FAKULTÄT FÜR !NFORMATIK

Technische, organisatorische und gesellschaftliche Aspekte der Privatsphäre unter den Bedingungen der vernetzten Gesellschaft

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieurin

im Rahmen des Studiums

Medieninformatik

eingereicht von

Gabriele Schneglberger, BSc.
Matrikelnummer 0726898

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer: Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Peter Purgathofer

Wien, 28. Jänner 2010 _____ _____
(Unterschrift Verfasser) (Unterschrift Betreuer)

Erklärung zur Verfassung der Arbeit

Gabriele Schneglberger, BSc.
Basling 8
4770 Andorf

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Andorf, im Jänner 2010

Gabriele Schneglberger, BSc.

Inhaltsverzeichnis

Kurzfassung

Privatsphäre ist ein wandelbarer, historisch und kulturell relativer Begriff. Es handelt sich um einen weit gefassten Begriff, es gibt keine klare (rechtliche) Definition. Die bisherigen *Konzepte* von Privatsphäre werden besprochen um zu zeigen, dass sie einander nicht ausschließen können und daher Veränderungen an der Konzeption von *Privatsphäre* notwendig sind. Es wird der *Wert* von Privatsphäre in unterschiedlichen Aspekten beleuchtet und der Frage nachgegangen, wie unterschiedlich der Begriff der *Privatsphäre* abgegrenzt wird und welche Gefahren diese Abgrenzung mit sich bringt.

Die Verletzung der Privatsphäre erfolgt häufig unbemerkt. Aus gutem Glauben heraus ist der Einzelne der Überzeugung „Überwachung ist nicht auf mich gerichtet“ doch das kann täuschen. Plötzlich wird ein Kredit verweigert, es kommen ungebetene Anrufe von Telemarketingunternehmen, es erfolgt eine nicht angekündigte Steuerprüfung, eine zweite Sicherheitsprüfung am Flughafen usw. Die Ursache dieser Vorkommnisse ist unklar und wird verborgen gehalten, daher werden sie nicht als Eindringen in die Privatsphäre gewertet. Zum anderen kommt immer wieder der Gedanke „wenn man nichts zu verbergen hat, hat man nichts zu fürchten“.

Die Auseinandersetzung mit Wissensentwicklung, Social Media, Datenschutz, Identitätsnachweis und Überwachung hat zum Ziel, die umfassende Problematik von *Privatsphäre* in ihren unterschiedlichsten Aspekten begreifbar zu machen. Die Prozesse der Informationsbeschaffung, der Verarbeitung von Information und der mögliche Datenmissbrauch in Zusammenhang mit Privatsphäre werden grundlegend besprochen und anhand von Beispielen im Rahmen der Themenschwerpunkte Wissensentwicklung, Social Media, Datenschutz, Identitätsnachweis und Überwachung aufgegriffen um so die übergreifende Problematik von *Privatsphäre* zu verdeutlichen.

Angesichts der kritischen Situation der *Privatsphäre* jedes Einzelnen werden Möglichkeiten aufgezeigt, wie sich der völligen Überwachung, der Identifizierung und Nachverfolgung ansatzweise entzogen werden kann und wie das Bewusstsein gegenüber *Privatsphäre* geschärft werden kann.

Abstract

Privacy is a changeable, historically and culturally relative term. There is a broad concept, there is no clear (legal) definition. The recent *concepts* of privacy are discussed in order to show that they are not mutually exclusive and that, as consequence, changes in the conception of privacy have become necessary. Different aspects of the *value* of privacy are shown and different *definitions* of the term *privacy* are being explored.

The violation of privacy is often unnoticed. With good faith, the individual is convinced that „surveillance is not directed at me," but this can be deceiving. Suddenly, a credit will be refused, unsolicited calls from telemarketing companies get in, a non-announced tax audit takes place, a second security check at the airport etc. The cause of these events is unclear and is kept hidden, so they are not realized as an invasion of privacy. Secondly, the idea keeps coming back „when you have nothing to hide, you have nothing to fear".

The aim of the discussion about *knowledge development*, *social media*, *data protection*, *identification* and *surveillance* is a deep understanding of the comprehensive problem of privacy in its many aspects.

The processes of gathering information, processing of information and the possible misuse of data related to privacy are fundamentally addressed and discussed using examples within the topics of knowledge development, social media, data protection, identification and surveillance in order to illustrate the overarching issues of privacy.

Given the critical situation of everybody's privacy-situation, different possibilities are identified to rudimentary elude total surveillance, identification and tracking and ways are demonstrated how to raise one's awareness of privacy.

Kapitel 1

Einleitung

1.1 Zielsetzung

Ziel der Arbeit ist es, die unterschiedlichen Problematiken aufzuzeigen, die hinter dem Thema *Privatsphäre* liegen, um dadurch der aktuell wahrnehmbaren unaufhaltbaren Tendenz zu Überwachung, Data Mining und damit sozialer Klassifikation entgegenwirken zu können. Zuerst muss der Begriff der *Privatsphäre* genau erörtert werden. Dies bildet die Grundlage, denn die Problematik rund um *Privatsphäre* ist der gemeinsame Nenner der nachfolgend besprochenen Themen Wissensentwicklung, Social Media, Datenschutz, Identitätsnachweis und Überwachung. Abschließend werden Möglichkeiten der Gegenwehr sowie der Schärfung des eigenen Bewusstseins gegenüber *Privatsphäre* aufgezeigt.

1.2 Kapitelübersicht

Die Arbeit beginnt mit einer umfangreichen Ausarbeitung des Begriffs der *Privatsphäre* mit Kapitel 2. Es werden bisherige Konzepte besprochen, der Wert von *Privatsphäre* erörtert. Es wird darin auch der Frage nachgegangen, wie unterschiedlich der Begriff der *Privatsphäre* abgegrenzt wird. Auf die Themen Informationsbeschaffung, Verarbeitung von Information und möglicher Datenmissbrauch im Zusammenhang mit Privatsphäre wird detailliert eingegangen um damit eine umfassende Grundlage zur Datenproblematik für nachfolgende Kapitel zu legen.

In Kapitel 3 wird aufgezeigt, dass Verdatung und Verwissenschaftlichung zu neuen Wissensarten und unterschiedliche Wissenslagen in verschiedenen Ebenen führen. Kritisch dabei ist die Beobachtung der asymmetrischen Wissensverteilung in der Gesellschaft zugunsten informationsreicher „Datenherren“.

Das Thema *Social Media* führt zu einer neuen Diskussion über Öffentlichkeit und Privatsphäre sowie öffentlicher Privatsphäre. *Privatsphäre* existiert

im realen Leben auch in der Öffentlichkeit, in der virtuellen Kommunikationswelt ist die Situation eine andere, darauf wird in Kapitel 4 näher eingegangen. Es wird beschrieben, warum Social Tools eine völlig neue Art der Gruppenkommunikation und -aktion ermöglichen. Kritische Anmerkungen zu Technikakzeptanz und Medientheorie beenden die Auseinandersetzung mit Social Media.

Kapitel 5 beleuchtet zuerst die Datenproblematik angesichts der Möglichkeit der Deutung von Daten und der Eigenverantwortung jedes „Datensubjekts“. Es wird die Frage nach der Interpretation der Daten und dem gezielten Erstellen von Persönlichkeitsprofilen („Data Mining“) gestellt. Die hinsichtlich der Sammelwut von Behörden und Unternehmen aufkommenden Bedenken werden mit Beispielen aus der Realität und dem Alltag bekräftigt.

Digital vernetzte Identifikationssysteme erlauben einerseits das Sammeln von Daten (und damit entsprechend die Möglichkeit des Datenmissbrauchs), andererseits stellen sie ein großes Geschäft für Unternehmen dar, die ID-Kartensysteme herstellen. In Kapitel 6 werden neben der genannten Thematik darüberhinaus die zur Zeit gängigste Art von Ausweisen, nämlich Chipkarten sowie biometrische Identifikation beschrieben.

In Kapitel 7 wird auf unterschiedlichste Formen der Überwachung eingegangen, die jedem Einzelnen im Alltag begegnen. Deutlich hervorgehoben wird dabei die umgekehrte Unschuldsvermutung. Aufgezeigt werden aber auch Aspekte, die zeigen, dass Überwachung auch zu einem Teil das eigene Einverständnis, eigene bestimmte Handlungen voraussetzt. *Social Sorting* wird erklärt und gezeigt, warum Überwachung zu sozialer Klassifikation führt. Der politische Aspekt von Überwachung wird erläutert um zu zeigen, wie dadurch nachhaltig das Verhalten von Bürgern beeinflusst wird. Auch in diesem Kapitel belegen Beispiele aus der Realität, dass eine kritische Haltung gegenüber Überwachung durchaus angebracht ist.

Das Kapitel 8 soll verschiedene Möglichkeiten aufzeigen, wie sich der völligen Überwachung, der Identifizierung und Nachverfolgung ansatzweise entzogen werden kann und wie das Bewusstsein über *Privatsphäre* geschärft werden kann. Die Möglichkeiten werden dabei nach individueller und gesellschaftlicher Ebene unterschieden. Auf gesellschaftlicher Ebene setzen sich beispielsweise kritische Gemeinschaften oder herausragende Persönlichkeiten für den Schutz der *Privatsphäre* ein. Aber auch Veranstaltungen oder Politik können einen Teil der Aufklärung auf gesellschaftlicher Ebene leisten. Die individuelle Ebene umfasst Maßnahmen, die direkt von einzelnen Personen ergriffen werden können. Diese bewegen sich mitunter an der Grenze zur Legalität, sollen aber gerade durch diese Überzogenheit Wege der Gegenwehr zeigen.

Der Eindruck, der durch die Auseinandersetzung mit *Privatsphäre* und entsprechend verwandten Themen entstand, wird in Kapitel 9 geschildert.

Kapitel 2

Begriffsklärung *Privatsphäre*

Privatsphäre ist ein wandelbarer, historisch und kulturell relativer Begriff. Es handelt sich um einen weit gefassten Begriff, es gibt keine klare (rechtliche) Definition. In diesem Kapitel sollen der Umfang und die verschiedenen Aspekte von *Privatsphäre* gezeigt werden. Es soll gezeigt werden, dass ein neues Konzept von *Privatsphäre* erforderlich ist um dem aktuellen und sich schnell verändernden Alltag entgegenstehen zu können.

Die bisherigen *Konzepte* von Privatsphäre werden besprochen um zu zeigen, dass sie einander nicht ausschließen können und daher Veränderungen an der Konzeption von *Privatsphäre* notwendig sind. Es wird der *Wert* von Privatsphäre in unterschiedlichen Aspekten beleuchtet. Es wird der Frage nachgegangen, wie unterschiedlich der Begriff der *Privatsphäre* abgegrenzt wird und welche Gefahren diese Abgrenzung mit sich bringt.

Abschließend werden die Themen Informationsbeschaffung, die Verarbeitung von Information und möglicher Datenmissbrauch im Zusammenhang mit Privatsphäre besprochen um damit eine umfassende Grundlage zur Datenproblematik für nachfolgende Kapitel zu legen.

2.1 Definition von *Privatsphäre*

Daniel J. Solove stellt in [Solove 2008] ein neues Konzept, eine neue Theorie von *Privatsphäre* vor bzw. eine Annäherung daran. Methodisch lehnt er den traditionellen Weg der Konzeptionalisierung ab. Er will *Privatsphäre* vielmehr gemäß Ludwig Wittgensteins Vorstellung über „Familienähnlichkeit“ sehen. Nach Wittgenstein weisen demnach bestimmte Konzepte *nicht nur eine einzige* allgemeine Charakteristik auf, sondern beziehen die Eigenschaften aus einem *allgemeinen Fundus ähnlicher Elemente.*

„Keine Privatsphäre“ meint heute oft die neue Erfindung der westlichen Welt – juristisch gesehen im Sinne von persönlichem Eigentum und Person als Eigentum, anders ist das beispielsweise in China [Stocker und Schöpf 2007, S. 57ff, David Lyon].

Ein Einzelner braucht die Gruppe, kann weder vollkommen getrennt von der Welt und allen Menschen leben noch kann der Einzelne völlig in Öffentlichkeit leben (das Leben würde oberflächlich werden). Was es ausmacht, sind die Kleinigkeiten, die eben nicht an die Öffentlichkeit sollen und ein Geheimnis für sich selbst bleiben [Solove und Schwartz 2008b, S. 40]. Genau das ist es, was *Privatsphäre* so wertvoll macht.

Privatsphäre bedeutet Kontrolle über das Wissen über sich selbst. Aber es ist nicht nur die Kontrolle über die Menge an Information, die im Umlauf ist, es sind auch die Modulationen von Qualität des Wissens. Es macht jemanden nichts aus, wenn jemand anderes etwas Allgemeines von ihm weiß, aber sobald der andere ein Detail kennt, fühlt sich der Betroffene in seiner *Privatsphäre* verletzt [Solove und Schwartz 2008b, S. 45] .

Die Aufgabe von *Privatsphäre* besteht auch darin, Unschuldige vor schadenbringenden Schlussfolgerungen aufgrund falsch interpretierter Informationen zu beschützen [Solove und Schwartz 2008b, S. 46]. Es muss jeder lernen, die Informationen zu verarbeiten und die eigenen Schlussfolgerungen über die Welt rundherum zu machen [Solove und Schwartz 2008b, S. 47]. Paul Schwartz spricht 1999 von constitutive privacy [Bennett 2008, S. 5]:

> protect the ability of individuals to speak freely and participate in public life on the internet

2.1.1 Unterscheidung zwischen *Privatsphäre* und dem Recht auf *Privatsphäre*

Es muss zwischen dem Konzept von *Privatsphäre* und dem Recht auf *Privatsphäre* unterschieden werden: Das Gesetz bestimmt nicht, was *Privatsphäre* ist, nur welche Situationen von *Privatsphäre* legalen Schutz benötigen. *Privatsphäre* als Konzept schließt mit ein, was *Privatsphäre* verursacht und wie sie gewertet werden muss. *Privatsphäre* als Recht schließt mit ein, bis zu welchem Maß *Privatsphäre* rechtlich geschützt wird und werden soll [Solove und Schwartz 2008b, S. 39ff]. Nach Solove besteht *Privatsphäre* aus vielen unterschiedlichen aber trotzdem ähnlichen Themen.

Die bisherigen Konzepte von *Privatsphäre* können in sechs unterschiedliche Arten unterschieden werden:

- Das Recht allein gelassen zu werden (Samuel Warren und Louis Brandeis [Warren und Brandeis 1890])
- Eingeschränkter Zugang auf sich selbst – die Möglichkeit sich von ungewünschtem Zugang durch andere zu beschützen.
- Geheimhaltungspflicht
- Kontrolle über die persönlichen Informationen
- Persönlichkeit – Schutz des eigenen Charakters, der Individualität und der Würde

- Intimität – Kontrolle über oder beschränkter Zugang zu einer nahen Beziehung oder intimen Lebensaspekten

Solove versteht unter der traditionellen Methode der Definition von *Privatsphäre* jene Methode, in der *Privatsphäre* von anderen Dingen getrennt wird und in unterschiedlichsten Vorkommen beschrieben wird. Er zeigt auf, wie unvollständig einzeln und unabhängig voneinander betrachtet die genannten Arten von *Privatsphäre* sind.

Louis D. Brandeis und Samuel D. Warren haben über die US-amerikanische Tradition des *common law* in einem Artikel im Harvard Law Review schon 1890 die griffige Formel des „Right to be let alone“ als Schutz von Privatsphäre und öffentlicher Belästigung eingebracht [Warren und Brandeis 1890]. Dabei geht es einerseits um eine erweiterte Definition des privaten „Eigentums“, nämlich an Gedanken, Gefühlen, Einstellungen oder Meinungen, andererseits um neue technische „Belästigungen“, wie durch unerwünschte Fotografie, gedruckte Portraits, Vervielfältigung privater Briefe oder Gerüchte in den Klatschspalten der Zeitungen. Die Vorstellung, der Staat könne sich solcher Techniken bedienen, bleibt im liberalen Amerika von 1890 freilich noch undenkbar.

2.1.2 Das Recht allein gelassen zu werden

Das Recht allein gelassen zu werden basiert auf einem Artikel von Louis D. Brandeis und Samuel D. Warren [Warren und Brandeis 1890]. Warren und Brandeis fordern die rechtliche Anerkennung eines Rechts auf Privatsphäre, welches sie als „das Recht, allein gelassen zu werden“ formulierten. Der Artikel bildet später die Grundlage für das Recht auf Privatsphäre in den Vereinigten Staaten. Es fehlt allerdings im Artikel die genaue Definition, was *Privatsphäre* ausmacht. Der Artikel war seiner Zeit voraus und eine wichtige Grundlage für die Entwicklung eines Konzepts zu Privatsphäre. Allerdings handelt es sich um ein zu umfangreiches und vages Konzept von Privatsphäre, da vor allem die Ursprünge des Rechts auf *Privatsphäre* im allgemeinen Gesetz erforscht wurden und erklärt wurde, wie es sich entwickeln könnte.

2.1.3 Eingeschränkter Zugang auf sich selbst

Der eingeschränkte Zugang auf sich selbst, meint jene Bedenken, inwieweit jemand den anderen zugänglich ist: In welchem Maß kennen uns andere, haben andere körperlichen Zugang auf jemanden und inwiefern erweckt jemand die Aufmerksamkeit von anderen. Eingeschränkter Zugang wird daher von drei Elementen geprägt: Verschwiegenheit, Anonymität und Einsamkeit. In dieser Definition allerdings fehlt die Berücksichtigung der Verstrickung der Regierung in die Entscheidungen betreffend des Körpers, der Gesundheit,

der sexuellen Ausrichtung und des Familienlebens von jemanden. Die Reduzierung von *Privatsphäre* alleine auf den eingeschränkten Zugang zu sich selbst ist also zu eng gefasst und unvollkommen.

2.1.4 Geheimhaltungspflicht

Die Geheimhaltungspflicht kann als Unterkonzept des eingeschränkten Zugangs auf sich selbst gesehen werden. Der Oberste Gerichtshof stellte in mehreren Verfahren fest, dass kein „begründeter Anspruch auf Privatsphäre“ besteht, sobald etwas der Öffentlichkeit mitgeteilt wird – selbst wenn es höchst unwahrscheinlich ist, dass auch nur irgendjemand das sehen oder entdecken könnte. Heikel allerdings ist, dass auch das eigene Zuhause und das Büro hier im Begriff „Öffentlichkeit“ enthalten sind. Das Durchwühlen von Müll ist damit rechtlich gesehen kein Verstoß gegen das Recht auf *Privatsphäre* .

Gruppen-*Privatsphäre* und selektive Geheimhaltung gehören zu diesem Bereich. Das Konzept der Geheimhaltungspflicht berücksichtigt nicht, dass jemand manche Dinge vor bestimmten Personen nicht zeigen will (privat halten will), vor anderen aber eben doch – selektive Geheimhaltung. Menschen erwarten *Privatsphäre* auch in der Öffentlichkeit, denn nicht alle privaten Angelegenheiten werden im Geheimen erledigt – und können es auch nicht.

Geheimhaltungspflicht alleine betrachtet das Konzept von *Privatsphäre* zu eng gefasst.

2.1.5 Kontrolle über die persönlichen Informationen

Das Konzept zur Kontrolle über die persönlichen Informationen scheitert daran zu definieren, was genau mit „Kontrolle“ gemeint ist. Ein weiterer Kritikpunkt ist die Tatsache, dass das „von anderen gesehen und gehört werden“ häufig als nicht das geringste Eindringen in die Privatsphäre empfunden wird.

Auch für dieses Konzept gilt daher wieder: zu umfangreich, zu vage aber andererseits auch zu eng gefasst.

2.1.6 Persönlichkeits-Konzept

Das Persönlichkeits-Konzept von *Privatsphäre* befasst sich mit dem Schutz der Integrität einer Persönlichkeit. Überwachung begrenzt die individuellen Wahlmöglichkeiten und schränkt daher die Freiheit ein. Persönlichkeit kann nicht als rein privat und persönlich gesehen werden, da jeder in der Öffentlichkeit lebt. Ein künstlerisches Werk bringt mitunter sehr viel des Lebens des Künstlers zum Vorschein, trotzdem wird es öffentlich gezeigt und wird mitunter für die Öffentlichkeit gemacht. Die Theorie von *Privatsphäre* als

Persönlichkeitsrecht erklärt nicht die entsprechende Definition von Persönlichkeit und ist daher unvollkommen.

2.1.7 Intimität

Intimität als Konzept von *Privatsphäre* beschreibt, dass *Privatsphäre* nicht nur für die individuelle Selbsterfindung notwendig ist, sondern auch für menschliche Beziehungen. Das Konzept sieht *Privatsphäre* als es eine Art von beschränktem Zugang oder Kontrolle und stellt den Wert von *Privatsphäre* bei der Entwicklung von persönlichen Beziehungen in den Vordergrund. Das *Privatsphäre* als Intimität-Konzept kann unvollkommen sein, wenn die genaue Bedeutung von Intimität nicht klar definiert ist. Meistens allerdings ist das Konzept zu eng gefasst, da all jene Angelegenheiten ausgeschlossen sind, die nicht die Charakteristiken von intimen Beziehungen miteinschließen.

2.2 Der Wert von *Privatsphäre*

Privatsphäre ist notwendig, um die Einzigartigkeit eines Menschen zu bewahren. *Privatsphäre* ermöglicht Menschen das Schaffen, Entdecken, Erleben und Experimentieren, losgelöst und unabhängig von gesellschaftlichen Normen und Zwängen mitunter auch um diesen besser mit einer klaren und überzeugten Haltung entgegenstehen zu können. *Privatsphäre* ist notwendig, damit ein Mensch sich selbst entdecken und entwickeln und das Selbstverständnis schärfen kann. Sie erlaubt die Diskussion und das Andenken politischer Veränderungen, das Schaffen einer Gegenkultur und ermöglicht Gesellschaftskritik. Wachstum und Entwicklung benötigen das Experimentieren und die Möglichkeit, die Meinung und Ansichten zu verändern, bevor sie öffentlich gemacht werden.

Allerdings kann *Privatsphäre* es erschweren, Vertrauen aufzubauen und den Ruf von Menschen zu beurteilen. Der Ruf von Menschen innerhalb einer Gemeinschaft ist jedoch wesentlich für das normale, ehrliche und partnerschaftliche Zusammenwirken innerhalb dieser.

Die Frage von *Privatsphäre* ist auch eine Generationenfrage: Die jüngeren Generationen wachsen in einer offenen Umgebung auf und sind daran gewöhnt/es scheint selbstverständlich keine *Privatsphäre* zu erwarten. Die Erwartungen an *Privatsphäre* schwinden, gleichzeitig messen Menschen *Privatsphäre* weniger Wert bei.

Privatsphäre gerät mitunter in Konflikt mit anderen Werten, vor allem wenn es um Kriminalität und nationale Sicherheit geht. Prävention und Schutz gegen Straftaten lassen Aspekte von *Privatsphäre* zurücktreten – die Regierung greift in *Privatsphäre* ein aus Zwecken der „Sicherheit“, nur wessen Sicherheit. Der Wert von *Privatsphäre* wird vor allem durch die Art und Weise sichtbar, wie sie die soziale Struktur, Kraft, die Demokratie und Freiheit beeinflusst, doch lässt sich dieser Wert messen?

Privatsphäre nur im individualistischen Zusammenhang zu sehen mindert deren Wert. Denn *Privatsphäre* einer einzelnen Person wiegt nicht die Interessen einer ganzen Gesellschaft auf. Bedenken *Privatsphäre* gegenüber entstehen nicht aus bestimmten individuellen Problemen heraus, sondern sie drücken Konflikte aus, die die gesamte Gemeinschaft betreffen. Der Einzelne wird zum Wohle der Gemeinschaft vor ihr geschützt. Um eine Theorie über den Wert von *Privatsphäre* aufstellen zu können, wird eine Theorie der Beziehung eines Einzelnen gegenüber der Gemeinschaft benötigt.

Die Probleme und Schwierigkeiten, die durch *Privatsphäre* -Verletzungen entstehen, haben häufig ihren Ursprung in sehr starken sozialen Normen. *Privatsphäre* ist ein Mittel um Normen zu regulieren, es ist ein Ventil für Menschen in Gesellschaften mit besonders ausgeprägten Normen. Auch wenn die Gefahr besteht, durch *Privatsphäre* die Normen nicht ernst zu nehmen, so ist sie doch notwendig um einer von Kontrolle durch zu viele Normen geprägten, autoritären Gesellschaft entgegenzuwirken. Soziale Kontrolle durch Normen gleicht einem starken Eingriff in das persönliche Leben eines Menschen und gleicht einer Versklavung der Seele. Einige der wichtigsten Rechte und Freiheiten wurden erst durch den Widerstand gegen bestehende Formen von sozialer Kontrolle möglich.

Privatsphäre wird durch soziale Normen geformt und kann daher nicht als Recht des Einzelnen gesehen werden. Es beschützt zwar einen einzelnen Menschen, allerdings nicht aufgrund der Persönlichkeit. Vielmehr beschützt *Privatsphäre* den einzelnen Menschen aufgrund der Vorteile, die *Privatsphäre* der Gesellschaft bringt.

Privatsphäre ermöglicht einen vielfachen Schutz gegen unterschiedliche Arten von Problemen, daher muß der Wert von *Privatsphäre* auch in pluralistischer Hinsicht gesehen werden.

2.3 Abgrenzung von *Privatsphäre*

Es gibt unterschiedliche Definitionen für die Abgrenzung des Privatheitsbegriffs. Auch wenn die verschiedenen Grenzziehungen zwischen privat und öffentlich zueinander teilweise inkonsistent sind (etwa in Bezug auf den Einschluss/Ausschluss des Wirtschaftsbereichs), so zielen sie doch auf die Autonomie der Personen innerhalb des jeweils als privat bezeichneten Bereichs ab [Gaycken und Kurz 2008, S. 234].

Privatheit kann nach Beate Rössler [Rössler 2001, S. 25] in drei unterschiedliche Arten unterschieden werden. Die Unterscheidung bezieht sich vorrangig auf eine einzelne Person, aber trotzdem notwendige Voraussetzung für einen überindividuellen, zivilgesellschaftlichen Begriff der Privatsphäre sind [Gaycken und Kurz 2008, S. 235]:

1. Die dezisionale Privatheit, die sich auf die Ebene der Entscheidungsfreiheit bezieht.

2. Die lokale Privatheit, in der es um Schutz des Wohnbereichs und Aufenthaltsdaten, aber auch um die Wahrung der leiblichen Integrität geht.
3. Die informationelle Privatheit, die den Schutz und die Kontrolle personenbezogener Daten beschreibt.

Die kontextbezogenen und unsichtbaren Anwendungen der neuen Computergenerationen haben eine einzigartige „Entschlüsselungsstellung“ in Bezug auf den gesamten Privatbereich.

2.3.1 Dezisionale Privatheit – Panopticon

In Bezug auf die individualisierte Mediennutzung und Informationsspeicherung ist häufig von einer quasi unvermeidlichen Reduktion des Schutzes privater Daten die Rede (vgl. [Rossnagel 2005]). Das *Panopticon* (deutsch: Panoptikum) steht für den Gedanken, dass in Gesellschaften mit allgegenwärtiger Medienpräsenz ein hohes Potential für eine gegenseitige Überwachung besteht [Gaycken und Kurz 2008, S. 236]. Aus der Überwachung folge eine Veränderung des Verhaltens und gegebenenfalls eine Selbstdisziplinierung. Diesen angenommenen Effekt der Selbstdisziplinierung durch ein Gefühl der Überwachung hatte ursprünglich der Philosoph Jeremy Bentham im Zusammenhang seiner Überlegungen zur Reform des Strafrechts mit seiner Idee von einem idealen Gefängnisbau, dem Panopticon, aufgenommen. Kritiker einer panoptischen Mediengesellschaft betonen daher die durch Überwachung hervorgerufene wahrscheinliche Einschränkung des individuellen Verhaltens, während in anderen Positionen hervorgehoben wird, dass soziale Kontrolle ohnehin (und auch aus guten Gründen) stattfinde und sich nur als Problem der Legitimationen darstelle. Auch die Beobachter von Kommunikation können in interaktiven Kommunikationsnetzwerken selbst wieder kontrolliert werden. So kann bei einer generellen Gleichheit der Kontrollmöglichkeiten Transparenz und nicht etwa Fremdbestimmung in den Vordergrund treten.

