universität wien

MAGISTERARBEIT

Titel der Magisterarbeit

Die Preisgabe sensibler Daten im Internet

Möglichkeiten einer Überwachung und ihrer Gefahren

Verfasser

Daniel Rudlstorfer Bakk. phil.

Angestrebter akademischer Grad

Magister der Philosophie (Mag. phil.)

Wien, im April 2010

Studienkennzahl lt. Studienblatt:	A 066 841
Studienrichtung lt. Studienblatt:	Publizistik- und Kommunikationswissenschaft
Betreuer:	Univ.-Prof. Dr. Hannes Haas

Danksagung

Vielen Dank an meine Diplomarbeitsbetreuer Hannes Haas und Herbert Hrachovec. Es gab eine Zeit an der Universität, in der den StudentInnen nicht immer gewährleistet werden konnte, wissenschaftliche Aufsicht und Fürsorge zu erhalten. Umso mehr freue ich mich, dass ich in beiden Instituten, an denen ich einreichen will, keine Probleme hatte, Betreuung zu finden. Ich bedanke mich dafür, dass die beiden Professoren mich, ganz im Sinne dieser Arbeit, nicht ständig kontrollierten bzw. überwachten, sondern sehr frei walten ließen, was mir neben einigen Anstrengungen auch unglaublichen Spaß bereitete, was in der vorliegenden Arbeit hoffentlich auch zum Ausdruck kommen sollte.

Ich bedanke mich auch bei meinen VordenkerInnen, von denen ich nicht zu wenige zitiert habe, die mir ein Fundament lieferten, auf das ich „nur“ noch aufzubauen hatte und die mir einen erheblichen Teil meiner Denkarbeit abnahmen. Martin Heidegger meinte, denken sei zugleich danken. Schon im Wort *Gedanke* steckt die vergeltende, wohlwollende Anerkennung.

Ich bedanke mich für die interessanten Gespräche mit meinen InterviewpartnerInnen, die sich für mich und mein Anliegen Zeit nahmen, was auf keinen Fall selbstverständlich ist, wenn ich einige Absagen bedenke.

Ich bedanke mich auch bei meinen Nerven, die standhielten, wenn ich manchmal dieses institutionell vorgeschriebene, standardisierte, individueller Kreativität kaum Platz lassende Werk verfluchte und wenn der äußere, sowie der selbst auferlegte Druck vor allem zum Ende hin größer wurde.

Oh oh. Der größte Dank gilt natürlich meiner Familie, besonders meinen Eltern und ihrer stetigen Unterstützung während des Studiums. Ohne sie hätte ich es in dieser Form nicht geschafft. Außerdem hätte nicht zumindest ein Elternteil eine akademische Ausbildung, wer weiß, ob ich mich für diesen Kurs entscheiden hätte können. Wie bekannt, prägt in Österreich das Bildungsniveau der Eltern den Bildungsweg der Kinder besonders stark.

Danke meiner Schwester Laura für das Engagement beim Übersetzen ins Englische.

Danke meinem Freund Berni für die Hilfe beim Formatieren der Arbeit.

Danke meiner geliebten Freundin Christina für die Arbeitsteilung beim Transkribieren und viele liebe Aufmunterungen.

Ich bedanke mich bei hunderttausenden LeserInnen.

Danke an die Universität Wien für viele schöne Jahre. Der Wissensdurst war im Verlauf meines Studiums nicht gestillt, sondern erst entfacht.

Eidesstattliche Erklärung

Hiermit versichere ich, dass ich die Magisterarbeit eigenständig und ohne fremde Hilfe verfasst und keine anderen als die angeführten Quellen und Hilfsmittel verwendet habe.

Des Weiteren versichere ich, dass die vorliegende Magisterarbeit weder im Inland noch im Ausland von mir oder anderen zur Erlangung eines Leistungsnachweises vorgelegt wurde.

Wien, im April 2010 Rudlstorfer Daniel

INHALTSVERZEICHNIS

1. Einleitung und Problemstellung

Die folgenreiche Ausrufung des Begriffs *Web 2.0* durch Tim O'Reilly Mitte der 2000er Jahre machte dieses Thema unglaublich populär. Eine Aufbruchsstimmung herrschte im Netz, Online-Firmen schossen wie Pilze aus dem Boden, kaum eine Tageszeitung kam seitdem noch ohne Internet-Teil oder einer Net-Seite aus, wo über digitale Möglichkeiten, Unternehmen, Erfolgsgeschichten, Gefahren usw. berichtet wird. Unweigerlich hat die Verlagerung Teile unseres sozialen Lebens und Handelns in den virtuellen Raum erhebliche Konsequenzen für die Gesellschaft. So heißt es auch im bekannten *Youtube*-Video *Web 2.0 ... The Machine is Us/ing Us* von Michael Wesch, das es auf über beachtliche 10 Millionen Views bringt: „We'll need to rethink a few things. We'll need to rethink copyright, authorship, identity, ethics, aesthetics, rhetorics, governance, privacy, commerce, love, family, ourselves." Das Internet birgt immense Möglichkeiten für das Zusammenleben, besitzt ein unglaubliches Potential an Informationsverarbeitung und -bereitstellung und Wissensgenerierung, vergleichbar mit einer neurophysiologischen Datenautobahn. So hat dieses Thema auch mich in seinen Bann gezogen. Es besitzt aber auch einige Risiken, die bei allem Optimismus nicht außer Acht gelassen werden sollten. Ein Punkt dabei ist der der Privatsphäre, den ich genauer unter die Lupe nehmen möchte. Oftmals wurde letztlich in Medien berichtet, durch den Boom der Social Networks sei die Privatsphäre in Gefahr (zu entschwinden). Die UserInnen führen einen unerotischen Datenstriptease vor, der seinem Publikum jedoch geradezu den Anreiz bietet, die Daten zu verfremden und zu missbrauchen. Das am öftesten vernommene Beispiel war das der ArbeitgeberInnen, die Profile von BewerberInnen in Social Networks auf berufshinderliche Preisgaben durchsuchen. Die Frage, die sich mir daraufhin aufdrängte war, ob es bei diesem Beispiel bleibt, ob das die einzige Gefahr an Social Networks und anderen Web 2.0-Plattformen ist. Wer kann solche Daten zu seinem Vorteil verwenden und zum Nachteil der Betroffenen? Wer kann sie nützen, wer davon profitieren? Da die Verwendung der Daten über eine bloße Beobachtung hinausgeht und ausschlaggebend für künftige Ereignisse rund um die Betroffenen sein kann, ist meiner Meinung nach das Wort *Überwachung* angebracht, wobei der englische Begriff *dataveillance*, übersetzt als *Datenüberwachung* noch besser zutreffen würde. Und darum soll es in der vorliegenden Arbeit schließlich gehen: Um eine sachliche Erörterung der Gefahren, die von einer Datenüberwachung der freiwillig preisgegebenen Daten ausgehen. Für eine umfassende, sich des Problems annehmende Argumentation bedarf es noch weiterer Fokussierungen. Wie ist es um die Privatsphäre bestellt? Warum geben wir sie

freiwillig auf? Wie wird sie von unserem Recht geschützt? Welche gesellschaftlichen Veränderungen bringt Überwachung? Was sind überhaupt ihre Vorbedingungen? Auf welcher Grundlage gedeiht sie? Mit welchen technischen Hilfsmitteln lässt sie sich am besten umsetzen? Und welche Vorteile muss sie zwangläufig auch haben, um sich eigentlich erst zu etablieren? All diese Fragen sollen in den folgenden Kapiteln diskutiert und beantwortet werden.

1.1 Erkenntnisinteresse und Zielsetzung

In dieser Arbeit soll das Themenfeld Überwachung genau analysiert werden. Verschiedene Perspektiven sollen eingenommen werden, dabei steht vor allem der gesellschaftliche Zusammenhang im Brennpunkt des Interesses. Wie wirkt also Überwachung in unserer Gesellschaft, lässt sich gar, wie es manche tun, von einer Überwachungsgesellschaft sprechen? Bezüglich der individuellen, kollektiven und gesellschaftlichen Vorteile und Gefahren, die eine Überwachung dann zu bieten hat, interessieren mich die Daten, die wir freiwillig veröffentlichen. Wird beispielsweise jemand von Sicherheitsbehörden als gefährlich oder verdächtig eingestuft und wird deswegen observiert, so ist dies nicht Thema der Arbeit. Dagegen will ich herausfinden, was die Daten, die wir beispielsweise in Social Networks preisgeben, in Foren schreiben, auf Foto- oder Video-Plattformen stellen, in Suchleisten tippen, an Überwachung ermöglichen.
Prägnant formuliert drückt sich das in folgender forschungsleitender Hauptfragestellung aus:

Lassen die Daten, die wir freiwillig im Internet hinterlassen, spezifischere Formen von Überwachung zu?

Um dieser Frage nachgehen zu können, müssen einige Prämissen und Vorbedingungen geklärt sein. Die Begriffe sind zu definieren, rechtliche Aspekte einzubringen, Motive zu hinterfragen, die Privatsphäre zu durchleuchten.
Den Rahmen dabei, an dem sich die Argumentation und Erörterung entlang hanteln, bilden die folgenden, spezielleren Forschungsfragen:

FF 1: Wie entsteht die Menge an Daten im Internet über uns?

FF 2: Was geschieht mit den persönlichen Daten im Web?

FF 3: Wird durch die Preisgabe unserer Daten Überwachung ermöglicht?

FF 4: Was sind die Vorteile, Nachteile und Gefahren einer solchen Überwachung?

Diese vier spezielleren Forschungsfragen, dienen wie gesagt dazu, leichter einem roten Faden, der sich durch die Arbeit ziehen soll, folgen zu können. Sie werden aber in Hinblick auf die empirische Untersuchung noch zu konkretisieren und mit Forschungshypothesen zu ergänzen sein.

Um einer der Wirklichkeit entsprechenden, zumindest stimmigen und sinnvollen Beantwortung meiner Forschungsfragen näher zu rücken, will ich auch die Erfahrung von ExpertInnen einbringen, die aufgrund ihrer beruflichen Situation entsprechendes Wissen mit mir zu teilen vermögen. Eine qualitative Befragung in Form von ExpertInneninterviews soll mir helfen, Indikatoren abzuleiten, die bestimmen, wie sich die freiwillige Preisgabe von Daten zu ihren Überwachungsmöglichkeiten verhält.

1.2 Aufbau der Arbeit

Im zweiten Großkapitel der Arbeit, den *theoretischen und rechtlichen Grundlagen* geht es um die Dimensionen *Daten* und *Privatsphäre*. Die beiden Begriffe werden definiert, rechtlich eingegrenzt, ideell wertgeschätzt und historisch betrachtet. Mit konkreten Fallbeispielen wird schließlich die Hypothese untermauert, dass wir schützenswerte Daten freiwillig veröffentlichen, um im weiteren Vorgehen die Motive der Selbstdarstellung im Web 2.0 sowie die Motive hinter Datensammlungen zu hinterfragen und dem digitalen Fußabdruck auf den Grund zu gehen.

Der dritte Teil verschreibt sich voll und ganz der Dimension der *Überwachung*. Diese wird im Sinne der nachfolgenden Inhalte definiert, woraufhin geprüft wird, inwieweit unsere Gesellschaft mit Überwachungsgesellschaft tituliert werden kann. Ein umfangreiches Kapitel beschäftigt sich mit Foucault und dem von ihm eingeführten Begriff des Panoptismus, der Überwachungs- und Kontrollmechanismen in westlichen Gesellschaften

beschreibt. Da Überwachung eng an Technik gekoppelt ist, spielt im Weiteren die Überwachung als Technologie eine Rolle, ebenso wie ihre mediale und technische Umsetzung. Es folgen Darstellungen und Motive der staatlichen sowie der wirtschaftlichen Überwachung, woraufhin die Vorteile und die Gefahren einer Überwachung, vor allem in gesellschaftlichem Sinne, nochmals angeführt und Lösungsansätze angedeutet werden.

Der vierte Teil der Arbeit steht ganz im Zeichen der empirischen Untersuchung. Zuerst werden das Forschungsinteresse und damit die Forschungsfragen und Hypothesen konkretisiert, um danach allgemein die methodische Vorgehensweise bei ExpertInneninterviews zu beschreiben. Im Anschluss werden die konkrete Durchführung der Datenerhebung, ihrer Aufbereitung und die Auswertungsmethode Schritt für Schritt angeführt. Gegen Ende werden die Interviews nach einem bestimmten Schema ausgewertet, um die Ergebnisse zu interpretieren und die Forschungsfragen sowie die Hypothesen hinsichtlich der Überwachungsmöglichkeiten freiwillig veröffentlichter Daten beantworten bzw. bewerten zu können.

2. Theoretische und rechtliche Grundlagen

2.1 Daten

2.1.1 Personenbezogene Daten

Daten werden aus verschiedenen „Zeichen eines Zeichenvorrats nach definierten Syntaxregeln gebildet“ (Bodendorf 2006: 1). Ein solcher Vorrat kann zum Beispiel das Alphabet oder ein Zahlensystem sein. Daten werden erst dann zu Informationen, wenn sie in einen Kontext einbezogen werden, ihnen also eine semantische Bedeutung zugeordnet wird. Werden mehrere Informationen pragmatisch verknüpft bzw. in ihrem Zusammenhang sinnvoll vernetzt, so kann Wissen entstehen.
Ein Beispiel wäre das Datenelement 100, das aus den Zeichen 1 und 0 mittels Syntax gebildet wird. Zu einer Information wird diese Zahl erst, wenn man sie in einen Kontext setzt, zum Beispiel 100° (Grad) als Temperatur. Vernetzt man mehrere Informationen sinnvoll, so weiß man, dass 100° heißes Wasser zu Verbrühungen führen kann, diese Temperatur in der Sauna aber (gerade noch) erträglich ist.
Daten, Informationen und Wissen sind ein Kontinuum und schwierig zu unterscheiden. Eher lassen sie sich über die beiden Pole Daten und Wissen beschreiben. Daten sind Einzelsymbole, strukturiert, isoliert, kontextunabhängig und haben eine geringe Verhaltenssteuerung, während Wissen als kognitive Handlungsmuster zu verstehen ist, die unstrukturiert, vernetzt, kontextabhängig sind und eine starke Verhaltenssteuerung implizieren. (vgl. ebd.: 2)

Das Wort *dare* ist lateinisch und bedeutet *geben*. Etymologisch war das Wort *Datum* einst etwas Gegebenes im Zusammenhang mit Schriften. Wird einer Schrift der Ausstellungstag hinzugefügt, wird es ein *Datum*, ein Dokument, eine Urkunde oder ein Zeugnis. „Der Kern des Datenmachens besteht darin, etwas Flüchtiges zu fixieren.“ (Rammert 2007: 20)
Heutzutage bezeichnen Daten Informationen, die einem/r MerkmalsträgerIn zuordenbar sind. Ein Individuum hat somit Passdaten, eine Organisation beispielsweise Personaldaten. Sie sind nicht gegeben, sie werden gemacht und stehen in einem bestimmten Deutungs- und Verwendungskontext. „Daten haben ohne Deutung keine Bedeutung.“ (ebd.: 26) Grundsätzlich sollen diese fixierten Informationen einen Nutzen, nämlich Kontrolle mit sich

bringen. Das Verhalten von Menschen, Dingen und Ereignissen soll mit ihrer Hilfe beobachtbar und beeinflussbar gemacht werden. (vgl. ebd.: 19f.)

Rammert stellt hier einen teleologischen Nutzen von Daten dar, der bereits unweigerlich zu den implizit konträren Begriffen der Überwachung und Kontrolle hinführt. Auch der rechtliche Ansatz zeigt, dass Daten etwas Schützenswertes sind, weshalb sich ein ganzes Bundesgesetz sowie eine Richtlinie der Europäischen Gemeinschaft auf sie beziehen.

So heißt es in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, in Artikel 2 (a):

> Im Sinne dieser Richtlinie bezeichnet der Ausdruck ‚personenbezogene Daten' alle Informationen über eine bestimmte oder bestimmbare natürliche Person (‚betroffene Person'); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;
> (Art. 2 (a) der Richtlinie 95/46/EG)

Umgesetzt ist diese Richtlinie im österreichischen Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000) §4 Zeile 1 Daten. Hier sind speziell personenbezogene Daten „Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist" (DSG 2000, §4 Z 1), wobei als Betroffene sowohl natürliche, wie auch juristische Personen und Personengemeinschaften gelten (vgl. DSG 2000, §4 Z 3).

Zu bedenken ist, dass Daten, die in einem bestimmten Zusammenhang als belanglos erscheinen, in einem anderen heikle Angelegenheiten betreffen und Persönlichkeitsrechte überschreiten können. Beispielsweise ist das Geschlecht eines Transsexuellen stets schützenswert, wie auch die Adresse eines adoptierten Kindes oder die eines Gerichtszeugens. Das heißt schließlich, dass „freie" Daten, die nicht schützenswert sind und sich einfach ohne Datenschutzregeln verwenden lassen, in dieser Form gar nicht existieren. (vgl. Schaar 2007: 102)

2.1.2 Sensible Daten

So definiert das Recht weiters „sensible Daten“ als „besonders schutzwürdige“. Gemeint sind „Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben“ (§4 Z 2).

Der Begriff der Sensibilität von Daten geht über den der Intimität hinaus. Intimität ist eine Form von Privatheit und hat eine eher erotische oder sexuelle Konnotation. Denn sie spricht eher eine Entblößung des Körpers an und hat mit Nähe und Verletzlichkeit zu tun. (vgl. Rössler 2001: 17) Das Feld der sensiblen Daten umfasst wie gerade gezeigt aber mehr, wie beispielsweise auch Gesundheit und politische Einstellungen.

2.1.3 Datenbanken

In der Praxis werden Daten oftmals in einer Datenbank aufbereitet. Im Wissensmanagement ist eine solche „eine einheitlich beschriebene Darstellung eines Weltausschnitts durch diskrete Daten auf externen und persistenten Speichermedien (z.B. Festplatten).“ (Bodendorf 2006: 7) Datenbanksysteme haben den Vorteil, dass man sie Daten übergreifend nutzen kann. Verschiedene Anwendungen können also auf dieselbe Datenhaltung zugreifen. Dies geschieht über definierte und standardisierte Schnittstellen. (vgl. ebd.)

2.1.4 Datenverarbeitung aus historischer Perspektive

Bereits in der Bibel wird von der ersten Volksschätzung der Geschichte gesprochen (vgl. Lukas 2, 1-3, Luther-Übersetzung), nichtsdestotrotz war es vor dem 18. Jahrhundert, also in vorindustriellen Gesellschaften unnotwendig, irgendwelche Daten des Volkes zu erheben. Mündliche Überlieferung, Praxis bezogene Vorführungen und Handschläge reichten für die Übertragung des Wissens und für die Abwicklung von Geschäften. Eine Dokumentation von persönlichen Verhältnissen beschränkte sich auf die herrschende Elite.
Allerdings gab es seit dem Spätmittelalter Ausnahmen wie auch die verschärften Zustände in der verpesteten Stadt zeigen: Italienische Stadtrepubliken begannen im 15. Jahrhundert

über Reisende, BettlerInnen und SoldatInnen Buch zu führen und sie mit individuellen Begleitbriefen, Passierscheinen usf.[1] auszustatten, um Nomadentum und Migration zu kontrollieren. (vgl. Purgathofer 2008: 197) Verbannte und Verurteilte wurden namentlich notiert. Eine Präzisierung forderte dann das Zeitalter der Inquisition. Umfangreiche Listen von Personen, die der Ketzerei verdächtig waren, wurden erstellt.

In den Zeiten der industriellen Revolution reichte die vertrauliche direkte Weitergabe von Informationen innerhalb personaler Beziehungen nicht mehr aus. Man hatte mehr flüchtige Kontakte, auf Märkten hatte man mit anonymen Menschen zu tun. Die Abnahme der personalen Wirtschaftsbeziehungen und die dadurch entstehende Unübersichtlichkeit führten zu einem Vertrauensverlust gegenüber den HandelspartnerInnen und forderten damit einen neuartigen Umgang mit Informationen. Der ermöglicht das Planen und Handeln der Individuen trotz Anonymität und bildet so eine wichtige Voraussetzung für moderne Gesellschaften.

Die Art und Weise der industriellen Produktion duldete nicht länger eine mündliche Überlieferung des Unternehmens-Know-how. Arbeitsteilung, maschinelle Prozesse, Warenlieferungen konnten nur aufrechterhalten werden, wenn Aufzeichnungen getätigt wurden, die als Hilfs- und Beweismittel oder Erinnerungen dienten. Dokumentation und Buchführung von Alltagsdingen waren notwendig. Zusätzlich brauchte die Industriegesellschaft mehr Daten bei der Massenproduktion für Steuerung und Kontrolle. (vgl. Rammert 2007: 22f.)

Erst viel später, knappe 100 Jahre, wurden maschinelle Prozesse auf die Datenverarbeitung selbst angewandt, in Form von Massendatenverarbeitung erstmals bei einer Volkszählung in den USA 1890/91 mittels Lochkarten.

Von da an trat der Computer seinen Siegeszug in raschen Schritten an, vor allem auch weil das Militär hohe Fördergelder in seine Erforschung und Verbesserung investierte. Vorerst waren Computer für durchschnittliche Haushalte unerschwinglich, sie wurden verwendet, wo riesige Datenmengen verarbeitet werden mussten, z.B. in der Buchhaltung, Meteorologie, für statistische Großerhebungen und wie bereits erwähnt für die militärisch genutzte Datenverschlüsselung. Aber bereits hier setzte Kritik an dieser Technologie ein: Man warnte vor den Gefahren und fürchtete ein Szenario, wie es George Orwell in *1984* beschrieb. Forderungen zum Schutz des Menschen und seiner Privatsphäre wurden laut.

[1] Der Passierschein, ein Vorläufer des Reisepasses war damals noch mit Privilegien verbunden, später mit Kontrolle von Pflichten, als er den Aufenthaltsort legitimierte. (vgl. Groebner 2004: 126)

In den 1980ern/90ern kam dann der Personal Computer auf. Erstmals war es dadurch für Klein- und Mittelbetriebe wie auch für Haushalte und Einzelne möglich, auf automatisierte Datenverarbeitung zuzugreifen. Er veränderte den Alltag enorm und derart, dass er wiederum unentbehrlich wurde. (vgl. Schaar 2007: 35ff.)
Datenschutzprinzipien, die für Großrechner entwickelt wurden, hielten dem Fortschritt nicht stand. Ein Beispiel aus dem deutschen Bundesdatenschutzgesetz ist das Prinzip der „Zutrittskontrolle“, das fordert, „Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren“ (zitiert nach Schaar 2007: 37). Heutzutage träfe diese Beschreibung so gut wie auf jeden PC oder Laptop zu, auf den meist, zumindest im öffentlichen Raum mehrere Personen zugreifen können. Auch die Software für Computer machte Riesensprünge. Programme zur Text- und Tabellenverarbeitung stellen keine Herausforderung mehr dar, auch Datenbanksysteme können an individuelle Bedürfnisse angepasst werden. Was hinterherhinkt, ist das Bewusstsein um die Risiken und ein verantwortungsvoller Umgang mit der unaufhaltbar fortschreitenden Technologie.

