Diskussion aufgenommen werden muss, zeigt sich an einem aktuellen Beispiel aus den Niederlanden: Ab 2007 lässt die

[372] vgl. Kapitel 3.1

niederländische Regierung Daten über jedes Kind erheben. In einer zentralen Datenbank, dem so genannten „Elektronisch Kinddossier“ sollen, von Geburt an Informationen zu Gesundheit, Bildungsweg, familiären Verhältnissen und Vorstrafen erfasst werden. Ziel sei es, dem Staat die Möglichkeit zu geben, Probleme von Kindern frühzeitig zu erkennen, entsprechend gegenzusteuern und den Informationsfluss zwischen den einzelnen Behörden zu fördern.[373] Somit wird mit Technik nicht nur versucht, soziale Probleme vordergründig zu lösen; vielmehr werden soziale Konfliktherde bereits postuliert, ehe sie überhaupt aufgetaucht wären. Wie vor der Überwachungskamera ein jeder verdächtig ist, so werden die Kinder hier pauschal zu potenziellen späteren Tätern, um den Einsatz der Datensammlung zu legitimieren.

Die voranschreitende technische Entwicklung bietet immer weitere Möglichkeiten von Kontrolle und Überwachung. Innerhalb der Bevölkerung scheint es eine große Akzeptanz dieser Systeme zu geben, die sich oftmals über das Argument einer Steigerung der Sicherheit in nahezu allen Bereichen des Alltags etablieren können. Gleichzeitig werden hier aber Grundrechte der Bürger, wie z.B. das Recht auf Informationelle Selbstbestimmung, tangiert. Selbst bei kritischen Bürgern, die um das Potenzial von Datamining und Überwachung wissen, hat sich eine Art Resignation manifestiert, die sich auf der Annahme gründet, man könne ohnehin nichts gegen die allgegenwärtige Überwachung tun.

Die wachsende Einschränkung der Bürgerrechte, das Missachten jeglicher Kinderrechte, die Verdächtigung der Bürger als potenzielle Delinquenten sowie das mangelnde Bewusstsein der Menschen über den Wert ihrer privaten Daten ergeben eine bedenkliche Mischung für die Demokratie in der von Technik durchsetzten Informationsgesellschaft. Die Erziehungswissenschaft ist angehalten, sich mit diesem Phänomen auseinander zu setzen und sie in ihren pädagogischen Konzepten zu berücksichtigen. Hier ergeben sich zukünftige Aufgaben für die politische Bildung, die Erwachsenenbildung, aber auch für die Medienpädagogik, deren Aufgabe es sein muss, einen kritischen Umgang mit neuen Medien zu vermitteln und die Tragweite der wachsenden Verbreitung technischer Kontroll- und Überwachungssysteme aufzuzeigen. Ziel einer politischen Bildung sollte es sein, den Wert privater Daten für die Demokratie zu betonen und eine kritische Öffentlichkeit für das Problem zu schaffen.

An vielen Stellen der Gesellschaft wird versucht, soziale Probleme mit Technik zu lösen; dabei werden falsche Erwartungen geweckt und Menschen wird der Glaube vermittelt, die Technik stelle die Lösung für soziale Probleme dar. Hier muss die Pädagogik aufmerksam sein, dass Erziehung nicht unter dem Vorzeichen der technischen Möglichkeiten neu definiert wird, da solche Systeme quasi das

[373] vgl. Heise 2005b und Elektronisch Kinddossier 2005

angestammte Wirkfeld der Pädagogik umformulieren und per Technik wegrationalisieren. Das heißt, nicht nur die Folgen einer technisch organisierten Kontrolle stellen ein Problem dar, sondern bereits die im Vorfeld ihrer Implementierung geweckten Erwartungen, die nämlich eine „schöne, heile Welt“ ohne Konflikte suggerieren. Wichtig wäre es an dieser Stelle, die Grenzen der Technik klar aufzuzeigen und zu verdeutlichen, dass zwischenmenschliche und soziale Probleme sich nie durch Technik bewältigen lassen, sondern diese sie nur verschieben und verlagern kann.

Dazu ist es notwendig, in der wissenschaftlichen Diskussion auf diese Punkte einzugehen und genau zu untersuchen, was die Technik und was die Pädagogik leisten kann. Die Erziehungswissenschaft muss sich also neu im Spannungsfeld der technischen Kontrollsysteme positionieren und Stellung beziehen, was Aufgabe der Technik und was Aufgabe der Pädagogik sein soll.

Das Thema Medien und deren Möglichkeiten sollte allgemein stärker innerhalb der Pädagogik aufgegriffen werden, und es muss über mögliche Folgen einer Erziehung mit Videoüberwachung und Ortungssystemen diskutiert werden. Will die Pädagogik weiterhin als jene Disziplin gelten, die vorrangig die Erziehung und die Vermittlung demokratischer Werte zum Thema hat, so muss sie als Profession Stellung beziehen und ihre bislang gepflegte Technikfeindlichkeit ablegen. Nur über einen offenen Diskurs können Vor- und Nachteile des Einsatzes technischer Kontroll- und Überwachungssysteme geklärt werden, und nur über einen gesellschaftlichen Aushandlungsprozess kann der Mensch befähigt werden, die Technik zu seinen Gunsten einzusetzen. Soziale Probleme können immer nur unter Menschen gelöst werden und nicht einer Technik überantwortet werden, die durch ein bloßes An / Aus, In / Out Normen setzt und festlegt, wer dazugehört und wer ausgeschlossen wird.