Es geht hier nicht oder nicht nur um die Beobachtung, Kontrolle, Identifikation eines orwellschen Überwachungsstaates, sondern um die Möglichkeiten, die im Prinzip jeder jedem gegenüber hat. Neben der Macht des Staates geht es vor allem um den Effekt dieser Möglichkeiten, darum, dass man im Prinzip gesehen, aufgespürt, beschrieben und damit kontrolliert werden *kann*, und zwar von jedem und überall. Das ist die eine Seite der Gefahr, die andere Seite ist die Tatsache, dass Personen selbst, je nach Kosten-Nutzen-Verhältnis, bereits sind, Privatsphäre aufzugeben bzw. zu „verkaufen“. Darüberhinaus kann jeder die Privatsphäre anderer (mithilfe erlernbarer Tools) im Internet ausspähen [Stocker und Schöpf 2007, Rössler, S. 34].

„Das Internet ist eine Kamera“ [Simanowski 2008, S. 59]. Assoziationen zu *Jeremy Benthams Panopticon* und *George Orwells Big Brother* sind unumgänglich. Doch der große Unterschied ist, dass die Datenspuren ab-

sichtlich hinterlassen werden – es wird nicht versucht, Big Brother zu entkommen, sondern man „zu ihm eilt, an die Tür klopft, ihn so umarmt, dass er, wie beim Boxen, die Schlagkraft verliert“, stellt Simanowski fest [Simanowski 2008, S. 59]. Die absurde Vorstellung findet durchaus Bestätigung in der politischen Theorie – Jean-François Lyotard sprach in den 1980er Jahren davon, *das System durch Überanpassung zum Kollabieren zu bringen.*

2.3.2 Lokale Privatsphäre

Der Begriff „*mobile Privatisierung*“ wurde 1974 von Raymond Williams geprägt [Williams 1992]. Er beschrieb damit die auf den ersten Blick widersprüchliche Beobachtung, dass Mobilität Privatisierung erfordert und fördert. Er war der Auffassung, dass mobile und entsprechend von der Familie entwurzelte Berufstätige in einer fremden Umwelt wenige Möglichkeiten zur Kontaktaufnahme haben. Doch gleichzeitig mit der beruflichen Mobilität der Erwerbstätigen erhöhten sich seit den 1990er Jahren auch die Präsenz und Mobilität von Medien und Informationstechniken. Die Wahrnehmung eines Ortes verändert sich in einem erheblichen Maß durch die Kommunikationsbeziehungen, die dort tatsächlich oder auch potentiell aufgebaut werden können [Gaycken und Kurz 2008, S. 239]. Personen können durch Kommunikation ihr Erleben einer Situation verändern – der Ort nimmt eine andere Wirklichkeit an. Denn Kommunikation eröffnet häufig erst bestimmte Handlungsoptionen, indem jemand besser informiert ist oder auch indem jemand sich in Beziehung setzt zu einem sozialen Netzwerk, das letztlich über den Zugang zu den normativen und epistemologischen Voraussetzungen einer geteilten Wirklichkeitswahrnehmung entscheidet. Nach Williams' Analyse waren mobile Personen auf den Rückzug in ihr Heim und die dort vorzufindenden Medien als künstliche Umwelten, also als Surrogate eines verlorenen Gemeinschaftskontextes, angewiesen. Heutzutage bleibt das Problem einer durch Mobilität erzwungenen Delokalisierung das gleiche, nur der Lösungsansatz unterscheidet sich. Neue Medien erlauben den Aufbau eines parallelen virtuellen Kontextes, eines privaten Schutzraums, der die Herausforderungen fremder und wechselnder Umwelten in den Hintergrund treten lässt.

2.3.3 Informationelle Privatheit

Der traditionelle Schutz der persönlichen Privatsphäre hat an Bedeutung verloren, dies erfordert zunehmend die Verantwortung jeder Person über die eigenen Daten (Selbstdatenschutz) [Gaycken und Kurz 2008, S. 241]. Es nützt nichts, wenn Personen wissen, dass sie beobachtet werden oder dass Informationen über sie gespeichert werden, wenn sie nicht beobachtet oder auf diese Weise erfasst werden wollen – denn es ist dann genau die Tatsache, dass sie sich auf die Beobachtung und Kontrolle einstellen müssen,

die sie daran hindert, selbstbestimmt, authentisch zu agieren. Je mehr Daten gesammelt werden, desto eher können diese auch missbraucht werden. Problematisch ist, dass der liberale Staat sich als einer präsentiert, der unbegrenzten Zugriff auf seine Bürger und Bürgerinnen haben kann und haben will. Inwieweit spielt der Staat eine Rolle als Garant der Autonomie, der negativen wie positiven Freiheit von Bürgern und Bürgerinnen? Stehen Freiheitsrechte und das Interesse an Autonomie auf der einen Seite, so muss für die Einschränkung dieser Rechte nicht nur ein gewichtiger Grund (wie etwa der Kampf gegen den Terror), sondern auch ein hohes Maß an Effektivität bei der Erreichung dieses Ziels in Aussicht gestellt sein. Genau dies scheint jedoch bei den neuen Sicherheitsgesetzen und Datenspeicherungen nicht der Fall zu sein [Stocker und Schöpf 2007, Rössler, S. 34-37].

2.3.4 Zivilgesellschaftlicher Privatbereich

Jessica Heesen unterscheidet zwischen persönlichem und bürgerschaftlichem Privatbereich [Gaycken und Kurz 2008, S. 242]. Im ersteren steht der Schutz der persönlichen Daten im Vordergrund. Bei zweiterem geht es um die Grenzziehungen zum staatlichen und/oder wirtschaftlichen Bereich. Nach Heesen können genau in diesem Bereich Sichtbarkeit und Präsenz im Gegensatz zur persönlichen Privatsphäre erwünscht und förderungswürdig sein. Die Beobachtung erhält im Zusammenhang mit der zivilgesellschaftlichen Sphäre die Bedeutung von Wahrnehmbarkeit. In diesem Zusammenhang ist die *identitätsstiftende Rolle der Beobachtung und Wahrnehmung durch Andere zu betonen.* Sichtbarkeit und wahrgenommen zu werden sind wichtige Voraussetzungen für die Ausbildung von Individual- und Gruppenidentitäten, deren Wert gegenüber einem rigiden Schutz der Privatsphäre in der Mediennutzung abgewogen werden müssen (vgl. [Phillips 2002]). David J. Phillips betont die positive Bedeutung der Identifizierung [Gaycken und Kurz 2008, S. 243]:

> (...) visibility is not always detrimental to individuals and social groups. The construction of identity, the naming of a group, the claiming of membership in a group, the representation and dissemination of knowledge of the group, is a strategy of political power. The political (and epistemological) question is not whether individuals are known and typified. We always are. Rather, it is a question of HOW individuals are known and typified – BY whom, TO whom, AS what, and TOWARD WHAT END we are made visible. [Phillips 2005, S. 95]

Die Unterscheidung zwischen Schutz und Herstellung von Privatheit ist notwendig. Schutz der Privatheit meint vor allem die Wahrung der Integrität der Person. Die aktive Herstellung eines Privatbereichs durch Kombination von

Schutzansprüchen und Verfahren zielt auf die gesellschaftspolitische Bedeutung der Privatsphäre als Raum einer lebensweltlichen Ressource zur Kontrolle staatlicher und ökonomischer Macht ab [Gaycken und Kurz 2008, S. 243].

Gefahren

Die Gefahren liegen zum einen im freiwilligen Verzicht auf informationelle Privatheit, zum anderen in der unfreiwilligen Kontrolle. Sowohl die freiwillige wie auch die unfreiwillige Verminderung des Schutzes informationeller Privatheit können dazu führen, dass bestimmte Formen und Dimensionen selbstbestimmten und authentischen Verhaltens nicht nur in geringerem Maße möglich werden, sondern auch als weniger relevant, weniger zentral, weniger konstitutiv für ein gelungenes Leben begriffen werden: Das hieße dann nämlich auch, dass das Selbstverständnis von Personen sich ändert, wenn und insoweit sie in wichtigen Hinsichten ihres Lebens darauf verzichten, unbeobachtet, unidentifizierbar, nicht zugänglich zu sein [Stocker und Schöpf 2007, Rössler, S. 35].

2.4 Systematik von *Privatsphäre*

Dieser Abschnitt behandelt die Themen Informationsbeschaffung, die Verarbeitung von Information und möglichen Datenmissbrauch im Zusammenhang mit *Privatsphäre* .

Das Informationszeitalter bringt neue und sehr unterschiedliche *Privatsphäre* -Probleme hervor. Notwendig ist eine genaue kulturelle Analyse mithilfe von historischen, philosophischen, politischen, soziologischen und rechtlichen Quellen. Es müssen jene Aktivitäten gefunden werden, die *Privatsphäre* -Probleme verursachen. Bereits 1960 hatte William Prosser vier, voneinander sehr unterschiedliche Arten von Aktivitäten beschrieben, die der *Privatsphäre* schaden [Prosser 1960]:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity that places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

Aktivitäten, die die *Privatsphäre* betreffen sind nicht zwangsläufig problematisch, vorausgesetzt eine Person gibt ihre Zustimmung zur entsprechenden Aktivität (z. B. Big Brother: Beobachtung (Überwachung?) rund um die Uhr).

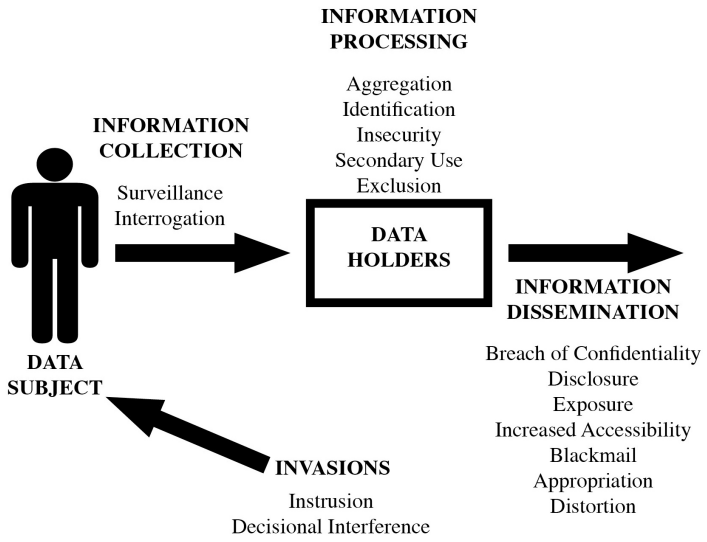

Abbildung 2.1: Solove's Modell der Systematik von *Privatsphäre* (aus: [Solove 2008, S. 104]).

Solove definiert vier Gruppen von Aktivitäten, die der *Privatsphäre* schaden [Solove 2008, S. 103] (siehe Abb. 2.1):

1. information collection
2. information processing
3. information dissemination
4. invasion

2.4.1 Information Collection

Das *Sammeln von Information* beinhaltet sowohl Überwachung als auch die Befragung. Das *Verarbeiten von Information* umfasst das Zusammenfassen und Anhäufen der gesammelten Daten, deren Identifikation, das unsichere Handhaben der Daten, den weiteren, zweckentfremdeten Gebrauch der gesammelten Daten sowie den Ausschluss jener Personen, deren Daten gesammelt wurden. Das *Weitergeben der Information* kann auf unterschiedliche Arten erfolgen. In Form eines Vertrauensbruchs – trotz Versprechens die Daten nicht weiterzugeben, werden diese trotzdem weitergereicht oder in Form der Daten-Offenlegung von vertraulichen Informationen zu der Person oder die Enthüllungen über die Person. Auch Erpressung, die Verwendung des Namens der Person zum eigenen Vorteil oder Rufschädigung betreffen das Weitergeben von Information. Der Eingriff in das Leben von Personen erfordert nicht zwangsläufig deren persönliche Informationen. Der Eingriff

erfolgt durch Formen der Besitzstörung oder auch durch Beeinflussung von Entscheidungen das private Leben betreffend, die über die entsprechende Person gefällt werden.

Die Annäherung von Solove setzt bei der Basis an, er will sich auf das Zusammenwirken der einzelnen Probleme konzentrieren. Dazu ist es notwendig, die Probleme zu erkennen und beschreiben zu können. Solove arbeitete daher mit dem Basis-Ansatz.

Nachfolgend werden Aspekte bestimmter Aktivitäten beschrieben, die der *Privatsphäre* Schaden zufügen.

Panoptischer Effekt

Heute bewegen sich Bürger ständig mit dem Wissen um die Möglichkeit einer Überwachung. Ob jemand gerade überwacht wird oder nicht, bleibt ungewiss, als Konsequenz darausverhält sich der Bürger immer so, als würde er gerade überwacht – dieser Vorgang wird auch als „Panoptischer Effekt“[1] bezeichnet und erklärt, warum auch das Nicht-Überwachen durchaus so wirkungsvoll sein kann wie das aktive Überwachen.

In den Vereinigten Staaten gibt es Gesetze betreffend der Überwachung, allerdings beziehen sich diese auf das *wo* und nicht auf die problematischen *Effekte*, die Überwachung nach sich zieht. So belastet das Wissen um oder die Angst vor der Überwachung auf öffentlichen Plätzen den Sinn von Entspannung und Freiheit, was Menschen genau in diesen Bereichen suchen. Das Gesetz scheint den Schwerpunkt mehr auf Geheimhaltung zu legen als auf einzelne, besondere Probleme und Schaden, der durch Überwachung entsteht. Überwachung führt zu Selbtszensur sowie Selbsthemmung und kann als Werkzeug für soziale Kontrolle gesehen werden.

Befragung und Verhör

Befragung und Verhör machen es für Menschen unerlässlich darüber nachzudenken, wie sie sich selbst verteidigen und rechtfertigen können und sollen aber auch wie das Verweigern desselben gerechtfertigt werden kann oder wie das Verweigern auf andere wirkt. Das Gesetz beschützt zwar vor Befragung, allerdings auf eine komplizierte und unsystematische Art und Weise. Der Schutz durch das amerikanische *Fifth Amendment* ist sehr eingeschränkt, es schützt nämlich nicht die Information an sich. Obwohl Befragung und Verhör großen Schaden und Probleme verursachen können (Zwang, Verbreitung privater Information und gezwungener Verrat) befasst sich das Gesetz über *Privatsphäre* nur in eingeschränkten Situationen damit [Solove 2008, S. 117].

[1] Der Begriff panoptisch geht zurück auf Jeremy Benhams architektonischen Gefängnisentwurf von 1791, genannt „Panoptikum“. Die Gefängniszellen wurden um einen Wachturm herum gebaut, die Wächter konnten jeden Gefangenen dadurch sehen, umgekehrt wussten die einzelnen Gefangenen nicht, ob sie gerade beobachtet wurden oder nicht.

Anhäufen und Zusammenfassen von Daten einer Person führen bei entsprechender Auswertung („Data Mining“, siehe Abschnitt 5.2) zu einem aussagekräftigen Portrait der entsprechenden Person. Menschen erwarten, dass es Einschränkungen gibt darüber, was über sie und andere herausgefunden werden kann. Das Gefährliche beim Anhäufen der Daten ist die Kombinationsmöglichkeit dieser. Personen geben in unterschiedlichen, voneinander unabhängigen Situationen bestimmte persönliche Informationen preis. Einzeln und situationsweise betrachtet ist dies unbedenklich. Erst das Zusammenführen all dieser Information, die Querverbindung der Daten und die Kombination bringen große Gefahr mit sich, da ein umfassendes Persönlichkeitsprofil – ein Portrait sozusagen der Person – entsteht. Umfangreiches Wissen über eine Person führt zu Macht, die jener Person gegenüber ausgeübt werden kann.

Digital Dossiers nennt Solove jene „Akten“, die Regierung und Geschäfte durch die Kombination von privaten Daten einer Person erhalten [Solove 2008, S. 119] – Akten, die ausgedehnte Aufzeichnungen bestimmter Personen enthalten.

> Increasingly, each individual is living alongside a counterpart who exists in the world of computer databases, a digital person constructed not of flesh and blood but of bits and bytes of data. [Solove 2004, S. 1-10]

Identifizierung

Kontrolle durch Identifizierung beeinflusst soziale Strukturen. Die Regierung bekommt mehr Macht über einzelne Personen durch deren Identifizierung. Identifizierung ist ein kritisches Hilfsmittel um radikale oder in Ungunst gefallene Bürger zu suchen und ist daher ein wirksames Mittel um Menschen zu kontrollieren. Identifizierung verhindert die Möglichkeit, dass jemand anonym oder pseudonym aktiv ist. Doch Anonymität und Pseudonymität schützen Menschen vor Vorurteilen basierend auf deren Identität und ermöglichen dem Menschen zu wählen, zu sprechen und Umgang zu suchen mit mehr Freiheit, da Anonymität und Pseudonymität vor der Gefahr durch etwaige Vergeltungsschläge schützen [Solove 2008, S. 125]. Die Gefahr der Identifizierung mittels so genannter ID-Nummer (ID) besteht darin, diese IDs mit Datenbanken zu verknüpfen. Sich identifizieren bedeutet demnach nicht mehr einfach nur seinen Namen zu nennen, sondern es bedeutet, sich mit Daten zu verbinden.

Sicherheitslücken – Identity Theft

Sicherheitslücken im Umgang mit persönlichen Daten kann als Konsequenz *Identity Theft* (Diebstahl der Identität) haben. Ein Dieb bedient sich der

Identität anderer um ein Verbrechen zu begehen. Dn Opfern von Identity Theft steht ein großer bürokratischer Aufwand dann bevor, um ihr „Dossier“ wieder zu bereinigen und mit allen Behörden abzustimmen. Bei Identitätsdiebstahl wird die Identität von Maschinen sichergestellt, daher wird dieser Diebstahl immer wahrscheinlicher/häufiger. Aber: *Können Identitäten gesichert werden? Nein, weil sie verwandelbar, verhandelbar, relativ und sozial sind* [Bennett und Lyon 2008, S. 176].

Jemand, der zu seinem eigenen Nutzen oder zu seiner eigenen Verwendung den Namen oder die Ähnlichkeit von jemand anderem annimmt, unterliegt der Haftung gegenüber dem anderen aufgrund der Verletzung der Privatsphäre (tort of appropriation) [Solove und Schwartz 2008a, S. 205].

Solove und Schwartz stellen allerdings in Frage, warum Berühmtheiten eigene Rechte betreffend deren Namen und Ähnlichkeit zugestanden werden sollen, wenn diese Identitäten doch künstlich erschaffen wurden durch andere [Solove und Schwartz 2008a, S. 213] .

Weitergabe von Daten

Unerlaubtes Weitergeben von persönlichen Daten passiert häufig ohne vorheriger Zustimmung der entsprechenden Person. Es gibt Situationen, in denen dies notwendig ist, beispielsweise um Kriminalität zu stoppen oder ein Leben zu retten. Die Palette an Möglichkeiten des Weitergebens von persönlichen Daten ist groß. Menschen müssen sich bewusst darüber werden, dass die Daten über sie möglicherweise in anderer Art und Weise weiter- und wiederverwendet werden. Dies ist der einzige Schutz für ein Individuum.

Zurückweisung

Zurückweisung entzieht Personen in beträchtlichem Ausmaß die Möglichkeit, Kontrolle über ihr eigenes Leben zu bewahren. Die Information über persönliche Daten einer Personen werden immer mehr dazu verwendet, wichtige Entscheidungen über die entsprechenden Personen zu fällen, allerdings ohne die Person selbst miteinzuziehen. Kontrollverlust über die eigenen Daten ist die Konsequenz.

2.5 Ein neues Konzept für *Privatsphäre*

Einzeln und für sich allein betrachtet wird deutlich, dass die beschriebenen, bestehenden Konzepte von *Privatsphäre* die Problematik entweder zu eng gefasst aufgreifen oder zu umfangreich und somit undeutlich sind. Jedes Konzept allerdings leistet seinen unverzichtbaren Beitrag für ein *neues* Konzept von *Privatsphäre* . Die Herausforderung eines neuen Konzepts besteht im Auffinden des gemeinsamen Nenners der vielfältigen Themen *Privatsphäre*

betreffend. *Privatsphäre* ist ein Zustand, der erzeugt wird und sich daraufhin dynamisch und ständig verändert.

Solove stellt deutlich heraus, dass die Überlegung sein muss, was von *Privatsphäre* erwartet werden *soll*, anstatt zu fragen, was von *Privatsphäre* tatsächlich erwartet wird [Solove 2008, S. 74]. *Privatsphäre* wird durch Normen und Gesetze konstruiert. Es ist ein Bedürfnis, das durch die „Aufdringlichkeit" der Gesellschaft entsteht. Ein Gesetz zu *Privatsphäre* ist ein Werkzeug, mit dem das Bedürfnis gedeckt werden soll. Das Gesetz soll also ein Werkzeug sein, das selbst jene Menge von *Privatsphäre* erzeugt, die jeder Einzelne benötigt.

Solove sieht in seiner Konzeption von *Privatsphäre* in [Solove 2008] diese als eine Menge von Schutzmaßnahmen gegen eine Vielzahl von verschiedenen aber trotzdem ähnlichen Problemen. Jedes Problem hat gewisse Gemeinsamkeiten mit anderen Problemen, aber daneben auch eigene, selbständige Eigenschaften, die das Problem ausmachen. Er möchte mit seinem Rahmenwerk [Solove 2008] einen Leitfaden für die Analyse von *Privatsphäre* schaffen. Der Wert von *Privatsphäre* ist nicht einheitlich, sondern variiert je nach den unterschiedlichen Zusammenhängen in denen *Privatsphäre* involviert ist. Er sieht den Wert von *Privatsphäre* auch nach dem Beitrag, den sie für die Gesellschaft leistet.

Für *Niels Gottschalk-Mazouz* sind starre Regeln in unübersichtlichen, sich schnell verändernden Situationen nicht hilfreich [Gaycken und Kurz 2008, S. 224]. Haltungen, Leitlinien oder Philosophien ermöglichen hier häufig die bessere Orientierung.

2.6 Aktuelle Gesetzeslage

Die Anzahl an Regelungen steigt, Gesetze und Anordnungen werden erweitert. Gleichzeitig steigt die Kritik darüber, ob das Konzept von *Privatsphäre* und die Vorschriften, die es erzeugt, gleich sind dem Ausmaß des sozialen Problems. Doch für einige ist *Privatsphäre nicht* das Gegenmittel zu Überwachung [Bennett 2008, S. 9].

Die aktuelle Gesetzgebung zu *Privatsphäre* wurde eher dazu geschaffen, die Verarbeitung von persönlichen Daten zu regeln und zu lenken als diese einzuschränken. Vorschriften zu *Privatsphäre* können nicht das ungebrochene Verlangen moderner Organisationen nach noch mehr persönlichen Daten verhindern oder einschränken. *Richtlinien helfen bei der Kontrolle aber verhindern oder stoppen die Datensammlung nicht. Privatsphäre* steht immer, wenn es um den Einzelnen geht, den Argumenten von sozialen Vorteilen der Überwachung gegenüber [Bennett 2008, S. 10].

Bennett sieht die Zukunft für ein Netzwerk von *Privatsphäre* -Anwälten in der anhaltenden, unnachgiebigen und informierten Artikulierung des sehr einfachen Theorems, dass Individuen ein Recht darauf haben, auf sie bezo-

gene Informationen zu kontrollieren.

2.7 Zusammenfassung

Privatsphäre ist ein weit gefasster Begriff und kann deshalb nur durch umfassende, viele Bereiche betreffende Schutzmaßnahmen gegen die Vielzahl von verschiedenen und trotzdem ähnlichen Problemen bewahrt werden. Der Wert von *Privatsphäre* kann an dem Beitrag bemessen werden, den sie für die Gesellschaft leistet.

Die Gesetze für *Privatsphäre* zu stärken alleine reicht nicht als Gegenmittel zur Überwachung. Als erster Schritt sollte jedem Einzelnen das Recht eingeräumt werden, die auf sich bezogenen Informationen zu kontrollieren.

Mit diesem Kapitel wurde die Grundlage geschaffen, um die umfassende Problematik von *Privatsphäre* in ihren unterschiedlichen Aspekten zu begreifen. *Privatsphäre* ist der *gemeinsame Nenner* um die Grundproblematik der in Folge besprochenen Themen, nämlich Social Media (siehe Kap. 4), Daten (siehe Kap. 5), Identitätsnachweis (siehe Kap. 6) sowie Überwachung (siehe Kap. 7) und Widerstand (siehe Kap. 8) zu verstehen.

Kapitel 3

Wissensentwicklung und *Privatsphäre*

> Wissen ist der erste Rohstoff, der sich bei Gebrauch vermehrt.
> [BRAND EINS 2009]

Die aktuelle Informationsrevolution wird durch die zunehmende Informatisierung der Gesellschaft erzeugt. Informations- und Kommunikationstechniken durchdringen alle Lebensbereiche. *Entwicklungen im Überschneidungsbereich Wissen und Technik* laufen in der Wissensordnung – der dritten Grundordnung neben der Rechts- und Wirtschaftsordnung – zusammen. Die Wissensordnung ist ein Schlüsselbegriff zum Verständnis des Informationszeitalters und wurde im wesentlichen durch Helmut F. Spinner geprägt [SPINNER 1994].

Der Bereich *Datenschutz* und neue unterschiedliche Delikte, die mithilfe von informationellen Mitteln begangen werden (Informationseingriffe, Datenmissbrauch, Lauschangriff, Vollerfassung des Bürgers durch „Persönlichkeitsprofile“ der Sicherheitsdienste, Computerkriminalität usw.) gehören dazu. Spinner macht dabei auf die „Verdatung“ aufmerksam, das ist die Technisierung *des Wissens selbst* zusätzlich zur wie bisher schon stattgefundenen Technisierung *durch Wissen* („Verwissenschaftlichung“).

Verdatung und Verwissenschaftlichung führen zu neuen Wissensarten und unterschiedliche Wissenslagen in verschiedenen Ebenen. Kritisch dabei ist die Beobachtung der *asymmetrischen Wissensverteilung in der Gesellschaft zugunsten informationsreicher „Datenherren“*, gleichzeitig leidet der Einzelne unter informationeller Überlastung.

3.1 Technikfolgen erster und zweiter Art

Der naturwissenschaftlich-technische Fortschritt ist so schnell, dass er von Wissenschaft und Politik kaum in der Geschwindigkeit zeitgleich erfasst wer-

den kann. So hinkt die Verankerung der Wissensordnung in der Verfassung hinterher. Genau dieser rasante naturwissenschaftlich-technische Fortschritt führt zum gegenwärtigen Wandel der Wissensordnung, definiert auch als *Technikfolgen zweiter Art.*

Technikfolgen erster Art der Mainstream-Technikfolgenforschung treten in Gestalt von Gefahren, Kosten, Katastrophen und Risiken auf[1].

Unter *Technikfolgen zweiter Art* werden die *Auswirkungen* (Wissenschaftswachstum, Informationsexplosion und die Verschmelzung von Technik und Wissen) der wissenschaftlich-technischen Entwicklungen auf die gesellschaftlichen Rahmen- und Randbedingungen für die Wissenschaft und Technik, in Gestalt eines *stillen Wandels der Wissensordnung* verstanden[2].

Die Auswirkungen der Technikfolgen zweiter Art auf die ordnungspolitischen Rahmenbedingungen ihrer selbst und die gesamte „kognitive Verfassung" der Gesellschaft sind noch kaum erforscht, genauso wenig wie die von ihnen ausgehenden Technisierungsprozesse des Wissens [Spinner 1994, S. 65].