2.2 Privatsphäre

Solche eben genannten, sensiblen Daten sind Teil unserer Privatsphäre. Wir selbst wollen bestimmen, wem, in welcher Weise Zugang zu uns, zu unseren Räumen und unseren Daten gewährt werden soll. In diesem Kapitel soll den Fragen nachgegangen werden, was unsere Privatheit ausmacht, wie sich der Begriff und seine Verrechtlichung historisch entwickelten und welche Bedeutung sie für unser Leben spielt.

2.2.1 Privatheit

Beate Rössler definiert Privatheit folgendermaßen:

> [A]ls privat gilt etwas dann, wenn man selbst den Zugang zu diesem ‚etwas’ kontrollieren kann. Umgekehrt bedeutet der Schutz von Privatheit dann einen Schutz vor unerwünschtem Zutritt anderer. ‚Zugang’ oder ‚Zutritt’ kann hier sowohl die direkte, konkret-physische Bedeutung haben, so etwa wenn ich beanspruche, den Zugang zu meiner Wohnung selbst kontrollieren zu können; es kann jedoch auch *metaphorisch* gemeint sein: in dem Sinn, dass

> ich Kontrolle darüber habe, wer welchen ‚Wissenszugang' zu mir hat, also wer welche (relevanten) Daten über mich weiß; und in dem Sinn, dass ich Kontrolle darüber habe, welche Personen ‚Zugang' oder ‚Zutritt' in Form von Mitsprache- oder Eingriffsmöglichkeiten haben bei Entscheidungen, die für mich relevant sind.
> (Rössler 2001: 23f.)

Dies meint also, dass bestimmte Personenkreise davon ausgeschlossen werden, in die Bereiche und Daten eines bestimmten individuellen Lebenszusammenhangs einzublicken und davon Kenntnis zu nehmen.
Die Räume und Dimensionen der Privatheit sind meist konventionell definiert, können auch gesetzlich abgesichert sein oder dem Individuum überantwortet werden. Das An sich Private existiert in dieser Form nicht, sein normativer Gesichtspunkt aber fordert die Ausbildung von Autonomie. Konfligieren diese beiden Positionen des Normativen und Konventionellen, ist aus liberaler Sicht die Frage nach der Grenze zwischen Privatem und Öffentlichem immer wieder neu zu stellen und zu bewerten. (vgl. auch Heesen 2008: 231)

Das aktuelle Interesse am Privaten innerhalb des wissenschaftlichen Diskurses verdankt sich drei unterschiedlich historischen Prozessen. Zum einen ist es die Intimisierung des Öffentlichen durch ehemals privat geheißene Themen aufgrund einer besonderen Betonung des Individuellen und des Authentischen; zum anderen durch Veränderungen im Geschlechterverhältnis. So ist der Thematik der privaten Sphäre in der Genderforschung eine bedeutende Rolle zugewiesen. Zuletzt stellt die gesellschaftliche Verbreitung von Informationstechnologien einen immensen Eingriff in die Privatsphäre von Personen dar, der den Schutz des Privaten als wertvoll erscheinen lässt. (vgl. Rössler 2001: 15)

Die Bestimmungen der Privatsphäre sind im Kontext von sozialgeschichtlichen, kulturellen und rollenspezifischen Rahmenbedingungen wandelbar, es gibt folglich mehr als *eine* Geschichte des Privaten. Trotzdem werde ich versuchen sie mit der Erwähnung mancher Eckpunkte zu erzählen.

2.2.2 Eine Geschichte des Privaten

Die Unterscheidung zwischen den beiden Seinsphären Öffentlichkeit und Privatheit gehen bis in die griechische Antike zurück. In den damaligen Stadtstaaten wurde die „private

Ordnung des Hauses (‚oikos')" von der „öffentlich-politischen Sphäre des Marktplatzes (‚agora')" (Schaar 2007: 15) getrennt. Die Römer übernahmen diese Ordnung, die sich bis in unsere Zeit fortsetzte. Von den Römern stammt auch das Wort Privatheit ab. *Privare* bedeutete als Verbum *berauben*, womit gemeint war, dass ein/e Bürger/in sich der öffentlichen Beobachtung entzog und damit dieser *beraubt* war. Das deutsche Wort *privat* ist seit dem 16. Jahrhundert geläufig und meint eine unabhängige Person oder ein für sich stehender Sachverhalt.
In vorindustriellen Gesellschaften war das Verständnis von Individualität ein ganz anderes als heute. Man wurde eher in eine Rolle, in eine Schicht hineingeboren, Positionen wurden vererbt. Mit den bürgerlichen Gesellschaften und dem Gleichheitsideal der französischen Revolution, löste man sich von einer ewig gottgegebenen, öffentlich inszenierten Rollenverteilung, wenngleich Klassen- und rollenspezifische Unterschiede in modifizierter Weise erhalten blieben. Vor allem das Bürgertum wollte nun seine individuellen Verhältnisse, seine geschäftlichen Entscheidungen in einen geschützten Raum zurückziehen. (vgl. ebd.: 15f.)

Den Medien kam beim Wandel von Privatheit und Öffentlichkeit eine bedeutende Rolle zu. Anfangs waren es die Zeitungen, die eine größere Öffentlichkeit schufen, diese also geographisch und auch sozial erweiterten. Im Gegensatz zu mündlicher Überlieferung und Briefverkehr, brachten Zeitungen Neuigkeiten schneller an eine breitere Masse. Der AdressatInnenkreis wurde vergrößert, die Übertragung schneller und die Kontrolle des/r Einzelnen über die Verbreitung (brisanter) persönlicher Details verringert.
Um der Öffentlichkeit nicht für jede Handlung Rechenschaft schuldig zu sein, wurde der Raum der Privatsphäre wichtiger, ein Raum, in dem das autonome bürgerliche Individuum, frei von Beobachtung war. „[J]e größer also der Radius der veröffentlichten Informationen wurde, desto dringender wurde der Schutz der Privatheit." (ebd.: 17)

Die Jahre um 1968 brachten eine Kehrtwende in der Bestimmung des Privaten. Von da an wurde die Privatsphäre kritischer beäugt, sie wurde als Ort gesehen, wo die herrschenden Machtverhältnisse ungehindert keimen und sprießen konnten. Die emanzipatorischen Bewegungen lokalisierten im Häuslichen repressive Geschlechterverhältnisse. Die eigenen Kinder wussten um die Nazivergangenheit ihrer Eltern nicht Bescheid und Autoritäten wie

Kirche, Politik, Universitäten wurden hinterfragt. Somit sollte das Private nicht mehr verheimlicht, sondern veröffentlicht werden.[2] (vgl. Heesen 2008: 231f.)

Mit der Entwicklung neuer Massenmedien und dem Wandel alter hat sich die Grenze zwischen Öffentlichkeit und Privatheit seit Mitte des 20. Jahrhunderts zunehmend verschoben bzw. ist sie ganz und gar undeutlich geworden. Der kommerzielle Druck und das Rennen um neue Sendeformate führten dazu, dass sich Massenmedien für das Private zu interessieren begannen. So berichten sie detailliert über das intime Leben von berühmten, „öffentlichen" Persönlichkeiten in Sport, Politik, Kunst, Pop, debattieren lieber über das Styling von PolitikerInnen als über ihre Tätigkeit, setzen Nichtprominente und ihre Alltagsprobleme ins Rampenlicht, wie in diversen Talkshows oder Reality-TV-Formaten. Dieser Verlust von Privatheit geht einerlei mit einer Banalisierung und Entpolitisierung einer stark von Medien geprägten Öffentlichkeit. Die politisch geprägte, in der griechischen Antike gewichtige Funktion der öffentlichen Ordnung scheint zu schwinden, wenn man als Beispiel die ausufernde Debatte über Bill Clinton und seine Praktikantin in den 90ern betrachtet.

In Zeiten von *Facebook*, *Youtube* und Co, in denen Einzelne aktiv an einem öffentlichen und weltweiten Mediengeschehen teilnehmen können, lässt sich feststellen, dass private Angelegenheiten freizügig und detailliert veröffentlicht werden. Sensible Details werden ans Tageslicht getragen, die vor Zeiten nicht einmal FreundInnen erfahren hätten. Chatrooms, persönliche Websites, digitale Fotoalben, Homevideos individualisieren den Mediengebrauch, offenbaren aber auch brauchbare Persönlichkeitsprofile der Öffentlichkeit. (vgl. Schaar 2007: 19 und Heesen 2008: 232)

Diese modernen, aber nicht unbedingt absehbaren Entwicklungstendenzen tragen es nach sich, dass diverse pessimistische, argwöhnische SozialwissenschaftlerInnen Kassandrarufe tätigen und vor extremen Verschiebungen, bis hin zur Auflösung der Grenze zwischen Öffentlichem und Privatem, warnen. Vom Verfall und vom Ende des Privaten wird seitdem genauso gesprochen (vgl. u.a. Whitaker 1999) wie vom Verschwinden einer politischen Öffentlichkeit. (vgl. Sennett 2001)

[2] Die Frauenbewegung brachte auch den Slogan „Das Private ist politisch" ans Tageslicht.

Diplomatisch und zutreffend beschreibt dieses Dilemma der unterschiedlichen Perspektiven Florian Rötzer, wenn er meint, „[w]ir stehen sicher nicht vor einem Ende des Privaten, wie das manchmal beschworen wird, wohl aber vor gewaltigen Veränderungen im Verhältnis von dem, was privat und was öffentlich ist.“ (Rötzer 2001: 174)

2.2.3 Die Verrechtlichung von Privatheit

Das „right to be let alone“ (Warren/Brandeis 1890) wurde erstmals 1890 von den amerikanischen Anwälten Samuel D. Warren und Louis D. Brandeis in ihrem Aufsatz „The Right to Privacy“ erwähnt. Sie leiteten es aus den Rechtsgrundsätzen des Schutzes der Person und des Schutzes des Eigentums ab. Dies bedeutet soviel, als dass der/die Bürger/in selbst darüber verfügen soll, wie viele ihn/sie selbst betreffende Informationen er/sie preisgeben will. (vgl. Coy 2008: 49) Aufgrund der Klatschpresse und dem Aufkommen der Photographie machten sie die informationelle Freiheit besonders der VIPs in den USA erstmals juridisch zum Thema. Zum großen gesellschaftlichen Diskurs wurde das Thema aber erst in den 50er, 60er Jahren des 20. Jahrhunderts als Computertechnologien aufkamen und die staatlichen Bürokratien diese nutzten, um Informationen zu sammeln und weiter zu verarbeiten.[3] (vgl. Rössler 2001: 13) Fast hundert Jahre nach dem Aufsatz von Warren und Brandeis mündete ihre Vorarbeit in Deutschland in das *Recht auf informationelle Selbstbestimmung*, bereits 1974 in den *Privacy Act* in den USA. Letzterer war eine Antwort auf die Debatten über die Auswirkungen des Einsatzes von Computern auf die Privatsphäre. Die Administration Kennedy hatte zuvor geplant, eine Datenbank einzurichten, die zu jedem/r US-BürgerIn Informationen bereitstellte. KritikerInnen warnten vor staatlicher Überwachung oder einer missbräuchlichen Nutzung dieser Informationen. Der *Privacy Act* klammerte aber Verbindlichkeiten für die Wirtschaft aus, weil er keinen Eingriff in den Wettbewerb tätigen wollte. Dieser Ansatz zeigte aber erhebliche Schwächen, wenn sich Unternehmen, die besonders aggressiv in Bezug auf Daten vorgingen, auch noch Wettbewerbsvorteile erringen konnten. Ein zweiter Schwachpunkt des US-Ansatzes ist der Entschluss, auf eine unabhängige Datenschutzkontrolle zu verzichten. Diese Schwächen versuchten die Europaratskonvention von 1981, die den nicht-öffentlichen Sektor bereits mit einbezieht, die Europäische Datenschutzrichtlinie 1995 und weitere Datenschutzgesetze der EU-Mitgliedstaaten auszumerzen. Ein Problem stellte dabei der Umgang mit der Wirtschaft

[3] Anlass des Artikels war Warrens Ärger über Übergriffe der Presse bei der Hochzeit seiner Tochter.

dar: Da die Marktlogik nicht unbedingt besseren Datenschutz erforderte, musste man Rahmenbedingungen schaffen, die einen bewussten, verantwortungsvollen Umgang mit personenbezogenen Daten hervorrufen oder in ökonomischer Hinsicht belohnen würden, um nicht von vornherein zum Scheitern verurteilt zu sein.[4] So meint der *Grundsatz der „Datensparsamkeit"*, der seit 2001 im deutschen Bundesdatenschutzgesetz verankert wurde, Systeme so zu gestalten, dass sie bei leistungsfähiger Arbeit möglichst wenige Informationen über Personen generieren sollten. (vgl. Schaar 2007: 52)
Die Gesetze für Datenschutz reichen für heutige Maßstäbe aber nicht mehr aus. Elektronische Datenverarbeitung ist allgegenwärtig und schließlich wurde der Datenschutz im Rahmen von Kriminalitätsbekämpfung stark zurückgedrängt.

2.2.4 Dezisionale und Lokale Privatheit

Ihrer Definition entsprechend teilt Rössler Privatheit in drei Dimensionen: die *lokale* Privatheit, die *informationelle* Privatheit und die *dezisionale* Privatheit.
In weiterer Folge interessiert mich vor allem die informationelle Privatheit, die beiden anderen Formen sind hier nur kurz angedeutet.

Dezisionale Privatheit meint den Schutz vor fremden Einflüssen bezüglich seiner Entscheidungen, aber auch seiner „Handlungen, Verhaltensweisen und Lebensweisen" (Rössler 2001: 145). Selbstbestimmung sollte gewährleistet sein, was bedeutet, dass andere (auch in Form von staatlichen und religiösen Instanzen) ihre Kommentare, ihre Urteile, Einflussnahmen, Einsprüche und Bewertungen zurückhalten sollten. Sexuelle Präferenzen fallen in den Bereich dezisionaler Privatheit, natürlich dürfen sie die Rechte anderer nicht verletzen. (vgl. auch Weber 2008: 291)

Lokale Privatheit bezeichnet den Schutz privater Räume, also der eigenen vier Wände, sowie den Schutz von Aufenthaltsdaten und der leiblichen Integrität. (vgl. auch Heesen 2008: 235) Hier sind dezisionale und informationelle Privatheit natürlicherweise gegeben. Private Räume sind eine Art Rückzugsgebiet, in denen Dritte nicht in unsere

[4] Das deutsche Wort *Datenschutz* wird gerne missverstanden, denn es bedeutet in seiner wörtlichen englischen Übersetzung ‚*data protection' Datensicherheit*. Der Begriff *Datenschutz* ist aber viel umfassender als der der *Datensicherheit*. Ersterer soll die Würde, die Handlungsfreiheit und die Privatsphäre der BürgerInnen gewährleisten. Letzterer fordert die technische Unterbindung von unzulässigen Zugriffen auf und Manipulation der Daten.

Entscheidungen einsehen und keine Informationen über uns erhalten. In der feministischen Debatte ist der private Raum besonders in den Brennpunkt der Aufmerksamkeit geraten, weil dort Handlungen geschehen können, die in die Rechte anderer eingreifen. Gemeint sind vor allem Frauen und Kinder bei ehelicher Gewalt. Gefordert wurde, dass diese Räume öffentlich, politisch gemacht würden, um sie erforderlicher Sanktionierungen nicht zu entziehen. (vgl. auch Weber 2008: 293)

2.2.5 Informationelle Privatheit

Warum sind wir im Alltagsleben so erbost, wenn FreundInnen intime Geheimnisse weitererzählen? Warum sind wir irritiert, wenn wir ohne unser Wissen (und gegen unseren Willen) beobachtet werden? Was stört uns daran, wenn Dritte uns mit unseren medizinischen Daten konfrontieren? Warum werden wir ungern darüber getäuscht, was mit Informationen über uns geschieht?

Wenn Privatheit die Kontrolle über den „Zugang" zur eigenen Person meint, dann ist *informationelle* Privatheit, die Kontrolle einer Person darüber, wer was in welcher Form über sie erfahren und wissen kann, sprich sie die „*Kontrolle* über die Preisgabe von Informationen" (Rössler 2001: 202) innehält. Damit ist gemeint, dass es die Person selbst in der Hand hat, Informationen weiterzugeben und andererseits zumindest abschätzen kann, wer was über sie weiß.[5]

Oft wissen wir aber gar nicht, dass wir die Kontrolle über unsere „informationelle Selbstbestimmung"[6] verlieren, wo, wie oft und durch wen dies geschieht.

> The creation, collection and processing of personal data is nearly a ubiquitous phenomenon. Every time we use a loyalty card at a retrailer, our names are correlated with our purchases and entered into giant databases. Every time we pass an electronic toll booth on the highway, every time we use a cell phone or a credit card, our locations are being recorded, analyzed and stored. Every time we go to see a doctor, submit an insurance claim, pay our

[5] Natürlich kann sich die Person in die Öffentlichkeit, zum Beispiel auf eine Straße wagen, auch wenn sie damit Informationen über sich preisgeben würde. Die Kontrolle darüber, somit auch der Entschluss dazu, bleibt schließlich bei der Person selbst.

[6] Das Recht auf „informationelle Selbstbestimmung" ist im deutschen Recht verankert. Es trifft auch auf das österreichische Recht zu, wenn im Grundrecht auf Datenschutz vor allem in den §§ 8 und 9 die Zustimmung als Rechtfertigungsgrund dezidiert ausgedrückt wird.

> utility bills, interact with the government, or go online, the picture gleaned from our actions and states grows finer and fatter.
> (Stalder 2002: 120)

Verletzungen der informationellen Privatheit sind folglich logischerweise dann gegeben, wenn eine Person ohne ihr Wissen und gegen ihren Willen in voyeuristischer Art beobachtet oder belauscht wird oder wenn zwar mit ihrem Wissen, aber gegen ihren Willen oder zumindest ohne ihr Einverständnis beispielsweise personenbezogene Daten von ihr an andere Unternehmen weitergegeben werden oder wenn sie selbst Informationen über sich mitteilt, die gegen ihren Willen in Form von Tratsch weitererzählt werden. Und doch sind sie selbst dann gegeben, wenn die Person davon weiß und es auch in Kauf nimmt, dass sie beispielsweise videoüberwacht wird, weil sie mit der Überwachung andere Vorteile verbindet. Und zwar deshalb, weil die Person in ihren Erwartungen enttäuscht wird in Hinsicht darauf, welches Wissen und welche Haltung und Einstellung ihr gegenüber Kommunikations- und InteraktionspartnerInnen (auch in Form von Institutionen) haben. Das heißt, die Person wird in ihren Annahmen getäuscht, „*in welcher Beziehung* sie [andere Personen und Institutionen, Anmerkung: D.R.] *aufgrund dieses Wissens* zu ihr stehen“ (Rössler 2001.: 205). Dies gilt auch für den letzten Fall der Videoüberwachung. Die Person weiß nicht, was andere wissen (diejenigen, die hinter den Monitoren sitzen). Sie trifft deshalb Annahmen auf falschen Voraussetzungen (zum Beispiel weiß sie nicht, mit wem sie es eigentlich zu tun hat) und ist in ihrer Selbstbestimmung verletzt, denn die Person rechnet nicht unmittelbar damit, dass ihr Verhalten filmisch digitalisiert aufgenommen und damit reproduzierbar, unabhängig von Ort und Zeit herzeigbar und analysierbar wird. Was aber, wenn die Person nie davon erfahren würde, dass sie heimlich beobachtet wurde? Selbst dann geht die Person von falschen Annahmen aus, handelt unter falschen Bedingungen und hätte sich, wüsste sie darüber Bescheid, eventuell anders verhalten, auch dies ist schließlich eine Verletzung eines Aspekts des selbst bestimmten, authentischen Verhaltens.

Soziale Beziehungen zu unseren Mitmenschen definieren sich ebenfalls darüber, wer welche und wie viele Informationen über uns erhält, erfährt, immer schon hat.

> Daß alle Beziehungen zwischen Menschen auf dem Wissen ruhen, das der eine von dem anderen hat - dies ist eine Tatsache von so banaler Selbstverständlichkeit, daß man nicht leicht an die gar nicht selbstverständlichen Nuancen und Maßbestimmungen dieses Wissens denkt und wie sehr sie, als Ursache und als Wirkung, die Sonderart jedes Verhältnisses charakterisieren. Denn nicht nur, was der eine von dem andern weiß, sondern dessen

> Verwebung mit dem, was er von ihm nicht weiß, gibt der Beziehung ihren Ton, ihren Umfang, ihr Tiefenmaß.
> (Simmel 1906: 108)

Ein/e gute/r Freund/in weiß sensiblere, intimere, geheimnisvollere Details über uns als der/die Arbeitgeber/in und will diese auch wissen. Hier in diesem Kontext präsentieren, inszenieren, stellen wir uns selbst anders dar als dort in jenem. Außerdem helfen uns gute Beziehungen zusätzlich, uns mit unserer Identität und Autonomie auseinanderzusetzen. Wenn wir uns in Frage stellen, uns erörtern, uns preisgeben, kann dieser interpersonelle Austausch konstitutiv für unser Selbstvertrauen und eben unsere Identität sein.
Ginge diese Form der „kontrollierten Selbstöffnung“ (Rössler 2001: 209) verloren, könnten wir Beziehungen nicht mehr unterscheiden, da selbst gewählte Abstufungen so nicht mehr möglich wären.

Natürlich unterliegt die Ziehung der Linie, die privates und öffentliches Leben teilt, gesellschaftlichen und kulturellen Konventionen sowie der individuellen Persönlichkeit.
Heesen sieht die Trennlinie zwischen Privatem und Öffentlichem zunehmend in den Verantwortungsbereich der betroffenen Personen selbst rücken, sie bestimmen ihren „Selbstdatenschutz“ (Heesen 2008: 241). Das Recht auf informationelle Privatheit scheint unter heutigen Bedingungen schwerer denn je umsetzbar, weil personenbezogene Daten ständig erhoben und weitergegeben werden. Das Individuum soll im Mittelpunkt technischer Dienstleistungen stehen.
Bei neuen Entwicklungen wie Videoüberwachung oder des Schutzes von Privatheit beim Surfen im Internet haben sich noch keine Konventionen herausgebildet, dafür sollten dann normative Prinzipien herangezogen werden. Die einzelnen Personen müssen sich hierbei auch auf die staatliche Kontrolle hinsichtlich ihres Informationsschutzes verlassen können. Neuere Informationstechnologien bergen die Gefahr in sich, dass sie den privaten Raum gegen unseren Willen weiter zurückdrängen. Andererseits sind wir bereit, mehr und mehr davon im Sinne anderer Interessen aufzuopfern, weil sich das Selbstverständnis von Personen zu ändern scheint und verkannt wird, dass authentisches, bewusst autonomes Handeln zentral für ein gelungenes Leben und für liberale Demokratien ist. (vgl. Rössler 2001: 213ff.)