Die Informationelle Selbstbestimmung ist elementar für eine Demokratie, deren Bürger sich ohne ständige Überwachung und die Gefahr der Manipulation am politischen Geschehen beteiligen können. Darüber hinaus muss das Recht auf Privatheit und persönlicher Autonomie eines jeden - und insbesondere die Rechte von Kindern und Jugendlichen auf ein humanes Aufwachsen ohne Vorverurteilung als potenzieller Abweichler - garantiert werden. Eine offene pluralistische Gesellschaft braucht Menschen, die einer Vielfalt gegenüber aufgeschlossen und die sich der Tragweite des Technikeinsatzes bewusst sind, so dass sie verantwortungsvoll mit ihren und den Daten anderer - vor allem ihrer Kinder – umgehen.

Wissen ist bekanntlich Macht – und es geht darum, wem wir in Zukunft diese Macht einräumen und wem nicht.

Literaturverzeichnis

ADEN, HARTMUT: Europäische Polizeikooperation – Konstruktion und Wandel von Legitimationsfiguren, in: HITZLER, RONALD; PETERS, HELGE (Hrsg.): Inszenierung: Innere Sicherheit, Daten und Diskurse. Opladen, 1998, S. 65ff

ARMITAGE, RACHEL: To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime. London, 2002 http://www.nacro.org.uk/data/briefings/nacro-2002062800-csps.pdf, 20.02.2003

ASSOCIATION OF TOWN CENTRE MANAGEMENT (ATCM); http://www.atcm.org/masterframe.htm, 21.02.2003

BABYNET: http://www.baby-net.org/, 01.10.2002

BALEN, STEVE MATHEW: Management of student behavior using closed circuit television monitoring, Saint Louis University, 1997

BANNISTER, JON; FYFE, NICHOLAS; KEARNS, ADE: Closed Circuit television and the city, in: NORRIS, CLIVE; MORAN, JADE; ARMSTRONG, GARY (Ed.): Surveillance, closed circuit television and social control. Aldershot/Brookfield (USA), Singapore, Sydney 1998, S. 21ff

BARMER-Ersatzkasse: Das aktuelle Gesundheitsmagazin, Wuppertal (2004) H.1

BARTH, THOMAS: Soziale Kontrolle in der Informationsgesellschaft. Systemtheorie, Foucault und die Computerfreaks als Gegenmacht zum Panoptismus der Computer- und Multimedia-Kultur. Pfaffenweiler, 1997

BECK, ULRICH: Risikogesellschaft: Auf dem Weg in eine andere Moderne. Frankfurt, 2003

BEHRENDES, UDO: Videoüberwachung: Bewertung von Örtlichkeiten für die Installation von Videoüberwachungsanlagen im Zuständigkeitsbereich der Polizeiinspektion Mitte. Internes Schreiben, des Polizeipräsidiums Köln, ZA 321 Qualitätsmanagement. Köln, 2003

BERGER, JOACHIM: E-Mail-Befragung des Pressesprechers der Kölner Verkehrsbetriebe vom 19.01.2005 zur Anzahl der installierten Videokameras

BERTELSMANN-STIFTUNG Gütersloh: Die Terrorabwehr in Deutschland weist weiterhin Lücken auf, http://www.bertelsmann-stiftung.de/de/druck/1013_13046.jsp, 27.01.2004

BIOMETRIE-INFO: http://www.biometrie-info.de, 11.09.02

BÖLSCHE, JOCHEN: Der Weg in den Überwachungsstaat. Reinbek bei Hamburg, 1979

BOGNER, ALEXANDER; LITTIG, BEATE; MENZ, WOLFGANG: Das Experteninterview: Theorie, Methode, Anwendung. Opladen, 2002

BOURDIEU, PIERRE: Physischer, sozialer und angeeigneter Raum, o.A., in: WENTZ, MARTIN (Hrsg.): Stadt-Räume: Die Zukunft des Städtischen. Frankfurt a.M., New York, 1991, S. 25ff. (Frankfurter Beiträge; Bd.2)

BLANKENBURG, ERHARD: Präventive Sicherheitspolitik in der Großstadt, in: HAMMERSCHICK, WALTER; KARAZMAN-MORAWETZ, INGE; STANGL, WOLFGANG (Hrsg.): Die sichere Stadt: Prävention und kommunale Sicherheitspolitik. Baden-Baden, 1996, (Jahrbuch für Rechts- und Kriminalitätssoziologie 1995), S. 169ff.