Sandor Gaycken kommt im Zuge seiner Auseinandersetzung mit der neuen technischen Situation zum Schluss, dass sowohl Mensch als auch Technik geistig-technisch auf-, um- und nachgerüstet werden [Gaycken und Kurz 2008, S. 35]. Das ist eine neue technische Situation. Nimmt man das Technotop dazu als Begriff für den von Mensch und Technik gemeinschaftlich bewohnten Lebensraum, kann man diesen Prozess auf die folgende Formel bringen: Das Technotop wird „vergeistigt". Gaycken macht auf eine notwendige Auseinandersetzung und Diskussion mit der entstehenden Kontrolltechnik (technisierte Überwachung), notwenig um einen „cultural lag"[3] zu verhindern, aufmerksam. Die Konsequenzen einer Technologie infolge der „kulturellen Verzögerung" erst nach deren Auftreten zu erkennen, sieht er besonders problematisch. Er sieht als eine der Kernfragen bezüglich der technischen Überwachung, ob sich nämlich Gerechtigkeit und Demokratie durch eine Technologie schützen lassen, welche die Freiheit und das geistige Leben beschränken kann und nicht vor Missbrauch zu bewahren ist. Die Antwort liegt im Wert der Freiheit des geistigen Lebens, welche eine wichtige kulturelle Errungenschaft des Menschen ist. Sie ist die Basis der gegenwärtigen Formen von Individualität und Gemeinschaft, von Kultur und Politik, von Wissen und Wissenschaft. Und sie ist vor allem auch die einzige reale Bezugsebene des Wertes der Freiheit.

[1] Quelle: http://www.rz.uni-karlsruhe.de/~Helmut.Spinner/

[2] Quelle: http://www.rz.uni-karlsruhe.de/~Helmut.Spinner/

[3] Diese These besagt, dass sich die Technik schneller entwickelt als die zu ihrem Einsatz nötigen Werte, so dass die materielle Kultur der immateriellen Kultur stets einen Schritt voraus ist (vgl. [Ogburn 1969]).

3.1.1 Technikfolgenproblematik

Spinner geht es in seinen Untersuchungen der Wissensordnung um die Wissensstruktur technischer Artefakte bestimmter Art sowie um die Technik(mit)-Bestimmtheit der neuen, mehr oder weniger technisierten Erkenntnisstile, Wissensarten und Wissenschaftsformen [Spinner 1994, S. 55]. Den aktuellen Stand der Forschung betreffend sieht Spinner eine Umorientierung der Forschungsanstrengungen unumgänglich [Spinner 1994, S. 63]: „Ein Umorientierung auf die unpopulärere, aber nicht weniger wichtige und noch sehr vernachlässigte Technikfolgenproblematik zweiter Art erscheint beim jetzigen Forschungsstand geboten, nicht zuletzt auch unter dem Aspekt der abnehmenden Grenzerträge herkömmlicher Folgenforschung."

3.2 Bedeutung der Wissensordnung

Die Bedeutung der *Wissensordnung* für die Gesellschaft liegt in ihrer Produktivkraft, dem wissenschaftlich-technischen Fortschritt, sowie Unterhaltungs- und Verwaltungsmittel (außerwissenschaftliche Information als Massenmedium der Kommunikation und Kontrolle). Vor allem durch die Leitfunktion als Weichensteller für die kognitiv-technischen Entwicklungen im informationstechnologischen Zeitalter macht die dritte Ordnung der ersten (Rechtsordnung) und zweiten (Wirtschaftsordnung) Ordnung gegenüber gleichrangig [Spinner 1994, S. 23].

> Wissen ist Wissen, zum speziellen Gebrauch außerdem wahlweise Ware, Sache, öffentliches Gut und Kulturgut. [Spinner 1994, S. 33]

> Wissen braucht eine Trägersubstanz, wie Grundstücke – aber anders als die mit ihrem Grund fest verbundenen Erdstücke kann es den Träger leicht wechseln, sei es das Gehirn eines Informationsfressers, das Papier eines Buches oder die Festplatte eines Computers. Wissen ist substanzlos wie modernes Geld, für das es keinen Goldstandard mehr gibt – trotzdem ist es geldartig. [Spinner 1994, S. 45]

Spinner hebt vier Eigenschaften von Wissen heraus [Spinner 1994, S. 47]:

- Wissen als *immaterielles Gut* steht in einem flüchtigen Verhältnis zum Besitz
- Wissen als *ideeller „Überbau"* ohne materielle „Basis" in einem engen Verhältnis zu den stützenden oder störenden Interessenslagen, insbesondere der Wissensträger (Datenherren)
- Wissen als gehabte oder geäußerte Meinung, an die man sich nicht halten muss, in einem problematischen Verhältnis zum Handeln

- Wissen als ohnmächtiger „symbolischer“ Aktivitätsmodus des „hypothetischen Verhaltens“ in einem grundsätzlichen Abhängigkeitsverhältnis zu den Mächten dieser Welt

Nach Spinner ergeben sich die Überlegungen zur Wissensordnung heute aus dem Zusammentreffen von drei Entwicklungen im inner- und außerwissenschaftlichen Bereich [Spinner 1994, S. 51]:

mit dem *informationstechnischen Durchbruch* zu Wissenstätigkeiten und Wissensbeständen neuer Art (Künstliche Intelligenz, Expertensysteme usw.) oder bislang unmöglicher Größenordnung (Informationsspeicherung ohne Kapazitätsbegrenzung, Datenverarbeitung im großen Stil, weltweite Übermittlung in Echtzeit usw.);

mit der *westlichen Renaissance des ordnungstheoretischen und ordnungspolitischen Denkens* infolge der geänderten weltpolitischen Lage, die in Osteuropa und in der Dritten Welt Neuordnungen möglich und nötig gemacht hat;

mit der *Erweiterung des Umweltbewusstseins durch Einbeziehung der informationellen Umwelten* in die Natur-, Kultur- und Gesellschaftsvorstellungen sowie in das Aufgabenfeld der Technikfolgenforschung.

3.3 Neuer Wissensschwerpunkt liegt bei den Datenherren

Die aktuelle Informationsrevolution (exponentieller quantitativer Wissenswachstum) wird verursacht durch die zunehmende Informatisierung der Gesellschaft infolge des Eindringens der Informations- und Kommunikationstechniken in alle Lebensbereiche [Spinner 1994, S. 67]. Gleichzeitig erfolgt eine *mengenmäßige Verschiebung des Wissensschwerpunkts zum Daten- und Regelwissen* sowie die konzentrierte Häufung bei bestimmten Stellen – vor allem staatlichen Behörden und privatwirtschaftlichen Organisationen, den so genannten „*Datenherren*“. Spinner unterscheidet zwischen wissenschaftlichen und außerwissenschaftlichen Wissensarten. Die außerwissenschaftlichen Wissensarten wiederum unterteilt er in Alltags-, Akten- und Medieninformation.

Spinner stellt fest, dass Meinungen spätestens mit ihrer Äußerung nicht mehr im ausschließlichen Privateigentum ihrer – sich meistens selbst enteignenden – Exbesitzer sind. Beeinträchtigungen der Meinungsfreiheit sieht er nicht als Verletzungen gewöhnlicher Rechte, sondern als Verstöße gegen Prinzipien der Wissensordnung [Spinner 1994].

Deutlich wird dies durch die Möglichkeit des Data Mining seitens der Datenherren, genau erläutert im Abschnitt 5.2.

3.4 Zukunft der Wissensordnung und Datenschutz

Spinner stellt für seine Weiterarbeit u. a. folgende Arbeitshypothesen auf [Spinner 1994, S. 112]:

1. Technisierung und/oder Kommerzialisierung größerer Informationsbereiche schaffen neue Bedingungen, aber noch keine neue Wissensordnung.
2. Was sich beim jetzigen Stand der Dinge daraus ergeben hat, ist sozusagen eine naturwüchsige Wissens-Unordnung, die für die Zukunft erst zu gestalten ist: rechtlich, wirtschaftlich, technisch, politisch, vor allem aber ordnungsmäßig!

Die zweite seiner Arbeitshypothesen (siehe Auflistung 3.4) zeigt deutlich, wie die Aufgabe der Neuordnung bisher dem Rechtsdenken überlassen wird, Spinner weist auf das Beispiel *Datenschutz* hin. Bereits Spinner merkt an, dass es so zu einem ordnungspolitischen Flickwerk wird, denn viele der Probleme sind nicht rechtsförmig darstellbar. Er kritisiert das ordnungspolitische Denken der Ökonomie hinsichtlich des Informationssektors – nach Spinner hatte die Ökonomie sich bisher nur der Wettbewerbsordnung auf Wissensmärkten angenommen und die weitere, wichtigere Wissensordnung sträflich vernachlässigt. Spinner fordert daher in seiner dritten Arbeitshypothese die Gleichstellung der Wissensordnung im Rahmen der gesamten Gesellschaftsordnung mit Wissenschaft, Politik, Publikum sowie allen anderen Teilordnungen.

3.5 Qualifiziertes Wissen und Amateurkult

Spinner nennt maßgebliche, weitgehend autonome Einflussfaktoren hinsichtlich der Technikfolgen erster und zweiter Art, getrennt oder verbunden [Spinner 1994, S. 114]:

- die *Technisierung des Wissens* (oder „Informatisierung“ im wissenstechnischen Sinne), mit der elektronischen Datenverarbeitung als Vorreitertechnik, deren Auswirkungen über die Speicherung, Verarbeitung, Vernetzung, Verwaltung längst auf die anderen Schwerpunkte der Wissensproblematik ausstrahlen, darunter immer noch am wenigsten auf die Wissenserzeugung;
- die *Kommerzialisierung von Wissensgütern*, insbesondere im außerwisschenschaftlichen Bereich;
- die *Globalisierung der Informationsströme* im nationalen und internationalen Rahmen, insbesondere im Geschäftsleben und bei den Massenmedien;

- teilweise als Reaktion darauf, aber im Endeffekt eher verstärkend, die *Privatisierung bestimmter Wissensarten oder Wissensbestände*, einerseits von Datenwissen zur Abschirmung der „höchstpersönlichen“ Privatsphäre gegen Informationseingriffe als erweitertes Persönlichkeitsrecht, andererseits von kommerzialisierbaren, geldwerten Wissensgütern zwecks Ausdehnung der Nutzungsmöglchkeiten als erweitertes Eigentumsrecht.

Diese vier Entwicklungen haben hinsichtlich Privatisierung und Kommerzialisierung eine Gemeinsamkeit: die weitgehende Entbindung von wissenschaftlichen Richtigkeits- und Gütekriterien für qualifiziertes Wissen.

> Weder für die technische Verarbeitung durch den Computer oder für die öffentliche Kommunikation durch Medien noch für den privaten Gebrauch als freie Meinung oder die wirtschaftliche Verwertung durch den Markt muss Wissen wahr, wichtig, sinnvoll, überprüft oder sonstwie qualifiziert sein. [Spinner 1994, S. 115]

Spinner sieht dennoch Möglichkeiten, die neue Wissensordnung systematischer, einheitlicher und einsichtiger aufzubauen. Er schlägt ein Gebot der einheitlichen Regelung für die drei eigenständigen Wissenszonen vor [Spinner 1994, S. 146]:

1. Ordungspolitischer Leitwert für die Qualitätszonen ist die *Veränderungsfreiheit allen Wissens*, ohne fundamentalistische Vorbehalte und protektionistische Ausschlussbefugnisse gegenüber Informationseingriffen in die gegebene Wissenslage.
2. Für die Schutzzonen gilt der gegengerichtete Leitwert der Beeinträchtigungsfreiheit der eigenen Position, also des Eingriffsverbots in den inneren Wissenskreis, zum Beispiel der höchstpersönlichen „freien Meinung“ oder informationellen Selbstdefinition.
3. Für die Verbreitungszonen gilt *Verkehrsfreiheit der Informationsströme*, einschließlich Gegeninformation, mit Chancengleichheit für beide Seiten (zu denen als dritter Informationsstrom das kognitive Hurenkind der Desinformation kommt).

3.5.1 Amateurkult als Qualitätskontrolle

Nach *Clay Shirky* ist die Idee des vom Benutzer erzeugten Inhalts („user-generated content“) des Internets nicht nur eine Theorie kreativer Möglichkeiten, sondern eine soziale Theorie über die Beziehung von Medien [Shirky 2008, S. 84]. User-generated Content führt dazu, dass die Filterung, ob ein Inhalt gut oder schlecht ist, sozial erfolgt. User-generated content ist ein

Gruppenphänomen geprägt von Amateuren ohne Beteiligung von Fachleuten und führt daher zur Sozialtheorie der Medienbeziehungen. Die Kommunikation erfolgt in kleinen Gruppen und nicht mittels Broadcast. Die Gemeinschaft wird zum Publikum. Shirky spricht auch von der „community of practice“ [Shirky 2008, S. 96], in der jede Gruppe Rat, Feedback und Ermutigung anbietet und die Motive dafür ausdrücklich nicht finanzieller Natur sind.

Andrew Keen warnt in seinem Buch „The Cult of the Amateur. How Today's Internet is Killing Our Culture“ vor der Diktatur der Masse, die Qualität durch Quantität ersetze: als Ranking in Suchmaschinen auf der Grundlage von Hits, als „social bookmarking“ von News auf der Grundlage des Lektüreverhaltens der Besucher einer News-Website oder als Überschüttung der Expertenmeinung durch Millionen Hobbyspezialisten in Wikipedia.

Nach Clay Shirky ist heute jeder ein „media outlet“ [Shirky 2008, S. 55]. Das Amateurwesen löst die Professionalität ab [Shirky 2008, S. 61]. Shirky sieht die Identität des Konsumenten heute so [Shirky 2008, S. 108]:

> Amateur production, the result of all this new capability, means that the category of „consumer“ is now a temporary behavior rather than a permanent identity.

Doch der Amateurkult lässt auch eine neue Form der Qualitätskontrolle entstehen. Twitter wird damit zu einem individualisierten Newsfeed dessen Nachrichten von Personen stammen, die gekannt werden, denen vertraut wird. Die Flut an Nachrichten wird demnach vertraulich vorgefiltert.

Werden Wikipedia, eine Enzyklopädie zusammengestellt von wenigen aktiven Internetnutzern, und die Encyclopedia Brittanica gegenübergestellt, so muss dem Lexikon von Amateuren doch eine gewisse Sorgfalt zugesprochen werden. Wikipedia bereichert mit dem Umfang an Einträgen das frei zugängliche Wissen im Netz.

3.5.2 Intellektuelle im Internet unerwünscht

Adam Sobocynski schreibt in einem Zeitungsartikel[4]:

> Es eint der Neid die Amateure. Was zu kompliziert erscheint, wird verhöhnt. Gemeinschaft soll endlich wieder sein, so noch Gesellschaft ist. Nicht anderes meinen Heil versprechende Begriffe des Netzes wie 'Interaktion', 'Partizipation' oder 'E-Community', die jene Selektionsmechanismen aus der Welt zu schaffen versprechen, auf deren Anerkennung jeder Aufklärungsdiskurs beruht.

Soboczynski begreift den Intellektuellen „als der, der er bislang war, Störenfried des Konsenses, Vermittler von Wissensbeständen, Korrektiv des Staats“

[4]DIE ZEIT Nr. 22 vom 20. Mai 2009, S. 45, „Das Netz als Feind“ von Adam Soboczynski

im Verschwinden. Seiner Ansicht nach wird der Intellektuelle „Internetrandzonen“ bewohnen und nur Foren besuchen, die ausschließlich von anderen Intellektuellen aufgesucht werden.

Social Tools also für die Masse nicht für den Individualisten im Sinne von Intellektuellen?

3.5.3 Political Remix Video

Jonathan McIntosh stellt das „Do it yourself“ vor den benutzer-generierten Inhalt. Er prägte das *Political Remix Video* (PRV).

Nach Jonathan McIntosh [Stocker und Schöpf 2008, S. 58ff] ist eine der wesentlichsten Eigenschaften der PRV-Arbeiten das *kritische Hinterfragen*. Nur eine Handvoll von Großkonzernen, in deren Besitz sich die Nachrichtensender und die Unterhaltungsindustrie befinden, sind die Macher und Hüter unserer Kultur.

Die Remixer verwenden die Taktik der *Identitätskorrektur*. Identitätskorrektur funktioniert in PRVs, indem Werbungen einflussreicher Institutionen kopiert werden, um deren sorgsam konstruiertes Image zu verändern oder zu „korrigieren“. Durch diesen Korrekturvorgang wird die Identität des Zielobjekts neu bestimmt, um die Kehrseite der Praktiken eines Unternehmens aufzuzeigen, während gleichzeitig humorvoll und ironisch mit der Marke gespielt wird.

Political Remix kann den Menschen das Gefühl von aktiver Partizipation und Eigenverantwortung verleihen, indem es ihnen ein Medium bietet, über das sie ihre eigene Wirklichkeit ausdrücken und sich kreativ engagieren können.

3.6 Zusammenfassung

Das ordnungspolitische Denken der Ökonomie kann nicht in gleicher Form auf den Informationssektor angewendet werden. Helmut F. Spinner stellt als Auswirkung der Technikfolgen erster und zweiter Art die weitgehende Entbindung von wissenschaftlichen Richtigkeits- und Gütekriterien für qualifiziertes Wissen fest, eine Beschreibung für den wachsenden Amateurkult. Der festzustellende Amateurkult hat allerdings auch seine positive Wirkung in Form eines Filters und einer (personalisierten) Qualitätskontrolle.

In der nachfolgenden Auseinandersetzung mit Social Tools (siehe Kap. 4) wird dargestellt, dass diese nicht nur für die breite Masse oder den wachsenden Amateurkult gedacht sind. Das Unterscheiden zwischen Amateuren und professionellen Schreiber wird aufgehoben durch eine Vielfalt an personalisierter und trotzdem hochgradig vernetzter Kommunikation, was eine bisher unmögliche Art der Gruppenaktion und -kommunikation ermöglicht.

Kapitel 4

Social Media

> „The moment we are living through, the moment our historical generation is living, is the largest increase in expressive capabilities in human history“,

so Clay Shirky im Juni 2009, als er im Rahmen eines Interviews[1] seine positive Sicht auf soziale Medien präsentierte. Mit seiner positiven Sicht gehört er (noch) zu einer Minderheit. Es überwiegen kritische Standpunkte gegenüber neuen, sozialen Medien, die nur allzu sehr vermeintliche Gefahren hervorheben.

Mit Social Tools ist das Internet *jetzt endlich jenes interaktive Medium geworden, das es sein sollte* – länderübergreifend, vorurteilsfrei, frei für jeden. Dieses Kapitel soll einen Überblick über die Entwicklung der Medien sowie der langsam gereiften Kritik gegenüber der neuen Kommunikationsmedien bieten. Aspekte der Selbstfindung werden dabei genauso behandelt wie die Auswirkungen auf die Werbewelt und die Verantwortung eines jeden einzelnen Benutzers selbst.

Social Media führen zu einer neuen Diskussion über Öffentlichkeit und Privatsphäre sowie öffentliche Privatsphäre. *Privatsphäre* existiert im realen Leben auch in der Öffentlichkeit, in der virtuellen Kommunikationswelt ist die Situation eine andere.

Es wird beschrieben, warum Social Tools eine völlig neue Art der Gruppenkommunikation und -aktion ermöglichen. Kritische Anmerkungen zu Technikakzeptanz und Medientheorie beenden die Auseinandersetzung mit Social Media.

[1] How social media can make history, Juni 2009, http://www.ted.com/talks/clay_shirky_how_cellphones_twitter_facebook_can_make_history.html.

4.1 Entwicklung der Medien

Buchdruck, aufgezeichnete Medien (Fotografie, Ton, Film) sowie Fernsehen und Radio prägen die Medienlandschaft des 20. Jahrhunderts. Es handelt sich um Broadcast-Medien (ein Sender an viele Empfänger) und zeigt deutlich, wie es den genannten Medien unmöglich ist, Konversation und Gruppenbildung miteinander zu verbinden. Medien, die gut sind für Konversation, ermöglichen keine Gruppenbildung und jene Medien, die Gruppenbildung ermöglichen, erlauben wiederum keine Konversation. Jeder in der Gruppe bekommt beim Broadcasting dieselbe Nachricht (Zeitung, Radio, Fernsehen).

Genau diese Situation hat sich durch die sozialen Medien verändert. Internet bietet gleichzeitig Unterstützung für Konversation und Gruppen („many-to-many“). Alle Medien werden digitalisiert, daher wird das Internet zum Hauptträger aller Medien.

Jeder ist Produzent und Konsument zugleich und nicht mehr nur Konsument, das ist eine bedeutende Veränderung in der Medienlandschaft. Jeder ist zum Akteur geworden, dadurch werden koordinierte globale Tätigkeiten möglich.

Die Medien heute sind global und sozial zugleich. Das Versenden von Nachrichten funktioniert heute verteilt-bidirektional durch die sozialen Netzwerke, nicht mehr in Broadcasting-Form (einer an viele). Nach Shirky besteht die Herausforderung in der Nutzung der neuen Möglichkeiten, die diese Veränderung in der Medienlandschaft bringen.

> It is a real cyberspace, known only to a subculture, which is growing at such a rate that it has a real chance of evolving into a spontaneous, bottom-up, surprisingly smoothly anarchic mass medium of the future. (...) geographically distributed computer-mediated communication is a social mechanism of great power, and the possible antecedent of a hybrid medium of the future where telepresence will find its place along with alphanumeric messages. [Rheingold 1991, S. 197]

Mit Social Tools ist das Internet *jetzt endlich jenes interaktive Medium geworden, das es sein sollte* – länderübergreifend, vorurteilsfrei, frei für jeden. Unüberhörbar ist dabei die stark negative Kritik dieser neuen Möglichkeiten, die Social Tools bieten, von Menschen, die das neue Leben einfach nicht verstehen wollen. Für viele scheinen sie über Nacht gekommen zu sein, doch bereits bei Usenet konnte der Prozess beobachtet werden [Rheingold 1991, S. 199]:

> Researchers can squirt electronic versions of their latest preprint, months before it appears in scientific journals, to the two dozen or three thousand desktops of their closet colleagues. It has happening, more or less unreported, for years.

4.2 Ursachen, Auswirkungen, Erfolg

Marshall McLuhan beschreibt das Medium als Botschaft [Kloock und Spahr 2000, S. 39ff.]: persönliche und soziale Auswirkungen von Medien, die sich *aus ihrer Anwendung heraus* ergeben. Technik verändert die Dimension von Raum und Zeit hinsichtlich, wie die Welt wahrgenommen wird. Die Botschaft des Mediums entspricht dem, was es mit dem Menschen macht und nicht dem Inhalt, der Inhalt verschleiert die Wirkungsweisen.

Zu den *verschleierten Wirkungsweisen der Social Tools* könnte man das Ziel des umfangreichen und umfassenden Profilings zählen zum Zweck einer möglichst zielgruppengenauen Werbung. Roberto Simanowski sieht in den Präsentationsportalen wie MySpace oder Facebook nur die Schaffung von Orten der Institutuionalisierung im Internet [Simanowski 2008, S. 66]. Orte von größtem Interesse für die Global Player aus Wirtschaft und Unterhaltungsindustrie.

Die Werbung muss immer unterhaltsamer, witziger, anspruchsvoller und gleichzeitig zum ästhetischen Trendsetter werden. Sie verkleidet sich als Inhalt und zehrt vom guten Ruf des Amateurs, der in Blogs oder auf YouTube in Erlebnisberichten und gut gemeinten Ratschlägen unbezahlt für ein Produkt wirbt [Simanowski 2008, S. 73].

Nach Simanowski musste den Internetbenutzern erst jemand die neuen Möglichkeiten der Selbstfindung schmackhaft machen. Ihnen einen Ort dafür anweisen, die Arbeit erleichtern und vor allem die Sache kostenlos anbieten. Für diese Dienste nahmen sie die zentrale Erfassung ihrer Daten in Kauf, deren Weitergabe an interessierte Dritte (denn alle Daten innerhalb dieser Portale gehören juristisch deren Betreiber) sowie die Belästigung durch Werbung und Umfragen.

MySpace und Facebook erinnern auch an die Bonuskarten, mit denen Kunden für einen lächerlichen Discount zur Preisgabe von Daten überredet werden, die für die Werbeindustrie interessant ist. (...) *Man wird Auge und Ohr nicht mehr abwenden können, und die Werbevideos werden nicht mehr am oberen Seitenrand platziert sein, an dem man sich irgendwann erfolgreich vorbeigelesen hat* [Simanowski 2008, S. 67].

Simanowski beruft sich auf den US-amerikanischen Soziologen Richard Sennett, für den Menschen nur dann gesellig sein können, wenn sie über einen gewissen Schutz voreinander verfügen [Simanowski 2008, S. 159]. Sennett spricht von der *Tyrannei der Intimität*, so der deutsche Titel seines Buchs aus dem Jahr 1974, denn je vertrauter man dem anderen sei, desto geringer werde der Spielraum, sich anders zu verhalten, als der andere erwartet. Rettung verheißt die Anonymität der Großstadt sowie gerade jene Technologie, die das Private öffentlich macht. Denn die Kommunikationsformen des Internets (Chat, Blog, Facebook usw.) werden durch die Freiheiten des Persönlichkeitsdesigns zu Probebühnen alternativen Verhaltens.

Facebook und Co. gewöhnen ihre Teilnehmer daran, intime Informa-

tionen über sich der ganzen Welt anzuvertrauen. Es ist normal geworden, dass der private Raum aus Glaswänden besteht. Die Überwachung ist nicht ideologisch begründet wie in Orwells „Big Brother"-Dystopie 1984, sondern pragmatisch-finanziell. Alle lieben Data-Mining, alle lieben Suchmaschinen [Simanowski 2008, S. 172].

Erst wenn die neuen Technologien vollständig in das Alltagsleben übernommen sind („normal" geworden sind), verändern sie die Gesellschaft. Social Tools sind daher eine Herausforderung für die moderne Gesellschaft. Jessica Heesen sieht im Handeln mit Kommunikationsmedien eine doppelte Verantwortung [Gaycken und Kurz 2008, S. 245]:

> Erstens geht es um eine Wahrung der persönlichen Integrität über Verhaltenskodizes in der Online-Kommunikation sowie Pseudonymisierungs- oder Anonymisierungsverfahren bei Nutzungsangeboten des Ubiquitous Computing. Zweitens geht es um die (institutionell verankerte) Herstellung gesicherter und unabhängiger Nutzungsmöglichkeiten von Informations- und Kommunikationstechniken für die Angelegenheiten der lebensweltlichen Privatsphäre zur Garantie ihrer *Reproduktions-* (zum Beispiel in Hinsicht kultureller Identitäten) wie auch ihrer *Artikulations*fähigkeit im Diskurs sozialer und politischer Geltungsansprüche.

4.2.1 Öffentliche Privatsphäre

Privatsphäre ist neben dem so genannten geistigen Eigentum eines der wichtigsten netzpolitischen Themen [Stocker und Schöpf 2007, Armin Medosch, S. 21]. Tools zur Selbstveröffentlichung offenbaren nicht nur unseren Blick auf das Private, *sondern* auch unser Verhältnis zur Öffentlichkeit [Stocker und Schöpf 2007, Ina Zwerger, S. 21]. Es scheint fast, als hätte sich ein neuer Persönlichkeitstyp gebildet, welcher die alten bürgerlichen Regeln über Scham und Anstand hinter sich gelassen hat [Stocker und Schöpf 2007, Zwerger, Medosch, S. 23]. Das Herzeigen-Wollen ist stärker als die Angst überwacht zu werden.

Die Akzeptanz und Verbreitung privater Webseiten, Mobiltelefonen, Teilnahme an sozialen Netzwerken wie Facebook, andere Nutzungsoptionen aus dem Web 2.0 wie Twitter usw. lassen auf eine Sorglosigkeit in Bezug auf den Datenschutz schließen. Soziale Netzwerke betrachtend erfordert die Ausübung der Selbstbestimmung die Möglichkeiten der Bewertung, Klassifizierung und indirekte Außendarstellung von Beziehungsqualitäten innerhalb der jeweiligen Informationssysteme (wer darf was von mir wissen).