2.2.6 Motive für Datensammlungen

Wer ist es eigentlich, der Daten sammelt und weitergibt und was sind die Motive dafür? Augenscheinlich ist das harmlose Motiv der Neugier, das den/die Voyeur/in anspornt oder den/die Hacker/in und das einen kleinen Einschnitt in die informationelle Privatheit darstellen kann. Andererseits werden Datensammlungen zu Rationalisierungs- und Effizienzzwecken vom Staat, von Wirtschafts- und Dienstleistungsunternehmen, von Versicherungen verfeinert und ausgebaut. Für diese spielt auch das Motiv des größtmöglichen Profits eine Rolle. All diese Motive sind nicht an sich schlecht, nur können sie umschlagen in das der Überwachung und Kontrolle, ohne Wissen und gegen den Willen der Betroffenen. (vgl. ebd.: 226)

2.2.7 Der Wert des Privaten

Das Argument, dass rechtschaffene BürgerInnen ja nichts zu verbergen hätten, entkräftete der erste deutsche Bundesbeauftragte für den Datenschutz Hans Peter Bull bereits 1984:

> Wie dem auch sei - die Behauptung, man habe vor den Behörden oder den Mitmenschen nichts zu verheimlichen, widerspricht allen Erfahrungen des Alltagslebens. Da will doch jeder nur das über sich, seine Familie, seinen Beruf und seine Geschäfte verbreiten, was ihm vorteilhaft erscheint, und selbst derjenige, der sich gern selbst ironisiert oder aus öffentlicher Selbstkritik Befriedigung gewinnt, vermeidet es im allgemeinen, sich ernsten Gefahren auszusetzen. Wer wird schon ohne Not bekennen, gegen ein Strafgesetz verstoßen zu haben? Wer wird durch unnötiges Offenbaren wirtschaftlicher Bedrängnis seinen Kredit gefährden? Und höchstens ein törichter Angeber wird durch unbedachtes Reden den Eindruck erwecken, nachrichtendienstliche Beziehungen zu unterhalten, so daß die Aufmerksamkeit der Sicherheitsbehörden auf ihn fällt.
> (Bull 1984: 11f.)

Abgesehen davon wird die Wichtigkeit der Privatsphäre ganz unterschiedlich bewertet. Auf der einen Seite plädieren John Stuart Mill bereits 1859 und Simson Garfinkel für den Wert der Privatsphäre. Sie sei die Basis für Freiheit und Leben an sich, für kreative Lebensentwürfe, die in Form von Gesellschaftsproblemlösungen wieder rückwirken und dadurch zum Allgemeinwohl beitragen. (vgl. Mill 1987, vgl. Garfinkel 2000) Andererseits meint David Brin, Privatsphäre und Datenschutz wären hinderlich für die Gewinnung von

Informationen, Wissen und Zurechenbarkeit, was eine freiheitlich gesinnte Gesellschaft wiederum erst begünstigt. (vgl. Brin 1998)

Dennoch fällt dem Schutz des Privaten eine Bedeutung zu, die nur schwer geleugnet werden kann. Denn in einer liberal-demokratischen Gesellschaft, die auf den Säulen „Freiheit, Gleichheit, Neutralität des Staates und Demokratie“ (Rössler 2001: 27) aufgebaut ist, ist Privatheit deshalb besonders wertvoll, weil das Funktionieren der Gesellschaft auf autonom handelnde Individuen angewiesen ist. Wenn es das *telos*, das Ziel und der Zweck der Freiheit ist, ein autonomes, selbst bestimmtes Leben zu führen, dann ist der Schutz des Privaten deshalb von so großer Bedeutung, weil nur die Bedingungen, Rechte und Ansprüche auf individuelle Privatheit die Autonomie in all ihren Facetten wahren, lebbar machen können. „[A]utonom ist eine Person dann, wenn sie sich die Frage stellen kann, welche Person sie sein will, wie sie leben will, und wenn sie dann so leben kann.“ (ebd.: 39) Dafür braucht sie Rückzugsgebiete, um sich selbst, Pläne und Ziele entwerfen, entwickeln und definieren zu können, um sich spontan und unbefangen verhalten zu können. (vgl. Heesen 2008: 234) So zieht man sich in den privaten Bereich zurück, wenn man andere Positionen, Handlungen, Meinungen nicht berücksichtigen will. Freiheitsrechte alleine reichen hier nicht aus, weil die Autonomie bereits beschädigt werden kann, wo Freiheitsrechte noch gar nicht berührt sind. Freiheitsrechte substantialisieren sich erst im rechtlichen Schutz des Privaten, auf den jedes Individuum auch zwecks eines gelungenen Lebens Anspruch hat. Würde im Umkehrschluss ein Mensch beliebige andere in seine Wohnung blicken lassen, sie bei seinen Entscheidungen mit einbeziehen und keinen Unterschied daraus machen, wem er was über sich erzählt, so wäre das neben einer Reduzierung seiner Privatsphäre auch ein immenser Eingriff in seine Autonomie.[7] (vgl. Rössler 2001: 26ff.)

Dies ist auch die wesentliche Funktion der Privatheit in der bürgerlichen Gesellschaft in ihrer heutigen Bedeutung: „In einer von individuellen Entscheidungen geprägten Gesellschaft muss die Privatsphäre gegen Einblicke Dritter geschützt werden, damit das individuelle öffentliche Handeln überhaupt möglich ist.“ (Schaar 2007: 16) Somit ist die Privatsphäre als Raum des Rückzugs zugleich auch unverzichtbare Voraussetzung für eine freie Meinungsbildung. Totalitäre Systeme haben versucht, diesen Raum neben dem öffentlichen zu besetzen und zu kontrollieren. Durch ihre enge Verbindung ist es nicht

[7] Totalitäre Staaten versuchen eben genau, private Bereiche ihrer BürgerInnen möglichst klein zu halten, um die für sie tendenziell gefährliche Autonomie zu unterdrücken.

möglich eine freie Öffentlichkeit zu schaffen, wenn es keinen Bereich gibt, in dem man unbeobachtet und unzensiert leben, reden, seine Werte vertreten und sich austauschen kann. „Freie Rede, freie Information und freie Meinungsäußerung würden ohne ein tief verankertes Recht auf Privatheit verkümmern." (ebd.: 15)

Liberal-demokratische Gesellschaften bedürfen autonomer Individuen, um all ihre Facetten einer hohen Lebensqualität und einer politisch mündigen Öffentlichkeit auszuspielen.

> Als ‚Privatleute' machen sie [die Bürgerinnen und Bürger, Anmerkung D.R.] gegenüber den versachlichten Gesetzen des Marktes und der verselbstständigten bürokratischen Apparatur des Staates den Anspruch auf Teilhabe an der Gestaltungsmacht der öffentlichen Gewalt geltend. Sie führen so den Eigensinn der in privater Lebensführung entspringenden Erwartungen in die Verhandlung über das ‚Öffentliche' ein.
> (Weiß 2002: 32)

2.3 Fallbeispiele zur Preisgabe sensibler Daten

In diesem Kapitel will ich Beispiele aus dem Social Network *StudiVZ* geben, die zeigen sollen, dass wir Daten über rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit und sexuelle Präferenzen, also genau solche Daten, die vom Recht als besonders schützenswürdig angesehen werden, freiwillig hergeben.

Da ich mir vor fast drei Jahren einen Account bei *StudiVZ* angelegt habe, wähle ich dieses Network für meine Fallbeispiele. Ich werde natürlich keine Personennamen nennen, werde also anonymisierend vorgehen, werde aber die Schritte beschreiben, die mich zu freiwilligen Nennungen sensibler Daten führen. Datumsstand ist der 14. Februar 2010.

Ich klicke, nachdem ich mich eingeloggt habe, auf meiner Startseite auf den Button *Meine Gruppen*. Über der Suchleiste gibt es den Button *Gruppen suchen*, den ich wähle.

Gebe ich in die Suchleiste das Wort Türke ein, bekomme ich 300 Treffer [Stand: 14.02.2010]. Ich wähle die Gruppe *"Ich bin kein Araber, kein Perser und kein Türke. ICH BIN KURDE"* aus, die 383 MitgliederInnen aufweisen kann. Ich klicke die Gruppe an, es

erscheinen unzählige Namen mit dazugehörigen Personenbildern. Ich muss nicht viele Bilder anklicken, um auf ein Profil zu stoßen, das für mich in keiner Form eingeschränkt ist, das heißt, dass im Grunde jede/r vollständig die Informationen einsehen und abrufen kann, die den engsten FreundInnen zur Verfügung stehen.

Ich kann zwar nicht beweisen, dass die Personen, die ihre Profile vollständig ausweisen, wirklich so heißen und wirklich ein Passfoto ihres Antlitzes ins Netz stellen oder aber ein Fake-Profil angefertigt haben bzw. ein Bot sind, „autonome Programme, die in definierten Umgebungen, […] Aufgaben selbstständig erledigen können." (Zeger 2009: 18) Die Namen sind aber nicht abgekürzt und klingen authentisch. Wer sich nicht sofort erkenntlich geben will in Social Networks, verwendet meist Namenskürzel oder verwendet Pseudonyme, die als solche erkannt werden. Die UserInnenfotos zeigen durchschnittliche Menschen, sind also keine Comicfiguren, VIPs, Graphiken, oder ähnliches. Zusätzlich finde ich so viele „offene" Profile, dass ich denke, in der Menge findet sich zumindest ein Original, was mir als Beweis im Grunde auch reichen würde.

Gebe ich *FPÖ* in die Suchmaske ein, erhalte ich 134 Treffer. Zwar sind die meisten Gruppennamen Phrasen, die gegen die FPÖ sprechen, aber die Gruppe *FPÖ Feldkirchen* weist zumindest elf MitgliederInnen auf. Wiederum entdecke ich vollständige Profile darunter.

Gebe ich Gewerkschaft in die Leiste ein, erhalte ich 101 Treffer. Ich wähle die Gruppe *GDL - Gewerkschaft deutscher Lokführer (Fahrpersonal)* mit 117 MitgliederInnen. Diese ist zwar eine Gruppe, mit MitgliederInnen, von denen die meisten wohl aus Deutschland stammen, doch soll das Beispiel zeigen, dass auch um die Gewerkschaftszugehörigkeit kein Geheimnis gemacht wird.

Gebe ich *zeugen jehovas* ein, erhalte ich 68 Treffer. Wiederum nehmen die meisten davon die Zeugen spöttisch aufs Korn. Die Gruppe *ZEUGEN JEHOVAS IM STUDI-VZ* hat immerhin 88 MitgliederInnen. Vollständige Profile finde ich schnell.

Gebe ich *sklerose* in die Maske ein, finden sich 39 Treffer. Die Gruppe *Multiple Sklerose Gruppe* hat 140 MitgliederInnen mit teilweise „offenen" Profilen.

Gebe ich *gay* ein, erhalte ich 300 Treffer. Die Gruppe *queer, schwul, gay, glücklich :D* mit 5.672 MitgliederInnen bezeugt, dass sexuelle Präferenzen bereitwillig angegeben werden.

Warum stellen sich Menschen so eindringlich selbst dar? Was lässt sie ihre eigene Privatheit vergessen? Diese Fragen sollen in den nächsten Kapiteln erarbeitet werden.

2.4 Selbstdarstellung im Web 2.0

2.4.1 Web 2.0

In weiter Folge der Kommerzialisierung des Internets machte Tim O'Reilly Mitte der 2000er den Begriff Web 2.0 populär.[8] (vgl. O'Reilly 2005) Web 2.0 stellt eine neuere, bessere Version des alten Internets dar (im Endeffekt bleibt es jedoch nur ein Schlagwort), das eine Reihe neuer, interaktiver Möglichkeiten für die UserInnen bot. Ein bedeutender Aspekt dieses modernen Mitmachwebs, wie man es auch zu beschreiben pflegt, ist, dass die Möglichkeit der Contentproduktion, also der Erstellung von Inhalten, von einer erschöpfbaren Quelle, nämlich der geringen Anzahl an RechteinhaberInnen für Inhalte, wie Verlage, KünstlerInnen, AutorInnen usw. übertragen wurde zu einer so gut wie unerschöpflichen Ressource an InhaltsproviderInnen, nämlich der UserInnen selbst. Sie selbst sollen zu AnbieterInnen werden. Informationshunger und Mitteilungsbedürfnis bilden eine perfekte Waage.

Social Networks kamen unter anderem auf. Diese Communities dienen dazu, eine Vielzahl von Bekannten, Freunden, Interessenskollegen usw. kennen zu lernen, mit ihnen in Kontakt zu stehen, zu kommunizieren und zu daten. Es wurde ohne genaue technische Kenntnisse möglich, eigene Profile in Social Networks anzulegen, Fotos, Videos, Texte und Audiodateien hochzuladen, sich selbst zu veröffentlichen. (vgl. Schaar 2007: 46) Dazu ist es obligatorisch zur Registrierung eine Vielzahl an Daten einzugeben. Einige davon sind zwar optional, wer jedoch wahrgenommen werden will, braucht ein anständiges, aussagekräftiges Profil. Wohnort, Alter, Schulbildung, Interessen, Geschwister, Art der FreundInnen, ein Selbstporträt gehören zu den gängigen Fakten. Politische Gesinnung, sexuelle Orientierung, Trink- und Rauchgewohnheiten sind etwas speziellere Angabefelder, werden von manchen

[8] Erfunden hat ihn Scott Dietzen, danach verwendet von Eric Knorr, Dale Dougherty und Craig Cline.

TeilnehmerInnen, wie gezeigt, auch ausgefüllt. Mit standardisierten Personendaten können Profile leichter erstellt, durchsucht, abgeglichen oder in Datenbanken eingetragen werden. Diese nutzen UserInnen einerseits selbst, um Leute mit gleichen Interessen oder ähnlichem Alter zu finden bzw. werden sie andererseits von den BetreiberInnen oder öffentlichen Behörden erstellt und abgeglichen wie es 2006 geschah, als BenutzerInnenprofile mit der US-amerikanischen Sexualtäter(Innen)datei abgeglichen wurde. (vgl. Zeger 2009: 31)

Community-Dienste wie *Facebook, Myspace, StudiVZ, Bebo, Orkut, Xing, www.livejournal.com, www.friendfinder.com, www.hi5.com, www.friendster.com*, usw. haben heute insgesamt über eine Milliarde MitgliederInnen. (Natürlich werden manche davon bei mehreren Diensten angemeldet sein). Täglich kommen 100.000 weitere dazu.
Es haben sich im Web mittlerweile auch Personensuchmaschinen herausgebildet, wie beispielsweise *www.123people.at* oder *www.world-check.com*, wovon manche mit staatlichen Behörden zusammenarbeiten und mit offiziellen Datenbanken über StraftäterInnen abgeglichen werden.
Der Google-Dienst *www.23andme.com* bietet an, den persönlich bereitgestellten DNA-Code nach Verwandtschaftsverhältnissen rund um die ganze Welt zu untersuchen.
Auf *Flickr* liegen weit mehr als drei Milliarden Fotos von UserInnen bereitgestellt auf. *Youtube*, ein Videoportal, liegt laut *Alexa* (*www.alexa.com*), das die Beliebtheit von Webseiten berechnet, auf Platz 3 der meistbesuchten Internetseiten. *Youporn* ist ohnehin ein Shootingstar des Webs. Wahlkampfreden, oppositionelle Aufschreie, Botschaften von extremistischen Gruppierungen, Musikvideos von bekannten bis unbekannten Bands und Missgeschicke öffentlich-berühmter Personen liegen auf diesen Bildportalen ebenso vor wie private Aufnahmen, die allerhand belanglose Tätigkeiten bis hin zur Pornographie bezeugen. (vgl. ebd.: 32ff.)

Die Rolle des Körpers und seine öffentliche Präsentation sind zwar „sowohl symbolisch besetzt wie konventionell reguliert und geschlechtsspezifisch kodiert“ (Rössler 2001: 270), diese Kodierungen und Konventionen scheinen sich aber im Web stark gewandelt zu haben. Auch die Scham vor einer körperlichen Präsentation, die auf individueller Ebene eine Rolle spielt, scheint abzunehmen. Wichtig ist jedoch, dass Menschen die Inszenierung der Körperlichkeit selbst kontrollieren können. Mit der Selbstdarstellung wollen sie einen bestimmten Ruf aufbauen. Die meisten zu bewertenden Bilder stammen auch von den

Betroffenen selbst, unangenehm wird es, wenn jemand ein fremdes Bild zur Schau und Bewertung stellt.

Eine Zensur erweist sich als schwierig. Wird ein radikaler Titel hier verboten, findet er bestimmt andere Portale, wo er veröffentlicht werden kann.
Außerdem richtet sich die Rechtslage nach dem Bundesland oder -staat, in dem der Webserver der BetreiberInnen ansässig ist. Während in Österreich oder Deutschland eine strenge Offenlegungs- und Impressumspflicht besteht, ist beispielsweise in Kalifornien der anonyme Betrieb von Servern erlaubt. Viele (unter anderem unseriöse) Internetunternehmen siedeln sich deshalb aus, weil ihnen die dortige Rechtslage entgegenkommt und der Standort für ihr Service nicht ausschlaggebend ist. (vgl. Zeger 2009: 39ff.)

2.4.2 Motive für die Selbstdarstellung

Sobald wir in die Öffentlichkeit schreiten und wir in Kontakt mit anderen Menschen treten, wirkt man, ob gewollt oder ungewollt, automatisch auf diese. Wir bemühen uns einen meist optimalen, zumindest stimmigen Eindruck zu hinterlassen, was man als Kunst der Selbstdarstellung bezeichnen könnte.

> Schon die Art, wie Personen sich kleiden, zeigt natürlich, dass sie sich selbst immer in bestimmter Weise präsentieren wollen und je nach Kontext auch präsentieren müssen. Das Bewusstsein, *dass* man auf andere wirkt, und die Furcht, *wie* man auf andere wirkt, gehören zu den ständigen und fundamentalen Aspekten menschlicher Selbstwahrnehmung.
> (Rössler 2001: 268)

Die Fähigkeiten bzw. Anlagen, wahrgenommen zu werden und Aufmerksamkeit zu bekommen, bilden ein Grundgerüst für unseren Selbstwert und das Vertrauen in die eigene Person. (vgl. Datenschutzkommission et al. 2010: 12)

Was im Web 2.0 passiert ist ähnlich wie es auch beim Telefonieren in der Öffentlichkeit mittels Handy oder bei Talkshows geschieht, wenn Menschen im TV in peinlichster Art Intimitäten anbieten und Privates inszenieren. Es geht um die „*Enthüllung des Privaten*, um die Ver-Öffentlichung traditionell immer noch als privat geltender intimer Details.“ (Rössler 2001: 312)

Die Handelnden geben ihr privates Wissen preis und schränken selbst ihre informationelle Privatheit ein bzw. geben sie diese ganz auf. Was den besten FreundInnen vorbehalten sein sollte, wird einsehbar für die Öffentlichkeit, zumindest für interessierte Fremde. Soziale Netzwerke lassen die Grenze zwischen Öffentlichkeit und Privatheit verschwimmen, jede/r kann sich selbst öffentlich darstellen, Privates weltweit bereitstellen. (vgl. Schaar 2007: 46f.)
Das Differenzierungsvermögen geht verloren, der individuelle Sinn für Privatheit. Auch Alan Westin wies schon darauf hin, dass ein Verlust von Privatheit nicht nur wegen moderner Informationstechnologien passieren könnte, sondern eben auch wegen der individuellen Bereitwilligkeit diese zu opfern (vgl. Westin 1967: 52ff.).[9] Ein mögliches Motiv dafür könnte auch ein gefühlter Bissen vom Kuchen des Ruhmes sein. „Wenn man schon die Veröffentlichung eines möglichst interessant inszenierten Lebens nicht direkt in Geld umsetzen kann, so doch wenigstens in Prominenz, und sei sie noch so lokal." (Rötzer 2001: 171)

Der Wunsch, eine Form von Prominenz zu erlangen, kann es auch sein, der uns sensible Daten im Netz preisgeben lässt. Wer sich in einem Network als gay outet, will vielleicht soziale Konventionen brechen, Ansehen erringen, gerade in dieser Hinsicht etwas bewegen, andere dazu aufrufen, selbiges zu tun, Homosexualität salonfähig zu machen, ein Coming Out tätigen. Wer eine Krankheit preisgibt, wird andere finden, die sich ebenso damit auseinandersetzen müssen, dagegen ankämpfen, Tipps geben können. Gemeinsames Leid ist geteiltes Leid, spricht der Volksmund. Wer seine politische Einstellung verrät, ist ohnehin stolz auf diese, wird sich erhoffen, bevorzugte Parteien anderen schmackhaft zu machen, weiß sich in seinem Umfeld ohnehin bestätigt.

Für die UserInnen geht es im Web 2.0 eben nicht nur ums dabei sein, sondern es geht vielmehr ums Mitwirken, darum, Einfluss nehmen zu können. Neben der Erstellung von Inhalten, gibt es die einfachere Möglichkeit, die Inhalte zu bewerten. Bewerten und bewertet zu werden, schafft Sinn und Bedeutung, ladet etwas mit Relevanz auf und somit wird fast alles beurteilt, die Körper, das Aussehen, Babys, NachbarInnen, Tattoos, Fahrzeuge, Lokale, LehrerInnen, bald vielleicht auch ÄrztInnen, SteuerberaterInnen, RechtsanwältInnen und NotarInnen. Die Postings und Profile, die wir in diesem Paralleluniversum abgeben, mögen uns mitunter sogar überleben, da sie in den ewigen Weiten der Speicherkapazitäten

[9] Er stellte auch erstmals den Zusammenhang zwischen dem Schutz der Privatsphäre und der Freiheit im Allgemeinen her.

irgendwo ein Plätzchen gefunden haben. Auch das könnte ein Anreiz sein, sich im Netz verewigen zu wollen, unsterblich zu sein.

Dennoch gaben in einer Umfrage von Harris Interactive online 59 Prozent der 2.513 befragten US-BürgerInnen an, sich bei der Preisgabe ihrer persönlichen Daten im Internet nicht wohl zu fühlen. Ein Viertel der Befragten fühlt sich überhaupt nicht wohl, wenn Daten genutzt werden, um Profile zu entwickeln und personalisierte Inhalte und Werbungen auszusenden. Ältere Menschen zeigten sich dabei deutlich skeptischer als diejenigen der Altersgruppen 18 bis 31 und 32 bis 43 Jahre.