BRÖCKLING, ULRICH; KRASMANN, SUSANNE; LEMKE, THOMAS: Gouvernementalität der Gegenwart: Studien zur Ökonomisierung des Sozialen. Frankfurt a.M., 2000

BUNDESVERFASSUNGSGERICHT Karlsruhe: Pressemitteilung Nr. 22/2004, http://www.bverfg.de/cgi-bin/link.pl?entscheidungen, 03.03.2004, dazu das Urteil vom 3. März 2004: 1 BvR 2378/98 und 1 BvR 1084/99

BUNDESVERFASSUNGSGERICHT Karlsruhe: BVerfGE 65, 1 – Volkszählung 1983, Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 - 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden

BUKOW, WOLF-DIETRICH; OTTERSBACH, MARKUS (Hrsg.): Die Zivilgesellschaft in der Zerreißprobe. Opladen, 1999

dies: Die Zivilgesellschaft in der Zerreißprobe, in: BUKOW, WOLF-DIETRICH; OTTERSBACH, MARKUS (Hrsg.): Die Zivilgesellschaft in der Zerreißprobe. Opladen, 1999, S. 11ff

BURCHELL, GRAHAM, et.al. (Ed.): The Foucault Effect: Studies in Gouvernementality. Hemel Hempstead (Harvester, Wheatsheaf), Chicago, 1991

BUTLER, JUDITH: Noch einmal: Körper und Macht, in: Honneth, Axel, Saar Martin (Hrsg.): Michel Foucault: Zwischenbilanz einer Rezeption. Frankfurt, 2003, S. 59

CASTEL, ROBERT: From Dangerousness to risk, in: BURCHELL, GRAHAM, et.al. (Ed.): The Foucault Effect: Studies in Gouvernementality. Hemel Hempstead (Harvester, Wheatsheaf), Chicago, 1991, 281-298

CINEBANK: http://www.cinebank-portal.de/Funktion/funktion.htm, 06.12.2002

COHEN, STANLEY: Visions of Social Control; Crime, Punishment and Classification. Cambridge (UK), 1985

CRM-FORUM: Naujoks, Frank: Kundenbindung muss sich rechnen, http://www.crmforum.de/news-archiv/archiv4104.html, 31.03.2005

DATENSCHUTZBERICHT 2003: Die Landesbeauftragte für den Datenschutz und Beauftragte für das Recht auf Information Nordrhein-Westfalen. Düsseldorf, 2003

DARPA: Total Information Awareness (TIA) System, http://www.darpa.mil/iao/TIASystems.htm, 6.12.2002

DAVIS, MIKE: City of Quartz. London, 1990

DE MARINIS, PABLO: Überwachen und Ausschließen: Machtintervention in urbanen Räumen der Kontrollgesellschaft. Pfaffenweiler, 2000

DELEUZE, GILLES: Unterhandlungen 1972-1990. Frankfurt am Main 1993

ders.: Foucault. Frankfurt a.M., 1987

ders.: Das elektronische Halsband: Innenansicht der kontrollierten Gesellschaft, in: Kriminologisches Journal 24. Weinheim, 1992, S. 181 – 186

DIPF: Deutschen Institut für internationale pädagogische Forschung, http://www.dipf.de/, 02.02.2005

DONZELOT, JAQUES: Wiederkehr des Sozialen – Von der passiven Sicherheit zur aktiven Solidarität, in: TÜTE: Wissen und Macht. Die Krise des Regierens. Tübingen, 1995, S. 54-59

DREYFUS, HUBERT L. et.al: Michel Foucault: Jenseits von Strukturalismus und Hermeneutik. Weinheim, 1994

DUDEN: Das Bedeutungswörterbuch. Mannheim, Wien, Zürich, 1985

DUDEN: Das große Wörterbuch der deutschen Sprache. Mannheim, Leipzig, Wien, Zürich, 1999

ELEKTRONISCH KINDDOSSIER: VWS: 25 Miljoen extra voor snellere invoering EKD, Pressemitteilung der Niederländischen Regierung, http://www.minvws.nl/persberichten/djb/2005/kabinet-in-operatie-jong.asp, 15.09.2005

ENDRUWEIT, GÜNTER; TROMMSDORFF, GISELA (Hrsg.): Wörterbuch der Soziologie. Stuttgart, 2002

ENGLER, STEFFANIE: Zur Kombination von qualitativen und quantitativen Methoden, in: FRIEBERTSHÄUSER, BARBARA; PRENGEL, ANNEDORE (Hrsg.): Handbuch Qualitative Forschung in der Erziehungswissenschaft. Weinheim, 2003

ENGELMANN, PETER: Vorwort zu: LYOTARD, JEAN-FRANÇOIS: Das postmoderne Wissen. Graz, 1986, S. 9-11

ERICSON, RICHARD V., HAGGERTY, KEVIN D.: Policing the Risk Society. Oxford, 1997

FEELEY, MALCOLM, SIMON, JONATHAN: Actuarial Justice: the Emerging New Criminal Law, in: NELKEN, DAVID (Ed.): The Futures of Criminology. London, New Delhi, 1994, S. 173ff

FINKEL, ROLAND: Kriminalitätsverhütung als gesamtgesellschaftliche Aufgabe, in: GÖSSNER, ROLF (Hrsg.): Mythos Sicherheit: Der hilflose Schrei nach dem starken Staat. Baden-Baden, 1995, S. 415ff

FLAHERTY, DAVID H.: Protecting Privacy in Surveillance Societies, Chapel Hill, NC: The University of North Carolina Press, 1989

FLEXOCARD: http://www.flexocard.de/index.php?path=0_1, 13.07.2005

FLICK, UWE; Qualitative Forschung: Theorie, Methoden, Anwendung in Psychologie und Sozialwissenschaften. Reinbek bei Hamburg, 1999

ders.: KARDOFF, ERNST VON; STEINKE, INES (Hrsg.): Qualitative Forschung. Ein Handbuch. Reinbek bei Hamburg, 2000