Doch genau durch das Gewähren und Verweigern von persönlichen Informationen gegenüber Beteiligten des Netzwerks hinterlässt man ein indirektes Profil des persönlichen Beziehungsnetzwerkes. Selbst Techniken zur

Anonymisierung und Pseudonymisierung von Identitäten verhindern nicht, dass Strategien der persönlichen Datenverwaltung ein fester Bestandteil der Fremd- und Eigenwahrnehmung werden. „In sozialen Netzwerken kann der Selbstdatenschutz insofern problematisch werden, als er ex negativo über das Verhalten und die Präferenzen der jeweiligen Nutzerinnen und Nutzer berichtet“, so Jessica Heesen [Gaycken und Kurz 2008, S. 241].

Clay Shirky beschreibt die aktuelle Auffassung von *Privatsphäre* im Internet in einem Interview[2] so: „Anything that is accessible to me, is also acceptable for me“. Er steht diesem sogenannten *social bargain* kritisch gegenüber und findet die Situation völlig unangemessen.

Als Beispiel vergleicht er die Situation der realen Welt mit der Welt der virtuellen *social tools*. Eine Gruppe von jungen Leuten steht vor einem Supermarkt und unterhält sich – es wäre unakzeptierbar, käme plötzliche jemand und stünde sich neben sie um zuzuhören und zuzusehen. Doch bei Facebook, Twitter usw. ist dies die „ganz normale“ Situation. Er kritisiert, dass junge Menschen in diese Situation hineingeboren werden ohne zu wissen, was sie vermissen.

Die aktuelle Gesellschaft hat seiner Meinung nach diese jungen Menschen dessen beraubt, was sie nicht wissen zu vermissen – nämlich eine besondere Art von *Privatsphäre* . *Social Tools* fehlt die Möglichkeit, zwischen Öffentlichkeit und Halb-Öffentlichkeit zu unterscheiden, denn jeder ist darin immer in der Öffentlichkeit, niemals nur halb in der Öffentlichkeit.

Es stellt sich daher die Frage, in welcher Öffentlichkeit wir wann und wo leben. Diese Frage erfordert Aufmerksamkeit, doch ermöglicht damit auch das Ausschöpfen der Möglichkeiten sozialer Medien ohne dabei die eigene Individualität und Privatsphäre zu verlieren. Es ist eine Forderung nach einer virtuellen privaten Öffentlichkeit.

4.2.2 Internet-Werbung

Alles, was eine Person im Internet macht, hinterlässt Spuren – mittels Cookies dauerhaft. Cookies waren ursprünglich als Cyber-ID angedacht [Parenti 2003, S. 101]. Selbst wenn der Anwender einstellt nur bekannte Cookies zu akzeptieren, ist er offen für eine große Anzahl ihm fremder Unternehmen: Unternehmen und dergleichen haben häufig zahlreiche Zusammenschlüsse, Mitglieder, Untergruppen und all diese gehören zum Unternehmen dazu, damit zählen deren Cookies zu den „bekannten“.

Suchmaschinen speichern alle eingegebenen Suchbegriffe mit der zugehörigen IP-Adresse (damit kann der Rechner bis auf eine Genauigkeit von 20km geortet werden) sowie Datum und Uhrzeit des Zugriffs. Alle Sucheingaben werden kontinuierlich festgehalten, was mit der Zeit zu einem umfangreichen Profil führt.

[2] Can Privacy exist on the Internet, 5. November 2007, http://www.switched.com/2007/11/05/can-privacy-exist-on-the-internet/.

Soziale Netzwerke wie Facebook oder Myspace präsentieren sich sehr vertraut – als wäre man unter Freunden. Das Gefährliche daran allerdings ist, dass es ein Schlüsselloch ist, durch das jeder (vor allem Unternehmen) seinen Blick werfen kann [Gaillard 2009, S. 54]. In Frankreich hat G29, eine Arbeitsgruppe zum Datenschutz, welche auch die Europäische Union berät, interveniert und von den großen Suchmaschinenanbietern die Löschung aller Daten nach sechs Monaten gefordert (bis dahin wurden alle Daten kontinuierlich gespeichert). Microsoft und Yahoo haben akzeptiert, Google verweigerte mit der Begründung, dass es die IP-Adressen nach neun Monaten anonymisiere. 2007 wurde Google dafür von den Big Brother Awards ausgezeichnet[3].

Die großen Mühen der Suchmaschinenhersteller zur Profilerstellung der Benutzer hat einen einzigen Hintergrund: Online-Werbung. Google hat um drei Milliarden Dollar Double Click[4] – eine Agentur spezialisiert auf digitales Marketing – gekauft.

Digitale Mundpropaganda und Selbstinszenierung 2. 0

Multiplikatoren können jene sein, die andere beeinflussen, aber auch jene, die sich für ein Produkt interessieren. Dem Physiker und Soziologen *Duncan Watts*[5] nach muss sich mehr auf die *Dynamik der Ausbreitung* als auf einige wenige sendungsbewusste Auserwählte konzentriert werden[6]. Er sieht in Twitter und Youtube neue Empfehlungsformen: Eine Botschaft wird an eine Gruppe geschickt, von der jemand einige Mitglieder kennt, aber es wird keine Antwort erwartet. Er sieht dies als eine Form der Selbstinszenierung. Informationen im Profil präsentieren stellvertretend den Teilnehmer. *Eine öffentliche Identität wird konstruiert.*

4.3 Die Macht der Gruppe

Clay Shirky setzt sich mit der Macht von Gruppenaktion auseinander [Shirky 2008]. Die soziale Sichtbarkeit wird durch Facebook usw. erhöht. Neue Arten von Gruppenbildungen sind durch die neuen Technologien (Twitter, Facebook usw.) möglich. Shirky ist der Ansicht, dass, wenn die Art und Weise der Kommunikation geändert werden kann (wie es im Moment passiert), auch die Gesellschaft geändert werden kann [Shirky 2008, S. 17].

Die neuen Werkzeuge (*Social Tools*) dazu werden unterschiedlich bezeichnet, beispielsweise als *social software*, *social media*, *social computing* usw. Hinter all den Bezeichnungen liegt eine gemeinsame Kernidee: teilen, kooperieren, gemeinsam Maßnahmen ergreifen, und das alles außerhalb des

[3] http://bigbrotherawards.eu.org/Google-Inc.html

[4] http://www.doubleclick.com/

[5] http://research.yahoo.com/Duncan_Watts

[6] brand eins Wirtschaftsmagazin, Heft 07 Juli 2009, „Tupperpartys funktionieren nicht im Internet“ von Dirk Liesemer und Max Rauner, S. 120ff

traditionellen Systems von Institutionen und Organisationen.

Die elektronischen Netzwerke ermöglichen neue Formen von gemeinsamer Aktion, ermöglichen die Schaffung von gemeinschaftlichen Gruppen, die größer und dezentralisierter sind als jemals zuvor in der Geschichte. Social Tools zeichnen sich dadurch aus, dass die Aktion von einer lose strukturierten Gruppe erfolgt, die ohne Management operiert und deren Ziel nicht Profit ist.

Wenn die Einstiegsbarrieren für die Teilnahme niedrig sind, sind Menschen nicht nur bereit teilzunehmen, sondern darüberhinaus auch bereit etwas gemeinsam auszuprobieren, selbst wenn nichts dabei herauskommt [Shirky 2008, S. 237].

Den Erfolg eines Gruppentools sichern eine einfache Beitrittsmöglichkeit und das Generieren-Lassen eines persönlichen Werts. Normalerweise sind die Einschränkungen bei Gruppenaktionen die Anzahl der beteiligten Personen (je mehr desto komplizierter, teurer,...) und die Dauer der Interaktion, diese Faktoren entfallen bei den Social Tools.

4.3.1 Gruppenidentität

Erst die Zusammenarbeit unter den Benutzern führt zu einer Art *Gruppenidentität*, sharing alleine bewirkt nur eine lose Ansammlung von Teilnehmern. Eine Form der Zusammenarbeit ist die Konversation. Die gemeinschaftliche Produktion ist eine aufwändigere Art der Zusammenarbeit. Strukturell ist der größte Unterschied zwischen dem Teilen von Informationen und der gemeinschaftlichen Produktion, dass letzteres zumindest gemeinschaftliche Entscheidungen erfordert und ist daher umständlicher zu erreichen als das einfache sharing.

Gemeinschaftliche Aktion ist die schwierigste Form von Gruppenbestrebungen, da viele Teilnehmer sich verpflichten müssen bei einer bestimmten Sache mitzumachen. Doch die aktuellen Kommunikationsnetzwerke – das Internet und Mobiltelefone - sind Plattformen, um Gruppen zu bilden und viele der dafür gemachten Werkzeuge (Mailinglisten, Mobiltelefone mit Kamerafunktion, usw.) setzen dies voraus. Die einfachen Möglichkeiten, eine Gruppe zu bilden, macht das ganze aus. Denn der Wunsch, Teil einer Gruppe zu sein die teilt, zusammenarbeitet oder gemeinsam agiert, wurde immer eingeschränkt durch Kosten. Jetzt wo Gruppenbildung so einfach wurde, sind Experimente mit neuen Gruppen und neuen Arten von Gruppen immer mehr zu beobachten [Shirky 2008, S. 54].

4.3.2 Kommunikation in Echtzeit

Der große Vorteil der Social Tools ist die Möglichkeit der *Koordination in Echtzeit*. Je mehr echtzeit-koordiniert die Gruppe ist, desto *weniger* können

die Reaktionen der Gruppe *vorhergesehen* werden. *Bei* Privatsphäre *geht es um den Konflikt, Kriminalität durch dessen Vorhersage zu vermeiden.*

Twitter vereint Echtzeit *und* Gruppen-Koordination. Soziale Netzwerke werden nicht durch die vielen Menschen mit hunderten von Verbindungen zusammengehalten, sondern durch einige wenige mit zehntausenden von Verbindungen.

4.4 Kritische Anmerkungen

4.4.1 Neue Technik und Veränderungen akzeptieren und damit leben

Vilém Flussers Annäherung an den heutigen Zustand (Fortschritt an Grenzen gelangt) besteht im Herausarbeiten einer Welt-, Menschen- und Gesellschaftssicht, die die Kommunikation ins Zentrum der Aufmerksamkeit rückt. Flusser bedauert die Veränderungen zum „Verlust innerhalb oder der ganzen „abendländischen“ Kultur“ nicht. Flusser betont hingegen, dass – anstatt dem Zerbrechen und Verschwinden der alten Schriftkultur nachzutrauern – dem neu Auftauchenden unsere ganze Aufmerksamkeit zu widmen ist. Wenn ein lebenswertes Leben in Zukunft möglich sein soll, das heißt für ihn die Erhaltung der menschlichen Freiheit und Würde, dann muss sich engagiert auf diese gravierenden Veränderungen eingelassen werden, um die Zukunft „heranzuholen“ und sie zu gestalten [Kloock und Spahr 2000, S. 77ff.].

Der Gesellschaftstyp heute (ermöglicht durch Vorhandensein der technischen Bilder) ist charakterisiert durch das Prinzip der Telematik (Telekommunikation und Informatik)[7]. Heute ist allerdings der Sender nicht mehr ein Automat, sondern Sender sind die Menschen selbst, durch Social Media (Vernetzung, Blogs, Facebook, Twitter usw.). Die telematische Gesellschaft ist das Jetzt, ist heute Realität.

4.4.2 Erfindung Buchdruck und Social Tools

Kann die Erfindung und Einführung des Buchdrucks verglichen werden mit der kommunikatorischen Revolution, die Social Tools mit sich brachten? Neil Postman bezieht sich in seiner Medientheorie auf die Funktion von Text durch die Einführung des Buchdrucks. Carl Adam Petri beispielsweise stellt den Computer in die Entwicklungslinie von Schrift, Buchdruck und technischen Kommunikationsmitteln, nicht die Rechentechnik [Hellige 2004, S. 325].

Nach Neil Postman ist „Der Mensch selbst [...] nicht denkbar ohne Medien“ [Kloock und Spahr 2000, S. 99ff.]. Medien prägen Kultur und soziales Milieu einer Gesellschaft. Medien verändern die für eine Kultur relevanten

[7] Telematik meint eine neuartige kommunikative Komplexität, die auf dem Prinzip des Apparates und der Automation von Medien beruht

Inhalte und das Wesen der Gemeinschaft. Postman spricht von einer „Medienrevolution“ (Buchdruck, optisch durch elektronische Medien und Computer). Aber reicht alleine die Bezeichnung „Computer“? Heute unterscheidet man eine Vielzahl von elektronischen (mobilen) (End-)Geräten, die als Medien verstanden werden.

Nach Postman erfolgte durch den Buchdruck die Demokratisierung von Wissen durch zunehmende Verbreitung und Vereinfachung von Texten mit einer „Wissensexplosion“ als Folge. Im Gegensatz dazu steht die „Elektronische Wissensexplosion“. *Siehe dazu im Vergleich Helmut Spinner (siehe Kapitel 3), der die außer Kontrolle gekommene Wissensexplosion in Form von einer informationellen Überlastung beschreibt.*

Elektronisch handelt es sich nach Postman bei Text um eine völlig neue Kommunikationswelt unabhängig von der direkten, zwischenmenschlichen Kommunikation. Die Entwicklung der Social Tools zeigt allerdings die Entwicklung zwischenmenschlicher Kommunikation hin zu einer Kommunikation mit elektronischem Schwerpunkt. Das Medium Text, das Postman nennt, muss heute auch ergänzt und erweitert werden mit Bild und Ton, welche inzwischen *gleichwertige Elemente zum Text bei der elektronischen Kommunikation* geworden sind.

Elektronische Medien (Postman: Fernseher und Radio) appellieren nach Postman an die persönliche Bequemlichkeit (sich wohl fühlen, abschalten, Wünsche erfüllen, Unterhaltung, sich informieren) wohingegen gedruckter Text ein hohes Maß an Selbstbeherrschung fordert, er fordert die Unterwerfung des Körpers unter den Geist.

Angst vor Social Media

Ist die damalige Sicht auf neu aufkommende elektronische Medien („Technik“) ähnlich der heutigen Sicht auf Social Media?

Neilman sieht das Technopol die vorbehaltslose Aktzeptanz gegenüber neuen Technologien, besonders des Computers, in allen Bereichen des gesellschaftlichen Lebens. Technik nimmt göttlichen Status ein, steht unhinterfragt als Garant für eine sichere und gute Zukunft. Er kritisiert das Fehlen eines öffentlichen Diskurses über die Konsequenzen für die Gesellschaft (positiver und negativer Natur). *Genau in dieser Ansicht über Technik kann eine Parallele zur heutigen „öffentlich vorangetriebenen“ Sicht der allgegenwärtigen Überwachung gesehen werden.*

Nach der „Werkzeugkultur“ und nach der „Technokratie“ ist das „Technopol“ die letzte Kulturstufe innerhalb einer Geschichte sich verändernder Technologien. Technopol hat sich dann durchgesetzt, wenn sich letztendlich alle Formen kulturellen Lebens der Vorherrschaft von Technik und Technologie unterworfen haben.

„Wir informieren uns zu Tode“ – alle Abwehrmechanismen gegen die Masse und das Chaos der Informationen sind zusammengebrochen denn:

Das Technopol ist ein Gedankengebäude ohne transzendentale Welterklärung, ohne ethische Basis. Postman prognostiziert als Ende dieser Entwicklung eine total gewordene technische Versklavung. Dieser Moment ist erreicht, wenn Menschen glauben, dass Technik ein Teil der Natur sei. Dann ist das Technopol Kulturzustand und Geisteszustand in einem geworden, denn Zwecksetzung und Sinngebung werden auf die Maschinen übergegangen sein.

Neilmans Ansicht kann auch etwas differenzierter gesehen werden: einerseits Zustimmung, da teilweise negative Folgen schon sichtbar sind, andererseits Ablehnung, weil positive Seiten bisher weder analysiert, hinterfragt oder umfassend aufgezeigt wurden.

4.4.3 Die Frage nach neuen Medientheorien

Insgesamt scheinen die Medientheorien von Virilo, Flusser, Postman, Benjamin „zu alt“, insgesamt etwas „zu überholt“, es fehlt der Bezug zur aktuellen Technik, die aus weitaus mehr als Fernseher und Radio besteht (davon abgesehen hat sich nicht nur die Technik an sich verändert, sondern insbesondere deren Funktion). Es geht immer wieder um den Vergleich von Text und Fernsehen. Doch Technik ist heute nicht mehr nur ein „Werkzeug“ zum Medienkonsum sondern, aktiver Teil des Lebens der Menschen selbst. Die genannten Medientheorien bilden eine wichtige Basis zur Auseinandersetzung mit Medien, vor allem in deren „Ermahnung“ Technik und deren Wirkung zu hinterfragen. Doch wo ist aktuelle Medientheorie von heute?

4.4.4 Erfolg der Social Tools

Alles muss zum Erlebnis werden – für Simanowski ist dies das Ergebnis der steigenden lokalen und sozialen Mobilität des Individuums im Zuge der Modernisierung [Simanowski 2008, S. 11]. „*Snappy news*“ könnten dazu verleiten, den Niedergang des Journalismus zu sehen [Simanowski 2008, S. 13]. Siehe dazu auch Qualifiziertes Wissen von Spinner (siehe Abschnitt 3.5).

„Die Bewohner der Erlebnisgesellschaft haben den Verlust der transzendentalen Letztbegründung des Lebens nicht nur vernommen, sondern auch beantwortet. Das Sinndefizit wird gefüllt mit Erlebnisintensität, Herkunft und Ziel, Vergangenheit und Zukunft treten zurück zugunsten des besonderen Augenblicks.“ [Simanowski 2008, S. 15].

Digitale Medien bestimmen die Kultur der Erlebnisgesellschaft so nachhaltig, dass die meisten *Abenteuer heutzutage im Internet* stattfinden [Simanowski 2008, S. 23]. Die digitalen Medien sind die Leitmedien der Erlebnisgesellschaft. Die Frage ist, wie sie diese in ihren vielfältigen Erscheinungsweisen bestimmen und welche neuen Formen der ästhetischen Erfahrung sie schaffen [Simanowski 2008, S. 24].

Simanwoski dazu [Simanowski 2008, S. 63]: „...man ist hier, wo alle

sind. Und man präsentiert sich, wie es alle tun. (...) ...Gruppenzwang eines konformistischen Selbstdesigns, dem jeder folgen muss, der <drin> sein will."

Die *New York Times* kämpft mit Problemen der Auflagenzahl, undenkbar noch vor Jahren. Alternative Geschäftsmodelle, angepasst an die Web 2. 0-Generation, wie beispielsweise den *Kindle*[8] kommentiert der Chefredakteur Bill Keller so[9]:

> (...) sondern nach Blackberry, iPod und iPhone nur ein weiteres Spielzeug für eine geräteverliebte Nation auf der Suche nach Ablenkung, permanentem Informationsdrama und kurzweiligem Zeitvertreib.

Befinden wir uns also inmitten einer geräteverliebten Erlebnisgesellschaft?

Aufmerksamkeitskämpfe und Datenpornografie

Zum Medium Internet merkt Simanowski u. a. an „Jeder bekommt seine 15 Megabyte Ruhm, ..." [Simanowski 2008, S. 55]. Die Kreditkartenbiographie verriet bisher nur, wann wo welches Produkt gekauft wurde, beim Online-Kauf hingegen werden zusätzlich auch die Produktdetails (Größe, Farbe, ...) bekannt. Nur das Ansehen von Produkten allein hinterlässt beim Online-Einkauf seine Spuren [Simanowski 2008, S. 58]. Alles, was in und mit dem Computer passiert, kann ausgespäht werden, sobald dieser online ist. Der Arbeitgeber recherchiert, der Staat schnüffelt (Deutschland: Bundestrojaner 2007 – Programm späht auf dem Computer ohne Wissen des Benutzers Dateien aus und versendet Daten).

Der vernetzte Mülleimer (Holländer Alex van Es, vernetzte im August 2000 seinen Mülleimer mit dem Internet; mithilfe des Barcode-Scanners auf seiner Website icepick.com wird der Müll aufgelistet) oder Kühlschrank ist der kürzeste Weg zur Erkundung von Verbraucherverhalten. Es ist Bestandteil des Profiling, das an Interessenten verkauft wird [Simanowski 2008, S. 60].

Kultur des Exhibitionismus wird heute mit großen Webportalen (MySpace, Facebook usw.) vorangetrieben. „Oder sucht jeder nur verzweifelt nach Zeugen für das eigene Dasein?" fragt Simanowski [Simanowski 2008, S. 61]. Simanowski sieht in den Webportalen wie MySpace und Facebook eher ein Beispiel dafür, wie die infividuelle Suche nach Selbstausdruck, von der das Internet seit seinen frühesten Tagen geprägt ist, schließlich massengerecht schematisiert und vermarktet wird als ein vom Publikum selbst geschaffenes

[8] Gerät von Amazon, um elektronische Bücher (E-Books), elektronische Zeitschriften und elektronische Zeitungen (E-Papers) zu lesen. http://www.amazon.com/kindle-store-ebooks-newspapers-blogs/b/ref=topnav_storetab_kinh?ie=UTF8&node=133141011

[9] DIE ZEIT Nr. 26 vom 18. Juni 2009, S. 15

Konsumobjekt, dem sich kaum jemand zu entziehen wagt im Zeitalter der Aufmerksamkeitsökonomie[10] [Simanowski 2008, S. 62].

4.5 Zusammenfassung

Social Media haben zu einem veränderten Kommunikationsprozess geführt, hochgradig vernetzt, multidirektional und gleichzeitig personalisiert. Es gibt allerdings erst wenige Befürworter und Unterstützer dieser Entwicklung, darunter ist beispielsweise Clay Shirky.

Die Angst vor der Veränderung durch die neue Kommunikation scheint die negative Sicht auf die neuen sozialen Medien zu verstärken. Die Gefahr liegt weniger in der neuen Art der Kommunikation als vielmehr in der Annahme, alles sei so wie in der Realität. Es fehlt den sozialen Medien allerdings die öffentliche Privatsphäre – diese ist in der Realtität völlig normal.

Der positive Kommunikationsaspekt wird beeinträchtigt durch die Unklarheit, was mit den Daten tatsächlich passiert. Daher soll im folgenden Kapitel (Kap. 5) besprochen werden, was das Sammeln von Daten mit Überwachung und Erstellung von Persönlichkeitsprofilen zu tun hat.

[10] Zum zunehmenden Kampf um das knapper werdenende Gut Aufmerksamkeit im Kontext des Internets vgl. [Goldhaber 1997, Franck 1998, Rötzer 1998]

Kapitel 5

Daten

Informations- und Kommunikationstechniken[1] haben inzwischen den Alltag durchdrungen, durch die Digitalisierung wird das Sammeln von Daten sowohl für Unternehmen als auch für Behörden aber auch jeden Einzelnen leichter und einfacher. Damit erhöhen sich auch die Möglichkeiten des Datenmissbrauchs (siehe auch Abschnitt 2.4). Dieses Kapitel beleuchtet zuerst die Datenproblematik angesichts der Möglichkeit der Deutung von Daten und der Eigenverantwortung jedes „Datensubjekts“. Es wird die Frage nach der Interpretation der Daten und dem gezielten Erstellen von Persönlichkeitsprofilen („Data Mining“) gestellt. Die hinsichtlich der Sammelwut von Behörden und Unternehmen aufkommenden Bedenken werden mit Beispielen aus der Realtiät und dem Alltag bekräftigt.

5.1 Datenproblematik

Das Gefährliche an der aktuell beobachtbaren Sammelwut sowohl von Behörden als auch von Unternehmen besteht in der Möglichkeit der *Interpretation der Daten*. Daten über jede Person werden gesammelt, dieser Vorgang ist sichtbar. Bedenklich ist dabei weniger die Situation des Beobachtet-Werdens, sondern vor allem die Ungewissheit, was mit Daten passiert, wer sie für welche Zwecke nutzt und auswertet bzw. ob überhaupt.

Die Deutung[2] beinhaltet gemäß der Definition auch das *Konstruieren von Bedeutung*. Welche Bedeutung wird den gesammelten Daten beigemessen, zugestanden, auferlegt? Bei der Videobeobachtung wird beispielsweise basierend auf Bewegungsmustern auffälliges Verhalten detektiert. Verhaltensmuster der Art und Weise von geführten Mobiltelefongesprächen – das Muster der Verbindungen – soll auffälliges Verhalten detektieren.

[1] Abkürzung: IKT

[2] Deutung bezeichnet den Prozess des Erkennens oder Konstruierens einer Bedeutung. Dabei ist es unerheblich, ob es sich um einen tatsächlichen oder vermeintlichen Erkenntnisprozess handelt. Quelle: http://de.wikipedia.org/wiki/Deutung.

Die Verantwortung dafür, etwas gegen die ungerechtfertigte Nutzung persönlicher (und anderer Daten) „zu tun“ liegt bei den Datensubjekten selbst. Anstatt sich auf die Verantwortlichkeit derer zu konzentrieren, die derartige Daten archivieren, wird einfach jenen, die Beschwerden haben, das Recht zugestanden, dass auf diese eingegangen werden muss.

Dies wurde auch von Priscilla Regan (1995) kritisiert, die argumentiert, dass Privatsphäre einen intrinsischen, allgemein bedeutsamen, öffentlichen und sozialen Wert verkörpert und der Einzelne deshalb nicht nur das Recht hat, Schutz vor den Folgen einer missbräuchlichen Nutzung persönlicher Daten zu verlangen, sondern dass *Institutionen, die auf derartige Daten zugreifen, vielmehr die Pflicht haben, Rechenschaft über die Nutzung von Daten abzulegen.* David Lyon [Stocker und Schöpf 2007, S. 57ff], siehe auch Abschnitt 2.4.

Die beste Möglichkeit, die Aufmerksamkeit von einer ausschließlichen Fokusierung auf die Privatsphäre abzuwenden, ist der Meinung von David Lyon nach Überwachung als „soziale Klassifikation“ (siehe auch Abschnitt 7.2) zu sehen [Stocker und Schöpf 2007, S. 57ff, David Lyon].

5.2 Data Mining

Data Mining meint das *gezielte Erstellen von Persönlichkeitsprofilen.* Persönliche Neigungen und gesellschaftliche Trends lassen sich so ablesen. Nicht das Aufnehmen einzelner Datenspuren, sondern das *Auswerten kollektiver Datenströme* ist nach David Lyon das Problem und die eigentliche Funktion von Überwachung: also das Etablieren von Informationsinfrastrukturen zur sozialen Selektion [Lyon 2006].

Helmut Spinner stellt im Rahmen seiner Forschungen zur Wissensordnung die konzentrierte Häufung von Wissen bei bestimmten Stellen fest und nennt diese Stellen „*Datenherren*“ (siehe Abschnitt 3.3).

Werner Rammert verbindet mit „Datenmachen“ etwas Flüchtiges zu fixieren. Auch er stellt fest, dass Überwachung zu einer Veränderung des Verhaltens der Beobachteten führt [Gaycken und Kurz 2008, S. 119]. Es gibt keine zentrale Datenmacht heute (Anm. noch nicht), man kann es eher als *Regime verteilter Kontrolle* sehen.

Gerrit Hornung setzt sich mit Datenschutz im Gefüge der Grundrechte auseinander [Gaycken und Kurz 2008, S. 250]. Er stellt eine Tendenz fest, dass staatliche Ermittlungstätigkeiten an Private (etwa Banken) ausgelagert werden[3].

Die meisten Menschen scheinen anzunehmen, dass die Inhalte, die sie mit anderen teilen, großteils von jener Gemeinschaft rezipiert werden, für die sie erstellt wurden. Man könnte dies als „beschränkte Privatsphäre“ bezeichnen. Aus Sicht der Benutzer ist diese Annahme oft richtig. Auf der

[3] So im Fall „Mikado“, siehe [Schnabel 2007]

Abbildung 5.1: Wer sind die Datenherren, die eine Blick auf uns geworfen haben? Bild aus [Sfar 2006].