Verwunderlich erscheinen beim Lesen dieser Umfrage die Personen, die zwar Unbehagen empfinden, trotzdem nicht darauf reagieren und keine mögliche Aktion setzen. Denn wie *Facebook*-Sprecher Tim Sarapani bei einer Diskussionsveranstaltung der Universität Berkeley zu Protokoll gab, hätten sich zuletzt (nach den jüngsten einseitigen Änderungen am *Facebook*-Datenschutzmodell) nur etwas mehr als ein Drittel der UserInnen mit den Datenschutzeinstellungen ihrer Profile befasst. Der Gegenschluss besagt, dass 65 Prozent der UserInnen auf ihre Kontrolle über die Einstellungen verzichten, was bedeutet, dass sie viel über sich verraten. (vgl. Futurezone o.A. 02.02.2010)

Auch der rechtliche Schutz bei der Verwendung sensibler Daten fällt dann weg, wenn „der Betroffene die Daten offenkundig selbst öffentlich gemacht hat“ (DSG 2000, §9 Z 1)
Heesen meint ohnehin, dass Selbstdatenschutz mehr und mehr gefragt sei. Jedoch lassen sich Systemeinstellungen zwar individuell regeln und folglich können besonders besorgniserregende Optionen unterbunden werden, doch verraten sie indirekt im Subtext ihrer Nutzungseinstellungen wieder etwas über die Person und zeigen persönliche Beziehungsstrategien, -verhalten und Präferenzen auf. Selbst Anonymisierungs- oder Pseudonymisierungsmaßnahmen wirken sich auf die Selbst- und Fremdwahrnehmung aus. (vgl. Heesen 2008: 241f.)

2.4.3 Selbstdarstellung als Meinungsfreiheit

Gewarnt wird von vielen Web-ExpertInnen, dass Personen nicht zu viele Daten ins Internet stellen sollen, weil dort viele Gefahren lauern. Damit werden Ängste und Misstrauen

geschürt. Andererseits meint Hans Zeger, der die Warnungen berechtigt, aber überbewertet ansieht, müssten sich Menschen dann selbst zensurieren, verstecken und ihr Recht auf freie Meinungsäußerung einschränken. Social Networks könnten unter dem Gesichtspunkt der freien Meinungsäußerung gesehen werden, anstatt des Exhibitionismus seiner MitgliederInnen. Jene ließe sich dann über das Verfassen von LeserInnenbriefe zu politischen Themen hin ausweiten. Zeger betrachtet die Web 2.0-Communities als technische Umsetzung der Stammtischkultur, als eine Art globaler Interessensgemeinschaften. Stammtische sind Räume, die weder der Privatsphäre im klassischen Sinn zugeordnet werden können, noch sind sie öffentlich. Sie entfalten sich in einem halböffentlichen Bereich, in einem Bereich „schwacher Öffentlichkeit“ (Zeger 2009: 59). Diese eher kleinen Gruppen haben nur Einfluss auf eine geringe Zahl von Personen und sind leicht zu überwachen und zu kontrollieren.

Auch Foren sind in Zahl ihrer TeilnehmerInnen oftmals nicht größer als ein Stammtisch, die physische Präsenz bleibt dagegen aus. Man kann sich nur seiner eigenen Körperlichkeit sicher sein.

Andererseits unterliegen Foren auch nicht mehr den lokalen kulturellen Vorverständnissen und Übereinstimmungen eines Stammtisches, sondern einem Wirrwarr diffuser internationaler Gepflogenheiten. Der „Versammlungsort“ ist nicht lokalisierbar. Nationale Gesetze haben kaum Zugriff auf getätigte Aussagen. Geäußerte Meinungen, die in einem Land unerwünscht oder verboten sind, zum Beispiel nationalsozialistische Aufrufe, können in einem anderen Land erlaubt sein.

Während Zitate am Stammtisch bald wieder der Vergessenheit anfallen, bleiben sie im Netz gespeichert und können ein Eigenleben entwickeln. Aussagen können reproduziert, aus dem Kontext gerissen, ohne die gewünschte Intention wiedergegeben werden usw.

Foren erscheinen deshalb als verdächtig und gegebenenfalls auch gefährlich, weil sie stets organisiert wirken. Eine Meinung tritt selten einzeln auf, sie wird bewertet, viele schließen sich ihr an. Ideen, Ziele oder zumindest Aufregungen werden gemeinschaftlich verfolgt. Der/Die Verfasser/in, der/die aus einer Empörung heraus Unwillen kundtut, könnte ein/e potentielle/r, organisierte/r Täter/in sein, die Identität sollte ausgeforscht werden. (vgl. ebd.: 56ff.)

2.5 Digitaler Fußabdruck

All die Spuren, die wir im Internet hinterlassen, lassen sich zu einem ziemlich genauen Nutzungsprofil zusammensetzen, das unserer Persönlichkeit und unseren Interessen entspricht. Wann nutzt jemand das Internet, wie oft, wonach sucht die Person, für welches politische Thema/Sportart/Hobby interessiert sie sich, welche elektronische Zeitung liest sie? All diese Informationen geben ein Abbild von uns, das nicht immer ganz korrekt sein muss, genau so gut kann es überholt und einseitig sein, von den Betroffenen können sie jedenfalls nicht mehr kontrolliert oder korrigiert werden.

Bereits 1984 schrieb Wasserstrom, dass die Daten, die über ihn im Laufe der Jahre gesammelt wurden, „could produce a picture of how I had been living and what I had been doing […] that is fantastically more detailed, accurate and complete than the one I could supply from my own memory." (Wasserstrom 1984: 326)

Daten wurden immer schon erhoben, nach einer Zeit nicht mehr benötigt und vergessen. Der große Unterschied im Internet ist die Tatsache, dass das Netz alles auf ungewisse Zeit speichern kann, also anders ausgedrückt nichts „vergisst". Wir hinterlassen Datenspuren, einen Digitalen Fußabdruck, der uns eventuell sogar überdauern wird.

> To be in cyberspace is to be recorded. Digital activities and objects are nothing but an ensemble of traces and records. Each electronic action in cyberspace implies the creation of tread marks [...]. Those digital footprints can be, by nature, reconstituted, recreated and saved indefinitely.
> (Barrera/Okai 1999: 1)

Begeht jemand eine Straftat, so ist es unzulässig, die Person zu einem wesentlich späteren Zeitpunkt damit zu konfrontieren, das gilt auch für Veröffentlichungen über verurteilte StraftäterInnen. Dazu bedürfte es derer Einwilligung und zusätzlich müsste der Sachzusammenhang hergestellt werden.
Was im realen Leben als „Recht auf Vergessenwerden" (Schaar 2007: 47) aufrechterhalten wird, ist folglich im Internet schwieriger zu realisieren. Zwar meint das Datenschutzgesetz in §27 Abs. 1: „Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, daß ihre Archivierung rechtlich zulässig ist und daß der Zugang zu diesen Daten besonders

geschützt ist“ (DSG 2000, §27 Abs. 1), dennoch gilt, wenn Informationen im Internet erst einmal veröffentlicht sind, werden sie auch nicht mehr vergessen. Selbst wenn der/die ursprüngliche Anbieter/in sie löscht, kann man nie sicher sein, ob ein/e User/in sie nicht bereits auf seinem/ihrem Computer gespeichert bzw. sogar wieder veröffentlicht hat. Der/die ursprüngliche Anbieter/in kann faktisch nicht mehr über seine Inhalte verfügen. Zusätzlich werden für ökonomische oder wissenschaftliche Zwecke Webangebote archiviert. Das Internetarchiv *www.archive.org* beispielsweise, 1996 in San Francisco gegründet, führt InteressentInnen mit seiner *WayBackMachine* zu längst gelöschten Websites. Zum Beispiel konnte ich teils zehn Jahre alte Kommentare von LeserInnen auf verjährten Aufmachungen der *ORF.at*-Website finden. Und auch Suchmaschinen finden zunehmend gezielter Aussagen diverser AutorInnen in Foren usw.

Als Beispiel eines digitalen Fußabdrucks kann folgendes Schicksal einer Lehrerin dienen, die ihren Job in einer renommierten Privatschule verlor, weil sie vor ihrer Lehrtätigkeit einen anstößigen Werbespot drehte, der im Internet auftauchte und von den SchülerInnen gesehen wurde. (vgl. Zeger 2009: 60)
Ein weiteres Beispiel ist ein Schüler, dessen Username nach diversen Beleidigungen, gerichtet an LehrerInnen und die Direktion, seiner IP-Adresse zugeordnet und er selbst somit ausfindig gemacht werden konnte. Ein Lehrer zeigte ihn polizeilich an. (vgl. Datenschutzkommission et al. 2010: 9)
Mittlerweile haben sich Reputationsfirmen im Web bewährt, die im Sinne des Selbstmarketings den ordentlichen Online-Ruf einer Person wieder herzustellen versprechen, wie zum Beispiel die Firmen *www.webreputation.com* oder *www.textweberei.at***.**

Um harte Aufpralle in der Realität zu vermeiden will die EU-Kommission mehr Medienkompetenz für ihre BürgerInnen. In den Leitlinien, die eine Empfehlung für EU-Staaten darstellen, wird insbesondere erwähnt, dass SchülerInnen über die Gefahren aufgeklärt werden sollen, die einer Preisgabe ihrer persönlichen Daten im Netz innewohnt. (vgl. Reding 2009: 6) Die Folgen einer Verwendung von Social Networks wie *Facebook*, *StudiVZ* und Co sollen klargemacht werden und über die Verarbeitung personenbezogener Daten aufgeklärt werden.

2.6 Zwischenfazit

Jeder Mensch will eine bestimmte Privatsphäre gewahrt wissen, deren Grenze aus individuellen, konventionellen, kulturellen Zusammenflüssen gezogen wird. Derzeit setzt sich eine gesellschaftliche Tendenz zur Beschneidung der persönlichen Privatheit durch. Unternehmen und Behörden versuchen mehr Daten zu sammeln, BürgerInnen haben die Bereitschaft, mehr Daten preiszugeben, weil der Informationsfluss und -austausch im Web ohnehin möglich und notwendig ist. Eine intakte Privatheit ist aber von großem Wert, sowohl für das Individuum als auch für eine liberale demokratische Gesellschaft. Wer autonom handeln will, braucht private Räume, muss private Entscheidungen treffen können und muss über Informationen, die ihn betreffen, verfügen können. Und wer eine Demokratie will, in der wirklich das Volk herrscht, braucht autonome BürgerInnen.
Im vorangegangenen Abschnitt konnte auch gezeigt werden, dass das österreichische Recht, sensible, personenbezogene Daten, die unsere rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder das Sexualleben betreffen, als besonders schützenswürdig ansieht. Unter anderem stellen wir aber genau solche heiklen Daten im Internet der Öffentlichkeit zur Verfügung. In Social Networks, verschiedensten Plattformen und Foren arbeiten wir selbst an einem detaillierten Profil über uns mit umfangreichen Soziogrammen, das von Interessierten nur mehr abgerufen zu werden braucht und somit unsere Privatheit beschneidet. Das Bewusstsein, dass die mediale Preisgabe von Daten Gefahren birgt, da solche auf lange Zeit archiviert werden, sie sich nachteilig auswirken und eventuell missbräuchlich verwendet werden könnten, scheint sich noch nicht ausgebildet zu haben. Der Reiz, sich selbst darzustellen und Content selbst zu produzieren, und eine gewisse zwanglose Sorglosigkeit lassen die UserInnen sogar darüber hinwegsehen, dass Einstellungen zur Privatsphäre selbst getätigt werden könnten, was den Schutz ihrer persönlichen Daten deutlich verbessern würde. Denn nach scharfer Kritik von Seiten der DatenschützerInnen mussten die BetreiberInnen zumindest mehr Schutzmöglichkeiten für Daten einrichten, um einen anständigen Ruf zu wahren.

Der nächste Themenblock bezieht sich auf die Möglichkeiten einer Überwachung unserer Daten. Kann jemand ein solches Ausmaß an Inhalt im Web, das produziert wird, überhaupt überwachen und wenn ja, wer sind diese Subjekte, Einrichtungen und Institutionen?

Anders formuliert würde die Frage aus informationsethischer Sicht lauten: „Wer hat wann, unter welchen Umständen, in welchem Umfang zu Informationen Zugriff“ (Weber 2008: 289) und fängt was damit an?

3. Überwachung

3.1 Beobachtung, Überwachung, Kontrolle. Eine Definition von Überwachung

Die Definition von Surveillance [Überwachung, D.R.], wie sie David Lyon knapp ausformuliert im Kontext seines Buches zur Überwachungsgesellschaft verwendet, „is any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered." (Lyon 2002: 2)

Diese Definition macht deutlich, dass Überwachung über eine reine Beobachtung hinausgeht. Etwas zu beobachten könnte mit dem Prozess des Sammelns und Verarbeitens von persönlichen Daten, einer Informationserhebung beschrieben werden. Wer beobachtet, nimmt genau wahr, und dazu gehört unumgänglich eine Verarbeitung und eine Verknüpfung mit anderen Informationen, in welcher Form auch immer. Überwachung aber impliziert eine Absicht, einen Zweck. Und den beschreibt Lyon als einen negativ konnotierten. Die Absicht, die hinter einer Überwachung steht, ist die, die Überwachten zu beeinflussen, sie zu beaufsichtigen, zu leiten und ihr Verhalten zu regeln. Eine Absicht, auf künftige Ereignisse Einfluss zu nehmen.

Das französische Wort *surveillance* bedeutet übersetzt unter anderem auch Aufsicht, in zweifachem Sinn: zum einen kann ich ein Kind beaufsichtigen, um es vor Unfällen zu bewahren, zum anderen, damit es keinen Unfug anstellt. Überwachung hat zwei Gesichter: „The same process […] both enables and constrains, involves care and control." (ebd.: 3) Überwachung liegt es inne, nicht nur psychische, soziale und tatsächliche Räume zu begrenzen, sondern sie auch zu eröffnen.
Im Grimmschen Wörterbuch hat *überwachen* noch die zusätzliche, gütige Bedeutung des *länger Wach-Seins*, wenn man ein Kind bei seinem Einschlafprozess begleitet und beschützt. (vgl. Nogala 2001: 152) Diese Bedeutung ist aber stark in den Hintergrund gerückt und in unserem Alltagsgebrauch nur mehr peripher bekannt.

Die ÜberwacherInnen, in diesem Fall die Eltern nehmen folglich immer Einfluss auf die künftigen Ereignisse rund um das Kind, wenn sie es beaufsichtigen. Solange das Kind den gewünschten Erwartungen entspricht, muss die Aufsicht nicht zwangsläufig in das

Geschehen eingreifen, wird das Kind aber bedroht, werden die Eltern sowohl einschreiten, als auch dann, wenn das Kind die Grenzen ausreizt und über den gepflegten Toleranzbereich hinaus Handlungen betreibt. Kontrolle entsteht, die jeden Erziehungsprozess begleitet.

Nach dem Kriminologen und Psychologen Detlef Nogala ist Überwachung dann auch „eine zeitlich und logisch miteinander verbundene Abfolge einzelner Kontrollakte“ (Nogala 2001: 151). Davon unterschieden, wird Kontrolle wiederum in der Systemtheorie als Vergleich eines Istwerts mit einem Sollwert verstanden, wobei gegebenenfalls ein korrigierender Eingriff folgen kann. Das Streben hin zu einer bestimmten Ordnung und ihr Realisierungswunsch sind dabei vorausgesetzt.

> Überwachende Aktivitäten spielen sich in einem sozialen Kontinuum ab, das von der gütigen und nützlichen Überwachung im Konsens, vielleicht sogar zum gegenseitigen Nutzen, über die proaktive Bearbeitung von Konflikten im Vorfeld bis zum Pol der repressionsbereiten Einschüchterung reicht. Überwachung zielt dabei immer auf die präventive Abwendung der Abweichung vom Sollwert und auf die Vermeidung der Realisierung von Konflikt und Risiko ab.
> (ebd.: 152)

Ein asymmetrisches, hierarchisches Verhältnis ist der Überwachung immanent, eine/r überwacht, eine/r wird überwacht. Darum kann sie als „Herrschafts- und Regulierungsstrategie verstanden werden, die im Interesse des Status quo herrschende Ordnung(en) präventiv sichern und notwendige Zwangsinterventionen auf ein Minimum reduzieren will.“ (ebd.: 152)

Jede Überwachungshandlung besteht aus drei Teilschritten:
Erstens werden Informationen erhoben und mit Sollwerten und Normen abgeglichen, zweitens werden die Informationen systematisch verarbeitet, d.h. sie werden in ein Referenzsystem eingetragen und mit Identifikations- und Lokalisierungsdaten in Verbindung gebracht. Drittens fällt eine Entscheidung über eine (notwendige) Intervention, die eine Sanktion nach sich ziehen kann. (vgl. ebd.: 153)

Beobachtung, Überwachung und Kontrolle sind ähnliche Begriffe, sie haben zueinander keine starren Grenzen und (können) ineinander übergehen. Beobachtung lässt Kontrolle und Überwachung zu. Nach Nogala lässt Kontrolle erst Überwachung zu, obwohl die beiden Begriffe nicht strikt zu unterscheiden sind. Überwachung umschließt den einzelnen

Kontrollakt in einer zeitlichen Dimension. Anders sieht es Gottschalk-Mazouz. Bei ihm geht der Begriff der Kontrolle über den der Überwachung hinaus. Während Überwachung beim Wissen stehen bleibt, „wer was tut oder tun kann“ (Gottschalk-Mazouz 2008: 218), ist Kontrolle das Verfügen-Können, „wer was tun kann oder tun muss“ (ebd.) und darüber, ob fremde Handlungen gelingen mögen oder nicht.
Diese Definierung von Überwachung würde aber auch der von Lyon widersprechen und eher dem Begriff der Beobachtung entsprechen, den ich vorher angesprochen habe, denn es fehlt darin die Absicht, mit diesem Wissen dann auch etwas anzufangen, sich einen Vorteil zu verschaffen, wenngleich diese nicht zwangsläufig umgesetzt werden muss.

Wenn ich folglich von Überwachung spreche, so meine ich damit, das Sammeln und Verarbeiten von personenbezogenen Daten, um Einfluss zu nehmen auf künftige Ereignisse, die diejenigen betreffen, deren Daten erhoben wurden. Kontrolle, in der Bedeutung von Überprüfung, Nachprüfung, Eingriff ist zu verstehen als Einzelakt im Feld der Überwachung.

3.2 Die Überwachungsgesellschaft

Während Michel Foucault, die absolute Überwachung in einer verpesteten, mittelalterlichen Stadt beschreibt, haben wir uns mittlerweile im 21. Jahrhundert zu einer Gesellschaft umgewandelt, in der sich die Überwachung ganz unauffällig, unmerklich einschleicht.

3.2.1 Die verpestete Stadt

Im 17. Jahrhundert gab es einen bestimmten Ort und einen bestimmten Zeitraum für das totale Überwachungssystem: Wenn die Pest in eine Stadt einfiel. Aus Angst vor dem Tod, vor dem unvorhersagbaren Kommen und Gehen, aus Angst vor dem Chaos und der Unordnung setzte die Macht eine rigorose Ordnung entgegen. Die Stadt wurde geschlossen, alle BewohnerInnen wurden in ihren Häusern und Wohnungen eingesperrt und durften außer in seltenen Ausnahmefällen nicht außer Haus gehen. Ein Verlassen des zugewiesenen Raumes wurde mit dem Tod bestraft, das galt auch für herumstreunende Tiere. Lebensmittel wurden bereitgestellt. Ein Syndikus hatte sein Gebiet (meist eine Straße) zu kontrollieren

und einer Instanz über ihm, dem Intendanten, Auskunft über Vorkommnisse zu geben. Dies bedeutete, dass sich täglich alle BewohnerInnen der Region durch ein bestimmtes Fenster oder Türloch bei ihm zeigen und über ihren Zustand berichten mussten. Dies diente der Kontrolle über Leben und Tod, niemand sollte Tote oder Kranke versteckt halten. Es wurde bis hin zum Bürgermeister Bericht erstattet, penibel registriert und Buch geführt. Den Behörden sollte nichts entgehen.
Dieses Vorgehen im Falle der Pest gleicht einer Disziplinierungsanlage. Analytisch wollte man dem verpesteten Chaos entgegenwirken. Zwar gab es auch anarchistischere Ansichten, Herr dieser Krankheit zu werden, aber die disziplinierte, hierarchische Vorgehensweise der absoluten Kontrolle hatte sich durchgesetzt.
Während der Herrschaft der Lepra wusste man sich als Gegenmaßnahme noch mit Ausschluss und Verbannung aus der Gesellschaft zu helfen, in Zeiten der Pestepidemie wurde ein vollkommenes und darum fortwährend als Maßstab dienendes Disziplinierungssystem, das auf Hierarchie und Überwachung setzt, etabliert. Nach und nach wurden im 19. Jahrhundert die beiden Maßnahmen der Ausschließung und der Disziplinierung an einem parzellierten Raum institutionalisiert und beispielsweise in der Einrichtung des Gefängnisses kombiniert.
(vgl. Foucault 1995: 251ff.)

Die Pest dient hier als Beispiel für die Angst der Menschen vor dem Chaos und den Drang hin zu mehr Kontrolle der Menschen, denn sie ist hier „mehr als nur eine Seuche: in ihr spiegelt sich vor allem auch die Bedrohung durch allgemeine Unordnung und unkontrollierte Bewegung wider.“ (Dürr 2004: 99f.) Pestkranke werden unter Quarantäne gestellt, isoliert, sorgfältig kontrolliert und überwacht. Die Gefahr ausgesetzter, aber „freier“ Asozialer war damit minimiert. Der ganze Apparat wurde mittels Abspeckung effektiver und ein exaktes Wissen über die Individuen kristallisierte sich heraus. Das Modell der Peststadt war Vorbild für eine spätere Entwicklung der Machtpraktiken. (vgl. Fink-Eitel 1989: 72) Die Überwachung seiner BewohnerInnen führte zu einer „Informations-, Entscheidungs- und Bewegungshierarchie“ (Dreyfus/Rabinow 1987: 222), die bis in die kleinsten Details vordrang.