FOEBUD: RFID Metroskandal
http://www.foebud.org/rfid/metroskandal, 23.05.2004

FOEBUD: Videoüberwachung, http://www.foebud.org/video/, 06.06.2005

FOUCAULT, MICHEL: Geschichte der Gouvernementalität I, herausgegeben von Sennelart, Michel, Frankfurt a.M. 2004 a

ders.: Geschichte der Gouvernementalität II, herausgegeben von Sennelart, Michel, Frankfurt a.M. 2004 b

ders.: Die Gouvernementalität, in: BRÖCKLING, ULRICH et. al: Gouvernementalität der Gegenwart. Frankfurt a.M., 2000, S. 41

ders.: Überwachen und Strafen; Die Geburt des Gefängnisses. Frankfurt a.M., 1994a

ders.: Das Subjekt und die Macht, in: DREYFUS, HUBERT L. et.al: Michel Foucault: Jenseits von Strukturalismus und Hermeneutik. Weinheim, 1994b, S. 243-261

ders.: Der Wille zum Wissen: Sexualität und Wahrheit I. Frankfurt a.M. 1983

FRIEBERTSHÄUSER, BARBARA; PRENGEL, ANNEDORE (Hrsg.): Handbuch Qualitative Forschung in der Erziehungswissenschaft. Weinheim, 2003

GEOSOFT: http://www.geosoft-gps.de/gps_infos/info_1.html, 10.02.2005

GESTRING, NORBERT et.al. (Hrsg.): Die sichere Stadt. Leverkusen, 2002, (Jahrbuch StadtRegion 2002)

GLASER, BARNEY G., STRAUSS, ANSELM L.: Grounded Theory: Strategien qualitativer Forschung. Bern, 1998

GÖSSNER, ROLF (Hrsg.): Mythos Sicherheit: Der hilflose Schrei nach dem starken Staat. Baden-Baden, 1995

MÜLLER-HEIDELBERG, TILL et al. (Hrsg.): GRUNDRECHTEREPORT 2002: Zur Lage der Bürger- und Menschenrechte in Deutschland. Hamburg, 2002

HAPPY DIGITS: https://www.happydigits.de/servlet/hdekwp34?action=register, 05.07.2005

HARDT, MICHAEL, NEGRI, ANTONIO: Empire. Cambridge (USA), 2000

HAMMERSCHICK, WALTER; KARAZMAN-MORAWETZ, INGE; STANGL, WOLFGANG (Hrsg.): Die sichere Stadt: Prävention und kommunale Sicherheitspolitik. Baden-Baden, 1996 (Jahrbuch für Rechts- und Kriminalitätssoziologie 1995)

HELTEN, FRANK; FISCHER, BERND: What do people think about CCTV? Findings from a Berlin survey, Working Paper No. 13 des Projektes Urbaneye. Berlin, 2004, http://www.urbaneye.net, 01.02.2005

HEISE-NEWS: Edeka setzt auf Fingerabdruck-Bezahlsystem. http://www.heise.de/newsticker/meldung/57055, 04.03.2005a

HEISE-NEWS: Niederländische Regierung lässt ab 2007 Daten über jedes Kind sammeln, http://www.heise.de/newsticker/meldung/63954, 15.09.2005b

HEISE-NEWS: Der digitale Verbraucher: gläsern mit RFID, Kundenkarten und Scoring? http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/58853&words=K%Fcnast, 21.04.2005c

HITZLER, RONALD; PETERS, HELGE (Hrsg.): Inszenierung: Innere Sicherheit, Daten und Diskurse. Opladen, 1998

ders.: HONER, ANNE; MAEDER, CHRISTOPH (Hrsg.): Expertenwissen. Die institutionalisierte Kompetenz zur Konstruktion von Wirklichkeit. Opladen, 1994

ders.: HONER, ANNE (Hrsg.): Sozialwissenschaftliche Hermeneutik. Opladen, 1997

HOHN, VALERIE V.: Videokameras in Kindergärten. Kindercam statt Kindercop, in: Drogenreport 1998, Ausgabe 4, S. 23-24

HOLMES, MARSHALL LEE: Student`s and staff`s perception of school safety and security in a suburban Ohio high school: A case study. University of Akron (Ohio), 1998

HONETH, AXEL ; SAAR, MARTIN (Hrsg.): Michel Foucault: Zwischenbilanz einer Rezeption. Frankfurt, 2003

HONECKER, MARTIN: Popanz Postmoderne. Theologische Kritik an einem inflationierten Begriff, in: Evangelische Kommentare 25, 1992, 263-266.

HORNBOSTEL, STEFAN: Die Konstruktion von Unsicherheitslagen durch kommunale Präventionsräte, in: HITZLER, RONALD; PETERS, HELGE (Hrsg.): Inszenierung: Innere Sicherheit, Daten und Diskurse. Opladen, 1998, S. 93ff

ILLINGER, PATRICK: Fischen im Daten-Ozean, in: Süddeutsche Zeitung, 58. Jhg/ 46. Woche (2002), Nr. 263, NRW-Ausg., 14.11.02, Titelblatt

BUNDESMINISTERIUM DES INNEREN: Eckpunkte zum Sicherheitspaket II, http://www.bmi.bund.de/dokumente/Pressemitteilung/ix_61828.htm, 06.10.2002