Ebene der Systembetreiber entsteht jedoch ein neues *Metawissen* über die engen Verbindungen zwischen verschiedenen Benutzern, die oft nicht einmal diesen selbst bewusst sind. Gesellschaftliche Verbindungen werden plötzlich in einem Ausmaß sichtbar, das vor Jahren noch unvorstellbar gewesen wäre. Es entsteht eine neue Welt der Sichtbarkeit (Benutzer vs. Systembetreiber). Dies birgt ein hohes Potenzial an „sozialer Klassifikation“ (siehe Abschnitt 7.2).

Letztenendes können alle aufgeteilten und unterschiedlichsten Akten des elektronischen Handels und der digitalen Buchhaltung einfach in neuen Metadateien zusammengeführt werden, welche sowohl geschäftlich als auch staatlich genutzt werden können. Wer sind die Datenherren, die einen Blick auf uns geworfen haben (siehe Abb. 5.1)?

5.3 Total Information Awareness (TIA)

In Washington D. C. gibt es seit den Anschlägen auf das World Trade Center (9/11) ein immenses Überwachungsnetzwerk, woraufhin Befürworter der individuellen Handlungs- und Gedankenfreiheit begannen Fragen zu stellen. Besonders bedenklich war das Fehlen jeglicher geschriebener Richtlinien oder Rahmen gemeinschaftlicher Beratungen für die weitere Entwicklung.

Die Amerikanische Bürgerrechtsunion (ACLU) wollte wissen: Wer überwacht die Videos? Wann ist das System komplett? Wie lange werden die Bänder aufbewahrt und von wem? Welche Behörden haben Zugriff darauf? Was wird unternommen um Video-Voyeurismus oder rassistische und obdachlosfeindliche Profilierung zu vermeiden? Obwohl niemand das totale Recht auf Privatsphäre hat, wenn er sich in der Öffentlichkeit bewegt, so haben die Menschen in Amerika zumindest den Schutz des *Fourth Amendment* gegen unangemessene Fahndung. Und es könnte argumentiert werden, dass, wenn die Polizei eine Person mit hochtechnisierter Ausstattung und intelligenten Kameras beobachtet, die mit Kriminaldatenbanken verbunden sind, tatsächlich eine unbefugte und verfassungswidrige Fahndung betreiben [Parenti 2003, S. 112].

Das Total Information Awareness (TIA) Projekt der Defense Advanced Research Projects Agency (DARPA) zeigt die kritische Verbindung zwischen der Spionage durch die Regierung und die Infrastruktur der alltäglichen Überwachung. Das TIA-Büro arbeitete an einem Plan, alle ganz unterschiedlichen Aufzeichnungen des täglichen Lebens zusammenzuführen (Kreditkartendaten, Überweisungen, Gesundheitsdaten, elektronische Rechnungen, Bibliotheksverzeichnisse). Diese Datenbank könnte dann zum Data Mining herangezogen werden um interessante und belastende Muster zu finden [Rosen 2002]. Verbunden war das ganze mit einem anderen Programm von DARPA – Human-ID – um biometrische Informationen von Videokameras und anderen Bildquellen mathematisch abzugleichen und die Ergebnisse dann durch andere Datenbanken laufen zu lassen um die entsprechenden Menschen zu finden. Dem Projekt TIA wurden zwar – wohl aufgrund des öffentlichen Entsetzens – nur ein Jahr später, 2003, die Mittel gekürzt. Aber einige der gefährlichen Funktionen werden unter veränderten Namen in anderen Projekten weiterverwendet [Parenti 2003, S. 203].

5.4 DNA-Datenbank

1991 wurde durch das US-Militär das größte Projekt für genetische Identifikation gestartet: eine DNA-Datenbank mit über $1,5$ Millionen Mitgliedern [Moffat 1992]. Das Argument für das Erstellen dieser DNA-Datenbank war die Möglichkeit der Identifizierung bei einem Todesfall (so auch das Argument für die Einführung der Fingerabdrücke hundert Jahre zuvor). Die Daten werden fünfzig Jahre gespeichert. Daraufhin begannen auch andere Staaten mit dem Aufbau von DNA-Datenbanken, indem Muster von verurteilen Mördern und Sex-Attentätern verwendet wurden [Raab 1992].

Besonders kritisch müssen DNA-Datenbanken betrachtet werden. Staat und lokale Behörden besitzen DNA-Muster von Personen. Diese Muster ermöglichen Einblicke in die persönlichsten Familienverhältnisse und das höchstvertrauliche Arbeiten des menschlichen Körpers, was das Wissen über die

Wahrscheinlichkeit des Auftretens verschiedenster Arten von genetischen Bedingungen und Krankheiten bereitstellt. Bedenklich ist, dass darüber gemutmaßt werden wird, welche genetischen Faktoren für Aggression, kriminelle Tendenzen oder ähnliches verantwortlich sind. DNA-Datenbanken sind daher um ein vielfaches gefährlicher als die bestehenden Datenbanken mit Fingerabdrücken oder Iris-Scans [Parenti 2003, S. 178].

In Südafrika wurde die Einrichtung einer DNA-Datenbank verschoben. Als Gründe dafür wurden die Verfassungsmäßigkeit und die noch nicht vorhandene Bereitschaft der Polizei genannt[4]. Trotzdem zeigt das Beispiel, dass es nur mehr eine Frage der Zeit ist, bis DNA-Datenbanken die bisherigen Datenbanken ablösen.

5.5 Beispiele der Auswertung persönlicher Daten

Die hinsichtlich der Sammelwut von Behörden und Unternehmen aufkommenden Bedenken werden mit Beispielen aus der Realtiät und dem Alltag bekräftigt.

5.5.1 Google kann hellsehen

Mithilfe der Internetsuchmaschine Google lässt sich die Entwicklung der Arbeitslosigkeit prognostizieren. Im Artikel der ZEIT trägt die Meldung darüber daher auch den Titel „Arbeitslosigkeit: Google kann hellsehen“[5]. Die Häufigkeit bestimmter Suchbegriff-Eingaben (z. B. Arbeitsamt, Jobbörse) verrät der Studie zufolge die Entwicklung des Arbeitsmarktes. In der Studie wurden die Suchanfragen zwischen Jänner 2004 und April 2009 mit der Entwicklung der tatsächlichen Arbeitslosenzahl verglichen und es zeigte sich ein enger Zusammenhang, der bis eineinhalb Monate vor Veröffentlichung der amtlichen Statistik Vorhersagen ermöglichen soll.

5.5.2 Personalisierung des Browsers

Marketingunternehmen hatten auch schon vor der Zeit des Web 2. 0 umfangreiche Profildaten von Kunden – offline-Daten. Gemeinsam mit den “neuen“ online-Daten (unter anderem mithilfe von Cookies erfasst) wird ein sehr genaues Kundenprofil erstellt. Die New York Times berichtet, dass nun einige Unternehmen damit begonnen haben, diese Ansammlung von Daten direkt mit dem Browser zu verbinden[6].

Zu diesen Unternehmen gehören *Acxiom*[7] und *Datran Media*[8]. Die Ver-

[4] http://www.itweb.co.za/index.php?option=com_content&view=article&id=27690:dna-database-delayed&catid=69:business&Itemid=58

[5] DIE ZEIT Nr. 25 vom 10. Juni 2009, S. 31

[6] New York Times, Montag, 10. August 2009, “Online Ad Tracking Gets Very Personal“

[7] http://www.acxiom.com/

[8] http://www.datranmedia.com/

knüpfung der on- und offline Daten erfolgt genau dann, wenn sich eine Person auf einer Webseite registriert oder durch Klicken auf ein E-Mail von einem Marketingunternehmen.

Das Ergebnis ist eine große Veränderung in der Art und Weise wie Konsumenten zukünftig das Internet antreffen werden. Menschen werden nicht nur ihnen angepasste Werbung sehen, sondern auch andere, ihnen angepasste Webseiten, die bei einem anderen Kunden wieder ganz anders aussehen können. Die Technologie, die das ermöglicht, ist eine alte – es sind die Cookies.

Trey Barrett von Acxiom sagt im genannten Artikel:

> Now, you're traveling the Internet with a cookie that indicates you're this type of consumer: age group X, income level, urban versus rural, presence of children in the household.

Konsumenten können sich dagegen wehren, indem sie den Browser keine Cookies annehmen lassen. Allerdings machen das einerseits viele nicht (u. a. weil sich unter Umständen manche Seiten nicht mehr öffnen lassen oder Services nicht mehr funktionieren), andererseits, so sagen *Privatsphäre* -Anwälte, ist es für Unternehmen einfach, Cookies ohne das Wissen des Konsumenten hinzuzufügen. Unberücksichtigt bleibt auch die Tatsache, dass inzwischen viele Unternehmen inzwischen über wenn auch nur kleinste Verbindungen zu einem gemeinsamen Großkonzern haben und hier die Option „Cookies Dritter nicht annehmen“ gar nicht erst zum Tragen kommt.

5.5.3 Privatangelegenheiten und Schutzauftrag des Staates

Shu-Min Lin sieht ein Paradoxon in der Tatsache, dass mehr *Privatsphäre* weniger Intervention durch den Gesetzgeber erfordert [Stocker und Schöpf 2007, S. 51ff]. Das steht im Konflikt mit der Forderung gegenüber der Regierung nach mehr Schutz der Privatsphäre. Problematisch ist dabei die *Privatsphäre* im Hinblick auf das Internet. Informationen, die zuvor nur mächtigen Institutionen zugänglich waren, können nun von jedermann übers Internet abgerufen werden. Auch kann man in der virtuellen Welt eine Vielzahl von Identitäten annehmen.

Für aktive Teilnehmer ebenso wie für passive Betrachter hat sich der Internet-Voyeurismus zur neuen Gruppentherapie entwickelt.

5.5.4 Vorratsdatenspeicherung

Dirk Engling setzt sich mit dem Thema Vorratsdatenspeicherung auseinander [Gaycken und Kurz 2008, S. 71] und verweist dabei auf das sehr treffend formulierte Volkszählungsurteil[9] von 1984, in dem ausführlich beschrieben wird, dass die freie Entfaltung, die jedem Bürger innerhalb freiheitlich-

[9] vgl. BVerfGE 65:1. [Deutschland]

demokratischer Grenzen zusteht, unter dem Eindruck leidet, auf Schritt und Tritt potentiell *für immer sichtbare Spuren* zu hinterlassen.

In der Frage nach möglichen Alternativen zeigt er das Beispiel auf, flächendeckend für alle Bundesbürger Fußfesseln einzuführen. Er sieht besonders kritisch, dass zwar eine Fußfessel eine Aufschrei der Empörung auslösen würde, dahingegen die kaum bemerkbare und bereits aktiv betriebene Speicherung der Bewegungsdaten des Mobiltelefons noch tiefer in die Lebensgewohnheiten der Betroffenen eingreift.

Zusammenfassend sieht er in der Vorratsdatenspeicherung ein mächtiges Überwachungsinstrument. Das Potential zum Missbrauch ist sehr hoch, während entsprechend motivierte Straftäter sich den Maßnahmen entziehen können. Die ermittlungstechnischen Alternativen wurden seiner Meinung nach nicht ausreichend diskutiert, der Zugriff auf die Daten nicht durch hohe Hürden begrenzt.

5.5.5 Die Sozialversicherungsnummer als neues Lieblingskind der Datenherren

In den *Schulen* wurde im Oktober 2003 die „Echtdatenübermittlung“ eingeführt „um damit eine Gesamtevidenz der Schüler zu erstellen“[10]. Regelmäßig werden die Daten durch Erhebungsblätter der Statistik Austria angefordert, Verwaltungsstrafandrohungen sollen die Rücklaufquote erhöhen. Vom Klassenbucheintrag über das religiöse Bekenntnis, Sportverletzungen und Betragensnoten werden alle erdenklichen Informationen zu jedem Schüler gespeichert, voraussichtlich 75 Jahre lang. Über eine Kontrollnummer sind diese mit den Stammdatensätzen verknüpft. Fehlte nur noch, dass als Kontrollnummer die Sozialversicherungsnummer verwendet wird. „Die für die Umsetzung der Bildungsevidenz verantwortlichen Bürokraten“ wurden für den Big Brother Award 2003 nominiert.

Wer in Zukunft *Spenden* steuerlich absetzen will, muss ab 2011 seine Sozialversicherungsnummer bei der Überweisung angeben. Grundlage dafür ist das Steuerreformgesetz 2009 des BM für Finanzen[11] Damit setzt sich das Bundesministerium für Finanzen über das E-Governmentgesetz hinweg, das in solchen Fällen ein nicht über Verwaltungsdatenbanken hinweg nachvollziehbares, bereichsspezifisches Personenkennzeichen vorschreibt. Für diese „Leistung“ wurde das BMF für den Big Brother-Award 2009 in Österreich nominiert[12].

Das Ausmaß über die möglichen Folgen der Verwendung der Sozialversicherungsnummer als eindeutigen Identifikator (ID) einer Person für fremde Zwecke dürfte noch unklar sein. Die Sozialversicherungsnummer ist eine der

[10] http://www.bigbrotherawards.at/2003/nominees/list_2003.php

[11] http://www.bmf.gv.at/Steuern/Fachinformation/NeueGesetze/Steuerreformgesetz2009/_start.htm

[12] http://bigbrotherawards.at/2009/Nominierungen

stärksten Identifikatoren eines Individuums. Sie begleitet den Menschen von der Geburt bis zum Tod und bleibt immer dieselbe. Auf Knopfdruck lassen sich so persönlichste Daten abrufen.

5.5.6 Bluttest von Bewerbern

Bluttests bei Bewerbungen – noch vor der Stellenzusage? Die Meldungen häufen sich, wie das Beispiel vom NDR zeigt[13]: „Im Rahmen der Eignungsuntersuchung wird auch ein Bluttest gemacht", teilte der Sender *ndr* mit. *Dieser könne Anhaltspunkte darüber geben, ob ein Mitarbeiter die vorgesehene Wochenarbeitszeit wird leisten können.* „In diesem Fall überschreitet der NDR die rechtliche Grenze", sagte der Arbeitsrechtler der Universität Bonn, Gerrit Forst, der Online-Ausgabe der „Tageszeitung".

5.5.7 Rekorddiebstahl von Kundendaten

Im August 2009 wurde vom Rekorddiebstahl von Kundendaten berichtet[14]. In den USA hatten die Behörden drei Männer angeklagt, die mehr als 130 Millionen Kredit- und Bezahlkartennummern gestohlen haben sollen. Es handelt sich um den größten Datendiebstahl, der je in den USA stattgefunden hatte. Die Verdächtigen sollen als Hacker in die Systeme von Einzelhandelsunternehmen eingedrungen sein.

5.5.8 SMS-Toiletten

Im schwedischen Malmö sind Toiletten, die nur gegen Eingabe eines via SMS gekauften Codes benützt werden können, ein Fall für Datenschützer geworden. Die Stadtverwaltung wollte die gespeicherten Telefondaten nutzen, um Vandalen aufspüren zu können. Datenschützer wollen nun wissen, wie lange die Telefonnummern der Benützer gespeichert werden[15].

5.5.9 Überführung der Kriminaltäter von morgen

Ein Beispiel für den Überehrgeiz Kriminaltäter von morgen bereits heute dank der Datenspeicherung zu finden hat sich in Wilmington, Delaware, abgezeichnet. Die dort ansässige Polizei begann eine Datenbank von Leuten aufzustellen, von denen die Behörden glaubten, dass sie irgendwann in der Zukunft eventuell gegen das Gesetz verstoßen könnten. Es waren Leute eingetragen, die noch gar kein Vergehen begangen hatten, insgesamt 200, wovon beinahe alle Schwarze oder Personen lateinamerikanischer Herkunft waren.

Die Aufgabe der Datenbank ist es Identitäten auszuarbeiten, Querverbindungen zwischen Personen und Plätzen herzustellen, sodass damit der

[13] FAZ online Feuilleton, 5. November 2009, http://www.faz.net/
[14] u. a. Die Presse, Der Standard, 19. August 2009
[15] u. a. Die Presse, 19. August 2009

Polizei ortspezifische Listen potentieller Verdächtiger zur Verfügung stehen, sollten sich Kriminaldelikte im entsprechenden Umfeld ereignen [Parenti 2003, S. 178].

5.6 Zusammenfassung

In diesem Kapitel wurde gezeigt, dass Bedenken gegenüber der Sammelwut von Behörden, Unternehmen und einzelnen Personen durchaus angebracht sind. Es wurde hervorgehoben, wie die Verwendung der Daten im Ungewissen liegt und für den Einzelnen nicht nachvollziehbar ist.

Das Sammeln von Daten bedeutet demnach nicht nur reine Überwachung, sondern ist auch ein Mittel zur sozialen Klassifikation. Der Wissensschwerpunkt liegt bei wenigen Datenherren, die durch das Vorhandensein von großen Mengen an Daten gezielt Persönlichkeitsprofile erstellen können. Es entsteht somit ein gefährliches Metawissen seitens der Datenherren.

Das Kapitel machte auf die Ungewissheit der Verwendung der persönlichen Daten aufmerksam. In der späteren Besprechung von Überwachung (siehe Kap. 7) werden Möglichkeiten zur Datensammlung mittels Überwachung aufgezeigt. Das Thema Identitätsnachweis (Kapitel 6) wird anschließend an dieses Kapitel genauer erläutert, da damit Daten direkt mit eindeutigen Identifizierern (beispielsweise Reisepass) in Verbindung gebracht werden können.

Kapitel 6

Identitätsnachweis

> Qui témoigne une fois de plus de l'inutilité des passeports en matière de police[1] [Verne 2000, S. 44].

Ausweise sind Werkzeuge der zeitgemäßen Regierungsgewalt (aber auch von Unternehmen) und lösen daher unterschiedlichste soziale und politische Probleme aus. Die Identifikationsprozesse sind Teil von Überwachung. Digital vernetzte Identifikationssysteme erlauben einerseits das Sammeln von Daten (und damit entsprechend die Möglichkeit des Datenmissbrauchs), andererseits stellen sie ein großes Geschäft für jene Unternehmen dar, die ID-Kartensysteme herstellen. Beschrieben werden die zur Zeit gängigste Art von Ausweisen, nämlich die Chipkarte, als auch biometrische Identifikation.

6.1 Digitale Identität

Persönliche Identifikation kann auf folgende Arten erfolgen:

1. Besitz (Pass, Ausweis)
2. Wissen (Passwort)
3. Handlung (Unterschrift oder Spracherkennung)
4. Existenz (Biometrische Daten)

Die neuen (digitalen) Identifikationsprozesse tragen durch die Klassifizierung der Einwohner anhand verschiedener Kriterien zur Überwachung bei. Dadurch werden Lebensmöglichkeiten, Status und Aussichten beeinflusst. Es geht um politische, administrative und technische Fragen. Wesentliche Fragen siehe [Bennett und Lyon 2008, S. 4].

Seit dem Web 2.0 geht es nicht mehr nur um die Verlinkung von Dokumenten sondern um die Vernetzung von Personen. Und die Personen scheinen

[1] Das zeigt wieder einmal mehr die Sinnlosigkeit von Pässen, wenn es um die Polizei geht (eigene grobe Übersetzung).

sich vernetzen zu wollen. Auf den Plattformen Facebook, Xing, usw. wird nicht nur ein soziales Netzwerk aufgebaut, sondern auch eine Reputation und ein Image. Der Aufbau dieser Identifikationssysteme ermöglicht den Benutzern nur, eine Identität und soziale Beziehungen innerhalb ihrer Systeme aufzubauen, wodurch sie eigentlich zu monolithischen Informationsbunkern werden. Man spielt mit verschiedenen Menschen verschiedene Rollen. Es gibt kein definiertes Interface, um das persönliche Profil etwa auf Xing mit dem auf anderen Plattformen zu verknüpfen. Aus diesem Grund gibt es einen *Trend zu offenen Identifikationsstandards und Protokollen für das Internet.* Die Diskussion darüber wird unter dem Schlagwort „benutzerzentrierte Identität“ geführt.

Was macht ein Sicherheitspolitiker, der ein solches System (verpflichtende Online-Identifikation) einführen möchte? Er beginnt bei Minderheiten. Identitätssysteme als Kontrollorgan, Kontrollmöglichkeit, Kontrolle. Ralf Bendrath zählt Beispiele auf im Rahmen seiner Betrachtung von digitaler Identität [Stocker und Schöpf 2007, S. 123]. Je nach technischer Auslegung wäre die Regierung als Provider der digitalen Identität dann in der Lage, das Verhalten der Bürger online nachzuverfolgen. Sie wäre jene erwähnte dritte Partei, die höchste Instanz in puncto Glaubwürdigkeit. Ist das ein Systemfehler oder ein Charakteristikum – fragt Bendrath [Stocker und Schöpf 2007, S. 123].

6.1.1 Hintergrund Identitätsbildung

In den letzten 50 Jahren verlagerte sich der Prozess der Identitätsbildung von relativ stabilen, hierarchischen Institutionen (Familie, Arbeitsplatz, Kirche) hin zum Einzelnen und seinem selbst gewählten Umfeld. Menschen verspüren verstärkt das Bedürfnis, einzigartig zu sein, suchen nach Anerkennung und Reputation.

Die Vernetzung des eigenen Lebens mit der Außenwelt ist kein passiver Akt des Beobachtens, sondern eine aktive Intervention, nicht zuletzt deshalb, weil bestimmte Ausschnitte der Realität als wichtig erachtet werden und ihnen erhöhte Aufmerksamkeit zuerkannt wird, während andere ignoriert werden. Die Vernetzung erfolgt durch selbstbestimmte Bemühungen von jedem Einzelnen, die Bedeutung wird daher auf sehr persönlicher Ebene erzeugt. In diesem Prozess wird daher gleichzeitig eine individuelle Identität und eine neue Welt erschaffen (Felix Stalder [Stocker und Schöpf 2007, S. 129ff]). Das Konzept des „vernetzten Individualismus“ spiegelt Formen von Identität wider, die zwischen dem vollkommen autonomen Individuum, das tief in seiner Privatsphäre verwurzelt ist, und dem gesichtslosen Mitglied eines Kollektivs, dessen Persönlichkeit der Gruppenidentität untergeordnet werden kann (Felix Stalder [Stocker und Schöpf 2007, S. 129ff]).

6.2 ID-Kartensysteme

Identitätskontrolle und -management erfolgt häufig durch ID-Kartensysteme. Der politische *und* technologische Trend geht hin zu nationalen Identifikationssystemen. ID-Karten tragen zu *social sorting* (siehe Abschnitt 7.2) und Überwachung bei. Einzigartige Identifikation birgt eine große Gefahr, wenn sie von „Machthabern“ (den Datenherren) durchsuchbar und mit Datenbanken verbunden wird. Dies kann zu undemokratischer und unberechenbarer Überwachung führen.

„Identification is regulated by identification systems identity cards“: Heute herrscht ein Oligopol[2] von Mitteln zur Identifizierung, man spricht vom sogenannten *Card Cartel* [Bennett und Lyon 2008, S. 11]. Identity Cards sind demnach ein Produkt, ein Ergebnis von „*corporate entities*, competing for contracts to use their solutions and of *technical standards* which shape the architecture and characteristics of identity card scheme in question“ [Bennett und Lyon 2008, S. 11]. In den USA erfolgt das Auslagern des Themas an das Unternehmen Digimarc [Bennett und Lyon 2008, S. 231]. Die Frage ist, wem es überhaupt erlaubt ist Identifizierung zu verlangen. Identifizierung früher gleicht nicht jener von heute. Das Ziel der Identifizierung von heute ist es, ein Risiko vorhersehbar zu machen, vorhersehen zu können [Bennett und Lyon 2008, S. 23]. Es geht um eine Risikominimierung, indem Ereignisse und Verhalten vorausberechenbar gemacht werden [Stocker und Schöpf 2007, S. 57ff, David Lyon]).

Es geht um *mehr* als nur *Privatsphäre* und Sicherheit das ganze Land umfassenden ID-Systemen, Beispiel *social sorting* (siehe Abschnitt 7.2). Soziale Klassifikation bleibt das notwendige Mittel dieser Technologien um größere Bevölkerungen zu verwalten [Bennett und Lyon 2008, S. 145]. Die Gefahr liegt im Verbinden von Datenbanken, noch *bevor* etwas passiert ist, diese Vorgehensweise ist sehr fragwürdig [Bennett und Lyon 2008, S. 24]. „Wir entwickeln uns zurück“, vor allem durch den Krieg gegen den Terror: *Jeder* ist jetzt ein potentieller Täter [Bennett und Lyon 2008, S. 93].

Das ID-Kartensystem setzt den Bürger dem Druck von Normalisierung und Konformität aus mit dem Ziel einen *wünschenswerten Bürger* zu erschaffen [Bennett und Lyon 2008, S. 108].

The excluded innocent [Bennett und Lyon 2008, S. 108]: Wir bewegen uns in Richtung eines neuen Faschismus, der von digital vernetzten Identifikationstechniken verteidigt wird. Wir stehen vor einer neuen Tyrannei der Sicherheit (Gewaltherrschaft). Die Hauptfragen lauten daher nach Midori Ogasawara [Bennett und Lyon 2008, S. 108]:

> Who is targeted, Who receives the benefits, Who decides who is who

[2] Wenige Marktteilnehmer bieten Gut an/fragen Gut nach, führt zu Verdrängungspolitik, Preisstarrheit und Preisführerschaft

Die Gefahr liegt in der Unklarheit darüber, was mit den Daten passiert und vor allem in der Möglichkeit der Zweckentfremdung der Daten. In [Bennett und Lyon 2008, S. 125, S. 128] wird einmal mehr die *Unklarheit darüber, was mit den Daten passiert*, hervorgehoben (siehe Abschnitt 2.4). Überlegungen zur Informationssicherheit müssen daher an erster Stelle bei ID-Systemen stehen.

Egal, ob es ID-Karten gibt – die Frage ist: *Wie* wird jeder *bereits jetzt* universal identifiziert und nachverfolgt? Sozialversicherungsnummer, Kreditkartennummer, Führerscheinnummer, Kundenkarten führen bereits jetzt zu einem umfassenden Profil von jedem Bürger, wenn all diese Daten miteinander verbunden werden. So können einzeln betrachtet harmlose Nummern zusammengefügt eine große Macht auf den Besitzer erzeugen. Soziologen sprechen vom sogenannten *function creep*, der Zweckentfremdung [Parenti 2003, S. 85].

6.3 Chipkarten

ID-Cards als Chipkarten, dadurch wird eine automatisierte und zentralisierte Datenverarbeitung möglich, aus diesem Grund sind sie *Machtinstrumente* für Diskriminierung, Freiheitseinschränkung und Überwachung.

David Lyon nennt die neue Überwachung auch *dataveillance* [Lyon 1994]. Es geht dabei nicht mehr (nur) um die Überwachung von Körpern, sondern um die Verfolgung des informationellen Doppelgängers. Das heißt allerdings nach Lyon noch lange nicht, dass die traditionelleren Überwachungsformen rückläufig sind sondern ganz im Gegenteil: Visuelles und biologisches Monitoring ergänzen die hochtechnologische computergesteuerte Überwachung [Parenti 2003, S. 4].

Wir werden nicht überwacht, sondern häufig „checken wir selber ein“. So gesehen ist es eine Umgebung voll mit Registrierungsstellen (Beispiel Bankomatkassen). Mike Davis nennt es auch *scanscape* [Davis 1990]:

> These notes upon what Mike Davis called the „scanscape“ can also be seen als altars where we genuflect[3] to authority, performing the quiet rituals of obedience by registering our locations in time and space.

Universelle personenbezogene Identifikatoren, Datenbanken und Netzwerke zeichnen die aktuelle Landschaft der digitalen Überwachung und erschaffen den *digitalen Schatten* jedes „Teilnehmers“. Überwachung findet nicht mehr auf den Körper bezogen, sondern auf dessen Daten bezogen statt [Parenti 2003, S. 84].