3.2.2 Unsere Gesellschaft als Überwachungsgesellschaft?

Überwachung ist keine Erfindung und auch nichts unmittelbar Neues. Es hat sie immer schon notwendigerweise gegeben, wo Menschen miteinander in Kontakt traten, zusammenlebten, interagierten und kommunizierten, beispielsweise in Vereinen, in Dörfern, in extremer Form auch im eben gezeigten Beispiel der verpesteten Stadt, usw. Was sich aber unterscheiden kann, ist welches Ausmaß Überwachung annimmt, „welchen Grad an Verhaltenskontrolle diese Gesellschaft ausüben will." (Weber 2008: 294) Wir alle überwachen und kontrollieren uns gegenseitig. Verhält sich jemand anders als der Rest, zum Beispiel, weil er/sie andere Klamotten trägt und wird dafür schief angesehen, so ist das nichts anderes als eine Sanktionierung eines nicht konformen Verhaltens, die das letzte Glied der Überwachungs- und Kontrollkette darstellt.
Die Frage, die wir uns stellen können, ist die normative, welche Gesellschaft wir haben wollen. Eine liberale, wie seit dem 18. Jahrhundert angestrebt, mit größtmöglicher Freiheit für alle oder bewegen wir uns davon weg, wie es nunmehr den Anschein hat, da sich latent und ubiquitär Überwachungstendenzen in unsere Gesellschaft einschleichen. (vgl. ebd.: 294f.) Oder wie es Phillips formuliert: "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: 95)

Gottschalk-Mazouz macht folgende Eigenschaften für die Begehrlichkeiten ganzheitlicher Überwachung, einer Überwachungsgesellschaft schlechthin aus (vgl. Gottschalk-Mazouz 2008: 216ff.):

- Überwachung soll *übergreifend* sein, das heißt, sie soll nicht nur die direkte Aktion, also die Ausführung einer Tat auskundschaften, sondern auch ihre Planung, Reflexionen und Reaktionen. Dies war auch bereits immer der Fall, soweit es möglich und wichtig genug war. Der Zugriff auf Informations- und Kommunikationsprozesse weitet das Ganze aber stark aus.
- Sie geschieht *multidimensional*. Neben audiovisuellen Daten können solche über Bewegung, Kommunikation und Tausch generiert werden.
- Sie geschieht nicht mehr temporär. Durch die jederzeitige Möglichkeit der Überwachung und die langfristige Speicherung der Daten wird sie *permanent*.

- Ihre Ergebnisse werden diachron und synchron *quervernetzt* und mit vorhandenen Wissensbeständen erweitert, abgeglichen und neu interpretiert.
- Sie ist *allseitig*. Man kann nicht mehr vom Überwachungsstaat, sondern muss von der Überwachungsgesellschaft sprechen, weil sie sich über eine Vielzahl von AkteurInnen erstreckt. Wie auch Rammert feststellt, kommt es nicht zu einer Zentralisierung oder gar Monopolisierung der Kontrollmacht, sie verzweigt sich eher in vielfältige, dezentrale Regimes, die Daten erzeugen und dokumentieren und die sich im gesellschaftlichen Raum voneinander abgrenzen und dann doch teilweise überschneiden. Daten und Datenformate aus dem Netz sind ohnehin nicht räumlich zentral, sondern parallel be- und verarbeitbar. (vgl. Rammert 2007: 23) Rötzer spricht anstelle des Großen Bruders von den „vielen Kleinen Schwestern“ (Rötzer 2001: 171).
- Überwachung ist bereits in Systemstandards und in die Produktion neuer Artefakte und Technologien *integriert*. Manche technisierten Handlungen sind so konzipiert, dass sie nur funktionieren, wenn man Überwachung über sich ergehen lässt. Ein Beispiel wäre die Registrierung bei Aktivierung oder dem Updaten einer Software.
- Sie läuft *automatisiert* ab. Niemand muss mehr Hilfsleute zur Überwachung aktivieren, es geschieht von selbst. Dasselbe gilt für die Auswertung der vielen Daten und entsprechenden Reaktionen. Auch sie sollen automatisiert werden, weil ihr Aufwand personell nicht mehr zu leisten ist.

Neben dem Zusammenwachsen der Infrastruktur privater, öffentlicher und militärischer Aspekte der Überwachung führt auch der Systemcharakter moderner Technik (Geräte und ihre Aktivitäten sind wechselseitig aufeinander angewiesen) zu einer vermehrten Kontrolle und automatisierten Auswertung. Das semantische Web und Ubiquitous Computing sind Entwicklungen, die künftig diesen Systemcharakter noch verstärken sollen, mit „Konsequenzen für die Dynamik von Information und Wissen“ (Gottschalk-Mazouz 2008: 221).

Ein Internet mit semantischen Strukturen könnte verstärkt als Übersetzer und Ordner auftreten und leichter Kategorien zu bestimmten Inhalten zuordnen; zum Beispiel, ob beim Sprechen über Netze, das Internet, Beziehungsnetze oder Fischernetze gemeint sind. Denn es zieht bei der Suche im Web nicht nur Begriffe heran, „die *in* der Seite vorkommen“, sondern auch „Aussagen *über* die Seite.“ (Bodendorf 2006: 131) Diese Metainformationen würden vor allem den Algorithmen und elektronischen AgentInnen dienen und

Kontrollmöglichkeiten erweitern. Mit Ubiquitous Computing ist eine vernetzte, intelligente Infrastruktur gemeint, die Menschen in ihrem Handeln und Können unterstützt. (Siehe weiter unten!)
Auch hier gilt, dass moderne Technikapparaturen und intelligente Softwareprogramme keine einseitige, konzentrierte, geradlinige Steigerung der Macht garantieren können, sondern viel eher auf verzweigte und interaktive Aktivitäten von Maschinen, Medien und Programmen hinauslaufen. (vgl. Rammert 2007: 23)

3.2.3 Datensammlungen

Warum ist gerade in unserem modernen Zeitalter eine Tendenz zu so riesigen Datensammlungen gegeben?

- Wenn der/die Einzelne nach mehr Freiheit strebt und diese auch zugebilligt bekommt, entstehen andererseits Unsicherheitsfaktoren, die durch die geringe soziale Kontrolle bedingt werden. Um den Willen der Sicherheit zu gewährleisten, greifen AkteurInnen zu Überwachungs- und Sicherheitstechnologien zurück.
- Staatlich Kontrollinstanzen wollen Personen bei Verdacht identifizieren und observieren. Eine Ausweitung auf einschlägigere Methoden, wie biometrische Identifizierungsmerkmale ist nahe liegend.
- Auch die Wissenschaften dringen tiefer in alle Bereiche des Lebens vor.
- Dadurch kommt es auch zu einer rasanten Entwicklung der Datentechnologien.
- Schlussendlich muss auch der/die Einzelne in seinen/ihren Lebensentscheidungen auf Daten zurückgreifen, die er/sie ansammelt. Eine zunehmende Individualisierung bringt auch mehr persönliche Verantwortung mit sich, die eine Vielzahl an Daten als unausweichlich erscheinen lässt.

(vgl. Rammert 2007: 18f.)

3.3 Der Panoptismus

Michel Foucault (1926-1984) schreibt in seinem Buch *Überwachen und Strafen. Die Geburt des Gefängnisses* (1975) von einem Wandel in der Denkart der westlichen Gesellschaften vom 17./18. zum 19. Jahrhundert. An dieser historischen Wende ging man über von Martern

zu verschwiegenen, subtileren Strafen, Theorien des Rechts wurden neu aufgestellt, Disziplin und Züchtigung wurden salonfähig. Nicht nur Gefängnisse dienten als Zuchtanstalten, auch die Gesellschaft erhaltende Einrichtungen wie Schulen, Krankenhäuser, Militärstützpunkte und Arbeitsstätten verschrieben sich, uns zu befrieden und zu zähmen.
Um sein berühmtes Kapitel über den Panoptismus zu verstehen, will ich vorher zwei wichtige Begriffe seines Werkes beschreiben, die untrennbar mit Prozessen der Überwachung verknüpft sind, den der Macht und den der Disziplinargesellschaft.

3.3.1 Der Machtbegriff bei Foucault

Der Machtbegriff bei Foucault orientiert sich eng an Max Webers.

> Macht bedeutet jede Chance, innerhalb einer sozialen Beziehung den eigenen Willen auch gegen Widerstreben durchzusetzen, gleichviel worauf diese Chance beruht. […] Der Begriff ‚Macht' ist soziologisch amorph. Alle denkbaren Qualitäten eines Menschen und alle denkbaren Konstellationen können jemand in die Lage versetzen, seinen Willen in einer gegebenen Situation durchzusetzen.
> (Weber 1980: 28f.)

Ähnlich bei Foucault, Machtausübung wird Führung, Vermögen, „das Feld möglichen Handelns der anderen zu strukturieren." (Foucault 1987: 257) Macht in seiner angewandten Form ist hier eine Weise des Einwirkens auf Handlungsmöglichkeiten, eine Art der Einflussnahme, die andere verändert.

Die Typen von Zielen der Machtausübung sind „Aufrechterhaltung von Vorrechten, Akkumulation von Profiten, Einrichtung einer statusbedingten Autorität, Ausübung einer Funktion oder eines Fachs." (ebd.) Die Strategie, die hinter einer Machtausübung steht, will dabei nicht unbedingt den direkten Sieg über eine/n Kontrahentin, sondern eine „Fixierung eines Machtverhältnisses" (ebd.: 260), die ein hohes Maß an Stabilität und Konstanz mit sich bringt. Kontrollmechanismen und Überwachungssysteme sind dabei nur instrumentelle Modalitäten der Machtausübung, sie sind eine Ausformung dessen, wie Macht wirken kann.

Doch wer ist der/die BesitzerIn der Macht? Sind es politische AkteurInnen, Reiche, Menschen in hohen Positionen oder EigentümerInnen technischer Infrastrukturen? Macht ist ein Ensemble so vieler Faktoren, sodass Macht „nicht einzelnen Personen oder Korporationen zufällt, sondern in einem reichlich unübersichtlichen Geflecht von Interessen Schritt für Schritt täglich neu ausgehandelt und verteilt wird." (Gottschalk-Mazouz 2008: 222)

Das bedeutet, „Macht ist eine allgemeine Matrix der Kräfteverhältnisse zu einer bestimmten Zeit in einer bestimmten Gesellschaft." (Dreyfus/Rabinow 1987: 217)

So beschreibt Foucault auch sein Forschungsvorhaben als Analyse, wie Machtverhältnisse wirken.

> Das ist ein außerordentlich komplexes Ganzes, bei dem man sich schließlich fragen muß, wie es in seiner Anordnung, in seinen Mechanismen, seinen wechselseitigen Kontrollen, seinen Anpassungsleistungen so subtil sein kann, wo es doch niemanden gibt, der das Ganze gedacht hat. […] Das Interessante liegt nicht darin, den Plan zu entdecken, der all dies angeleitet hat, sondern die Strategie herauszufinden, wie sich die Stücke plaziert [sic!] haben.
> (Foucault 1976a: 112f.)

3.3.2 Macht in der Disziplinargesellschaft

In der Disziplinargesellschaft, wirkt die Macht direkt auf die Körper. Sie unterliegen Zwängen, Verboten und Verpflichtungen. Dies trifft in jeder Gesellschaftsform zu, einiges an den Techniken des 18. Jahrhunderts lässt sich aber als Neuerung bzw. Intensivierung beschreiben.

Die Größenordnung der Kontrolle findet eine neue Dimension, nämlich die des Details. Auf den tätigen Körper wird ein fein abgestimmter Zwang ausgeübt, der in Bewegungen, Gesten und Schnelligkeit seinen Ausdruck findet.

Der Gegenstand der Kontrolle verschiebt sich vom Verhalten und der Körpersprache hin zu „Ökonomie und Effizienz der Bewegungen und ihrer inneren Organisation" (Foucault 1995: 175). In der Übung, zum Beispiel der militärischen, können diese Elemente gesteigert werden.

Zuletzt ändert sich die Durchführungsweise der Kontrolle. In den Mittelpunkt einer von nun an durchgängigen Zwangsausübung rücken die Vorgänge einer Tätigkeit und nicht ihr Ergebnis. Zeit, Raum, Bewegungen werden bis ins kleinste codiert. (vgl. ebd.)

Herangezogen werden also Körper, die bis ins kleinste Detail analysiert, zerlegt, neu zusammengesetzt, umgeformt und vervollkommnet werden sollen, um sie in einen größeren Gesamtkörper einzugliedern, wie beispielsweise in die Armee oder in die Fabrik. Hier hat die Form der Arbeitsteilung eine Kräfte steigernde Wirkung. (vgl. Fink-Eitel 1989: 76f.)

Diese Methoden der Unterwerfung und der Nutzbarmachung der Kräfte und Individuen nennt Foucault die *Disziplinen*. Er meint zwar, dass es diese in Klöstern und Armeen schon lange gegeben habe, im Laufe des 17. und 18. Jahrhunderts wurden die Verfahren der Disziplinierung aber zu allgemeinen Herrschaftsformen. Der Übergang von einer vormodernen, feudalen Souveränitäts- zu der modernen Disziplinargesellschaft geschah, weil von einer kostspieligen, unsicheren Ordnung, in der beispielsweise der Monarch seine Armee ausschickte, um einen Aufstand zu rächen, zu einer effizienteren, produktiveren gewechselt werden sollte. (vgl. Dürr 2004: 52) Man musste „etwas anderes finden: die emsigen, gleichmäßigen, unauffälligen Disziplinen." (Foucault 1976c: 75)

Die Disziplinen sollen ein Verhältnis schaffen, das die Körper umso gefügiger macht, je nützlicher sie sind, umso nützlicher je gefügiger sie sind. Sie ersetzen dabei nicht andere Machtformen, sondern besetzen alte, vorhandene, schleichen sich zwischen sie, verbinden sie, erweitern sie und verfeinern ihre Wirksamkeit und lässt „die Machtwirkungen bis in die feinsten und entlegensten Elemente dringen." (ebd. 1995: 277) Überwachung und Kontrolle dienen als ideale Praktiken der Disziplinartechnik, die nicht sporadisch, sondern stetig und regelmäßig ausgeübt werden sollen.

Unsere westlich-liberalen Gesellschaften würde Foucault folglich als Disziplinargesellschaften beschreiben. Praktiken der Disziplin lassen sich auf die Gesellschaft ausweiten, innerhalb der sie ein wirksames Netz von Beziehungen aufbauen, das diesen zusammenhängenden Machtraum erst herstellt und begünstigt. Was Foucault damit meint und beschreibt, ist „die *Disziplinarordnung* beziehungsweise die *Disziplinargesellschaft* als der Ort der konkreten Aktualisierung dieser abstrakten Ordnung." (Dürr: 2004: 17)

Wichtig dabei ist wiederum der Begriff der Macht, den Foucault voraussetzt. Sie lässt sich nicht von Personen akkumulieren, sondern lässt sich als Apparatur beschreiben, die die Gesellschaft erst laufen lässt, denn „[i]n der hierarchisierten Überwachung der Disziplinen

ist die Macht keine Sache, die man innehat, kein Eigentum, das man überträgt; sondern eine Maschinerie, die funktioniert.“ (Foucault 1995: 228f.)

Sie trägt in der Disziplinargesellschaft eben keine Spuren eines Schlachtfeldes in sich, äußert sich nicht in brüllendem Kampfgeschrei, sondern agiert stets strategisch, kühl und diskret. Foucault sucht einerseits nach Strategienkomplexen der Macht und andererseits danach wie sie in den Individuen und ihren zwischenmenschlichen Beziehungen verankert sind.
Er knüpft seinen Machtbegriff eng an die Neuzeit im Sinne einer Pastoralmacht als Ordnung, „in der ein individuierender und zugleich totalisierender Zugriff der Machtmechanismen und Erkenntnisverfahren eine völlige Beschlagnahme des Lebens und Alltags intendiert“ (Dauk 1989: 107). Die Pastoralmacht verlor selbst an Einfluss, übertrug sich jedoch auf gesellschaftliche Institutionen. Die Disziplin übernimmt die Institution des Klosters, die Humanwissenschaften beerben die Beichte, die dem Menschen sagte, wer er ist. Diese Pastoralmacht bezieht ihre Grundlagen aus der Inquisition, die das römische Recht mit der individuierenden Sequenz Verhör-Geständnis und damit mit der Beichte verband. (vgl. ebd.: 106ff.)
So meint auch Dürr, dass die Macht den Individuen einen Platz in der Gesellschaft zuordnet, sie entlang eines parzellierten Raumes auffädelt.

> Macht äußert sich immer in einer bestimmten Form des In-Beziehung-Setzens (von Gegenständen sowie Subjekten), welche über die jeweiligen individuellen Entscheidungen der Akteure hinausgeht und von als Knotenpunkte der Macht fungierenden gesellschaftlichen Institutionen vermittelt wird. Die Disziplinarmacht etwa setzt durch die Vermittlung von Institutionen wie Gefängnis, Schule, Kaserne et cetera Subjekte zueinander in eine Beziehung, die durch deren Eingliederung und deren jeweilige Funktion innerhalb eines mechanischen Gesamtapparates sowie - auf diachronischer, evolutiver Ebene - durch das Maß der individuellen Einpassung in diesen charakterisiert ist.
> (Dürr 2004: 126)

Die Disziplin selbst aber ist eine Technik und nicht Institution, sie ging aber in Institutionen ein und wurde selbst wiederum von ihnen eingesetzt. (vgl. Dreyfus/Rabinow 1987: 183)

Macht und die Disziplinen sind nichts, was rein repressive Elemente aufweist, sie sind nicht an sich Verwerfliches, sie entstanden erst durch ihr unglaublich produktives Potential.

„Macht ist der *eine* Integrationszusammenhang produktiver Disziplin, der die Subjektivität und Individualität der Menschen nicht unterdrückt, sondern allererst hervorbringt.“ (Fink-Eitel 1989: 78)

> Denn wenn die Macht nur Unterdrückungsfunktionen wahrnähme, wenn sie nur noch auf die Weise der Zensur, des Ausschließens, des Absperrens, der Verdrängung, in der Art eines großen Über-Ichs arbeitete, wenn sie nur auf negative Art ausgeübt würde, wäre sie sehr zerbrechlich. Wenn sie stark ist, dann deshalb, weil sie auf der Ebene des Begehrens positive Wirkungen produziert - das weiß man inzwischen - und auch auf der Ebene des Wissens. Die Macht, weit entfernt davon, Wissen zu verhindern, bringt es hervor. Wenn man ein Wissen über den Körper hat ausbilden können, dann war dies möglich über eine Gesamtheit militärischer und schulischer Disziplinen. Ausgehend von einer Macht über den Körper war ein physiologisches, organisches Wissen möglich.
> (Foucault 1976a: 109)

Ganz eng ist die Verstrickung, die Macht und Wissen zusammenbindet. In der Lust am Detail zum Körper entstanden Humanwissenschaften wie Psychologie, Statistik und Anthropologie. Das generierte Wissen festigt die Machtstrukturen innerhalb der Gesellschaft, die dieses erst wieder hervorbringen.
Foucault geht es um die Form der wirksamen Machtverhältnisse, die in den modernen Gesellschaften wirken und wie sie sich zur Form des Wissens beziehen, das in ebendiesen vorherrscht und Gültigkeit erlangt.
Auch der Volksmund kennt die Weisheit *Wissen ist Macht*. Wissen ermöglicht Handlungen und verleiht einem so „Macht, etwas zu tun, das man sonst nicht tun könnte (sei es gegenüber dem Überwachten, sei es Dritten gegenüber)“ (Gottschalk-Mazouz 2008: 221). Wissen ist auch eine strategische Ressource, indem man Wissensbestände vorenthalten oder verändern kann. Auch in dieser Form kann Wissen Macht verleihen. Wer andere kontrolliert, kann seinen Willen leichter durchsetzen.

3.3.3 Die Mittel der guten Abrichtung

In diesem Kapitel wird versucht, folgende Fragen zu beantworten: Kann man beim Menschen von einer Dressur sprechen und wer steht hinter einer solchen? Wie werden wir gut abgerichtet? Ist Überwachung Teil einer Erziehung, die Fügsamkeit lehrt?
Die Disziplinarmacht bedarf einfacher Mittel, um erfolgreich zu sein:

Dies ist der „hierarchische Blick“, eng verbunden mit der „normierenden Sanktion“ (Foucault 1995: 220). Beide sind schließlich kombiniert im Verfahren der Prüfung.

3.3.3.1 Die hierarchische Überwachung

Die Herkunft der hierarchischen Überwachung geht genealogisch gesehen auf die kirchliche Pastoralmacht zurück. Schon der christliche Gott war allsehend, dadurch allwissend und er konnte die Strafe als Instrument der Läuterung einsetzen. (vgl. Purgathofer 2008: 196) Auch der/die Pastor/in, was lateinisch Hirte/in bedeutet, hat seine Schafe zu ihrem Wohle zu führen. Um dieser etwas diffusen Verpflichtung nachzukommen, können ihm viele Mittel recht sein, wie Erkennen und Unterscheiden, Beobachtung, Überwachung, Sanktionierung, er wird seine Schafe vergleichen und miteinander in Konkurrenz setzen, sie hierarchisch gliedern nach Maßstäben ihres moralischen Wohlverhaltens. Der Hirte kann als Überwachungsinstanz begriffen werden, dasselbe gilt auch für Eltern und PädagogInnen. Nach und nach wird die Überwachung in vielerlei Funktionen des Disziplinarapparats integriert und macht die Person des/r Hirten/in sogar entbehrlich. (vgl. Dauk 1989: 117)

Der zwingende, hierarchische Blick lässt Machteffekte im Bereich der Techniken des Sehens entstehen. Zu kontrollierende Personen werden mit seiner Hilfe sichtbar gemacht. Dieser Bereich des Sehens, der unauffälligen, aber vielfältigen Überwachungsblicke, wurde von den Wissenschaften lange Zeit ausgespart. Größere Technologien wie Fernrohre, Linsen fanden mehr Beachtung und Eingang in der Kosmologie und der Optik, während die Kunst des Sehens, ohne gesehen zu werden eher übersehen wurde. Obwohl sie es war, die ein neues Wissen über den Menschen formierte.
Eine bedeutende Rolle spielt dabei die Architektur, das Muster der Anstalten. So ist das Militärlager, das als Modell für weitere Einrichtungen wie Arbeitersiedlungen, Spitäler, Asyle lange Zeit als Vorbild diente, mit einer künstlich angelegten Stadt vergleichbar. Die Architektur war genau bestimmt, denn im Militärlager hat die Macht prophylaktisch, intensiver und zugleich diskreter zu sein als anderswo, da sie sich über bewaffnete Individuen spannt. (vgl. Foucault 1995: 221f.) „[E]in System der genauen Überwachung [garantiert] die Machtausübung.“ (Dauk 1989: 118) Die einander kontrollierenden Überwachungsblicke sind jeweils einzelne Elemente in der Gesamtheit der Machtausübung.

Entscheidend war nicht mehr, wie in den Jahrhunderten zuvor, die Gebäude prunkvoll auszustatten und wie bei Festungen beabsichtigt, den äußeren Raum zu überwachen. Die Architektur war ausgerichtet, ihre Insassen detailliert zu kontrollieren. Und nicht nur das, sie sollte einen Schritt weiter gehen und diese beeinflussen und nach und nach verändern.
Krankenhäuser sind nicht mehr einzig ein Dach über dem dahinvegetierenden Elend. Sie sollen so konstruiert sein, dass Ärzte den Verlauf der Genesung beobachten können, eingreifen, pflegen und behandeln. Frischluftzufuhr muss gesichert sein, die Kranken sollen von den Gesunden getrennt werden.
Wände, Zwischenräume, Durchgänge und vor allem Durchblicke waren auch in der Militärschule, der École Militaire des Finanziers Pâris-Duverney in Paris genauestens geregelt. Die bewusst gefertigten Einrichtungen verfolgten einen vierfachen Zweck: Ausschweifungen sollten strikt unterbunden werden, ebenso wie Homosexualität, das Militär fügsam sein oder gemacht werden und schließlich sollten fähige Offiziere mit gleichsam kräftig gebauten Körpern herangezogen werden.
(vgl. Foucault 1995: 222ff.)