JAEGER, ULRICH: Big Brother auf Rädern, in: Der Spiegel (2000) H. 15, S. 142

KARAZMAN-MORAWETZ, INGE: Was macht Stadtbewohner unsicher? Unsicherheitserfahrungen in 2 Wiener Stadtvierteln und ihre strukturellen Hintergründe, in: HAMMERSCHICK, WALTER; KARAZMAN-MORAWETZ, INGE; STANGL, WOLFGANG (Hrsg.): Die sichere Stadt, Prävention und kommunale Sicherheitspolitik. Baden-Baden, 1996, S. 22ff., Jahrbuch für Rechts- und Kriminalitätssoziologie 1995

KETZER, CHRISTINE: Technische Überwachungssysteme in der Demokratie. Vom Werden der Kontrollgesellschaft; in: HERTZFELDT, HELLA; SCHÄFGEN, KATRIN (Hrsg.): Demokratie als Idee und Wirklichkeit. 2. korr. Auflage, Berlin, 2003

KIDZMED: Kidz-Med TEDDYCAM™ MONITOR, http://www.kidzmed.com/teddy.php, 14.07.2005

KINDERCAM: http://www.kindercam.com, 10.2.2005

KLINGST, MARTIN; PFEIFFER, CHRISTIAN: Tatort Deutschland, Kriminalitätsentwicklung im vereinten Deutschland: Empirische Befunde – Erklärungsansätze – Rechtspolitische Folgen, in: GÖSSNER, ROLF (Hrsg.): Mythos Sicherheit: Der hilflose Schrei nach dem starken Staat. Baden-Baden, 1995, S. 27ff

KNEER, GEORG; NASSEHI, ARMIN; SCHROER, MARKUS (Hrsg.): Soziologische Gesellschaftsbegriffe: Konzepte moderner Zeitdiagnosen. München, 1997

ders.: Zivilgesellschaft, in: KNEER, GEORG; NASSEHI, ARMIN; SCHROER, MARKUS (Hrsg.): Soziologische Gesellschaftsbegriffe: Konzepte moderner Zeitdiagnosen. München, 1997, S. 228ff

KLOTZ, KARLHORST: Flanieren unter Video-Augen, http://www.heise.de/newsticker/result.xhtml?url=/newsticker/data/jk-04.07.02-002/default.shtml&words=Video%FCberwachung , 03.09.2002

KOHL, ANDREAS: Videoüberwachung im öffentlichen Raum. Europäisches Zentrum für Kriminalprävention e.V. (Hrsg.), in Wirtschaftschutz & Sicherheitstechnik, Heft 11/1997 und Heft 12/1997

KOWAL, SABINE; O`CONNELL, DANIEL: Zur Transkription von Gesprächen, in: FLICK, UWE; KARDOFF, ERNST VON; STEINKE, INES (Hrsg.): Qualitative Forschung: Ein Handbuch. Reinbek bei Hamburg, 2000, S. 437ff

KRASMANN, SUSANNE: Die Kriminalität der Gesellschaft: Zur Gouvernementalität der Gegenwart. Konstanz, 2003

dies.: Regieren über Freiheit: Zur Analyse der Kontrollgesellschaft in foucaultscher Perspektive, in: Kriminologisches Journal, Weinheim 1999

KREISSL, REINHARD: Die Konjunktur Innere Sicherheit und die Transformation der gesellschaftlichen Semantik, in: HITZLER, RONALD; PETERS, HELGE (Hrsg.): Inszenierung: Innere Sicherheit, Daten und Diskurse. Opladen, 1998, S. 155ff

KREMPL, STEFAN: Der digitale Verbraucher: gläsern mit RFID, Kundenkarten und Scoring? http://www.heise.de/newsticker/meldung/58853, 21.04.2005

KÜNAST, RENATE: Wirtschaft muss sorgsamer mit Kundendaten umgehen, WDR-Nachrichten, http://www.wdr.de, 21.04.2005

LANGE, HANS-JÜRGEN: Die ambivalente Rolle des Staates in der Sicherheitsgesellschaft. Zur Individualisierung des Staats- und Sicherheitsverständnisses. http://www.dgs2002.de/Abstracts/JP/langehaj.htm, 02.10.02

ders.: Die Sicherheitsgesellschaft, in: Die Mitbestimmung online, Ausgabe 7/2002, http://www.boeckler.de/mitbestimmung, 07.10.2002

LEGNARO, ALDO: Konturen der Sicherheitsgesellschaft: Eine polemisch-futurologische Skizze, in: Leviathan: Zeitschrift für Sozialwissenschaft 25 (1997), N. 2, S. 271-285

LEMKE, THOMAS: Eine Kritik der politischen Vernunft: Foucaults Analyse der modernen Gouvernementalität. 3. Auflage, Hamburg 2002

LINDENBERG, MICHAEL; SCHMIDT-SEMISCH, HENNING: Sanktionsverzicht statt Herrschaftsverlust: Vom Übergang in die Kontrollgesellschaft, in: Kriminologisches Journal, Weinheim, 1995

LUSTIG, SYLVIA: Kontrollierte Kontrolleure: Über die Erweiterung des ´intelligence system` der bayerischen Polizei, in: HITZLER, RONALD; PETERS, HELGE (Hrsg.): Inszenierung: Innere Sicherheit, Daten und Diskurse. Opladen, 1998, S. 79ff