[3] niederknien

6.3.1 Beispiel BioP@ss

„BioP@ass“ ist ein Projekt der Europäischen Union und soll einen EU-weit gültigen elektronischen Personalausweis im Chipkartenformat umsetzen[4]. Neu dabei ist, dass auch die Identifikation im Internet bedacht wurde, welche durchaus mehr Funktionen benötigt als der Gebrauch in der realen Welt. BioP@ss soll demnach auch eine sichere und webbasierte Authentisierung sowohl bei Behörden- und Regierungsdienstleistungen als auch bei Geschäften aller Art bieten. Das Projekt kann auch als großes Geschäft betrachtet werden – vor allem für die beiden Halbleiterkonzerne Infineon und NXP sowie den Chipkartenhersteller Giesecke & Devrient (G & D). Die drei genannten Konzerne gehören zum insgesamt elfköpfigen Team von Unternehmen aus sechs europäischen Staaten, die beauftragt sind, mit dem Forschungsprojekt BioP@ss eine hochsichere Chipartenplattform zu entwickeln. Das Projekt soll Ende Juni 2011 abgeschlossen sein, das Gesamtbudget beläuft sich auf etwa 13 Millionen Euro und wird zur Hälfte von den Partnern aus Industrie und Wirtschaft getragen.

6.4 Biometrische Identifikation

Constanze Kurz setzt sich mit dem Thema Biometrie auseinander [Gaycken und Kurz 2008, S. 100]. Die biometrische Durchdringung des Alltags in Form von Verifikations- und Identifikationssystemen erwartet die Bundesbürger schon in naher Zukunft: Gesichtserkennung bei Zugangskontrollen und auf Reisen, Fingerabdrücke zum Starten eines Fahrzeuges, multimodale biometrische Identifikationskarten am Arbeitsplatz, Erkennung von Stimmmustern am Telefon, Geldabheben am Automaten und Bezahlen im Restaurant mit dem Daumenabdruck oder biometrische Bezahlsysteme für Kinder bei der Schulspeisung können schon bald alltäglich werden. Die Gründe für die Entwicklung neuer Verfahren zu Authentifikation liegen auf der Hand: Altbekannte Mechanismen wie die Verwendung von Wissen (Zahlencodes, Passwörter) oder physischen Token (Chipkarten, Schlüssel) haben Schwächen. Der Einsatz biometrischer Authentifikationssysteme hat für den Benutzer gegenüber traditionellen Methoden mit Passwörtern oder Zugangskarten den Vorteil, dass ein Gesicht, eine Hand oder ein Fingerabdruck weder vergessen noch verloren noch an Dritte weitergegeben werden kann.

6.4.1 Mehr Sicherheit durch biometrische Daten

Das Argument der Sicherheit muss stark hinterfragt werden, beispielsweise bei Reisedokumenten. Dass das Fälschen von Reisepässen für die Planung terroristischer Anschläge allerdings gar keine Rolle spielt, zeigen zurückliegende Attentate. Die Täter bewegten sich im Vorfeld der Planungen weitge-

[4] Die Presse, Magazin „Forschung“, Ausgabe November 2009, S. 42/43

hend unauffällig und besaßen gültige Ausweisdokumente. Dennoch wird immer wieder der Sicherheitsgewinn durch Reisedokumente mit biometrischen Daten betont. Überdies fand bisher weder eine gesellschaftliche Diskussion noch eine hinreichende Erprobung der Technologie statt, stellt Constanze Kurz fest [Gaycken und Kurz 2008, S. 103].

6.4.2 Internationale Normen und Regeln

Auf die Frage nach international gültigen Regelungen, die gewährleisten, dass biometrische Daten deutscher Staatsbürger nicht in die Datenbanken anderer Staaten gespeichert werden, antwortete die Bundesregierung lapidar: „Die Speicherung der biometrischen Daten deutscher Reisender im Rahmen der Passkontrolle dritter Staaten erfolgt ausschließlich nach dem Datenschutzrecht des jeweiligen Drittstaates“[5]. Die in guter Qualität vorliegenden digitalen Daten des Gesichtsbildes und des Fingerabdruckes sind also zur globalen Speicherung freigegeben, stellt Constanze Kurz fest [Gaycken und Kurz 2008, S. 109].

Mit der Speicherung der Referenzdaten biometrischer Merkmale in großen Datenbanken sind neben den bekannten Problemen, wie etwa Verwechslungen oder falsche Datenspeicherung durch fehlerhafte Algorithmen, bereits Gefahren vorprogrammiert, die der biometrischen Technik innewohnen: Identitätsdiebstahl durch berechtigten oder unberechtigten Zugriff, Cross-Matching über Datensätze oder Erlangung medizinischer Überschussinformationen, wie sie etwa bei Gesichtern oder Iriden vorkommen können. Es fallen also nicht nur Identifikationsspuren von Menschen an, auch medizinische oder psychologische Daten werden gespeichert. Die Forschung, in welcher Detailtiefe solche Informationen aus biometrischen Daten gleichsam als „Beifang“ gewonnen werden können, befindet sich jedoch erst am Anfang. [Gaycken und Kurz 2008, S. 110]

6.4.3 Gefahren

Constanze Kurz [Gaycken und Kurz 2008, S. 113] bemerkt außerdem, wenn berücksichtigt wird, dass eine biometrische Merkmalserfassung von einem Menschen nicht mehr widerrufen werden kann, haben Erkenntnisse über erfolgreiche Angriffe, aber auch über inhärente Schwächen der Technologie Brisanz. Festzuhalten bleibt, dass die biometrische Vollerfassung nicht nur teuer und hinsichtlich des Sicherheitsgewinns fragwürdig, sondern auch ausgesprochen riskant unter den Gesichtspunkten des Datenschutzes, der Überwindungssicherheit und damit des Identitätsdiebstahls ist.

[5] Antwort der Bundesregierung auf die Anfrage der Fraktion Die Linke im Bundestag „Sicherheit der biometriegestützten Reisepässe“, BT-Drucksache 16/161, 9. Dezember 2005, S. 2

Das große Risiko sieht Constanze Kurz in der Tatsache, dass die unkontrollierte, vielleicht sogar grenzüberschreitende Verwendung biometrischer Daten durch Behörden oder kommerzielle Datensammler und die Entstehung von Biometriedatenbanken auf Grund der unfreiwilligen Preisgabe des digitalen Gesichtsbildes und des Fingerabdruckes im Zuge der Einführung biometrischer Pässe ein *viel zu wenig diskutiertes Risiko* für jeden Bürger darstellen.

6.4.4 Ausblick Nanotechnlogie

Wann wird die Nanotechnologie Chipkarten und Biometrie abzulösen? Noch scheint dieses Thema niemand ernst zu nehmen, doch es gibt bereits erste Arbeitsgruppen [Gaillard 2009, S. 64ff]. Das Unternehmen „Inside Contactless“ hat bereits zehn Millionen Rfid-Chips an China ausgeliefert, damit dort die Studenten auf dem Campus verfolgt werden können. Dafür erhielt das Unternehmen 2003 den Big Brother-Award[6]. Mit Nanotechnologie wird das alles viel einfacher, vor allem *unbemerkt* möglich werden. Damit hat niemand mehr Gewissheit, ob er nun alleine ist oder nicht. Die Gesellschaft wäre dann eine diktatorische.

6.4.5 Beispiel INES

In Frankreich wurde der Vorschlag gemacht, eine biometrische ID-Karte namens INES (Identité Nationale Électronique Sécurisée) einzuführen. Damit wäre zum ersten Mal die ID-Karte mit verschiedenen nationalen Registern (Geburten, Todesfälle, Hochzeiten, Fingerabdrücke, digitale Fotos, Pässe) verbunden gewesen. Die biometrischen Daten wären im Chip, auf sie könnte mithilfe von RFID zugegriffen werden. 2005 wurde das Projekt erstmals in Frankreich durch Nicolas Sarkozy eingeführt. INES rief großen und unvorhergesehenen Widerstand hervor, selbst nach dessen Zurückweisung. Auch das CNIL (Commission Nationale de l'Informatique) äußerte sich damals skeptisch gegenüber der Idee INES [Bennett 2008, S. 141].

6.5 Ursprung von ID-Systemen

Man muss zurück zu den Ursprüngen von ID-Systemen (koloniale Wurzeln). Der Beginn der Überwachung liegt in der Kolonialzeit, in der Zeit der Sklaverei [Parenti 2003, S. 14]. Dies war auch der Beginn von Formen des Identitätsnachweises. ID-Systeme waren damals ein Instrument um Menschen auszubeuten, ein Instrument der Unterdrückung und ein Instrument für den Wirtschaftswachstum. ID-Systeme dienen nur der Unterwerfung und Ausrottung von politischen sowie wirtschaftlichen Minderheiten [Bennett und Lyon 2008, S. 107].

[6] http://bigbrotherawards.eu.org/Inside-Contactless.html

Weiße Sklavenhalter sahen sich gezwungen, ein System zur Identifizierung der schwarzen Sklaven einzuführen, damit sie diese besser kontrollieren konnten. Das neue System machte Identität zu einem Werkzeug sozialer Kontrolle und wurde Ursache von Kämpfen unterer sozialer Schichten. In der damaligen Gesellschaft wurde Überwachung das entscheidende Machtinstrument [Parenti 2003, S. 14].

Soziologisch gesehen war der Sklaven-Pass damals mehr durch *Gemeinschaft* als durch *Gesellschaft* gekennzeichnet. Der Pass ist ein Produkt aus der sozialen Welt mit persönlichem Kontakt, nicht von jener Welt mit viel einer komplexeren, bürokratischeren Gesellschaft mit anonymen und standardisierten Formen von Verbindungen zwischen Personen [Parenti 2003, S. 19]. *Peter Purgathofer* stellt fest, dass damals mittels *Social Engineering* (gekonnte zwischenmenschliche Beeinflussung) das System der Passkontrolle[7] überlistet werden konnte [Gaycken und Kurz 2008, S. 203].

6.5.1 Entwicklung unterschiedlicher Identifizierungstechniken

Der Pass ist eine wichtige Überwachungstechnologie [Parenti 2003, S. 31]. Pässe sind eine der frühesten Werkzeuge für staatliche Kontrolle. Militärische Pässe und Pässe, gemeinsam mit dem Überwachungsregime der Sklaverei, haben wesentlich zur heutigen Entwicklung der modernen Technologien zur Identifizierung und Registrierung beigetragen [Parenti 2003, S. 31].

Die Basisstruktur moderner Identifizierung hat ihre historischen Wurzeln in der Fotografie, der Bertillonage[8] und dem Daktyloskopie (Fingerabdruck) [Parenti 2003, S. 34]. Wichtig war die Übertragbarkeit der Informationen. Durch den Telegraphen wurden daher die genannten neuen Identifizierungsmechanismen verstärkt und die Bertillonage vom Fingerabdruck abgelöst. Identifizierungsmaßnahmen, die von Staaten, Behörden usw. genutzt werden, müssen schnell und eindeutig sein.

6.6 Zusammenfassung

Der Prozess der Identitätsbildung verlagerte sich von hierarchischen Institutionen (Familie, Arbeitsplatz, Kirche) hin zum Einzelnen selbst und seinem selbst gewählten Umfeld. Elektronische Identitätsnachweise werden bedenkenloser akzeptiert. Bereits im Kapitel 5 wurden Möglichkeiten des Datenmissbrauchs, nicht zuletzt dank Vorhandenseins der Daten in digitaler Form, aufgezeigt. Das Geschäft und der Profit, die hinter der Einführung von (nationalen) ID-Kartensystemen stecken, gehen zu Lasten des Sicherheitsstandards, vor allem länderübergreifend betrachtet.

[7] System der Sklavenpässe zur Feststellung der Identität von Sklaven

[8] Die Bertillonage ist die Bezeichnung für ein von Alphonse Bertillon entwickeltes anthropometrisches System zur Identifizierung von Personen anhand von Körpermaßen. Quelle: {http://de.wikipedia.org/wiki/Bertillonage}

Einmal mehr wurde durch die Beschreibung der Thematik der Identitätsnachweise deutlich, dass es sich dabei – in digitaler Form – um eine Maßnahme handelt, die unweigerlich zu sozialer Klassifikation führt. Soziale Klassifikation bleibt das notwendige Mittel dieser Technologien um größere Bevölkerungen zu verwalten. Einmal mehr auch wurde deutlich, wie sehr die Verwendung der persönlichen Daten im Unklaren liegt.

Auch das Thema Identitätsnachweise hinterlässt Ungewissheit hinsichtlich der Verwendung der persönlichen Daten. In der folgenden Besprechung von Überwachung (siehe Kap. 7) werden weitere Möglichkeiten gezeigt, wie täglich Daten über jeden einzelnen gesammelt werden.

Kapitel 7

Überwachung

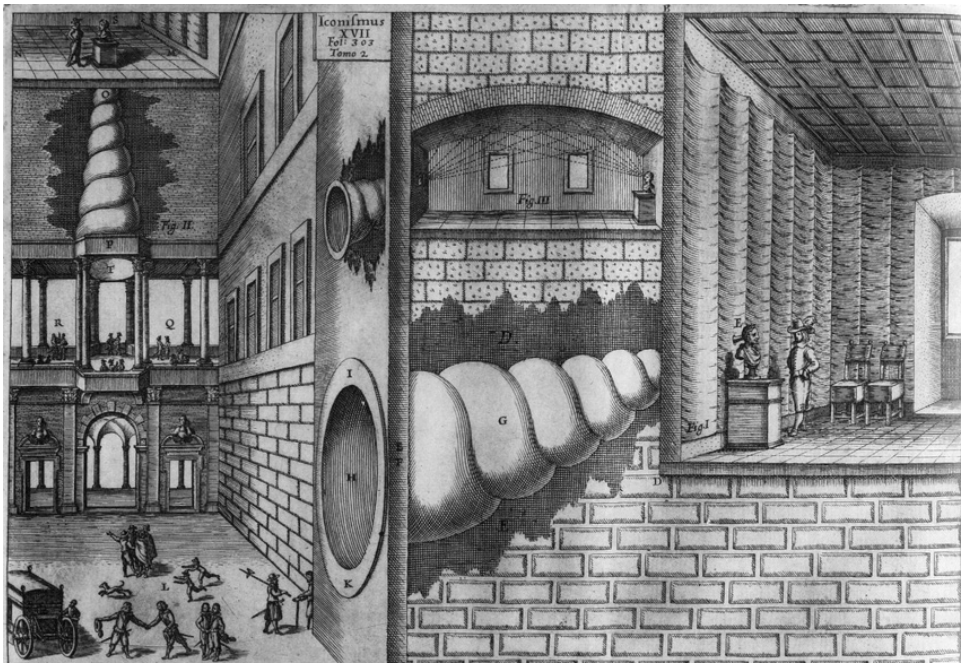

Abbildung 7.1: Athanasius Kircher (1601-1680): Skizze zur Konstruktion von geheimen Abhörstationen, 1650. Bild aus [Robin 2009, S. 206].

Die Verletzung der Privatsphäre erfolgt häufig unbemerkt. Aus gutem Glauben heraus ist der Einzelne der Überzeugung „Überwachung ist nicht auf mich gerichtet“, doch das kann täuschen. Plötzlich wird ein Kredit verweigert, es kommen ungebetene Anrufe von Telemarketingunternehmen, es erfolgt eine nicht angekündigte Steuerprüfung, eine zweite Sicherheitsprüfung am Flughafen usw. Die Ursache dieser Vorkommnisse ist unklar und wird verborgen gehalten, daher werden sie nicht als Eindringen in die Privatsphäre gewertet.

Zum anderen kommt immer wieder der Gedanke „wenn man nichts zu verbergen hat, hat man nichts zu fürchten“ [Bennett 2008, S. 97]. Athanasius Kircher (1601-1680) skizzierte bereits 1650 die Konstruktion von geheimen Abhörstationen (siehe Abb. 7.1).

In diesem Kapitel wird auf unterschiedlichste Formen der Überwachung eingegangen, die jedem Einzelnen im Alltag begegnen. Deutlich hervorgehoben wird dabei die umgekehrte Unschuldsvermutung. Aufgezeigt werden aber auch Aspekte, die zeigen, dass Überwachung auch zu einem Teil das eigene Einverständnis, eigene bestimmte Handlungen voraussetzt. *Social Sorting* wird erklärt und gezeigt, warum Überwachung zu sozialer Klassifikation führt. Der politische Aspekt von Überwachung wird erläutert um zu zeigen, wie dadurch nachhaltig das Verhalten von Bürgern beeinflusst wird. Auch in diesem Kapitel belegen Beispiele aus der Realität, dass eine kritische Haltung gegenüber Überwachung durchaus angebracht ist.

7.1 Überwachungsdilemma des Alltags

Unsere persönlichen Daten interessieren nicht nur die *Polizeiakten* (es ist einfacher einen Eintrag zu bekommen als diesen wieder loszuwerden). Vor allem wollen all jene unsere Daten haben, die uns *Produkte* verkaufen wollen. Und sie sind bereit, all unsere Daten in Register aufzunehmen – unsere Vorlieben, unsere Farben vor allem aber unser Geld, um uns zu helfen es wieder auszugeben, für Produkte, die immer genauer der Zielgruppe angepasst werden können.

Die Erfassung verschiedenster persönlicher Daten durch *Unternehmen* erfolgt häufig, ohne dass wir uns dessen bewusst sind, durch unsere unbewusste Zusammenarbeit mit den Unternehmen (beispielsweise die in die Suchmaschine eingegebenen Suchbegriffe oder die online-Bezahlung).

Auch soziale Netzwerke wie Facebook oder Twitter helfen Dritten die persönlichen Daten von uns zu vervollständigen. Mobiltelefonie erlaubt die Ortung von Personen und die Nachverfolgung, auch im Nachhinein. Die Computer speichern selbst jene Daten, von denen der Benutzer glaubt, dass sie gelöscht wurden. Chipkarten, die als Zahlungsmittel im öffentlichen Verkehr verwendet werden können – wie beispielsweise der Navigo Pass[1] – verfolgen die Spur der Reisenden. Die Videoüberwachung speichert unsere Bilder ,ohne dass wir eine Kontrollmöglichkeiten hätten. Alles, was im Internet nachgeschlagen wird, trägt dazu bei, das Verzeichnis unserer persönlichen Daten zu vervollständigen. Selbst die Haustiere mit einem Chip im Ohr werden in einer Kartei erfasst.

In [Gaillard 2009] werden humorvolle Möglichkeiten aufgezeigt, sich des Registriertwerdens zu entziehen (siehe Abb. 7.2).

[1] http://en.wikipedia.org/wiki/Navigo_pass

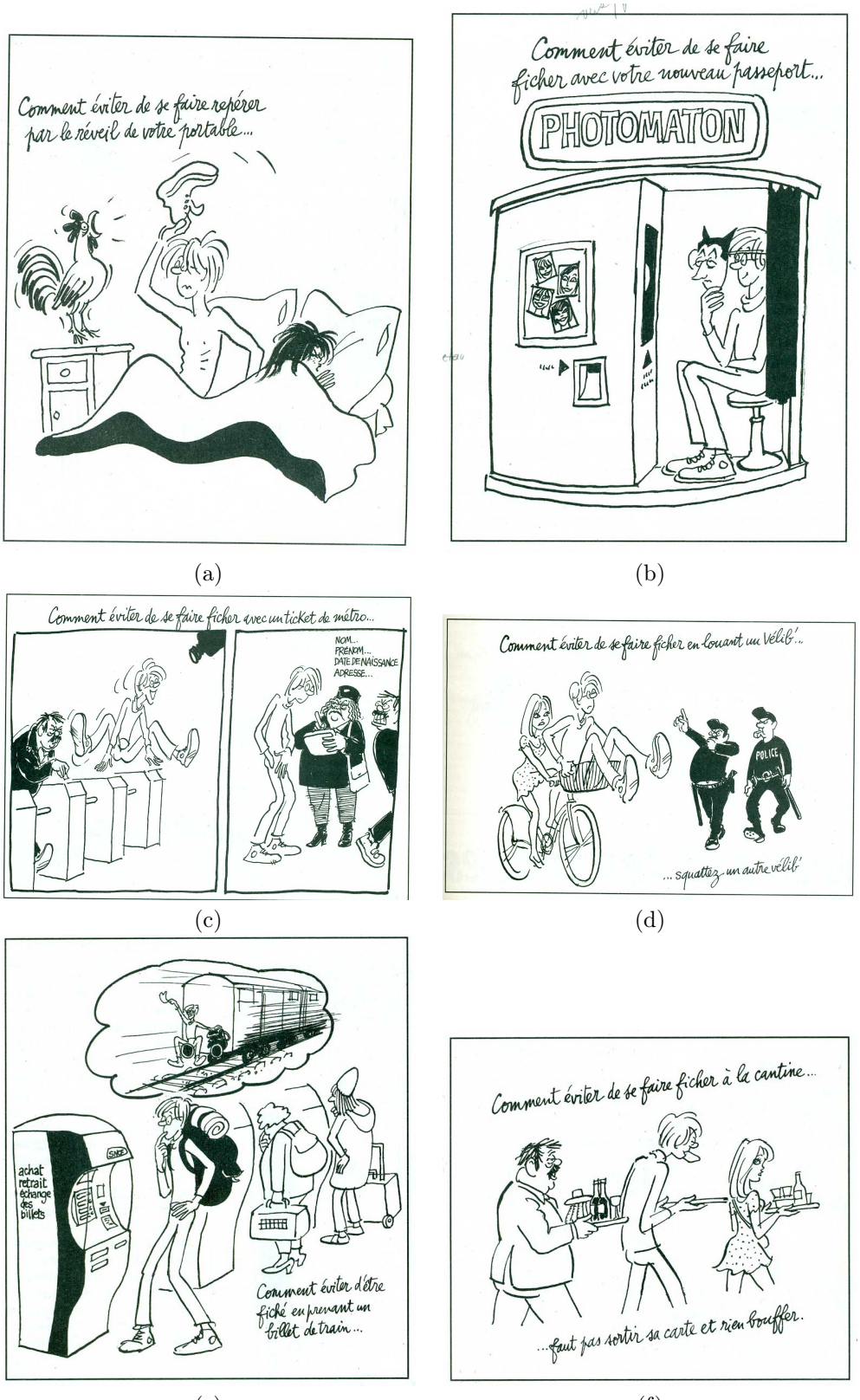

Abbildung 7.2: (a-h) Ein humorvoller Blick auf Möglichkeiten, sich des Registriertwerdens zu entziehen: (a) Wecker, (b) Passfoto, (c) U-Bahn, (d) Leihfahrrad, (e) Zugticket und (f) Kantine. Bilder aus [Gaillard 2009].

7.1.1 Nichts zu verbergen oder: Unschuldsvermutung umgekehrt

Wenn man nichts zu verbergen hat, warum soll man sich dann Gedanken machen [Parenti 2003, S. 8]? Zahlreiche Beispiele in dieser Diplomarbeit zeigen, wie sehr das Prinzip der umgekehrten Unschuldsvermutung bereits den Alltag durchdrungen hat. Argumente gegen die ausufernde Überwachung werden oft mit abstrakten Rechten und der Angst vor theoretischen Konsequenzen zurückgewiesen. *Philip Agre* fasst es so auf [Agre 1999]:

> With environmental pollution you can at least see the smoke and oily seabirds, but with invasions of privacy the information flows silently, out of sight, and then you can't figure out how they got your name, much less which opportunities never knocked because of the bad information in your file.

Colin J. Bennett appelliert, jüngere Menschen schon ab dem frühesten Alter für *Privatsphäre* -Themen zu sensibilisieren [Bennett 2008, S. 220]. *Deidre Mulligan* hingegen sagt in einem persönlichen Gespräch mit Bennett[2], dass Jugendliche MySpace, GMail, Facebook usw. wohl deshalb nicht als Bedrohung sehen, weil ihnen diese Instrumente viel Macht geben. Allerdings werden sie diese Macht sowohl positiv als auch negativ erleben. Mulligan denkt, dass Jugendliche ein besseres Verständnis von der Beziehung zwischen technologischem Design und Privacy haben [Bennett 2008, S. 220].

Die umgekehrte Unschuldsvermutung war Thema bei Chaos Radio Karlsruhe vom 14. März 2005[3] und bei German Haxx0r Radio vom 15. Juli 2009[4].

7.1.2 Überwachung ist bidirektional

Roberto Simanowski hat zum Thema Überwachung folgenden Schluss gezogen [Simanowski 2008, S. 176]:

Die Überwachungstechnologie befindet sich nicht allein in den Händen von Big Brother, sondern wirkt bidirektional. Wenn jedes Handy eine potentielle Überwachungskamera ist, bleibt die Aufnahme von Willküraken der Staatsmacht nicht mehr auf die zufällige Anwesenheit eines Hobbyvideofilmers angewiesen.

Die Bidirektionalität hat ihre Grenzen, wenn es um die Effizienz der Erhebung und Auswertung von Daten geht. Eine wirkliche Datenschutzgefährdung entsteht erst, wenn die von unterschiedlichen Institutionen und Unternehmen erhobenen Daten kombiniert werden, wenn also die

[2] Gespräch zwischen Colin J. Bennett und Deidre Mulligan, 17. April 2007.

[3] Radio Chaotica Podcast, http://www.podcast.de/episode/124392/Radio_Chaotica_-_Video\%C3\%BCberwachung

[4] C-RaDaR Potcast, http://www.podcast.de/episode/1319828/C-RadaR_August

GPS-Sicherheitsdienste, die Kreditkarteninsitute, die Internet-Provider, die Mobilfunkunternehmen usw. ihre Daten abgleichen. Diese Abgleichung kann aus wirtschaftlichen Gründen erfolgen oder von staatlichen Behörden angeordnet werden.

Überwachung und der Schutz davor gehen zuweilen Hand in Hand, wie das Gesetzespaket „Family Privacy and Protection Act“ zeigt (2004). Es verbot zum einen versteckte Überwachungskameras und forderte zum anderen, alle Websites mit pornographischem Inhalt unter einer speziellen Domain (.prn) zu registrieren.

Zur Videoüberwachung in Städten stellt Shu-Min Lin die Frage [Stocker und Schöpf 2007, S. 51ff]: Genießen wir diese Publicity, die früher den Superstars vorbehalten war? „Am besten lächeln wir also recht freundlich, während wir den roten Teppich des Ruhms entlangschreiten.“

7.1.3 Überwachung: ein Gewöhnungseffekt von klein auf?

> Kindheit 2009, das ist ein Leben im Überwachungsstaat, in einer Diktatur des Guten. Keine langweiligen Nachmittage zu Hause, weil immer irgendein Erwachsener für Beschäftigung sorgt, keine öden Besuche bei Verwandten am Wochenende, sondern Zirkus, Museum, Konzert, Ballonfahren.[5]

Werden nachkommende Generationen von klein auf an die „Überwachung“ sowie ein Leben-als-Animation/Leben-als-Erlebnis gewöhnt?

7.2 Social Sorting

Die Nutzung von Informations- und Kommunikationstechnologien im Rahmen neuer Ausprägungen des Risikomanagements führen in der Überwachungsgesellschaft und im Sicherheitsstaat zu neuen Formen der Klassifikation die tief greifende soziale, ökonomische und politische Veränderungen mit sich bringen.

Die moderne Klassifikation fand im Computer sein ideales Instrument. Überwachungssysteme basieren auf IKT-Anwendungen. Die neue feststellbare Entwicklung im Bereich Überwachung lautet daher: Chancenmaximierung und Risikominimierung. Heute ist der Klassifikationsvorgang zur Routine geworden. Wer weiß, auf welcher Grundlage ein Kreditantrag unerwartet abgelehnt oder ein unschuldiger Terrorverdächtiger festgehalten wurde? Natürlich kann der Auswahlprozess harmlos und gerechtfertigt sein – Überwachung ist schließlich immer eine zweischneidige Angelegenheit; soziale Klassifikation hat jedoch auch immer direkte Folgen (zum Guten oder Schlechten)

[5] Nr. 32 vom 30. Juli 2009, S. 12, „Ich will doch nur spielen“ von Tanja Stelzer

für die Lebenswirklichkeit von Menschen. Heute erfolgt – nicht zuletzt wegen 9/11 – eine *präventive Intervention* auf Basis von Risikoanalysen: Planung, Vorhersage, Vorrechte und Genehmigungen.