Die Disziplinarinstitutionen haben einen richtigen Apparat geschaffen, der beobachtet, registriert und dressiert.

> Der perfekte Disziplinarapparat wäre derjenige, der es einem einzigen Blick ermöglichte, dauernd alles zu sehen. Ein zentraler Punkt wäre zugleich die Lichtquelle, die alle Dinge erhellt, und der Konvergenzpunkt für alles, was gewußt werden muß: ein vollkommenes Auge der Mitte, dem nichts entginge und auf das alle Blicke gerichtet wären.
> (Foucault 1995: 224)

Doch zu viele Blicke treffen hier noch auf den/die ÜberwacherIn selbst, wie es der spektakuläre Machttyp des/der Souveräns/in bevorzugte, die Blicke sollen schließlich nur mehr auf die Überwachten gelenkt sein. (vgl. Dauk 1989: 118) Der Disziplinarblick hat die schwierige Aufgabe, eine Dichotomie zu vereinen. Einerseits sollte er in so viele Berührungspunkte wie möglich eingewoben sein, ständig präsent und lückenlos verteilt. Andererseits hat er so diskret wie möglich zu sein; nicht auffallend und dadurch hemmend, sondern fein und unbemerkt soll er seine Funktion ausüben, Leistungssteigerung als

Schlagwort. (vgl. Foucault 1995: 224f.) Die Idee des Panoptikums beruht auf ganz ähnlichen Überlegungen.[10]

So geschah auch in den Fabriken eine Umgestaltung im Bereich der Kontrolle. Die Spezialisierung der Überwachung wurde zu einem „unabdingbaren Bestandteil der Produktionsmittel." (Dreyfus/Rabinow 1987: 188) Eine Überwachung von „außen", bei der Inspektoren in gelegentlichen Rundgängen das Reglement durchsetzten, musste nach und nach einer „inneren" weichen, die in die Arbeitsprozesse integriert wurde. Nicht nur die Produktion, Rohstoffe und die Qualität von Produkten standen im Fokus der Aufmerksamkeit, vielmehr rückten Arbeitsabläufe, Verhalten und Fleiß der ArbeiterInnen in den Mittelpunkt. Sofort wirkte sich diese intensive und stetige Präsenz und Begleitung der AufseherInnen auch auf die Umgangsformen aus. Die KontrolleurInnen nahmen bald einen Befehlston an, gingen mit Härte und Strenge gegen die Masse vor. Fehler, Unfähigkeiten und Veruntreuungen der ArbeiterInnen sollten ausgemerzt werden, um Verluste an Gewinnen und am Kapital kleinstmöglich zu halten, Überwachung als ökonomischer Faktor.

Durch die steigende Quantität an Schulen und SchülerInnen zieht der hierarchische Blick auch in den Klassenräumen und der Erziehungstätigkeit ein. SchülerInnen wurden besondere Aufgaben zuteil. Sie unterstützten als „Offiziere" die Lehrkraft einerseits bei materiellen Tätigkeiten, wie Tinte und Papier austeilen, andererseits bei überwachenden Diensten. Einige Jahrzehnte später kommen zu den überwachenden Aufgaben auch didaktische hinzu.
(vgl. Foucault 1995: 225ff.)
Die Überwachung dient hier als pädagogische Methode ebenfalls einer kontinuierlichen Leistungssteigerung von innen heraus. Sie ist keine Erfindung des 18. Jahrhunderts, sondern kam schleichend, hervorgebracht und durchzogen von neuen Machtmechanismen. Mit diesen gemeinsam bildet sie eine integrierte, selbstständige, vielfältige und anonyme Disziplinargewalt.

> Denn die Überwachung beruht zwar auf Individuen, doch wirkt sie wie ein Beziehungsnetz von oben nach unten und bis zu einem gewissen Grade auch von unten nach oben und nach den Seiten. Dieses Netz ‚hält' das Ganze und durchsetzt es mit Machtwirkungen, die sich gegenseitig stützen: pausenlos überwachte Überwacher.
> (Foucault 1995: 228)

[10] Laut seinem Bruder kam Jeremy Bentham diese Idee erstmals bei einem Besuch der Pariser École Militaire.

Diese Maschinerie der Macht funktioniert. Auch wenn es in der Hierarchie ein Oberstes gibt, hängt die Macht nicht von ihm ab. Nicht der/die Akteur/in, die Organisation selbst lässt die Sache funktionieren. (vgl. Dreyfus/Rabinow 1987: 188)
Der ganze gediegene Apparat produziert Macht, verteilt die Individuen. So ist die Disziplinarmacht in sich widersprüchlich: Sie ist indiskret, indem sie sogar in den hintersten Winkeln und dunkelsten Schatten in Lauerstellung hockt, keinen übersieht, nicht einmal die Überwacher selbst. Und sie ist diskret, indem sie ganz verschwiegen und unbemerkt ihre gleichmäßigen Bahnen dreht, während sie auf die Körper zugreift. Sie baut sich nicht auf Ausschreitungen und Gewalt auf, funktioniert eher nach den geometrischen Grundsätzen von Optik und Mechanik und wird dabei umso weniger körperlich, je physikalischer sie ist. (vgl. Foucault 1995: 229)

Die Überwachung wird in die gesellschaftlichen Funktionen der Ökonomie, der Medizin und der Pädagogik integriert, die Kontrolle soll dabei immer leistungs- bzw. funktionssteigernd sein. So lässt sie sich in alle Bereiche der Industriegesellschaften einordnen, die sich mit Produktion befassen und deren Ordnung angetrieben werden soll. „Allein eine spürbare Überwachung (die mit Sanktionen droht) zwingt zur Sache. […] Individuen reagieren auf dieses Mittel und werden mit seiner Hilfe in Betrieb gehalten.“ (Dauk 1989: 119)
Der Überwachungszwang ist Grundbedingung eines „rein rationalen Verhaltens“ (ebd.). Er macht das Verhalten der Individuen, auf welche er einwirkt, formbar und verändert es antreibend und korrigierend, schlichtweg produktiv. „Die Vergleichbarkeit wird nur durch den überwachenden Blick aktiviert, der allerdings in zunehmendem Maße fiktiv wird. Die fiktive Beziehung zum Überwacher bewirkt dann das, was als Selbstkontrolle und Selbstdisziplin erscheint.“ (ebd.) Zugleich ist sie Motor des Produktionsapparates, weil sie zur Steigerbarkeit, zur Weiterentwicklung verleitet und sogar zwingt.

3.3.3.2 Die normierende Sanktion

Gemeint ist nicht diejenige Strafe bzw. Sanktion, die vom Justizapparat erfasst und auferlegt wird, sondern eine Strafe, die in Bereichen wirken soll, die zu fein für die Justiz ist und damit durch das allgemeine Strafgitter fallen würde.
So bildet sich gerade in Schulen, Kasernen und Manufakturen eine „Mikro-Justiz“ heraus, die eigene Gesetze, Formen und Instanzen birgt. Sie hat die Aufgabe das Verhalten, das von einer gewissen Norm abweicht, das für die großen Bestrafungssysteme aber nicht erfassbar ist, weil es versteckt und nicht schwerwiegend auftritt, zu sanktionieren. Sie greift bis in die kleinsten Bereiche der Zeit zur Bestrafung von Abwesenheit, der Tätigkeit zur Bestrafung von Ablenkung und Unaufmerksamkeit, des Körpers zur Bestrafung von Fehlhaltung und Unsauberkeit und der Sexualität zur Bestrafung von fehlendem Anstand. Als Sanktionen dienen kleine Demütigungen, Entziehungen und auch körperliche Züchtigung. Sie begleiten den Lern- oder Arbeitsprozess und entfalten sich, wenn ein Fehler begangen oder ein „natürliches“ Niveau, das man in einer bestimmten Altersklasse voraussetzen könnte, nicht erreicht wird. (vgl. Foucault 1995: 230f.)

Die Disziplinarstrafe arbeitet vor allem korrigierend. Viele solcher Strafen dienen Arbeitsabläufe zu verbessern, Übungen zu wiederholen, Lernen zu intensivieren. Auch heute soll die Strafaufgabe helfen nachzubessern, Abweichungen zu minimieren. Es geht nicht darum, das verletzte Gesetz zu rächen, sondern um eine Einschärfung des gebrochenen Reglements, um das Dressieren und Abrichten.
Nicht nur negative Sanktionen spielen im Disziplinarsystem eine Rolle. Auch positive, also Belohnungen werden vergeben. Dadurch macht sich ein Spektrum breit, in das von den guten bis zu den schlechten alle SchülerInnen in beliebiger Abstufung eingeteilt werden können. Nicht wie in der Strafjustiz, die nur Straffällige notiert, werden hier alle Individuen erkannt und durchschaut und sogar zueinander hierarchisiert. Die Disziplinarmacht geht so weit, dass sie die Individuen belohnt und bestraft, indem sie diese in den Rängen auf- und absteigen lässt.
Die Disziplinarmacht ordnet hier die Individuen nach ihrem Verhalten, der Tauglichkeit und bereits für eine spätere Verwendung innerhalb der Gesellschaft. Andererseits will sie ihnen stetigen Druck auferlegen, sich zu bessern und sich einer Einheitsnorm anzugleichen. Sie bestimmt Normen und will die Individuen normalisieren. Sie nimmt gewisser Maßen auch

Einfluss auf größere gesellschaftliche Apparate wie die Strafjustiz oder das Gesundheitswesen. Das Normale wird zwingend für das Individuum. (vgl. ebd.: 232ff.)

„Diese Zwangsgewohnheiten bringen das hervor, was als Norm gelten wird und etablieren damit allererst das ‚Soziale' als Normalität." (Dauk 1989: 120) Erst nach der Festsetzung dieser „normalen Gewohnheiten" steigt dann der humanwissenschaftliche Diskurs ein, der diese Normen begründet, charakterisiert und spezifiziert. Normalität wird zum Abrichtungsmechanismus. Die Leitlinie ist die Regel, wer davon abweicht, wird bestraft. Die Norm, die zugleich das moralisch Gute darstellt wird durch Dressur (beispielsweise langes Üben) eingeprägt. Die Individuen entwickeln aufgrund einer möglichen Belohnung den Ehrgeiz, gut, besser, angepasst und anerkannt zu sein. Auf einer Skala, die sich zwischen den Polen einer Norm, dem Paar gut-schlecht auftut, lassen sich die Individuen sortieren und ihre Daten erheben. Auf die Individuen wird ein Druck ausgeübt, sich aneinander anzugleichen. Eine Ordnung entsteht, die bestraft, wiederum ist es die Strafe, die ordnet. Eine besondere Eigentümlichkeit dieser Ordnung besteht darin, dass die hinteren Plätze der Skala selbst wie Sanktionen agieren. (vgl. ebd.: 120f.)

3.3.3.3 Die Prüfung

Die Prüfung ist das, was die beiden vorangehenden Instrumente der Überwachung und der normierenden Sanktion am stärksten kombiniert. Sie verbindet moderne Formen von Macht und Wissen in einer einzigen Technik.
„Die Prüfung verzahnt die Techniken der Überwachungsbeziehung mit den normierenden Strafmechanismen und setzt mit dieser Kupplung die Korrektur des faktischen Individuums zum normalen hin in Gang." (Dauk 1989: 124) Hauptsächlich beruht die Durchschlagskraft der Disziplin auf diesem simplen Mechanismus. Die Prüfung, die in diversen Institutionen stark ritualisiert verankert ist, schafft es, Individuen sichtbar zu machen. Der Vergleich mit einer Fotographie liegt nahe, bei der das Individuum für einen kurzen Augenblick sich selbst und allen anderen erhellt wird, dokumentierbar, übertragbar und angreifbar für Urteile. (vgl. ebd.)

Zum einen kann die Disziplin darin ihre Stärke und Macht demonstrieren, zum anderen wird formal ein bestimmtes Wissen und eine Wahrheit manifestiert. Durch die Machtbeziehungen

wird hier ein Wissen geformt und „überprüft“. Dieses Wissen ist politisch besetzt, da es nicht bloß darum geht zu wissen, sondern immer auch impliziert, dass dieses Wissen etwas ermöglichen kann und soll. (vgl. Foucault 1995: 238f.)
Durch die ständige Überprüfung von Kranken in Spitälern kristallisierte sich der Beruf KrankenpflegerIn, Krankenschwester erst heraus. Es formierte sich ein detailgetreues Wissen über Kranke und Verletzte, deren Untersuchung und Heilung, das die Medizin wissenschaftlich bzw. epistemologisch machte. Das Haus der Fürsorge wurde zu einem „Ort der Erkenntnisbildung und -übertragung“ (ebd.: 240).
Andererseits ist die Schullaufbahn mit Prüfungen gespickt. Bisher diente die Prüfung als Abschluss für eine Lehre, der zu diesem Zeitpunkt lediglich zeigen sollte, dass eine Wissensübermittlung stattgefunden hatte. Nun aber kann der/die LehrerIn ständig erheben, welches Wissen von den SchülerInnen angenommen wurde und kann selbst ein Netz von Erkenntnissen über die SchülerInnen knüpfen. Die Pädagogik als Form der Wissenschaft entsteht. (vgl. ebd.: 239ff.)

Welche Kennzeichen und Unterscheidungen zu anderen Formen der Machtausübung machen nun die Prüfung aus?
Noch im 16./17. Jahrhundert der traditionellen Macht sollte jegliches Licht auf den Herrscher, die Herrscherin fallen. Die Subjekte durften sich in seinem/ihrem Glanze um die wenigen verirrten Strahlen streiten bzw. bekamen sie nur soviel davon ab wie der/die HerrscherIn ihnen zugestand. In der Disziplinarmacht sollte sich das umkehren. Die Individuen sollen zu sichtbaren Objekten gemacht werden, die Disziplinargewalt selbst im Dunkeln bleiben. (vgl. Dreyfus/Rabinow 1987: 189) Durch die ständige Möglichkeit gesehen werden zu können, werden die Individuen unterworfen, objektiviert, zugerichtet und im Raum der Macht verteilt. Die Prüfung dient als Zeremonie genau dieser Visualisierung und Objektivierung. (vgl. Foucault 1995: 241ff.)

> Examen und Tests erlauben nun eine neue Form von Statistik, die individueller Leistungen, aufgetragen auf einer Zeitachse. Die Entwicklung des Individuums wird objektivierbar: eine ungeheure Sammlung empirischer Daten beginnt (wobei das Empirische dem künstlichen Testfeld entnommen ist), die schließlich in den modernen Datenbanken gipfeln (wo sie jederzeit für beliebige Zwecke abrufbar sind).
> (Dauk 1989: 130)

Ein weiteres Kennzeichen der Prüfung ist, dass sie aus jedem Individuum, einen dokumentierbaren Fall mit all seinen Eigenschaften, Maßen, Beschreibungen und Bemessungen macht. Unzählige Daten und Dokumente werden registriert und gespeichert und beschreiben den Menschen in seiner Individualität. So wohnt es einer „Schriftmacht" inne, unter anderem genauestens zu dokumentieren, wofür ein gewisser Soldat sich eignet, Verwundete und Tote zu zählen, in Spitälern Genesungsverläufe und Entwicklungen zu erfassen und Bilanzen zu ziehen und in Schulen Fortschritte und Eignungen der SchülerInnen festzustellen. In Feudalsystemen war es noch ein Privileg von KönigInnen und Adeligen, wenn Lebens-, HeldInnengeschichten und Stammbäume über sie kundgetan wurden, sie individualisiert wurden. Später waren es eher Abnormale, Kranke, Wahnsinnige, Delinquente, deren Biographie interessierte und die man zu erforschen suchte. Anstatt der Erinnerungsberichte sollten Beobachtungen notiert werden, anstatt einer pompösen Zeremonie sollte still und heimlich überwacht werden. „Die Akte ersetzt das Epos." (Dreyfus/Rabinow 1987: 190) Der einzelne Fall sollte nicht nur detailliert aufgenommen, sondern auch korrigiert und normalisiert werden. Die Individualität dient der Beherrschung und Kontrolle. Gerade die Prüfung ist die Form, die die Individualität besonders herausstreicht und den Menschen auf seiner persönlichen Einzelheit fixiert.

Durch diese Wirkungsweisen konnte sich allmählich eine Disziplinarmacht durchsetzen, ein neuer Zugriff auf die Körper. Die Prüfung konstituiert Individuen als Wirkungen und Objekte von Macht und Wissen. (vgl. Foucault 1995: 246ff.) Der Körper des Individuums ist das Objekt der Erkenntnis, zugleich wird er subjektiviert, was zwei Bedeutungen hervorhebt: zum einen die Vereinzelung und Individualisierung, zum anderen die Unterwerfung unter das System. (vgl. Dauk 1989: 125)

Eine strikte Buchführung dieser Daten ermöglichte auch eine statistische Verwertung.

> Der ans Examen angeschlossene Aufzeichnungsapparat ermöglicht so nicht nur die Konstitution des Individuums als analysierbaren Gegenstand, sondern auch den Aufbau des Vergleichssystems. Das Individuum tritt in das Feld des Wissens und die Einzelbeschreibung in den Betrieb des wissenschaftlichen Diskurses ein.
> (Dauk 1989: 125)

Gruppen und kollektive Tatbestände werden charakterisiert, Abweichungen der Individuen von der Regel festgestellt und diese in der Gesellschaft verteilt. Es entstand eine Wissenschaft vom Menschen, vom Individuum.[11] (vgl. Foucault 1995: 243ff.)

Diese modernen Wissenschaften benötigen, generieren, deuten und archivieren Daten, „um die Gegenstände ihrer jeweiligen Disziplin zu konstituieren und zu kontrollieren." (Rammert 2007: 21) Dinge und Phänomene sollen fixiert und zu methodisch geprüften Fakten verwandelt werden.
Die Wissenschaften greifen dabei selbst auf eigene Disziplinarpraktiken zurück. Im Verfahren der Prüfung verbinden sich die „Erzeugung und Kontrolle des Wissens, Überwachung und Anpassung der Geprüften an die gegebenen Wissensstandards" (Fink-Eitel 1989: 78).

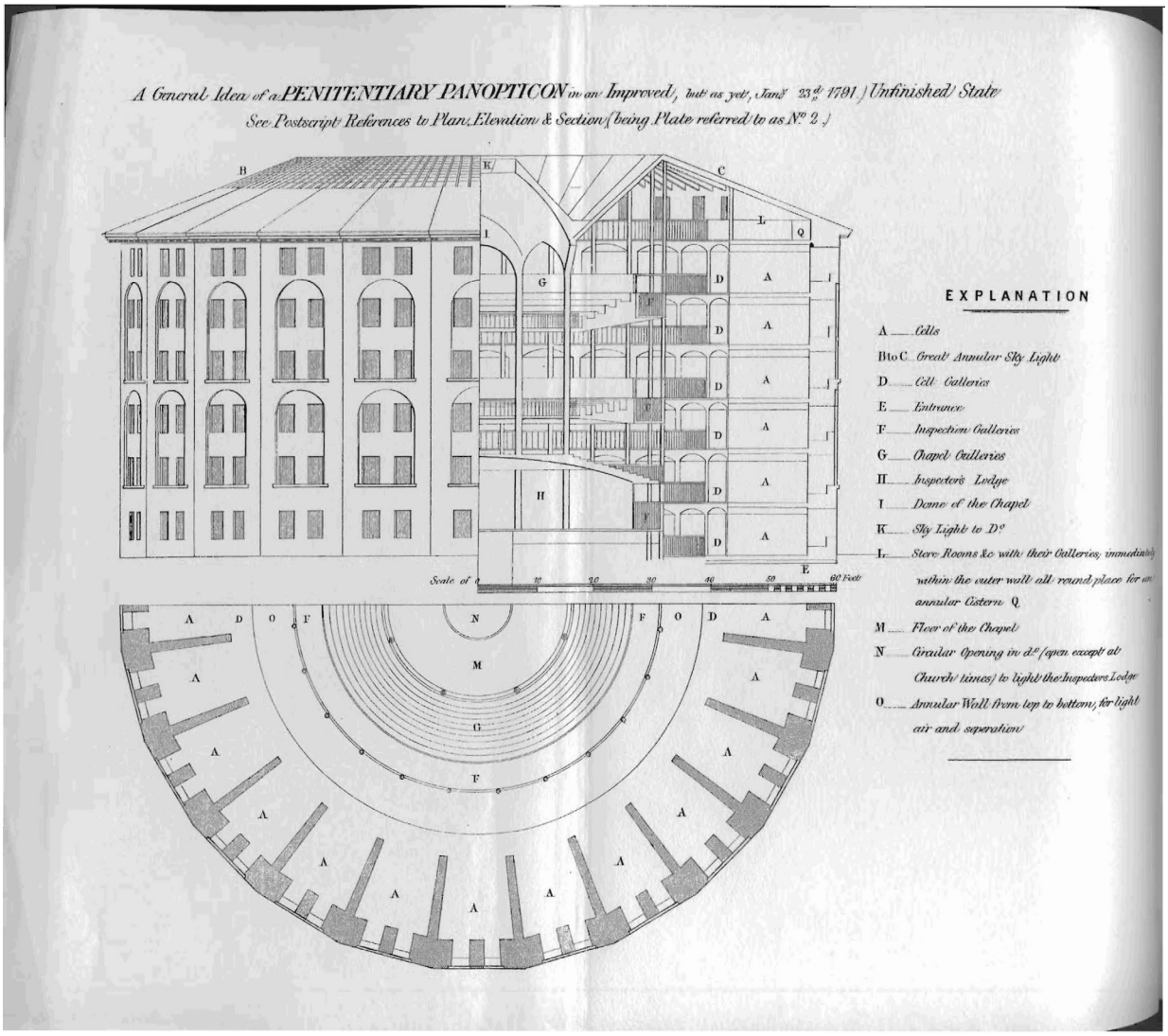
3.3.4 Das Panoptikum

Jeremy Bentham lieferte 1787 die Idee des Panoptikums, eine architektonische Überwachungsmaschine, die zugleich wegsperren, kontrollieren und modifizieren sollte, ein konkretes Beispiel dafür, wie Macht funktioniert. Um einen Überwachungsturm wurden ringförmig Zellen angeordnet, die sowohl zum Turm hinweisend als auch an der Außenwand, große Fenster installiert hatten. Damit waren diese Zellen durchleuchtet, jede Bewegung der individualisierten und stets sichtbaren Insassen konnte vernommen werden, während diese selbst in den verdunkelten Turm keinen Einblick hatten und nicht erkennen konnten, ob, wer und wie viele Personen sie gerade beobachteten. Der Gefangene „ist Objekt einer Information, niemals Subjekt in einer Kommunikation." (Foucault 1995: 257) Die Zellen zueinander waren durch dicke Mauern getrennt, sodass es keine Absprachen der Zelleninsassen untereinander geben konnte, keinen schlechten Einfluss, keine Fluchtpläne. Diese Architektur des Panoptikums sollte nach Bentham nicht nur auf Gefängnisse angewendet werden, wenn dies auch sein Paradebeispiel war, sondern auch auf andere Institutionen wie Hospitäler, Schulen, Arbeitsstätten. Hier dienten die Trennwände zur Eindämmung von Keimen, dem Schutz vor Zerstreuung sowie der Vermeidung von

[11] Ein sehr treffendes Beispiel wäre die Entstehung der Pseudowissenschaft Anthropometrie, die aufgrund biologischer Merkmale VerbrecherInnen von NormalbürgerInnen unterscheiden zu können glaubte. Regelhaftigkeiten wurden angenommen und Abweichungen sichtbar gemacht. Man träumte von präventiver Sozialhygiene. (vgl. Feyerabend Erika 2002)

Unfällen und Schlägereien; als Aufreihung abgeschotteter Individuen. (vgl. Bentham 1791: 40ff.)