LOYALTY PARTNER: http://www.loyaltypartner.de, 05.01.2005

LYON, DAVID: The Electronic Eye, The Rise of Surveillance Society, Cambridge (USA) et.al., 1994

ders.: Postmodernity. Buckingham et.al., 1999

ders.: Surveillance Society: Monitoring Everyday Life. Buckingham et.al., 2001

ders.: Surveillance after September 11, Cambridge (USA) et.al., 2003

LYOTARD, JEAN-FRANÇOIS: Das postmoderne Wissen. Graz, 1986

MARINIS, PABLO DE: Überwachen und Ausschließen, Machtintervention in urbanen Räumen der Kontrollgesellschaft. Pfaffenweiler, 2000

MARX, GARY T.: The Surveillance Society: The threat of 1984-style techniques, in: The Futurist, Juni 1985, S. 21 - 26

MAYRING, PHILIPP: Einführung in die qualitative Sozialforschung. Weinheim, 1996

MC CAHILL, MICHAEL: Beyond Foucault: towards a contemporary theory of surveillance, in: NORRIS, CLIVE; MORAN, JADE; ARMSTRONG, GARY (Ed.): Surveillance, closed circuit television and social control. Aldershot/Brookfield (USA), Singapore, Sydney, 1998, S. 41ff

McLUHAN, MARSHALL: Die magischen Kanäle: Understanding Media. Düsseldorf, Wien, 1968

METRO: Zukunftswerkstatt, http://www.metro.de, 23.05.2004

MEUSER, MICHAEL; NAGEL, ULRIKE: Das Experteninterview – Wissenssoziologische Voraussetzungen und methodische Durchführung, in: FRIEBERTSHÄUSER, BARBARA; PRENGEL, ANNEDORE (Hrsg.): Handbuch Qualitative Forschung in der Erziehungswissenschaft. Weinheim, 2003

dies.: ExpertInneninterviews – vielfach erprobt, wenig bedacht, in: BOGNER, ALEXANDER et.al. (Hrsg.), Opladen, 2002

MOBIL: Kundenmagazin der Deutschen Bahn AG, Hamburg 2002, H.8

NEGRI, ANTONIO; HARDT, MICHAEL: Empire: Die neue Weltordnung. Frankfurt a.M., 2002

NARR, WOLF-DIETER (Hrsg.): Wir Bürger als Sicherheitsrisiko: Berufsverbot und Lauschangriff- Beiträge zur Verfassung unserer Republik. Reinbek bei Hamburg, 1977

NELKEN, DAVID (Ed.): The Futures of Criminology. London, New Delhi, 1994

NOCK, STEVEN L.: The Costs of Privacy, New York, 1993

NOGALA, DETLEF: Sicherheit verkaufen: Selbstdarstellung und marktstrategische Positionierung kommerzieller ´Sicherheitsproduzenten`, in: HITZLER, RONALD / PETERS, HELGE (Hrsg.): Inszenierung: Innere Sicherheit, Daten und Diskurse, Opladen 1998, S. 131ff

ders.: Ordnung durch Beobachtung: Videoüberwachung als urbane Einrichtung, in: GESTRING, NORBERT et.al. (Hrsg.): Die sichere Stadt. Leverkusen 2002 (Jahrbuch StadtRegion 2002), S. 33ff

ders.: Social Control Technologies. Verwendungsgrammatiken, Systematisierung und Problemfelder technisierter sozialer Kontrollarrangements. Dissertation Berlin, 1998

NORRIS, CLIVE; MORAN, JADE; ARMSTRONG, GARY (Ed): Surveillance, closed circuit television and social control. Aldershot/Brookfield (USA), Singapore, Sydney, 1998

dies.: Algorithmic surveillance: the future of automated visual surveillance, a.a.O., S. 255-275

NORRIS, CLIVE; ARMSTRONG, GARY: The Maximum Surveillance Society: The Rise of CCTV. Oxford, New York, 1999

O2: http://www.o2online.de/, 15.09.2004

PAYBACK: Prämien nach Punkten, http://www.payback.de/pb/ui/,534,,?parea=SubNavi, 02.03.2005

PETERMANN, THOMAS / SAUTER, ARNOLD: Biometrische Identifikationssysteme, Sachstandsbericht des Büros für Technologiefolgenabschätzung beim Deutschen Bundestag, Arbeitsbericht Nr. 76, http://www.tab.fzk.de/de/projekt/zusammenfassung/Ab-76.pdf, 04.10.2002

PETERS, HELGE (Hrsg.): Soziale Kontrolle: Zum Problem der Nonkonformität in der Gesellschaft. Opladen, 2000

PETERS, BÄRBEL; SCHETSCHE, MICHAEL: Innere Sicherheit und Cyberspace, in: HITZLER, RONALD; PETERS, HELGE (Hrsg.): Inszenierung: Innere Sicherheit, Daten und Diskurse. Opladen, 1998

PIEPER, MARIANNE / RODRIGUEZ, E. G. (Hrsg.): Gouvernementalität: Ein sozialwissenschaftliches Konzept in Anschluss an Foucault. Frankfurt a.M., 2003

PRENGEL, ANNEDORE (Hrsg.): Handbuch Qualitative Forschung in der Erziehungswissenschaft. Weinheim, 2003, S. 481ff

dies.: ExpertInneninterviews – vielfach erprobt, wenig bedacht, in: BOGNER, ALEXANDER; LITTIG, BEATE; MENZ, WOLFGANG: Das Experteninterview: Theorie, Methode, Anwendung. Opladen, 2002, S. 71ff