David Lyon sieht soziale Klassifikation als jenen Vorgang, der dazu führt, dass unterschiedliche Gruppen mit unterschiedlichen Lebensrealitäten und damit automatischer Diskriminierung konfrontiert sind. Mit dieser Entwicklung geht natürlich auch ein hohes Maß an Überwachung durch den Staat einher [Stocker und Schöpf 2007, S. 58ff, David Lyon]. Dies führt langsam zu einer Auflösung der Privatsphäre der Bürger und zu einer zunehmenden Verschwiegenheit und Geheimniskrämerei der Verwaltungseinrichtungen [Stocker und Schöpf 2007, S. 129ff, Felix Stalder].

7.3 Überwachung ist politisch

Routinemäßige Überwachung geht einher mit politischer Repression und hat darüberhinaus auch eine weitere „fruchtbare“ Funktion, indem sie hilft, *politisch nützliche Formen von Wissen und Verhalten hervorzurufen und zu konstruieren* [Parenti 2003, S. 9].

Privatsphäre schützt die individuelle Freiheit und Autonomie einer Person. Rössler bemerkt zur Videoüberwachung [Stocker und Schöpf 2007, Rössler, S. 34]:

> (...) Aber man hat nicht die Erwartung, dass solcherlei Gesehen- und Registriertwerden auf Filme aufgenommen wird und damit reproduzierbar, ortsunabhängig und zeitunabhängig vorführbar wird, analysierbar, übermittelbar, kontrollierbar.

Freiheit und Autonomie werden ersetzt durch Gehorsam und Vertrauen in die Autorität [Parenti 2003, S. 207].

Für *David Lyon* ist Überwachung „any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered“ [Lyon 2001]. Später ergänzt Lyon noch, dass Überwachung die „focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction “ [Lyon 2007] ist.

Für die starke Überwachung in Amerika kann nur bedingt 9/11 verantwortlich gemacht werden. Auch davor schon existierte in Amerika eine Kultur von Angst und eine Begeisterung für Überwachung. Berücksichtigt werden muss die beliebte private Eigenheimsicherheit, die Faszination von Reality-TV-Sendungen [Parenti 2003, S. 183ff].

Colin J. Bennett hebt hervor dass bei der Überwachung neben dem Beobachten auch die Klassifizierung und das *social sorting* eine wichtige Rolle spielen [Lyon 2003b].

Überwachungssysteme kompensieren die immer schwächer werdenden, persönlichen sozialen Beziehungen zwischen Menschen, wo Mechanismen für

soziale Integration verstärkt verschwinden und abstrahiert werden. Überwachung als notwendiges Verbindungsstück, das Vertrauen schafft durch eine „Gesellschaft von Fremden “ [Lyon 2003a].

Menschen lernen in einer Umgebung nicht-existenter oder stark eingeschränkter *Privatsphäre* anders. Ist sich der Einzelne der Beobachtung bewusst, so schränkt das das akzeptable Spektrum von Glauben und Verhalten ein. Konstante Beobachtung jeder Bewegung oder Fehler wird zuerst die Wahlmöglichkeiten auf jene der Masse einschränken. Das Ergebnis wird ein fundamentaler Umschwung im Bereich unseres Charakters sein. Die Bedingung einer nicht-existenten *Privatsphäre* fügt nicht nur der Ausdrucksmöglichkeit der Individualität Schaden zu, sondern lässt auch langsam die Sehnsucht danach verschwinden. [Solove und Schwartz 2008b, S. 48]

7.3.1 Überwachungsprojekt Indect

Das Forschungsprojekt der EU namens *Indect*[6] (*Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment*) soll Wege finden, Informationen aus dem Netz, aus Datenbanken und von Überwachungskameras zu verbinden – zu einem automatischen Bevölkerungsscanner.

Indect ist der Traum der EU vom Polizeistaat. Dem Bericht von ZEIT ONLINE [7] zufolge finanziert die EU seit Jahresbeginn 2009 ein Forschungsprojekt, das all die bestehenden Überwachungstechnologien zu einem Instrument verbinden soll. Mit *Indect* (Intelligent information system supporting observation, searching and detection for security of citizens in urban[8] environment) soll es möglich werden, dass alles gesehen und verfolgt werden kann. Für das auf fünf Jahre angelegte Projekt sind zur Zeit 14, 86 Millionen Euro angesetzt. Es soll dazu dienen, das Internet anhand von Suchroutinen („Gewalt“, „Bedrohungen“, „abnormales Verhalten“) zu durchsuchen.

Für die Polizei soll Indect ein Werkzeug sein, um „verschiedenste bewegliche Objekte“ zu beobachten (Schiffe, Fahrzeuge und Menschen).

Auch eine Suchmaschine wird im Rahmen des Projekts entwickelt, die anhand von Wasserzeichen Bilder und Videos wiederfinden und schnell verwalten kann. Es soll unter anderem eine Suchmaschine erstellt werden zur schnellen Ermittlung von Personen, Dokumenten und Suchprogrammen, die „ständig“ und „automatisch“ öffentliche Quellen wie Websites, Foren, User-Gruppen, Fileserver, P2P-Netwerke und „individuelle Computersysteme“ durchsuchen. *Das heißt, alle Blogger, Netzaktivisten, Twitter-Mitglieder usw., im Prinzip die gesamte Online-Bewegung ist grundverdächtigt („Unschuldsvermutung umgedreht“). Am besten also das Internet abschaffen.*

[6] http://www.indect-project.eu/

[7] http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung

[8] Ein Aufruf, aufs Land zu ziehen? Soll so der Städtezuwanderung entgegengewirkt werden?

Das Hauptziel ist die Verknüpfung aller Daten aus dem Netz mit Daten aus anderen Datenbanken. Genau darin jedoch liegt die Gefahr des Projekts angesichts der *Privatsphäre* eines jeden Bürgers (siehe Abschnitt 2.4).

Daten aus dem Netz sollen beispielsweise mit Bildern von Videoüberwachungskameras oder mit Daten von Mobiltelefonen verbunden werden. Das Ziel so scheint es: in irgendeiner Weise auffällig gewordene Menschen schnell entdecken und langfristig verfolgen können („trackable, controllable.“).

Wer beispielsweise auf YouTube ein Drohvideo gepostet hat, der soll mithilfe von Überwachungskameras gesucht, via Suchmaschine identifiziert und mittels tragbarer Geräte von Polizisten verfolgt werden können.

Wird das Projekt umgesetzt, wäre es der Albtraum jeder Bürgerrechtsbewegung. Verbindet es doch alle einzelnen Überwachungsinstrumente, die bereits jetzt installiert sind, wie Videokameras, Vorratsdatenspeicherung, Handy-Ortung, Gesichtserkennung oder Telefonüberwachung, zu einem einzigen Spähprogramm. Rechtlich ist diese Form der Überwachung längst in den Polizeigesetzen der Länder und des Bundes verankert. Das Projekt Indect zeigt deutlich, wie weit dieses Konzept gehen und wie tief es in die Gesellschaft eindringen kann.

Begriffe wie Unschuldsvermutung oder gerichtsfester Beweis verlieren in diesem Zusammenhang ihre Bedeutung, ersetzt das Projekt doch die gezielte Suche nach Verdächtigen durch das vollständige und automatisierte Scannen der gesamten Bevölkerung.

Text teilweise übernommen aus[9].

7.3.2 Polizeiakten am Beispiel Frankreich

Mehr als die Hälfte aller französischen Staatsbürger kann ihren Namen in einer Polizeiakte finden [Gaillard 2009, S. 43]. So gibt es beispielsweise Register zu Sprayer (Octopus), Obdachlose (FSDRF), Münzfälscher (FNFN), Luftfahrt-Passagiere (FPA), Pass-Besitzer (Delphine), städtische Unruhestifter (Gevi), Personen mit Hausverbot in Stadien (Fnis), Personen, die im Ausland geboren sind (FNR), Reisende mit Reisezielen in heiklen Ländern usw. Es existieren nicht weniger als 45 Register der Polizei, ein Viertel davon basiert auf keiner rechtlichen Grundlage. Die genannten Beispiele zeigen, wie schwierig es inzwischen ist, in keiner Polizeiakte aufzutauchen.

Zu den besonders umfangreichen Akten gehört FAR (Fichier alphabétique de renseignements[Auskunft]), das Auskunftsregister, mit 60 Millionen eingetragenen Namen, das Register ist der Gendarmerie zugeordnet. Das Ziel von FAR ist es, genaue Kenntnis der Wohnbevölkerung zu haben, insbesondere über ihre eventuelle Gefährlichkeit [Gaillard 2009, S. 44]. Das Register ist illegal, daher sollte die Gendarmerie es eigentlich bis Oktober 2010 zerstören. Die Entsorgung hat noch nicht begonnen und das Register

[9] http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung

wird weiterhin mit Informationen gefüllt.

Das Gegenstück der Polizei zu den Auskunftsakten FAR der Gendarmerie ist das RG (Renseignements généraux – allgemeine Auskünfte), darin sind 900.000 Franzosen erfasst. Durch interne Umstellungen im Innenministerium werden die Akten von zwei Institutionen betreut: dem DCRI[10] gehören 20% der Akten (jene die staatliche Angelegenheiten betreffen), die restlichen Akten entfallen auf Sdig[11]. Sdig gründete daraufhin Evige (Exploitation documentaire et valorisation de l'information générale). Zusätzlich zu den allgemeinen Informationen des RG mussten bei Edvige noch pikante Informationen über die Gesundheit und sexuelle Orientierung ergänzt werden (diese wurden aus den RG-Akten 2004 entfernt). Im Oktober 2008 holte sich das Innenministerium das Edvige-Register wieder zurück und gab ihm einen neuen Namen: Edvirsp (Exploration documentaire et valorisation de l'information relative à la sécurité publique). Einträge zu Gesundheit und sexueller Orientierung wurden offiziell entfernt, allerdings bleiben unter der Bezeichnung *Aktivitäten* weiterhin *Meinungen* in den Akten bestehen (Informationen über politische, philosophische, religiöse Meinungen oder Mitgliedschaft bei Gewerkschaften).

Das DCRI (das 20% der Akten des RG hält) erzeugte als Reaktion auf das Edvige ein Register namens Cristina (Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux).

7.4 CCTV – Videoüberwachung

Videoüberwachung unterscheidet zwischen öffentlicher (öffentliche Plätze) und privater (Bus, Bahnhöfe, Schulen, Supermärkte, Busstationen, U-Bahn, Ein- und Ausgänge von Krankenhäusern, Einkaufszentren, Parkgaragen usw.) Videoüberwachung – genau hier beginnt meiner Meinung nach schon das Durcheinander, die Unklarheit.

Bereits 2007 wurde der präventive Charakter von Videoüberwachung mit einer Studie des IAURiF[12] widerlegt (Studie zu Videoüberwachung in Schulen) [Gaillard 2009, S. 46]. Geht es nach Frankreichs Präsident Nicolas Sarkozy, so ist Videoüberwachung „un moyen fondamental de la politique de sécurite“[13]. Kritiker der Videoüberwachen nennen es vielmehr das Schaffen jener Illusion, dass alles unter Kontrolle sei. Soziologen sprechen außerdem vom Nebeneffekt der *sozialen Klassifikation* (siehe Abschnitt 7.2), da Polizisten ihre Aufmerksamkeit vor allem auf Männer jünger als 30 und eher farbig legen. Scotland Yard musste 2009 zugeben, dass in London die Videoüberwachung zur Aufklärung von nur 3% aller Straßendiebstähle half [Gaillard

[10] Direction centrale du reseignement intérieur
[11] Sous-Direction de l'information général
[12] http://www.iaurif.org/
[13] ein grundlegendes Mittel der Sicherheitspolitik (eigene Übersetzung)

2009, S. 49].

Wer stellt sicher, dass die Videobänder nur für den dafür vorgesehenen Zweck genutzt werden und nach einem Monat zerstört werden? Die Gefahr von Videoüberwachung liegt in der Fernwartung, denn dafür wird das Internet herangezogen. Eine Frage der Zeit, bis die Kameras in die Macht fremder Hände gelangen (oder sind sie es schon?).

7.4.1 Gesichtserkennung und Bewegungsmuster

Seitens der Polizei wird beispielsweise in Frankreich bereits die Videoüberwachung der Zukunft vorbereitet: Videoüberwachung mit integrierter Gesichtserkennung anhand einer Basisdatenbank von registrierten Personen – in London wird dies bereits jetzt umgesetzt.

Währenddessen beschäftigt sich die Universität von Norwich[14] bereits mit der Weiterentwicklung visueller Überwachungstechnik. Es wird dort versucht, eine Software zu erstellen, mit deren Hilfe Lippenlesen möglich wird. Die Software vergleicht mithilfe einer Bibliothek an gefährlichen Begriffen – Beispiel „Bombe“ – die Aufzeichnungen. Sprachwendungen wie “Das Mädchen ist eine Bombe“ garantieren bereits jetzt so manch amüsanten Alarm [Gaillard 2009, S. 49].

Eine andere Innovation ist die Erkennung von verdächtigen Bewegungsmustern. In Luton analysiert eine experimentelle Aufstellung von acht Kameras Bewegungsverläufe von Körpern und kann bereits etwa fünfzig verdächtige Verhaltensweisen detektieren [Gaillard 2009, S. 49].

7.5 Kleine Auswahl wahrer Begebenheiten

7.5.1 Ortung und Abhören von (Mobil-)Telefonen am Beispiel Frankreich

Durch die Mobiltelefone ist es heute möglich, die Spur von einer Person (die ein Mobiltelefon bei sich trägt) genau nachzuverfolgen – wo war die Person zu welchem Zeitpunkt. Je mehr Funkmasten es gibt, desto genauere Ergebnisse liefert die geographische Ortung von mobilen Objekten. Per Knopfdruck können die Mobilfunk-Netzbetreiber (Beispiel Frankreich, z. B. orange) den Anschluss jedes beliebigen Teilnehmers an die staatliche Abhörmaschinerie weiterleiten, so der Fall in Frankreich. Jedes Mal, wenn das Mobiltelefon in Reichweite einer Funkantenne kommt, verbindet es sich neu und gibt so wieder den aktuellen Aufenthaltsort bekannt. In Paris ist eine Ortung bis auf 20 Meter genau möglich. Ein Wechsel der SIM-Karte alleine reicht nicht, um seine Spuren zu verwischen, denn es wird die Hardware-Nummer des Mobiltelefons registriert.

[14] http://www.norwich.edu/

Abbildung 7.3: Mobile Abhöreinheiten sind in der Standortauswahl gefordert („*Beeindruckend dass alle diese Anrufe von Pizza handeln*“ – „*Und wenn das ein Code ist?*“ – „*Wir parken vor einer Pizzeria...*“, eigene grobe Übersetzung). Bild aus [Gaillard 2009].

Neben der Ortung ist ein wesentliches Überwachungsmerkmal die Möglichkeit des Abhörens durch Mobiltelefone – auch bei ausgeschalteten Geräten. Erst wenn der Akku aus dem Mobiltelefon genommen wurde, ist Abhören nicht mehr möglich. Durch das Gesetz „Perben 2“[15] vom März 2004 wurde die Praxis des Abhören eines Mobiltelefons offiziell legalisiert. Jedes Jahr werden in Frankreich 31.000 Telefone abgehört. Einem hohen Beamten in Frankreich ist es erlaubt, jeden beliebigen Menschen abzuhören, solange dies der Wahrheitsfindung dient. Alleine 2008 hatte die französische Kriminalpolizei 4 Millionen Aufträge betreffend Telefonie.

Das DCRI (Direction centrale du renseignement intérieur)[16] sowie bestimmte Einheiten der Kriminalpolizei haben darüberhinaus eine Spezialausstattung, die es erlaubt, abzuhören ohne vorher nachzufragen. Bis zu zehn Leitungen können gleichzeitig in einem Umkreis von 800 m in Paris oder drei Kilometern auf dem Land abgehört werden. Es handelt sich dabei um Relais-Antennen. Der Vorteil dabei ist dass keine Autorisation dafür notwendig ist. Kleine Lastwagen sind die größere Version des Koffers. Nicht nur die Telefongespräche im Umkreis werden abgehört, sondern alle Mobiltelefone der überwachten Zone werden identifiziert [Gaillard 2009, S. 50ff]. Abbildung 7.3 zeigt einen humoristischen Blick auf diese Methode.

[15] http://fr.wikipedia.org/wiki/Loi_Perben_II_du_9_mars_2004
[16] Zentraler Inlandsgeheimdienst

7.5.2 Chipkarte Navigo

Die Abonnenten der Pariser Métro haben einen „Navigo-Pass“ [Gaillard 2009, S. 57ff], der mit einem elektronischen Chip ausgestattet ist, so lässt sich die genaue Spur des Abonnenten verfolgen. Der Navigo-Pass kann abonniert oder als Prepaid-Karte gekauft werden. Dank des elektronischen Chips lassen sich nun die genaue Fahrtstrecke samt Aufenthaltsort und -zeit analysieren. Die Verwaltung weiß genau, wo wann wieviele Menschen unterwegs sind und – bei Abonnenten – auch wer. Alle Informationen sind plötzlich zentralisiert. Die Analyse in Echtzeit ist nun möglich, ja Tagesgeschäft. Diese plötzliche Zentralisierung aller Daten stellt eine enorme Gefahr dar.

7.5.3 Die Post bringt allen was – und noch viel mehr

Ein ehemaliger Direktor einer Mailingfirma startete einen Selbstversuch. Er schickte an seine Wohnadresse einen Brief, nur anstatt seines echten Namens setzte er jenen eines berühmten Bischofs ein. Er klebte noch auf seinen Briefkasten das Namensetikett mit dem falschen Namen. Zehn Tage später erhielt er die erste Werbesendung, adressiert an den falschen neuen Namen, weitere gut 60 Sendungen trafen in den beiden Folgemonaten ein. Den neuen Briefträgern wird viel abverlangt. 2001 musste der Datenschutzverband der Post verbieten, dass sie ihre Briefträger beauftragt, Alter und Beruf des Familienoberhaupts zu schätzen von dem Gebiet, für das der jeweilige Briefträger zuständig war. Diese Arbeit des kleinen Berichterstatters (Briefträger) birgt großen Nutzen für die Post, denn so kann sie die Adressen mit speziellen Zusatzinformationen (Vorlieben, Abonnements, ...) teuer – bis zu einem Euro pro Stück – verkaufen. So wird unser Postkasten in eine Sparbüchse für die Post verwandelt. Beispiel aus [Gaillard 2009, S. 44].

7.5.4 Schöne neue Haushaltsautomatisierung

Mit Hilfe neuer Haushaltsautomatisierung ist es möglich, beispielsweise die Heizung über das Mobiltelefon zu steuern. Der Eigentümer eines Zweitwohnsitzes in Biarritz, Frankreich, hatte in seiner Wohnung eine neue Heizung einrichten lassen, der Elektriker präsentierte ihm einen Wunderkasten zum Preis von um die 1.500, 00 Euro. Mit seinem Telefon kann nun der Eigentümer durch eine einfache Nummernkomposition die Heizung von der Ferne steuern (ein- und ausschalten, Temperaturregelung,...). Der Eigentümer ist skeptisch, ob dies notwendig sei, daraufhin nennt ihm der Elektriker das schockierende Argument. Mit Hilfe dieser Wunderbox kann sich der Eigentümer jederzeit über sein Telefon mit der kleinen Box verbinden und hört nachweisbar alles, was in seinem Appartement passiert. Die französchische „Fédération des professionnels de l’électricité et l’électronique“ nimmt dazu Stellung und sagt, diese kleine Box sei auf jeden Fall legal und ergänzt außerdem, dass im Moment nicht klar sei, wie oft und wo diese Ausstattung in

Frankreich bereits verkauft wurde [Gaillard 2009, S. 50].

7.5.5 Bitte lächeln – der Radiowecker klingelt

Auf www.espion-on-line.com wurde die Anzeige für ein drahtloses Kamera-Set in einem Radiowecker gefunden. Für 700 Euro kann das Gerät erworben werden (Ausführung als Radiowecker oder MP3-Player). Sobald der Radiowecker mit Strom versorgt wird, funktioniert die Kamera und übermittelt Video und Audio (!!) an den Empfänger. Es geht aber auch anders, indem dem „Zielobjekt“ der Beobachtung ein Mobiltelefon der Marke Nokia geschenkt wird. Denn zum Preis von 150, 00 Euro können mittels einer auf spion-on-line vorgestellten Software alle ein- und ausgehenden SMS direkt auf das Mobiltelefon des Beobachters übertragen werden. Um nur 150, 00 Euro mehr hat der Beobachter auch noch das Recht auf das Mithören von „Umgebungsgeräuschen“. Dazu ruft der Beobachter das Zielobjekt an. Auf dem entsprechenden Mobiltelefon des Beobachteten scheint dieser Anruf jedoch nicht auf, denn der Anruf wird automatisch dank der Software unterbrochen. Für 200, 00 Euro mehr können die großen Spiele beginnen. Sobald sich der Telefonspion aktiviert, erhält der Beobachter eine SMS und muss „nur mehr zuhören“. Doch beim Kauf der genannten Ausstattung läuft der Käufer große Gefahr, registriert zu werden (...) [Gaillard 2009, S. 51].

7.5.6 Weltbekannt dank Web 2. 0

„Alles Gute zum Geburtstag, Marc!“ las Marc, als er die Ausgabe 28 von „Le Tigre“[17] 2008 durchblätterte[18]. Die Redaktion der Zeitschrift hatte damals beschlossen, in jeder Ausgabe (monatlich) ein Profil eines anonymen Internetbenutzers zu veröffentlichen.

Marc fand im Artikel Fotos (von Flickr.fr), persönliche Daten (von Facebook: single, heterosexuell, seit letzten September in einem neuen Büro), Informationen zu seinen Partnerschaften (Claudia im letzten Frühling – charmant, kurze Haare, hübsche Beine – die Jenniffer ersetzte, mit der er zwei Jahre zusammen war) und zahlreiche andere Daten. All diese Daten hatte die Redaktion rein aus dem Internet zusammen gestellt.

Damit nicht genug. Als die lokale Presse davon erfuhr, fand sich Marc mit Fotos darin wieder, es wurde über die Geschichte groß Bericht erstattet. Sogar das Fernsehen berichtete. Eine Klage von Marc gegen das Medienunternehmen wurde abgewiesen, weil der Journalist vollkommen legal gehandelt hatte.

Die starken Reaktionen auf die erste Veröffentlichung der neuen Kolumne überrollte die Redaktion, die Aktion wurde bisher nicht mehr wiederholt.

[17] http://www.le-tigre.net/

[18] http://www.heute.de/ZDFheute/inhalt/5/0,3672,7509477,00.html

7.5.7 2000 Familien videoüberwacht in London

In London leben 2000 Familien mit schwierigen Familienverhältnissen einem Zeitungsbericht zufolge[19] in Wohnungen, die rund um die Uhr von Kameras überwacht werden. Der zuständige Minister Ed Balls hat das Programm mit dem Namen „Respekt“ dem Bericht zufolge bereits auf 20.000 Familien aufgestockt. Eltern, die alkohol- oder drogenabhängig sind, ihre Kinder nicht mehr zur Schule schicken und staatliche Hilfe ablehnen, werden vor die Wahl gestellt. Entweder ziehen sie in eine der so genannten *Sin Bins* (Strafbank) mit permanenter Video-Überwachung oder es werden ihnen die Kinder oder die Wohnung weggenommen.

7.6 Zusammenfassung

In dem Kapitel wurde deutlich gemacht, dass jeder Einzelne gefordert ist, sich der unterschiedlichen Formen und Aspekte der Überwachung bewusst zu werden. Überwachungstechnologien in unterschiedlichsten Arten und Formen haben inzwischen den Alltag durchdrungen, umso wichtiger ist es, sich neuen Maßnahmen entgegenzustellen oder zumindest diese kritisch zu hinterfragen. Im Kapitel 8 werden Möglichkeiten gezeigt, wie mehr Bewusstsein gegenüber Datensammlung und Überwachung geschaffen werden kann. Darüberhinaus werden Ideen der Gegenwehr präsentiert.

[19] KURIER, 8. August 2009, S. 8

Kapitel 8

Widerstand

> „we stand on the threshold of what might be called the Age of the Goldfish Bowl. [...] A couple of generations hence, will some automated society look upon privacy with the same air of amused nostalgia we now reserve for, say, elaborate eighteenth-century drawing room manners?“ [Solove 2008, S. 4, Myron Brenton]

Dieses Kapitel soll verschiedene Möglichkeiten aufzeigen, wie sich der völligen Überwachung, der Identifizierung und Nachverfolgung ansatzweise entzogen werden kann und wie das Bewusstsein über *Privatsphäre* geschärft werden kann. Die Möglichkeiten werden dabei nach individueller und gesellschaftlicher Ebene unterschieden. Auf gesellschaftlicher Ebene setzen sich beispielsweise kritische Gemeinschaften oder herausragende Persönlichkeiten für den Schutz der *Privatsphäre* ein. Aber auch Veranstaltungen oder Politik können einen Teil der Aufklärung auf gesellschaftlicher Ebene leisten. Die individuelle Ebene umfasst Maßnahmen, die direkt von einzelnen Personen ergriffen werden können. Diese bewegen sich mitunter an der Grenze zur Legalität, sollen aber gerade durch diese Überzogenheit Wege der Gegenwehr zeigen.

8.1 Gesellschaftliche Ebene

Die Herausforderung liegt darin, ein Bewusstsein für die ständig anwachsende Bedrohung sich ständig verändernder und weiterentwickelnder Formen von Überwachung zu schaffen. Inzwischen vergeht kaum mehr ein Tag, an dem nicht von einem „Überwachungszwischenfall“ – ob nun wirtschaftlich, bürgerrechtlich und arbeitsrechtlich – berichtet wird. Das wachsende Bewusstsein jedes Einzelnen soll eine Gegenströmung erzeugen.

Obwohl täglich in den Medien von Verletzungen der *Privatsphäre* in unterschiedlichsten Formen berichtet wird, scheint die Grundstimmung immer noch zu sein, dass es einen selber nicht betrifft. Es betrifft jeden und zwar in

unterschiedlichster Form und in allen Bereichen, daher ist jeder aufgerufen, sein Bewusstsein zu schärfen und der tatsächlichen Situation zu begegnen. In diesem Abschnitt soll gezeigt werden, wie jeder auf gesellschaftlicher Ebene Wege finden kann, sich mehr zu informieren.

8.1.1 Kritische Gemeinschaften

Die Gesellschaft wird in dem Anliegen, sich zu informieren um sich zu schützen, unter anderem von einer Reihe kritischer Gemeinschaften unterstützt, nur einige davon seien beispielhaft aufgezählt:

- Privacy International[1] (PI)
- q/uintessenz[2]
- Chaos Computer Club[3] (CCC)
- Electronic Frontier Foundation[4] (EFF)
- Big Brother Awards (siehe Abschnitt 8.1.3)

Privacy International ist eine Bürgerrechtsgruppe, die sich seit fast zwanzig Jahren für die Verteidigung der persönlichen *Privatsphäre* einsetzt. Weltweite Kampagnen, internationales Netzwerken und Forschung sollen Menschen davor schützen, dass Regierungen und Unternehmen immer mehr versuchen die Privatsphäre von Menschen zu verletzen. PI ist eine nichtstaatliche, gemeinnützige Organisation.

q/uintessenz ist ein „Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter“. Gemeinsam mit anderen Gruppen von fünf Kontinenten führt quintessenz bereits seit 1996 weltweit Kampagnen durch. Gemeinsam mit Privacy International und Gruppen für „cyber rights“ wird seit 1999 jährlich der Big Brother Award (siehe Abschnitt 8.1.3) verliehen. Die Mitglieder von quintessenz kommen aus den unterschiedlichsten Bereichen wie etwa Technik, Wissenschaft, Journalismus oder Kunst. Der kostenlose Newsletter „q/depesche“ erscheint seit 1998 beinahe täglich und informiert über Themen zu elektronischer Überwachung, Zensur, Copyright, Copyleft und ähnlichem.