Abbildung 1: Plan für das Panopticon



Quelle: (Bentham 1995: 172)

Somit war ein Gebäude, eine Maschine geboren, die ein unglaublich steiles hierarchisches Gefälle auftut. Die Macht funktioniert hier immerwährend in seiner kühlen Architektur, es ist egal wer überwacht und aus welcher Absicht, - es sollen auch Inspektoren und Besuchergruppen ins Panoptikum eingelassen werden, die dann auf einen Blick, den herrschenden Zustand erfassen, sowohl die Überwachten wie auch die ÜberwacherInnen beobachten, somit soll das Panoptikum demokratisch kontrolliert sein - die InsassInnen können sich dessen nie bewusst sein und passen aus Angst vor einer jederzeit möglichen Beobachtung das Verhalten dem wirkenden Reglement an. Ruhe, Eifer und Befolgung der

Anordnungen werden mechanisch, unkörperlich und gewaltarm umgesetzt, man bedarf keiner Ketten und Gitter mehr. Dadurch ist das Panoptikum ein sehr ökonomischer Betrieb, denn durch die asymmetrische Verteilung[12] der Blicke reicht ein geringer Bestand an Personal. Neben diesem Effekt der sparsamen Disziplinierung kann das Panoptikum einem weiteren Zweck dienen: hier lässt sich hervorragend experimentieren, dressieren, beobachten und registrieren wie in einem Labor. Man kann an Kranken Arzneien austesten und die Ergebnisse protokollieren, man kann an Gefangenen verschiedene Bestrafungen versuchen, man kann die Einführung neuer Verfahren und Techniken an SchülerInnen überprüfen und bewerten. Wissen breitet sich aus und eröffnet neue Erkenntnismöglichkeiten. (vgl. ebd.: 44ff.)

Dieses „wissenschaftliche Gefängnis" schafft es in einem, sowohl die Macht wie auch die Produktion, sei es Besserung, sei es mehr Output, zu steigern. Dabei lässt die Möglichkeit einer steten Überwachung die bevorzugten Handlungsweisen bereits präventiv einsetzen, was wiederum die Anzahl der ÜberwacherInnen auf ein Minimum beschränken lässt.
Benthams Idee eines Panoptikums war auch stets politisch technologisch gefärbt. Es sollte nicht nur im geschlossenen Rahmen Verwendung finden, sondern diente als verallgemeinerungsfähiges Modell.

> [I]t will be found applicable, I think, without exception, to all establishments whatsoever, in which, within a space not too large to be covered or commanded by buildings, a number of persons are meant to be kept under inspection.
> (Bentham 1791: 40)

Das Gefängnis ist zugleich der Ort, an dem Strafen vollzogen sowie die bestraften Individuen beobachtet werden; einerseits natürlich überwacht und andererseits sollten die Individuen hier erkannt und ihr Besserungsverlauf dokumentiert werden. „Das Gefängnis ist der Ort, an dem sich ein klinisches Wissen über die Sträflinge formiert. […] Der Gedanke des Panopticon […] hat im Gefängnis seinen bevorzugten Realisierungsort gefunden." (Foucault 1995: 319)

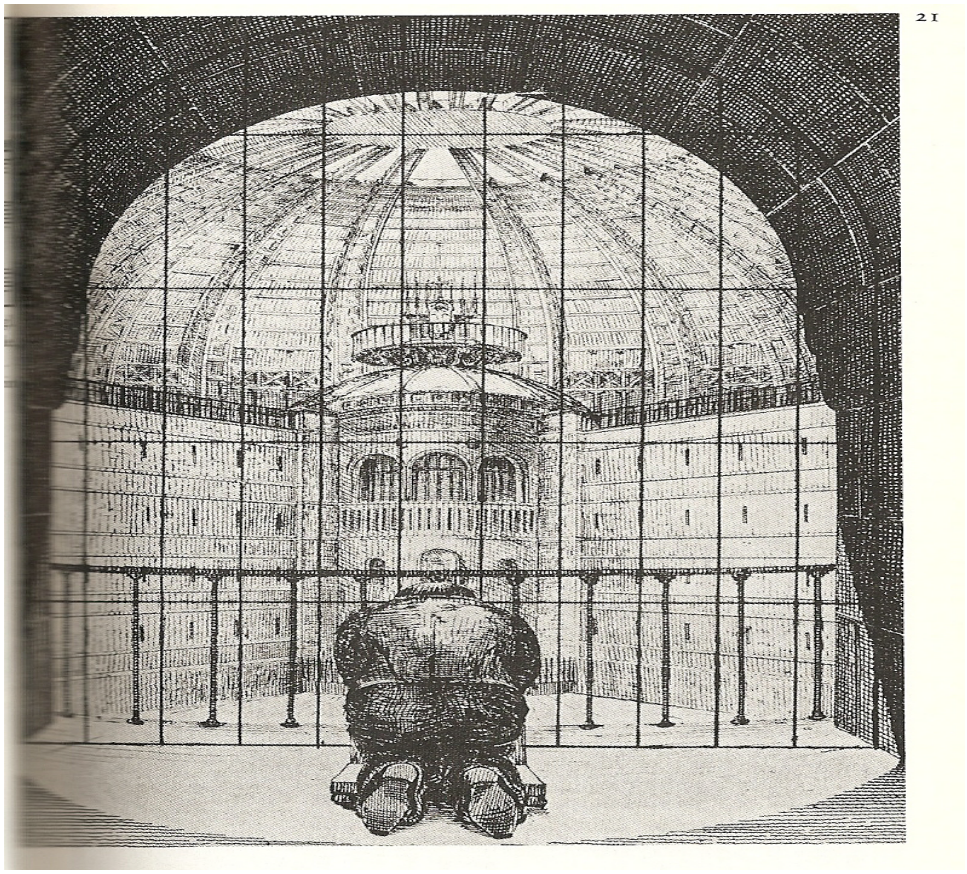
Foucault will mit diesem Modell von Bentham das „Kräftediagramm der Disziplin" (Dauk 1989: 127) aufzeigen. Jede/r kann Macht ausüben. Sie wird entindividualisiert, anonymisiert, strukturell und automatisiert.

[12] Sogar ein akustisches Abhörsystem sollte eingerichtet werden, war aber technisch nicht umsetzbar.

3.3.5 Panoptismus als Selbstdisziplinierung

Der Panoptismus ist eine abstrakte Machtform, die die Überwachten selbst zu ihren Überwachern macht, die Überwachung wird dadurch lückenlos und bleibt ständig aufrecht erhalten. Er hat in der Architektur des Panoptikums nur eine seiner Realisierungsformen, wenn auch eine konkrete und ideale gefunden. Er ist dabei eng verknüpft mit dem Wissen über die Entwicklung der Individuen, „genauer: von deren Angleichung an die disziplinären Erfordernisse“ (Dürr 2004: 59). Die Individuen werden durch ein Wissen markiert, das ihren Abstand bzw. ihre Nähe zu einer bestimmten disziplinären Norm misst. Der Panoptismus „sorgt dafür, dass sich die Aufmerksamkeit der Individuen auf sich selbst richtet, und dass bei ihnen eine Selbstproblematisierung entlang disziplinärer Normen und Regeln einsetzt“ (ebd.). Damit haben wir eine Verschiebung: der/die ÜberwacherIn wird unwesentlich, die Häftlinge üben selbst an sich diese Funktion aus. „Die Taktik der Disziplinarmacht besteht also darin, Verhalten überschaubar, vorhersehbar und objektivierbar zu machen.“ (ebd.: 70)

Abbildung 2: N. Harou-Romain, Plan für Strafanstalt, 1840. Ein Häftling verrichtet in seiner Zelle sein Gebet vor dem zentralen Überwachungsturm.



Quelle: (Foucault 1995: Bild 21)

Foucault überträgt das Konzept des Gefängnisses mit der Technik der Selbstdisziplinierung auf moderne Gesellschaften. Während die Ordnung in der verpesteten Stadt noch auf Leben und Tod reduzierend wirkte, sollte sie nun erhöhend und verstärkend sein. Sie sollte die Gesellschaftskräfte steigern, Bildung, Gesundheit, Wirtschaft und Moral anheben und sich vor allem auch auf den gesamten Gesellschaftskörper ausdehnen. „Das Panopticon liefert die Formel für diese Verallgemeinerung." (Foucault 1995: 268) Ganz subtil sollten die Disziplinarsysteme in die Gesellschaft eingeflochten werden und kaum bemerkbare Zwänge in dieser Disziplinargesellschaft etablieren. Die Menschen im öffentlichen Raum fügen sich somit einem vorgestellten oder realen Konformitätsdruck und „handeln entsprechend der internalisierten Erwartungen an sie." (Weber 2008: 294f.)

Foucault geht hier auf Nietzsche zurück, der in seinem 1887 erschienenen Werk *Zur Genealogie der Moral* moralische Normen durch die Instanz des persönlichen Gewissens und Schuldbewusstseins verinnerlicht und kontrolliert sah. Durch Jahrhunderte lang währende äußere Gewalt in Form brutaler Strafen bildete sich ein Gedächtnis, welches das Gewissen bei jeder möglichen oder bereits geschehenen Übertretung einer sozialen, moralischen Norm eine innerliche Sanktion bzw. Selbstbestrafung ausführen lässt. (vgl. Fink-Eitel 1989: 70f.) Moral dient „als Werkzeug innerer Disziplinierung und Normalisierung des Menschen" (ebd.: 74).

Wenn die Disziplin die Individuen entlang der Linie der Arbeit verteilte, „so hat der endlos verallgemeinerungsfähige Panoptismus die Vervielfältigung solcher Achsen hervorgebracht." (Dauk 1989: 129) Er ist eine Machtform, die sich auf das gesamte Leben der Individuen erstreckt, er durchdringt alle Lebensbereiche, steigert sie, kontrolliert sie. Es gelingt das „Kunststück, die Individuen einzeln und als Masse in ein Normierungsnetz einzuspannen, in dem diese selbst die Normierungen in Vergleichung mit den anderen für sich übernehmen und die Normalisierung vorantreiben." (Dauk 1989: 129)
Ein Verhalten, das sich einer fremden Erwartungshaltung anpasst, ist aber der Vorstellung einer liberalen Gesellschaft konträr.

> Noch einmal abgebildet auf jenes Gefüge von Wissen, Erwartungen, selbstbestimmtem Verhalten, heißt dies: wenn ich *immer schon* erwarten muss, dass andere Leute mehr, anderes über mich wissen, als ich eigentlich, nach den üblichen, traditionellen Konventionen und Vorstellungen erwarten können sollte und erwarten wollte, dann kann

> mein Verhalten *immer schon* daraufhin gespielt sein: dann ist mit solcher Verletzung informationeller Privatheit *immer schon* eine Perspektivenverschiebung verbunden, so dass ich gezwungen bin, auf mich und mein Verhalten eine Perspektive einzunehmen, die ich, aus je nach Kontext unterschiedlichen Gründen, nicht einnehmen will oder die ich nicht einnehmen wollte und die einzunehmen ich mich mittlerweile - selbstverständlich, permanent - gewöhnt habe.
> (Rössler 2001: 221)

In Gesellschaften mit allgegenwärtiger Medienpräsenz besteht ein hohes Potential für gegenseitige Überwachung, die zu Veränderungen im Verhalten und Selbstdisziplinierung führen kann. Interaktive Kommunikationsstrukturen setzen aber nicht wie bei Benthams Modell auf ein hierarchisches Gefälle a priori, so Heesen, sondern es sind Möglichkeiten zur „gegenseitigen Kontrolle“ (Heesen 2008: 237) gegeben. Transparenz kann somit in den Vordergrund treten, es muss nicht zwingend Fremdbestimmung sein.

3.3.6 Die panoptische Gesellschaft

Doch wie kam es zu dieser schleichenden Umwälzung? Warum rückten derartige Institutionen vom Rand der Gesellschaft in deren Mitte? Denn Benthams Panoptikum diente, wenn auch sehr utopisch, als Vorlage für zahlreiche Projekte.[13]
Die Ausweitung der Disziplinartechniken auf die Gesamtgesellschaft hatte sehr verborgene Gründe und Vorstufen:
(vgl. Foucault 1995: 263ff.)

Im 18. Jahrhundert ist ein starker Bevölkerungsschub zu bemerken. Absolutistische, souveräne, feudale Machtformen können dieser großen Bevölkerungszahl, darunter viele Nomaden und der damit verbundenen gesteigerten, kostspieliger werdenden Produktionskraft nicht mehr Herr werden. Ein neues Disziplinarsystem entwickelt sich, das wie jedes Machtsystem grundsätzlich darauf abzielt, die Vielfältigkeit der Menschen zu ordnen. Die spezifischen Charakteristika an den Disziplinen sind fünferlei:

- Kosten, die bei der Durchsetzung der Macht entstehen, sollen möglichst gering gehalten werden, sowohl im wirtschaftlichen Sinne durch geringe Ausgaben, wie auch im politischen durch Unauffälligkeit, geringen Widerstand, usw.

[13] Es wurde aber nicht in seiner theoretisch entworfenen, idealen Form Eins-zu-eins umgesetzt.

- Die Wirkung der Macht soll intensiv und lückenlos auf den ganzen Gesellschaftskörper ausgedehnt sein.
- Die Effizienz der Macht soll sich diskret auf medizinische, militärische, industrielle und pädagogische Einrichtungen und Apparate übertragen.
- Die Unterworfenen sollen deutlich sichtbar gemacht werden.
- Alle, die mit dem System in Berührung kommen, sollen in sein Funktionieren miteinbezogen werden. (vgl. Dreyfus/Rabinow 1987: 224)

„Es gilt also gleichzeitig die Fügsamkeit und die Nützlichkeit aller Elemente des Systems zu steigern." (Foucault 1995: 280) Im Vordergrund stehen Produktivität und ihre Steigerung, Wertschöpfung und Ausnutzung. Die Disziplinen versuchen unüberschaubare Vielfältigkeiten handlicher, einheitlicher zu machen, Regeln zu schaffen, festzusetzen und horizontale Verbindungen zu verhindern, die zu Aufständen und Organisationen führen können. Dadurch führen sie ein hierarchisches System ein, versuchen die Individuen abzuschotten.
Von den unterworfenen Subjekten bildet sich ein getreues Wissen, die Machtausübenden werden vergegenständlicht. (vgl. ebd.: 279ff.) Diese Form der Disziplinargewalt kam als Modell für verschiedene Institutionen und politische Regimes, nicht nur für das kapitalistische, in unvermeidlich abgeschwächter Form zum Tragen und ging allmählich auch über deren Grenzen hinaus. „Ihre beeindruckendsten Erfolge hatten die Disziplinarmaßnahmen in jenen Gesellschaftsbereichen, denen Integration von Produktion, Nutzen und Kontrolle oblag" (Dreyfus/Rabinow 1987: 225).

Die Disziplinen, die früher vorrangig einen negativen Nutzen zu erfüllen hatten im Sinne von Wegschließung von Gefahren, Ausgrenzung erhielten einen zweiten, positiven: Sie sollten auch erziehen, errichten, züchten, nutzbar machen. Beispielsweise wurden die Elementarschulen anfangs eingeführt, um Unwissenheit, Müßiggang und Bettlerhorden vorzubeugen. Im späten 18. Jahrhundert, zu Beginn der Revolution begann sich das Verständnis zu ändern: Die Kinder sollten für die Zukunft kräftige, gesunde Körper antrainieren und Fertigkeiten und Kenntnisse für die spätere Arbeit erwerben. Somit gelangten die Disziplinen in die zentralen, produktiven gesellschaftlichen Bereiche, dehnten sich auf die Institutionen aus und disziplinierten bereits vorhandene.
Ein weiterer Schritt war, dass sich die Disziplinen von den Institutionen auf das Umfeld derer auszuweiten und frei zu wirken begannen. Nicht ausschließlich wurden schlechte

SchülerInnen gemaßregelt, auch bei deren Eltern und NachbarInnen wurde nachgefragt, kontrolliert und überwacht, wie es soweit kommen konnte und was diese selbst nicht „falsch“ machen würden. Kleinere Spitäler sollten ambulante Hilfe für die BewohnerInnen der umliegenden Zone anbieten, Informationen über sie sammeln und an Autoritäten weitergeben. Religiös motivierte Mildtätigkeitsvereine gaben sich selbst die Aufgabe, wirtschaftlich zu unterstützen und politisch beruhigend zu handeln, indem sie die Armen in ihren Territorien besuchten und nachforschten, wie es um deren Lage bestimmt war oder auch dubiose Gaststätten mit einem moralischen Auge inspizierten. (vgl. Foucault 1995: 263ff.)
Auch die Delinquenz schien als geeignetes Mittel, die Überwachung von den Gefängnissen auf den gesamten Gesellschaftsapparat hinauszutragen. Entlassene Häftlinge können durch ihre Verwebungen mit dem Gefängnis nach wie vor leicht kontrolliert werden. Durch die Erschwernisse einer Resozialisierung können ihnen leichter Aufgaben im Spitzelwesen oder im Denunziantentum angetragen werden. Indem es ehemalige StraftäterInnen in Kontakt miteinander bringt, unterliegt bald eine ganze Gruppe bzw. ein geschlossenes Milieu von DelinquentInnen der Überwachung. (vgl. Foucault 1995: 362f.)
„Ohne Delinquenz gibt es keine Polizei.“ (Foucault 1976b: 40) Das ist der Grund, weshalb die Delinquenz unter anderem auch nützlich ist. Erst sie macht es ertragbar, dass bewaffnete Uniformierte sich mitten unter die Bevölkerung mischen können, sie kontrollieren und überwachen. Die Angst vor der Delinquenz legitimiert den Polizeiapparat. (vgl. auch Foucault 1976d: 50)

Der Panoptismus kam als dunkle Seite der Aufklärung neben einem egalitären, kodifizierten Rechtssystem. Die Disziplinen sollten dem Anschein nach die Verlängerung und Verästelung des Rechts bis in die kleinsten Zwischenräume sein. Während das Recht aber nur seiner Form nach besteht und gleiche Rechte garantiert, sind es die Disziplinen (neben den Klassen), die die Ideale eines Rechtssystems gleichberechtigter Individuen unterschreiten, ein hierarchisches, asymmetrisches Gefälle einrichten, die Körper und Kräfte unterwerfen und sogar als eine Art Gegenrecht fungieren. Der Panoptismus ist ein Zwangsverfahren, das die vertraglich abgesicherten formellen und rechtlichen Freiheiten auflöst und von unten her die Rechtsstrukturen einer Gesellschaft bearbeitet und somit die wirklichen Machtmechanismen walten lässt. Das Recht wurde der Normalisierung geopfert. (vgl. Dreyfus/Rabinow: 1987: 226)

Vor allem den armen Klassen sollte beim Übergang vom Gewohnheitsrecht zum Strafgesetzbuch eine „Grundgesetzlichkeit“ eingeimpft werden, sie sollten moralisiert werden. So gab ihnen der Apparat der Strafjustiz gewisse Regeln, die sie zu verinnerlichen hatten, auf die sie regelrecht abgerichtet wurden, wie die Sesshaftigkeit, den Arbeitsgehorsam oder aber die Grundregeln des Eigentums und des Sparens. (vgl. Foucault 1995: 368)
Wie der L’Atelier schreibt: „Keine andere Klasse ist einer ähnlichen Überwachung unterworfen; diese Überwachung ist fast mit der gleichzusetzen, die an den entlassenen Häftlingen praktiziert wird; sie scheint die Arbeiter in die Kategorie der sogenannten gefährlichen Klasse einzuordnen.“ (L’Atelier, 5/6, März 1845 zitiert nach Foucault 1995: 369)

Das Disziplinarsystem sichert einem Individuum eine richtige Disziplinar-Ausbildung zu, stets begleitet von einer kontrollierenden Institution und in seiner Kanalisation gefangen: ein Findelkind sollte in einer Kleinkinderbewahranstalt oder in einem Asyl unterkommen, von da geht es in die Schule, sollte es nicht arbeiten können, wird es von einem Wohltätigkeitsbüro aufgenommen, ist es krank, kommt es in ein Spital, im Alter kommt es in ein Altersheim, nach begangenen Verbrechen in eine Strafanstalt wie das Gefängnis. Somit nimmt sich diese panoptische Gesellschaft auch derer an, die es aus- bzw. einzuschließen scheint. Von Anfang an steht das Individuum im Kraftfeld des verallgemeinerten panoptischen Systems, züchtigende Mechanismen tun sich auf, Disziplinarzwänge werden versammelt, es wird straff eingegliedert und überwacht. (vgl. Foucault 1995: 388f.)

Die Disziplinen gehen dabei einerlei mit einem wissenschaftlichen Fortschritt. Durch verfeinerte Machttechniken eröffnen sich neue Wissenschaften vom Menschen wie die klinische Medizin, die Psychologie, die wiederum durch die vermehrten Kenntnisse die Machtwirkungen zu vervielfältigen wissen. Foucault vergleicht die Disziplinen und die Prüfung mit der „Erfindung“ der Inquisition im 12./13. Jahrhundert und ihrer Methode der Untersuchung, die die Wissenschaften von der Natur begünstigten. Langsam drang die Disziplinarprüfung von unten in die juristische Untersuchung, die ihren Ursprung in der Inquisition fand, ein und änderte sie ab. (vgl. ebd.: 279ff.)