RANKL, WOLFGANG; EFFING, WOLFGANG: Handbuch der Chipkarten: Aufbau, Funktionsweise, Einsatz von Smart Cards. München, Wien, 2002

REEVE, ALAN: The panopticisation of shopping: CCTV and leisure consumption in: NORRIS, CLIVE; MORAN, JADE; ARMSTRONG, GARY (Ed): Surveillance, closed circuit television and social control. Aldershot/Brookfield (USA), Singapore, Sydney, 1998, S. 69ff

REISCHL, GERALD: Unter Kontrolle: Die fatalen Folgen der staatlichen Überwachung für Wirtschaft und Gesellschaft. Frankfurt a.M., Wien, 2002

REUBAND, KARL-HEINZ: Gesellschaftlicher Wandel, Kriminalität und Kriminalitätsfurcht, in: Neue Praxis, Heft 6; S. 479-504

RÖTZER, FLORIAN: Überwachungskameras zur Verhaltenserkennung, http://www.heise.de/tp/deutsch/special/krypto/6242/1.html, 08.06.1998

ders.: Neues Video-Überwachungssystem, http://www.heise.de/tp/deutsch/inhalt/te/7113/1.html, 12.03.2001

ders.: Bessere Straßenbeleuchtung statt Überwachungskameras, http://www.heise.de/tp/deutsch/html/result.xhtml?url=/tp/deutsch/inhalt/te/12824/1.html&words=CCTV, 30.06.2002

ders.: Big Brother für Kinder, http://www.heise.de/tp/deutsch/html/result.xhtml?url=/tp/deutsch/inhalt/glosse/5990/1.html&words=Big%20Brother%20Kinder, 20.10.02

ders.: Politiker fordern mehr Überwachung zur Verhinderung von Terror, http://www.heise.de/bin/tp/issue/r4/dl-artikel2.cgi?artikelnr=20490&mode=print, 11.07.05

RONNEBERGER, KLAUS: Die Sicherheitsgesellschaft, Repression und Exklusion im städtischen Raum, Vortrag vom 3.5.2002 in Innsbruck, http://www.catbull.com/rechtshilfe/ronneberger.pdf, 02.10.2002

ders.: LANZ, STEPHAN; JAHN, WALTHER: Die Stadt als Beute. Bonn, 1999

RUHMANN, INGO: Jobkiller, Geheimdaten, Überwachungsstaat. Stuttgart, 1985

SAETNAN, ANN; DAHL, JOHANNE; LOMELL, HEIDI: Views from under surveillance: Public opinion in a closely watched area in Oslo, Working Paper No. 12 des Projektes Urbaneye, Oslo 2004, http://www.urbaneye.net, 01.02.2005

SCHOELER, ANDREAS VON (Hrsg.): Informationsgesellschaft oder Überwachungsstaat? Strategien zur Wahrung der Freiheitsrechte im Computerzeitalter. Opladen, 1986

SCHORB, BERND; THEUNERT, HELGA; SCHELL, FRED: Wer beherrscht hier wen? Die Gewalt der „Neuen Medien“. München, 1991

SCHRADER, HANS-HERMANN: 18. Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten 2000/2001, http://www.hamburg.datenschutz.de, 20.10.2002

SCHULZKI-HADDOUTI, CHRISTIANE: Vom Ende der Anonymität. Hannover, 2001

dies.: Datenjagd im Internet. Hamburg, 2001

dies: Nordrhein-Westfalen führt Video-Überwachung ein, http://www.heise.de/newsticker/meldung/29229, 19.07.2002

dies.: Bürgerrechte im Netz (Hrsg.), Opladen 2003

dies.: Im Netz der Inneren Sicherheit, Hamburg 2004

SIEGLE, JOCHEN A.: Bauchlandung für Big Brother, in: Der Spiegel, Online-Ausgabe http://www.spiegel.de/netzwelt/politik/0,1518,232552,00.html, 28.01.2003

SIERING, FRANK: Big Brother im Kindergarten, in: Computer & Co, Beilage der Frankfurter Rundschau, 08/1999, S. 34 ff

STEINERT, HEINZ: Prävention als kommunale Aufgabe: Jenseits von Polizei und Strafrecht, in: GÖSSNER, ROLF (Hrsg.): Mythos Sicherheit: Der hilflose Schrei nach dem starken Staat. Baden-Baden, 1995, S. 403ff

STOA (Scientific and Technological Options Assessment): Eine Bewertung der Technologien für eine politische Kontrolle, Aktualisierte Zusammenfassung als Unterlage für die September-Tagung 1998, http://www.europarl.eu.int/stoa/publi/166499/execsum_de.htm#2.1, 04.09.2002

STRAUSS, ANSELM: Grundlagen qualitativer Sozialforschung. München, 1998

STRECK, MICHAEL: Eilschritt zum Überwachungsstaat, in: die tageszeitung, Ausg. West, 15.11.2002, S. 10

TAGESSCHAU: Bundesdatenschützer ruft Gesetzgeber zur Räson
http://www.tagesschau.de/aktuell/meldungen/0,1185,OID4274624,00.html, 21.04.2005

TCHIBO: Funküberwachungssystem,
http://www.tchibo.de/is-bin/INTERSHOP.enfinity/eCS/Store/de/, 10.02.2005

TEDDY-CAM:
https://ssl.kundenserver.de/s36476739.einsundeinsshop.de/sess/utn153d74b9640f7a2/shopdata/0005_Spezialkameras+=28Einzelanfertigung=29/product_overview.shopscript, 03.09.2002