Der Chaos Computer Club ist die größte europäische Hackervereinigung und engagiert sich unter anderem für technische Forschung, Kampagnen, Veranstaltungen, Politikberatung und Publikationen im Spannungsfeld technischer und sozialer Entwicklungen. Der CCC besteht aus mehreren

[1] http://www.privacyinternational.org/
[2] http://www.quintessenz.org/
[3] http://www.ccc.de/
[4] http://www.eff.org/

dezentralen lokalen Vereinen und Gruppen, die sich in regelmäßigen Veranstaltungen organisieren.

Electronic Frontier Foundation setzt sich für die digitalen Rechte von Personen und der Gesellschaft ein und arbeitet auch an der Aufklärung von Presse und Politik mit. EFF ist eine gemeinnützige Organisation und wird aus Spenden finanziert.

8.1.2 Herausragende Persönlichkeiten

Im Engagement um den Kampf für *Privatsphäre* können einige Personen hervorgehoben werden, wie beispielsweise der kanadische Journalist, Blogger und Science-Fiction Autor *Cory Doctorow*[5], Jura-Professor der Havard University und Gründer der Creative Commons[6]-Initiative *Lawrence Lessig*[7] oder der Österreicher *Erich Möchel*[8], Aktivist der ersten Stunde im Kampf für Privatsphäre und Datenschutz, Gründer von q/uintessenz und den Big Brother Awards sowie Mitglied im International Board of Advisors von Privacy International. Sie alle verbindet das unermüdliche persönliche Engagement für die Rechte der Menschen, für Privatsphäre und Datenschutz. Diese Persönlichkeiten und deren Bemühungen sind wesentlich für das Bestehen der kritischen Gemeinschaften sowie der Weiterentwicklung und des Schaffens des Bewusstseins gegenüber der Problematik von *Privatsphäre* und Datenschutz.

8.1.3 Big Brother Awards

Mit den Big Brother Awards soll darauf aufmerksam gemacht werden, wie erschreckend weit bereits Behörden, Unternehmen und Organisationen in die Privatsphäre der Menschen vorgedrungen sind und diese verletzen.

Jedes Jahr werden im Rahmen der Big Brother-Awards besonders erschreckende Beispiele von Datenmissbrauch und Eindringen in die Privatsphäre nominiert – und zwar von der Öffentlichkeit, jeder darf mitstimmen. Der Big Brother Award wird an jene Personen, Institutionen, Behörden und Firmen vergeben, die sich im Feld der Überwachung, Kontrolle und Bevormundung ganz besonders verdient gemacht haben. Die Gewinner bekommen einen Preis und einen Platz in der Hall of Shame, gemeinsam mit den Vorgängern alle Jahre[9].

Die Big Brother Awards werden neben Österreich auch international, in unterschiedlichen Ländern, vergeben[10]. Unter der Jury befinden sich unter

[5] http://craphound.com/
[6] http://creativecommons.org/
[7] http://www.lessig.org/
[8] http://moechel.com/
[9] http://bigbrotherawards.at/
[10] http://bigbrotherawards.org/

anderem Rechtsanwälte, Akademiker, Berater, Journalisten, Menschenrechts-Aktivisten, Künstler, Hacker usw.

Hinter Big Brother stehen die Organisation *Privacy International*[11] sowie eine immer größer werdende Anzahl von mit ihr verbundenen Menschenrechtsorganisationen.

8.1.4 Politische Reaktion

Die Piraten Partei[12] tritt gegen Überwachung und für die Freiheit des Wissens ein. Weltweit gibt es bereits registrierte sowie aktive, nicht registrierte Piratenparteien, weitere Gründungen sind geplant.

Die *schwedische Piratenpartei* hat bei der Wahl zum Europäischen Parlament am 7. Juni 2009 laut den vom EU-Parlament veröffentlichten Zahlen 7,1 Prozent der Stimmen geholt. Damit stellen die Piraten einen der insgesamt 18 schwedischen Abgeordneten im EU-Parlament[13].

Die *Piratenpartei Deutschlands*[14] wurde 2006 gegründet. Zur Bundestagswahl 2009 in Deutschland wurde sie erstmals offiziell in 15 Bundesländern zur Wahl zugelassen. Ein unkommentierter Vergleich des Stimmanteils bei den Wahlen ist in der Tabelle 8.1 zu finden.

Stimmanteil der Grünen bei ihrer ersten Bundestagswahl in Deutschland 1980 in Prozent	1,5
Jahre, die vergingen, bis sie erstmals in den Bundestag einzogen	3
Jahre, die vergingen, bis sie erstmals im Bund mitregierten	18
Stimmanteil der Piratenpartei bei ihrer ersten Bundestagswahl 2009 in Prozent	2,0

Tabelle 8.1: Unkommentierter Vergleich der Piratenpartei in Deutschland mit den Grünen [BRAND EINS 2009, S. 14].

8.2 Individuelle Ebene

Colin J. Bennett stellt fest, dass Strategien des Widerstands im Allgemeinen auf individueller Ebene stattfinden. Neben den „Neutralisierungstechniken" von Gary Marx (siehe Abschnitt 8.2.1) nennt er als weiteres Beispiel den

[11] http://www.privacyinternational.org/

[12] http://www.pp-international.net/

[13] http://www.chip.de/news/Europawahl-Piratenpartei-zieht-ins-Parlament-ein_36811900.html

[14] http://www.piratenpartei.de/

pensionierten Stadtrat aus Kingston, Ontario, der seine Visa-Rechnung über 230 $ in 985 Raten bezahlte, häufig in Pennies, um damit gegen die Auslagerung der Kreditkarten-Verarbeitung in die Vereinigen Staaten zu protestieren [Bennett 2008, S. 129].

Im Rahmen der Verleihung der Big Brother Awards 2009[15] wird an die Verantwortung der Menschen gegenüber sich selbst appelliert, der Datenschutz wird als *Gesellschaftsaufgabe* gesehen.

8.2.1 Neutralisierungstechniken von Gary Marx

Gary Marx präsentiert „*Eleven generic techniques of neutralization*“ [Marx 2003]. Seine sogenannten Neutralisierungstechniken nutzen die logistischen und ökonomischen Einschränkungen, Widersprüche und Lücken innerhalb von Überwachungssystemen. Marx argumentiert, dass „humans are wonderfully inventive at finding ways to beat control systems and to avoid observation“. Marx nennt elf Bewegungen, die der Einzelne anwenden kann um zu blockieren, zerstreuen, blockieren usw. um damit das Überwachungssystem zu umgehen [Marx 2003]:

> 1) discovery moves, 2) avoidance moves, 3) piggy-backing moves, 4) switching moves, 5) distorting moves, 6) blocking moves, 7) masking (identification) moves, 8) breaking moves, 9) refusal moves, 10) cooperative moves, and 11) counter-surveillance moves.

Die Kriterien reflektieren die Ansicht des Beobachters und betonen das visuelle Verhalten. Die einzelnen Kategorien schließen dabei einander nicht aus und greifen teilweise ineinander über. Die strategischen Handlungen, sowohl vom Beobachteten als auch vom Beobachter, können mit Bewegungen in einem Spiel verglichen werden. Die Beispiele stammen von Beobachtungen und Interviews von Marx.

discovery moves: Entdecken Überwachung feststellen und entdecken: Das Verhalten wird der Situation angepasst, je nachdem ob Überwachung durchgeführt wird oder nicht (Beispiel: Autofahrer bremst ab, sobald Polizei oder Radargerät in Sicht).

avoidance moves: Vermeiden Verhalten, das auf die Feststellung von Überwachung folgt. Es existiert eine zeitliche, geografische oder methodische Ersetzung zu Zeiten und Plätzen, in denen vermutet wird, dass keine Überwachung erfolgt (Beispiel: einen Supermarkt mit Kundenkarten vermeiden, Telefonieren von einem Münzfernsprecher aus).

[15] http://bigbrotherawards.at/2009/Gala

piggy-backing moves: Konfrontation Direkte Konfrontation mit Überwachung: Eine Kontrolle wird übergangen oder Information beschützt indem ein legitimiertes Subjekt oder Objekt begleitet bzw. sich daran angehängt wird (Beispiel: im Parkaus sehr eng dem vorausfahrenden Auto nähern und damit der Registrierung entgehen).

switching moves: Übertragung Übertragung von Tests, Zertifizierung und Validierung, damit ein authentisches Ergebnis jemandem oder etwas übertragen wird, zu dem es nicht gehört (Beispiel: Weitergeben einer Eintrittskarte, einer Lizenz usw., die normalerweise jemand anderer benutzt und jemand anderem gehört).

distorting moves: Manipulation Manipulation des Überwachungsprozesses, sodass zwar technisch gültige Ergebnisse erzielt werden, allerdings Testergebnisse ungültig werden (Beispiel: Ergebnisse des Lügendetektortests, indem auf einen im Schuh versteckten Reißnagel getreten wird).

blocking moves: Blockieren und Maskieren zielen ausschließlich auf kommunikative Aspekte von Überwachung ab (Beispiel: Faraday-Käfig, Taschen innen mit Aluminium oder Panzerband ausgekleidet um das Tracken mittels RFID zu verhindern, Anrufnummer-Unterdrückung usw.).

masking (identification) moves: Identitätsverschleierung Maskieren schließt das eben genannte Blockieren mit ein, allerdings geht Maskieren noch darüberhinaus, indem Identität, Status und/oder Ort und Erreichbarkeit des zu überwachbaren Subjekts/Objekts verschleiert werden (Beispiel: Entfernung der Seriennummern, Tragen von Handschuhen). Der Unterschied zu Blockieren ist, dass das verschleierte Objekt von falschen Schein-Objekten ersetzt wird (falsche Seriennummer) um die Verschleierung nicht erkennbar zu machen (Beispiel: Name auf Kundenkarten falsch angeben).

breaking moves: Zerstören von Überwachungsgeräten Überwachungsgeräte sollen funktionsunfähig gemacht werden, da das vorhin genannte Blockieren mit hoher Wahrscheinlichkeit entdeckt wird (Beispiele: Videomonitore mit Farbe besprühen).

refusal moves: Nein-Sagen Das „just say no“ von Gary Marx meint dabei die Überwachung zu ignorieren. Dieses Verhalten soll zeigen, dass der Überwachungsgewalt keine Achtung gezollt wird und keine Rücksicht darauf genommen wird (Beispiele: Wenn die Telefonnummer verlangt wird, antworten, dass „keines in Besitz ist“, Sozialversicherungsnummer nicht einfach so bekanntgeben auf Verlangen).

cooperative moves: Gemeinsame Sache Machen Um Überwachung umgehen zu können, kann es notwendig sein, gemeinsame Sache zu machen mit den Überwachern (Beispiel: Der persönlich gut befreundete Polizeichef löscht einen Dateneintrag seines Sohns über Trunkenheit am Steuer).

counter-surveillance moves: Entgegentreten Das ist vor allem ein Appell an die Überwacher selbst. Jene, die Überwachungssysteme kontrollieren, sollten dazu gezwungen werden, all jenen, die beobachtet werden, wieder die Ruhe zurückzugeben.

8.2.2 Social Engineering

Peter Purgathofer stellt fest, dass mittels *Social Engineering* (gekonnte zwischenmenschliche Beeinflussung) das System der Passkontrolle[16] überlistet werden konnte [Gaycken und Kurz 2008, S. 203]. Wie könnte diese Art der Beeinflussung mittels Social Engineering heute aussehen, wäre dies im digitalen Zeitalter noch möglich?

8.2.3 Tarnanzug

> Was wäre, wenn die Spuren unserer urbanen Präsenz in Grenzbereiche der Aufmerksamkeit entschwinden? Was wäre, wenn man Unsichtbarwerden als soziale Handlungsstrategie propagiert, die es gilt einzuüben und zu praktizieren? Was wäre, wenn wir den Überwachungsmanien Kulturtechniken entgegensetzen, mit denen wir uns an unsere Umgebung so konsequent adaptieren und darin integrieren, dass wir unbemerkt beobachten, handeln und kommunizieren können?[17]

Das Projekt „macghillie – just a void“ ist ein Projekt, das in Grenzbereichen urbaner Wahrnehmung das Phänomen der gleichzeitigen Sichtbarkeit/Unsichtbarkeit/Nichtsichtbarkeit untersucht. Die Figur trägt einen Tarnanzug (Ghillie Suit) und durchquert die Stadt, tagelang (siehe Abb. 8.1).

Bei der ersten Betrachtung des Projekts – insbesondere der Fotos[18] – werden damit das Hinwegsetzen über die Möglichkeit des Identifiziert-Werdens als Mensch deutlich und ein Weg gezeigt, sich der Überwachung zu entziehen. Die detaillierte Projektinformation allerdings zeigt, dass es um das Wesen des *macghillie* geht: distanziert, sinnlos, niemand will ihn sehen.... usw. Das Projekt würde sich allerdings gleichermaßen dazu eignen Überwachung „vorzuführen“ und damit ad absurdum zu führen.

[16] System der Sklavenpässe zur Feststellung der Identität von Sklaven
[17] http://macghillie.krcf.org/category/info
[18] http://macghillie.krcf.org/category/aussen

Abbildung 8.1: Ein Stadtspaziergang mit Tarnanzug.

8.2.4 Brillen mit Infrarot-LEDs

Eine Idee, die im Web kursiert, ist, Brillen mit Infrarot-LEDs[19] auszustatten. Vorausgesetzt die Überwachungskamera hat keine Infrarot-Sensoren, erscheint statt des Gesichts ein leuchtender Punkt. Die Infrarot-LEDs überstrahlen die Konturen des Gesichts und machen damit Gesichtserkennung undurchführbar. Technisch wird diese Idee allerdings intensiv diskutiert, unter anderem auf *Boing Boing Gadgets*[20].

8.2.5 Hoodies

Mit Hoodies (aus dem Englischen: Kapuzenpullover), dessen Kapuzen seitlich mit Gesichtern bedruckt sind, kann Videoüberwachung überlistet werden, da Gesichtsmerkmale zwar erkannt werden, es sich dabei allerdings um einen Aufdruck handelt (siehe Abb. 8.2)[21]. Head Hoods aus New York bietet solche mit Gesichtern bedruckte Hoodies in einer großen Auswahl an, von Mozart über Michael Jackson bis hin zu Barack Obamas Aufdruck auf der Kapuze.

Hoodies sind den englischen Sicherheitsbeamten oder besser den CCTV-Überwachern ein Dorn im Auge. Aus diesem Grund wurde beispielsweise im

[19] Light Emitting Diodes
[20] http://gadgets.boingboing.net/2008/06/27/diy-anticctv-glasses.html
[21] http://www.headhoods.com

Abbildung 8.2: Hoodie (Kapuzenpullover) mit seitlichem Gesichtsaufdruck. Bild von Boing Boing Gadgets.

Bluewater Shoppingcenter (größtes Shoppingzentrum Europas südlich von London) das Tragen von Kopfbedeckungen, darunter auch Hoodies, verboten[22].

8.2.6 Digitale Rebellion

Die wachsende Verfügbarkeit von Daten und die Veröffentlichung von Millionen von Daten: Die Konsequenzen dessen sind weder in der täglichen Praxis noch in der Gesetzgebung oder Politik bekannt [Stocker und Schöpf 2007, Stocker, Schöpf, S. 13]. Erforderlich wird ein juristisches Problembewusstsein und eine gesellschaftliche Bewertung von Privatsphäre unter den neuen Bedingungen. Gerfried Stocker und Christine Schöpf sprechen von „der (unfreiwilligen) digitalen Transparenz und (freiwilligen) Veräußerung von Privatheit“ [Stocker und Schöpf 2007, S. 13].

Ina Zwerger und Armin Medosch sehen nicht nur die Gefahr der Reduzierung von menschlichen Beziehungen auf die Ebene von technischen Schaltungen. Sie sehen auch so etwas wie ein *Diktat des Verbundenseins* entstehen. Kreativer Widerstand könnte sich ihrer Meinung nach in Form von Privacy-Architekturen auf der Basis von Open-Source-Software und offenen Standards etablieren. Sie sehen als besten Weg, Öffentlichkeiten zu schaffen

[22] Artikel ZEIT ONLINE vom 16. 1. 2007, http://www.zeit.de/2007/03/Big-Brother

und zu fördern, die „common“ sind und aus Commons bestehen. Diese zivilgesellschaftlichen Öffentlichkeiten, die der Multitude gehören, ermöglichen es, Handlungsfreiräume zu erhalten oder wiederzugewinnen und ein lautstarkes öffentliches Leben zu führen [Stocker und Schöpf 2007, Zwerger, Medosch, S. 25].

Overview – Ein Gruppenbild von oben

Im Rahmen des Ars Electronica Festivals 2007 wurde ein Gruppenbild von oben erstellt. Dabei handelte es sich um die gewissermaßen inverse Inszenierung eines an sich längst gängigen Beobachtungs- oder Kontrollszenariums, in dem jedoch das Beobachtet-Werden durch die aktive Rolle der Beobachteten ad absurdum geführt wird: Jeder ist aufgerufen, im zeitlichen Raster eines hochauflösenden Luftbild-Scans der Stadt Zeichen der Wahrnehmung dieses Vorgangs in den Stadtraum zu setzen und damit eine eigene Botschaft gen Himmel zu senden [Stocker und Schöpf 2007, S. 202ff].

8.3 Zusammenfassung

Die Möglichkeiten, sich über *Privatsphäre* zu informieren sind vielfältig, bedürfen aber persönlicher Initiative. Das Kapitel hat verdeutlich, dass niemand sich der alltagsdurchdringenden Überwachung widerstandslos hingeben muss und dass der Einzelne nicht alleine ist. Informationen der kritischen Gesellschaften, Aufmerksamkeit gegenüber der täglichen Meldungen in den Medien zu Verstößen gegen *Privatsphäre* helfen dabei, das Bewusstsein zu schärfen. Mit kleinen Handlungen kann jeder Einzelne bis zu einem gewissen Grad der totalen Überwachung entgegenwirken.

Kapitel 9

Schlussbemerkungen

> Six isolated people live in their apartments, side by side, oblivious to each other and the violent process of deterioration happening to them, their apartments, and the earth. (...)
>
> In their passivity and isolation, the inhabitants emerge as the true form of death, while the rooms they inhabit maintain the ongoing transformation of life. The potential of life, then, exists only in the process of death. Eventually all forms of life are consumed by new life. The implacability of decay results in an explosion of life. (...) [*Six Apartments*, 2007, Reynold Reynolds]

Der Film *Six Apartments*[1] (2007) von Reynold Reynolds wird getragen von einer Stimmung der Hoffnungslosigkeit, der Melancholie. Die Bewohner erfahren nie, was der Betrachter sieht, nämlich, dass im Tod eine große Aktivität von Leben steckt. Man wundert sich, ob das wohl ein positives Zeichen für den Planten sein könnte. Die Situation erinnert an die Ohnmacht der Bevölkerung gegenüber der allgegenwärtigen und unterschiedlichsten, vielfältigen Datensammlung und Überwachung.

Wie kann man *Immunität* wahren in einer Gesellschaft, in einem Staat angesichts einer Autorität, in der die umgekehrte Unschuldsvermutung als alleinige Wahrheit und Wahrhaftigkeit gesehen wird? Besteht eine Möglichkeit in Form akademischer Immunität, mit der Freiheit offiziell als Forscher sich ab der Norm verhalten zu dürfen (was die Vorraussetzung wäre für die Weiterentwicklung, die Freiheit und Autonomie eines jeden Menschen)? Ist eine weitere Möglichkeit der Beruf als Privacy-Anwalt? Nur, auf welche Seite stellt sich dieser um immun zu sein? Somit dürfte diese Alternative weniger in Frage kommen, da die Fronten klar sind.

Sind Social Tools der Ausweg, ein Fluchtwinkel? Im Moment überwiegt die kritische Sicht auf Social Tools, wohl weil Kritik scheinbar von jenen Menschen gemacht wird, denen der Einblick und das Verständnis für dieses

[1] http://reynold-reynolds.com/six/index.htm

völlig neue Leben fehlt. Sie glauben vielleicht immer noch, dass irgendwann alles wieder so wird, wie es war. Gezeigt wird das auch an den fehlenden Medientheorien, die die positive Seite beleuchten.

Die Gesetze für *Privatsphäre* zu stärken alleine reicht nicht als Gegenmittel zu Überwachung. Als erster Schritt sollte jedem Einzelnen das Recht eingeräumt werden, die auf sich bezogenen Informationen zu kontrollieren. Doch vor allem die aufgezeigten Beispiele aus der Realität zeigen ein trauriges Bild, nämlich dass scheinbar die Datensammelwut und Überwachung immer umfangreicher werden und inzwischen im Alltag zur Normalität gehören. Deutlich wurde auch, wie groß die Ungewissheit über die Verwendung der Daten ist. Im Gegensatz zu George Orwells 1984 ist nicht die Tatsache des Beobachtet-Werdens die Gefahr, sondern das Nicht-Wissen, was mit den Daten passiert, und die Unkenntnis jener Prozesse, die im Verborgenen liegen. Im Kapitel 8 wurden Möglichkeiten der Gegenwehr und der Schärfung des Bewusstseins gegenüber *Privatsphäre* gezeigt. So liegt aktuell die Bringschuld immer noch beim Datensubjekt – also jedem Einzelnen – selbst.

Literaturverzeichnis

[Agre 1999] Agre, Phil (1999). *Department of Information Studies*. http://polaris.gseis.ucla.edu/pagre/notes/99-12-26.html.

[Bennett 2008] Bennett, Colin J. (2008). *The Privacy Advocates: Resisting the Spread of Surveillance*. The MIT Press.

[Bennett und Lyon 2008] Bennett, Colin J. und D. Lyon (2008). *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. Routledge.

[Davis 1990] Davis, Mike (1990). *City of Quartz: Excavating the Future in Los Angeles*. Verso.

[brand eins 2009] eins brand (2009). *Wirtschaftsmagazin Ausgabe 11*. http://www.brandeins.de/.

[Franck 1998] Franck, Georg (1998). *The Economy of Attention*. Viking Penguin, New York.

[Gaillard 2009] Gaillard, Michel, Hrsg. (2009). *Je te vois!*. SA Les Editions Maréchal – Le Canard Enchaîné. http://www.lecanardenchaine.fr/.

[Gaycken und Kurz 2008] Gaycken, Sandro und C. Kurz, Hrsg. (2008). *1984. exe*. transcript Verlag.

[Goldhaber 1997] Goldhaber, Michael H. (1997). *The Attention Economy and the Net*. First Monday, 2(4).

[Hellige 2004] Hellige, Hans Dieter, Hrsg. (2004). *Geschichten der Informatik: Visionen, Paradigmen, Leitmotive*. Springer-Verlag.

[Kloock und Spahr 2000] Kloock, Daniela und A. Spahr, Hrsg. (2000). *Medientheorien: Eine Einführung*. Wilhelm Fink Verlag München.

[Lyon 1994] Lyon, David (1994). *The Electronic Eye: The Rise of Surveillance Society*. University of Minnesota Press, Minneapolis, MN, USA.

[Lyon 2001] Lyon, David (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

[Lyon 2003a] Lyon, David (2003a). *Surveillance after September 11th*. Cambridge: Polity Press.

[Lyon 2003b] Lyon, David, Hrsg. (2003b). *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. Routledge.

[Lyon 2006] Lyon, David (2006). *Security, Seduction and Social Sorting: Urban Surveillance*. In: Bansal, Lipika, P. Keller und G. Lovink, Hrsg.: *In the Shade of the Commons: Towards a Culture of Open Networks*, Kap. 2, S. 30–42. Impress, New Delhi.

[Lyon 2007] Lyon, David (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press.

[Marx 2003] Marx, Gary (2003). *A Tack in the Shoe: Resisting and Neutralizing the New Surveillance*. Journal of Social Issues, 59(2):369–390. http://web.mit.edu/gtmarx/www/tack.html.

[Moffat 1992] Moffat, Susan (1992). *Plan for DNA Database Assailed*. Los Angeles Times.

[Ogburn 1969] Ogburn, William (1969). *Kultur und sozialer Wandel*. Luchterhand.

[Parenti 2003] Parenti, Christian (2003). *The Soft Cage: Surveillance in America – From Slavery to the War on Terror*. Basic Books.

[Phillips 2002] Phillips, David J. (2002). *Negotiating the Digital Closet: Online Pseudonyms and the Politics of Sexual Identity*. Information, Communication and Society, 5(3):406–424.

[Phillips 2005] Phillips, David J. (2005). *From Privacy to Visibility: Context, Identity, and Power in Ubiquitous Computing Environments.*. Social Text, 23(2):95–108.

[Prosser 1960] Prosser, William L. (1960). *Privacy and Freedom*. California Law Review, 48:383, 389.

[Raab 1992] Raab, Selwyn (1992). *Plan for DNA Database Assailed*. New York Times.

[Rheingold 1991] Rheingold, Howard (1991). *Virtual Reality: The Revolutionary Technology of Computer-Generated Artificial Worlds – and How It Promises to Transform Society*. Touchstone.

[Robin 2009] Robin, Harry (2009). *The Scientific Image: From Cave to Computer*. W. H. Freeman and Company, Publishers.

[Rosen 2002] Rosen, Jeffery (2002). *Total Information Awareness*. New York Times Magazine: The Year in Ideas.

[Rossnagel 2005] Rossnagel, Alexander (2005). *Das rechtliche Konzept der Selbstbestimmung in der mobilen Gesellschaft*. In: *Mobilität – Telematik – Recht*, S. 53–75. Taeger, Jürgen and Wiebe, Andreas.

[Rössler 2001] Rössler, Beate (2001). *Der Wert des Privaten*. Suhrkamp Verlag.

[Rötzer 1998] Rötzer, Florian (1998). *Digitale Weltentwürfe. Streifzüge durch die Netzkultur.*. Carl Hanser.

[Schnabel 2007] Schnabel, Christoph (2007). *Das „Mikado-Prinzip“*. Datenschutz und Datensicherheit (DuD), 6:426–430.

[Sfar 2006] Sfar, Joann (2006). *La Vallée des Merveilles*. Dargaud.

[Shirky 2008] Shirky, Clay (2008). *Here Comes Everybody: The Power of Organizing without Organizations*. Penguin Books Ltd.

[Simanowski 2008] Simanowski, Roberto (2008). *Digitale Medien in der Erlebnisgesellschaft: Kultur – Kunst – Utopien*. Rowohlt Verlag GmbH.

[Solove 2004] Solove, Daniel J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. NYU Press.

[Solove 2008] Solove, Daniel J. (2008). *Understanding Privacy*. Harvard University Press.

[Solove und Schwartz 2008a] Solove, Daniel J. und P. M. Schwartz (2008a). *Privacy and the Media*. Aspen Publishers.

[Solove und Schwartz 2008b] Solove, Daniel J. und P. M. Schwartz (2008b). *Privacy, Information and Technology*. Aspen Publishers.

[Spinner 1994] Spinner, Helmut F. (1994). *Die Wissensordnung. Ein Leitkonzept für die dritte Grundordnung des Informationszeitalters*. Leske + Budrich.

[Stocker und Schöpf 2007] Stocker, Gerfried und C. Schöpf, Hrsg. (2007). *Ars Electronica 2007: Goodbye Privacy*. Hatje Cantz Verlag.

[Stocker und Schöpf 2008] Stocker, Gerfried und C. Schöpf, Hrsg. (2008). *Ars Electronica 2008: A New Cultural Economy – The Limits of Intellectual Property*. Hatje Cantz Verlag.

[Verne 2000] Verne, Jules (2000). *La tour du monde en 80 jours*. Librairie Générale Française.

[Warren und Brandeis 1890] Warren, Samuel D. und L. D. Brandeis (1890). *The Right to Privacy*. Harward Law Review, 4:193–220.

[Williams 1992] Williams, Raymond (1992). *Television, Technology and Cultural Form*. Routledge.