THE GUARDIAN:
http://www.guardian.co.uk/uk_news/story/0,3604,785071,00.html, 03.09.2002

TRACKYOURKID: http://www.trackyourkid.de/index3.php, 25.03.2004a

dies. Sicherheitsgarantie:
http://www.trackyourkid.de/sicherheitsgarantie.php, 25.03.2004b

dies.: Nutzen: http://www.trackyourkid.de/nutzen.php, 25.03.2004c

dies.: Dienst: http://www.trackyourkid.de/derdienst.php, 25.03.2004d

URBANEYE: http://www.urbaneye.net/index.html, 20.01.2004

VEIL, KATJA: Raumkontrolle: Videokontrolle und Planung für den öffentlichen Raum, im World Wide Web veröffentlichte Diplomarbeit im Rahmen des Studiums der Stadt- und Regionalplanung an der Technischen Universität Berlin. Berlin 2001;
http://de.geocities.com/veilkatja, 10.04.2004

dies.: Urbane Sicherheitsstrategien - das Beispiel Coventry, in: GESTRING, NORBERT et.al. (Hrsg.): Die sichere Stadt. Leverkusen, 2002, (Jahrbuch StadtRegion 2002), S. 117ff

WATCHMEGROW: http://www.watchmegrow.com, 10.02.2005

WDR: Londoner Innenstadt seit heute maut-pflichtig, Radionachricht vom 17.02.2003, ausgestrahlt 10:45 Uhr;
http://www.wdr.de/nachrichten/chronol.phtml?ts=200302172

WEHRHEIM, JAN: Die überwachte Stadt: Sicherheit, Segregation und Ausgrenzung. Opladen, 2002

ders.: Großstadt zwischen Ambivalenz und Überwachung - Eine aktuelle Retrospektive, in: GESTRING, NORBERT et.al. (Hrsg.): Die sichere Stadt. Leverkusen, 2002, (Jahrbuch StadtRegion 2003) S. 16

WEICHERT, THILO: Sicherheitsrisiko Ausländer. Die informationelle Sonderbehandlung von Nichtdeutschen, in: GÖSSNER, ROLF (Hrsg.): Mythos Sicherheit: Der hilflose Schrei nach dem starken Staat. Baden-Baden, 1995, S. 251ff

WENTZ, MARTIN (Hrsg.): Stadt-Räume: Die Zukunft des Städtischen. Frankfurt a.M., New York, 1991 (Frankfurter Beiträge Band 2)

WHERIFY: GPS Personal Locator for Children,
http://www.wherifywireless.com/prod_watches.htm, 04.09.2002

WHITAKER, REG: Das Ende der Privatheit: Überwachung, Macht und soziale Kontrolle im Informationszeitalter, München 1999

WIKIPEDIA: Die freie Enzyklopädie: Wissen,
http://de.wikipedia.org/wiki/Wissen, 03.09.2005

WILSON, JAMIE: Girl to get tracker implant to ease parents' fears, in: The Guardian,
http://www.guardian.co.uk/uk_news/story/0,3604,785071,00.html,
03.09.2002:

WOLFF, STEPHAN: Wege ins Feld und ihre Varianten, in: FLICK, UWE; KARDOFF, ERNST VON; STEINKE, INES (Hrsg.): Qualitative Forschung: Ein Handbuch. Reinbek bei Hamburg, 2000, S. 334ff

ZIPS, MARTIN: Videokameras an Schulhöfen und Plätzen, in: Süddeutsche Zeitung, 06.07.1999, S. 10

Abbildungsnachweis

Abbildung 1	Wehrheim, Jan: http://kai.iks-jena.de/bilder/cctv-leipzig.jpg, 18.09.2005
Abbildung 2	TCHIBO: Funküberwachungssystem,http://www.tchibo.de/is-bin/INTERSHOP.enfinity/eCS/Store/de, 10.02.2005
Abbildung 3	eigene Aufnahme, 10.7.2003
Abbildung 4	eigene Aufnahme, 10.7.2003
Abbildung 5	eigene Aufnahme, 10.7.2003
Abbildung 6	Magnetkarten: http://www.flexocard.de/index.php?path=0_1, 13.07.2005
Abbildung 7	DARPA: http://www.darpa.mil/iao/TIASystems.htm, 6.12.2002
Abbildung 8	Wherify: http://www.wherifywireless.com/prod_watches.htm, 04.09.2002
Abbildung 9	eigene Aufnahme, 10.1.2005
Abbildung 10	eigene Aufnahme, 10.1.2005
Abbildung 11	eigene Aufnahme, 10.1.2005
Abbildung 12	eigene Aufnahme, 10.1.2005
Abbildung 13	eigene Aufnahme, 10.1.2005
Abbildung 14	eigene Aufnahme, 10.1.2005
Abbildung 15	eigene Aufnahme, 10.1.2005
Abbildung 16	dm Drogeriemarkt: http://www.dm-drogeriemarkt.de, 14.2.2005
Abbildung 17	eigene Aufnahme, 10.1.2005
Abbildung 18	Müller-Zantop, Teleshoppingpräsentation, 2001
Abbildung 19	http://www.trackyourkid.de, 19.5.2005
Abbildung 20	http://www.trackyourkid.de, 18.05.2005
Abbildung 21	http://www.trackyourkid.de, 19.5.2005