Foucaults Thesen sind als Warnung zu verstehen, denn die Bedrohlichkeit eines Panoptismus, der totalen Überwachung und Kontrolle, die im heutigen Zeitalter dank elektronischer Datenverarbeitung näher scheint denn je, wirkt in Händen eines totalitären, autoritären Regimes wahrlich Furcht einflößend. Doch auch Demokratien sind nicht gefeit vor einer Macht, die sich subversiv zum Recht lautlos über den gesamten Gesellschaftskörper erstreckt und je mehr Wirkung entfaltet, je verborgener und unsichtbarer ihre Praktiken fungieren, sodass „wir für unsere ureigenste Subjektivität halten, was in Wahrheit Produkt disziplinierender und normalisierender Macht ist.“ (Fink-Eitel 1989: 79)

3.3.7 Die Rolle der Polizei im panoptischen System

Die Polizei hat für Ordnung und Sicherheit zu sorgen und Gefahren für diese abzuwehren. Sie ist an die Weisungen der Staatsanwaltschaft gebunden, vermitteln für diese. Für die Umsetzung ihrer Aufgaben darf die Polizei auch zu Zwangsmitteln greifen, solange sie sich an gesetzliche Befugnisse hält, beispielsweise Durchsuchungen oder Verhaftungen. Sie ist für die Gewährleistung von Sicherheit darauf angewiesen, Daten zu ermitteln. (vgl. Schaar 2007: 149) Dabei entzieht sich die Polizei teilweise der demokratischen Kontrolle, da sie Strukturen und Abläufe intransparent hält. Sie argumentiert, dass dies eine Voraussetzung für ihr zielorientiertes Handeln wäre. (vgl. Lemke 2008: 167ff.)

Die Idee, an den Justizapparat ein Überwachungsorgan zu koppeln, entstand im 18. Jahrhundert, weil man dachte, dass nicht die Grässlichkeit der Strafen, sondern ihre Gewissheit in den Vordergrund treten sollte. Jedem Verbrechen, jedem Vergehen sollte mit Sicherheit seine ihm zugeordnete Bestrafung folgen. Um die Hoffnung zu tilgen, einer Strafe aufgrund mangelnder Aufklärung des Verbrechens zu entrinnen, musste man nicht strenger und brutaler agieren, sondern wachsamer. (vgl. Foucault 1995: 122f.)
Der Polizeiapparat war zu Zeiten einer souveränen Gewalt an ebendiese gebunden. Er war der verlängerte Arm, der die gesellschaftliche Disziplin zu gewährleisten hatte, ein zentralisiertes Organ, das bis in die kleinsten Schaltstellen Macht ausübte und das den Willen und die Willkür der absoluten Gewalt zu übertragen und auszuführen hatte.
Diese Verstaatlichung der Disziplinarmechanismen in Form der Exekutive hatte zur Folge, dass ihr Netz ausgeweitet wurde, es erfasste nun den Raum zwischen den geschlossenen

Institutionen wie Schulen und Krankenhäuser und wirkte kontrollierend und so unsichtbar wie möglich bis in die Poren der Gesellschaft als „Interdisziplin und Metadisziplin“ (ebd.: 276).
Jede Handlung, jede Meinung, jede Verhaltensweise sollte erfasst werden. Die Polizei war als Staatsapparat zwar an die politische Macht angebunden, entwickelte aber schnell eine Eigenart in ihrer Ausübung. Mit vielen Augen und Aufmerksamkeiten will sie den Gesellschaftskörper durchdringen. Dabei folgt sie nicht nur einer Richtung von oben, also dem Willen des Souveräns, sie hat auch Ansuchen von unten nachzugehen, wenn beispielsweise NachbarInnen oder PfarrerInnen Personen wegen Ruhestörung oder etwaigen Ungehorsams anzeigen. Anders als im Justizwesen wird bei der Polizei jedes Abweichen von der Norm, jede Auffälligkeit registriert und protokolliert und anders als die Justiz ist sie viel enger mit der Disziplinargesellschaft verstrickt, wobei sie die Funktion einer Disziplinierung nicht absorbiert und nicht alleinig ausübt. (vgl. ebd.: 273ff.)

3.4 Technologische Entwicklungen innerhalb der Gesellschaft

3.4.1 Überwachen als technisiertes Handeln

Mit Erlaub lässt sich sagen, dass Überwachung aufgrund ihrer technischen Artefakte wie ein simples Fernglas und ihrer Handlungsweisen, also Techniken wie Beschattung immer schon technisiert war. „Technik dient insofern der Verlängerung oder dem Ersatz von (Sinnes-)Organen“ (Gottschalk-Mazouz 2008: 210). Das Neue daran ist, dass Überwachungsmittel und unsere Handlungsstränge stark technisiert wurden. So erfahren die technischen Überwachungsartefakte ständige Verbesserungen in Quantität und Qualität, Überwachungshandlungsweisen bedürfen Mobiltelefone und Computer, um effizientere Auswertungsergebnisse zu erlangen und schlussendlich sind Speicherung und Verarbeitung der Daten durch die Digitalisierung und den Abgleich mit technisierten Wissensspeichern völlig neuen Möglichkeiten ausgesetzt. Andererseits greifen wir bei unseren Kommunikations- und Informationshandlungen vermehrt auf technische Artefakte, wie Mobiltelefone, Computer und Internet zurück, was die Vorgänge, sprich Veränderungen an Menschen und Objekten und ihr Tun, wiederum leichter überwachen lässt. Das heißt, „[ü]berwacht werden, aus Bequemlichkeits- und Praktikabilitätsgründen heraus, mit

technisch hochgerüsteten Mitteln genau diejenigen Handlungsvollzüge, die in hohem Maße technisiert sind.“ (ebd.: 213)

3.4.2 Die Vergeistigung des Technotops

Sandro Gaycken sieht derzeit eine technische Revolution ablaufen, die in Ausmaß und Schwere mit der Industrialisierung und ihrer Folgen für die Gesellschaft vergleichbar ist. Technisiert wird dabei eine ganze Palette an menschlichen Eigenschaften. Eine neue Dimension wird erreicht, die mit Veränderungen des Bestehenden einhergeht. „Das Technotop wird ‚vergeistigt’.“ (ebd.: 35) Das Technotop - der Begriff stammt von Günter Ropohl - ist der Lebensraum, den sich Mensch und Technik symbiotisch teilen. Technik ist zu definieren als Sachtechnik im Sinne von vergegenständlichten, verkörperten Technologien, als „ganze[s] Arsenal aller Mittel, Instrumente und Werkzeuge […], durch die die Resultate der menschlichen Arbeit gesteigert werden“ (Berdiajew 1971: 10) und die vom Menschen zu bestimmten Zwecken gemacht sind. Nichts an unserer städtischen Umwelt ist nunmehr „natürlich“, alles ist technisch zugerichtet, nutzbar gemacht, von Wohnräumen über Infrastruktur bis zu unserem Werkzeug, selbst Parks und Erholungsgebiete sind begradigte, bereinigte, künstliche Natur. Das Biotop wurde vom Technotop als unsere Eigenumgebung abgelöst. Nun wurde es erstmals möglich, dass uns Maschinen bei typisch menschlich geistigen, rezeptiven und verbalen Fähigkeiten zu unterstützen vermögen. Seien es Kameras, die sehen, Computer, die rechnen, Mikrofone, die hören, Netzwerke, die kommunizieren usw. Technik unterstützt uns nicht mehr wie in früheren Zeiten bei physisch anstrengenden Arbeiten, sie dient mittlerweile der Verwendung und Erweiterung unserer kognitiven Kapazitäten. Diese Dimension wird auch bestehenden Technologien ergänzend zugefügt. Dabei gewöhnen wir uns schnell an diese Hilfsmittel, sodass man auch umgekehrt behaupten kann, unser Denken werde, genau deshalb, weil wir darin auf Instrumente zurückgreifen, technisiert. Unser Technotop wird also allgegenwärtig vergeistigt. Der Mensch schafft es erstmals, „auch seine geistigen Fähigkeiten selbst zu bevorteilen.“ (Gaycken 2008: 34) Wenn Heidegger von der „Zuhandenheit“ als „Seinsart des Zeugs“ spricht (Heidegger 1972: 69f.), kann man in seiner Terminologie bleibend nun von der „Zu-Geistesheit“ des Zeugs (Gaycken 2008: 34) sprechen. Zwar gab es in der Geschichte immer wieder erhebliche Schritte, die geistige Fähigkeiten stützten, wie die Erfindung der Schrift, doch erst jetzt haben sich Entwicklungsströme derart verknotet, dass

von einer Revolution gesprochen werden kann. Zum einen lernten Maschinen das Sprechen und erhielten damit Potentiale, die mit dem verbalen Denken zusammenhängen. Zum anderen können sie mit erhöhtem Grad an Selbstständigkeit kognitive und kommunikative Abläufe ausführen. Und zugleich wurden sie alltagstauglich, ihre Effizienz überholte die Kosten.
Jede neue Technologie kann als Ausgangslage für den weiteren Weg der Menschen gesetzt werden, denn sie ermöglicht sowohl für das Individuum wie auch für die Gesellschaft neue Lebensformen und Entwicklungsfelder. Der Mensch hat sich an sie zu gewöhnen und an ihr neu auszurichten. Die Industriegesellschaft, Globalisierung, Demokratien konnten (und nicht mussten) sich unter anderem von den Faktoren spezifischer Technologien ausgehend formen. (vgl. ebd.: 28ff.)

Das Technotop hat die Vorteile an sich, dass es uns vor der Willkür und den Gefahren der nackten Natur schützt. Es bringt uns Sicherheit, Geborgenheit, Konstanz, stabile Verhältnisse und Überleben verbunden mit Qualität. Kurz keimte auch der Gedanke auf, Technik könnte die Lösung für all unsere Probleme sein, könnte uns von Not und Elend befreien. Ein solcher Optimismus wich aber bald einem Realismus, der in der Technik als Art „zweiter Natur“ wie Maxim Gorki sie bezeichnete, zugleich auch Nachteile und Gefahren witterte. So hatte die Industrialisierung beispielsweise auch Arbeitslosigkeit zur Folge, der Bau von Waffen die Zerstörung ganzer Landstriche. Es sind die Naturgefahren und Katastrophen einer „zweiten Natur“ wie man mit Gorki sagen könnte. (vgl. ebd.: 36f.)

3.4.3 Missbrauchstendenziöse Technologien

Ein Fehlschluss wäre die Behauptung, dass Technik an sich gut oder böse, also zu bewerten sei. Immer stehen Menschen hinter der Technik, die sie erschaffen, einsetzen, nützen, verkaufen, usw. Ihnen darf man nicht die Verantwortung für ihr Handeln absprechen. Ihr Interesse an den Nachteilen von Technik bzw. ihr Desinteresse an den möglichen Folgen lässt immer wieder neue Atombomben entstehen und Umweltverschmutzung auf hohem Niveau halten. (Dies soll nicht bedeuten, dass nicht auch hart und erfolgreich an sozial- und umweltverträglicher Technik gearbeitet wird.)
Technik lässt sich missbrauchen, doch ist technischer Missbrauch schwer zu definieren, denn ein elektrischer Stuhl wurde ja geradezu produziert, um zu töten. Gaycken definiert ihn

darum folglich: Wenn Technik Menschen von Not und Elend befreien soll und zwar alle Menschen, so liegt Missbrauch bereits dann vor, wenn diese Befreiung asymmetrisch nur einigen, auf Kosten von anderen, gilt, wenn damit also Unrecht, Ungerechtigkeit, Gewalt, bewusste Abhängigkeitsverhältnisse, Unterdrückung, usw. realisiert werden.
Da Missbrauch eine Handlung ist, in diesem Fall eine technische, sind die Verantwortlichen immer Einzelpersonen, die eine solche ermöglichen und vollziehen und nicht die Technik selbst, eben EntwicklerInnen, ProduzentInnen, NutzerInnen.
Dennoch kann man Technologien verorten, deren Gebrauch einen Missbrauch zur Folge hat. Diese „missbrauchstendenziösen Technologien“ (ebd.: 40) sind problematische Fehlentwicklungen, nützen eher wenigen und schaden vielen und werden einzig durch soziale Regulierungen entschärft. Die Gefahr geht aber von ihrer Existenz aus, denn in einem anderen politischen Kontext durch einen möglichen Machtwechsel oder in einem anderen Regime kann durch die Korrektur einiger Bestimmungen ihr Einsatzgebiet stark ausgereizt werden. Eine Atombombe ist und bleibt eine Gefahr, auch wenn relativ friedliche, globale Verhältnisse derzeit keinen Einsatz gerechtfertigen würden. (vgl. ebd.: 37ff.)

3.4.4 Überwachungstechnologien

Die Überwachungstechnik fällt genau in jenen Schnittpunkt der Vergeistigung des Technotops und ist damit eine Technologie der neuen Epoche. Sie sieht, hört, kommuniziert, entdeckt, versorgt, usw. und fällt damit in den Bereich vergeistigter Technik. Andererseits unterstützt sie menschlich geistige Prozesse und ist damit auch der Technisierung des Geistes zuordenbar. Und schließlich lässt sich über sie behaupten, dass sie asymmetrisch wenigen hilft und viele benachteiligt, da Überwachung von einer überschaubaren Menge (von jenen, die sich die teure und spezialisierte Infrastruktur leisten können) ausgeübt werden kann, die davon Betroffenen (jene, die Kommunikationstechnologien nutzen) aber eine größtmögliche Anzahl erreichen sollen. Sie ist ein „Machtmittel der Kontrolle […] des bewussten und unterbewussten, physischen und geistigen Lebens“ (ebd.: 41) und damit eine missbrauchstendenziöse Technologie. Sie stellt eine erste durchgehende, große Gefahr in den Anfängen des vergeistigten Technotops dar. Auch sie wird durch Gesetze und politische Begebenheiten reguliert: So lockerte der 11. September 2001 die Bestimmungen für die Verfolgung von TerroristInnen. Überhaupt hängt viel von der Definition ab, wer als

TerroristIn zu gelten hat, in Japan wurden UmweltschützerInnen von Greenpeace zu TerroristInnen erklärt, in Italien Fußballhooligans. (vgl. ebd.: 35ff.)

Überwachungstechnologien lassen sich unterscheiden in solche, die „direkt zur hoheitlichen Kontrolle entwickelt oder implementiert werden“ (Hornung 2008: 250). Diese Überwachungstechnologien im engeren Sinne umfassen beispielsweise Überwachungskameras, biometrische Identitätspapiere, eine DNA-Verbunddatei, usw. Überwachungstechnologien im weiteren Sinne sind solche, mit deren Hilfe Daten zu anderen Zwecken gesammelt werden (was vor allem in der Privatwirtschaft vorkommt), „auf die dann zu hoheitlichen Zwecken zugegriffen wird“ (ebd.). Der elektronische Zugriff auf Kontostammdaten von Banken und Kreditinstituten oder Mautdaten ist ein Beispiel hierfür.

3.4.5 Überwachungstechnik und -medien

Wenn man bedenkt, dass wir vor knapp 25 Jahren Daten noch mit Hilfe von Lochkarten und erheblichem Aufwand eingeben und auswerten mussten, wird die revolutionäre Entwicklung in diesem Bereich klar und deutlich. Riesengroße Rechenzentren verarbeiteten „offline“ Datensätze, wie sie heute leicht ein Laptop bewältigt oder aus dem Internet bezieht. Heute werden miniaturisierte Prozessoren nicht nur in Computer, sondern in allerlei Gegenstände des Alltags eingebaut, beispielsweise in Autos, CD-Player und Küchengeräte. Der nächste Schritt, diese Technik zu verbinden, also die Geräte zu vernetzen, ist dann nahe liegend, wenn man sich davon einen Zusatznutzen erhoffen darf. Ein gerne ins Spiel gebrachtes Beispiel ist der Kühlschrank, der selbständig die Milch nachbestellen kann, wenn diese zur Neige geht. Neben diesen Vorteilen tut sich auch eine dunkle Seite dieser Vernetzung auf, die wir gerne außer Acht lassen: Unser Verhalten wird nachvollziehbar. Dieses wird beobachtet, notiert, registriert und auch bewertet. Zum Beispiel unser Verhalten im öffentlichen Raum, den nach und nach elektronische Augen einnehmen: Videokameras. (vgl. Schaar 2007: 12ff.)

3.4.5.1 Videokameras

Eine Videokamera stellt schlechthin das „sichtbarste Symbol umfassender Überwachung“ (Schaar 2007: 59) dar. Visuelle Überwachungsphantasien reichen bis zu den Anfängen der Photographie und der Fernsehtechnik zurück. (vgl. Hempel 2008: 86) Der Durchbruch der Videokamera, auch Closed Circuit Television genannt, kam aber erst, als in Großbritannien die minderjährigen Mörder eines Kindes mithilfe der aufgezeichneten Bilder identifiziert werden konnten. Ausgemacht scheint ab diesem Zeitpunkt, dass Videoüberwachung unsere Sicherheit erhöht, wie von Seiten der Polizei auch argumentiert wird (vgl. dazu Wendt 2008: 123) Zu selten wird diese angenommene Proportionalität nachgeprüft.

Nicht nur nebenbei bemerkt, ist London, die wohl am lückenloseste Video überwachte Hauptstadt Europas (300 mal am Tag würde ein/e EinwohnerIn durchschnittlich gefilmt (vgl. Hempel 2008: 92), zugleich auch die gefährlichste laut *Neuer Zürcher Zeitung*, sie hat die höchste Kriminalitätsrate. (vgl. Neue Zürcher Zeitung 2007 und Van Dijk et al. 2005) Die Verbrechensrate sei dort seit Einführung der Kameras kaum gesunken. (vgl. Illetschko/Krichmayr 2009: 13) Dies lässt am direkten Erfolg der Videoüberwachung stark zweifeln.

Unabhängig davon werden Videoüberwachungsanlagen installiert, wohin das Auge reicht. In Österreich haben wir derzeit geschätzte 250.000 Stück mit steigender Tendenz. (vgl. Krichmayr 2009: 13) Die Bilder werden gespeichert und können auch nachträglich ausgewertet werden. Was fehlt ist einerseits die Gewissheit, dass Videoüberwachung an speziellen Plätzen und in konkreten Situationen wirklich Abhilfe leisten kann und andererseits, ob nicht alternative Ansätze eher die Sicherheit erhöhen würden, wie zum Beispiel eine verbesserte Unterführungsbeleuchtung. Einzelfälle dienen als Beweise für die Ausweitung der Überwachungsinstallationen. Dennoch konnte die Videokamera in diesen Fällen das Verbrechen und seine Vorbereitung nicht verhindern, sondern „lediglich“ aufklären. Die Wirksamkeit konnte in vielerlei Studien signifikant nur in besonders gefährdeten und unübersichtlichen Zonen, wie in Parkhäusern nachgewiesen werden, an öffentlichen Plätzen bewirken Überwachungsanlagen zur Prävention kaum etwas, sie verdrängen die Kriminalität maximal in Seitenstraßen und Randgebiete. (vgl. Schaar 2007: 60f.) Einige Studien zeigten, dass sich trotz des Wissens um Videokameras bei PassantInnen, die Angst vor Kriminalität nicht verringert bzw. das Sicherheitsempfinden

nicht erhöht. „Kameras vermitteln nicht mehr Sicherheit. Vielmehr deuten sie entweder auf eine hohe Kriminalitätsbelastung hin oder üben auf den Passanten einen Überwachungsdruck aus, der sich in einem Gefühl der Unsicherheit selbst wiederum Ausdruck verschafft.“ (Hempel 2008: 95) Eher führen Kameras also zu Angst vor ständiger Verhaltenskontrolle als zu deren Verringerung. Soziologische Studien weisen auch darauf hin, dass sich Menschen im Visier einer Kamera unauffälliger verhalten, um keine Missverständnisse herauszufordern. (vgl. Illetschko/Krichmayr 2009: 13) Ob Kameras auf VerbrecherInnen wirklich abschreckend wirken, ist ebenfalls zu hinterfragen. TäterInnenbefragungen brachten ans Tageslicht, dass geplante Verbrechen auf die Bedingungen des Ortes, an dem es ausgeführt werden soll, abgestimmt werden. Eine einfache Kappe ist bereits ein guter Schutz gegen die künstlichen Argusaugen. (vgl. Hempel 2008: 97)

Gegensätzlich argumentiert Polizeihauptkommissar Rainer Wendt, Bundesvorsitzender der deutschen Polizeigewerkschaft, dass Videoüberwachung nachweislich Kriminalitätsbrennpunkte entschärfe und es dabei auch nicht zu einer Verdrängung der Kriminalität aus den überwachten Bereichen in Seitengassen komme. Das Sicherheitsempfinden in der Bevölkerung steige. Videoüberwachung diene der Gefahrenabwehr, der Aufklärung begangener Straftaten und der Vermeidung künftiger. (vgl. Wendt 2008: 128)

Einerseits schränken Videokameras also Formen kontrollierter Selbstdarstellungen ein, andererseits können sie auch helfen, Missstände aufzudecken wie ein Video bewies, das Polizisten zeigte, die einen Unschuldigen niederknüppelten. Die informationelle Privatheit der Polizisten war bei der unerwünschten Überwachung verletzt, nichtsdestotrotz hatte das Video förderliche Effekte hinsichtlich eines demokratischen, egalitären Panoptikums. (vgl. Rössler 2001: 232)

Gründe für den Anstieg von Videoüberwachung von Washington D.C. bis Teheran sind neben den erwarteten Vorteilen für die lokale und nationale Kriminal-, Stadt- und Verkehrspolitik auch militärische Interessen. „[J]edes potentielle zivile System [ist] immer schon Teil der militärischen Strategie“ (Hempel 2008: 92). Strategien der Kriegsführung haben sich gewandelt, Städte als Kriegsschauplätze sind keine Tabuthemen mehr. Viel eher gilt es, den unklaren, asymmetrischen Bedrohungen im urbanen Raum zu begegnen. Dabei hilft ein Überwachungssystem, auf das von Seiten des Militärs stets zugegriffen werden

kann, wie die Handlungen nach den terroristischen Anschlägen in London im Jahr 2005 belegen. (vgl. ebd.: 85ff.)

Was Videokameras definitiv nicht leisten können, ist menschliches Personal zu ersetzen. Menschen können jemandem körperlich helfen, Auskunft geben und strahlen mehr Sicherheit aus. Kameras hingegen können nicht in Geschehensabläufe eingreifen (vgl. ebd.: 97) und benötigen wiederum Personal, das die auf Monitore projizierten Bilder besieht, manchmal mangelt es aber an benötigten Hilfskräften, die manchmal auch mit zu vielen Monitoren in ihren Verantwortungsbereich gleichzeitig konfrontiert sind. (vgl. Schaar 2007: 61ff.) Darum fordert Wendt auch, professionell geschulte Personen hinter den Monitoren und ständig bereite Eingreifkräfte, die mit den Kameras zusammenarbeiten. Videoüberwachung soll Aufgabe der Polizei sein, private, gewinnorientierte Unternehmen sollten gar nicht in Erwägung gezogen werden.
Unverdächtige Menschen werden mit ihren individuellen Verhaltensweisen aufgezeichnet. Dieses Gefühl ständiger Beobachtung kann zu Verunsicherung und angepasstem Verhalten führen. Der Einsatz von Videotechnik sollte nicht inflationär ermöglicht werden, sondern sich auf gefährdete Bereiche beschränken, in denen sie mit Effizienz Lösungsansätze bieten kann. (vgl. Wendt 2008: 128)

Moderne Videoüberwachung arbeitet nicht mehr analog mit Videokassetten, sondern ist von der Aufnahmen bis zur Übertragung und Speicherung vollständig digitalisiert, was bedeutet, dass 24 Stunden am Tag und sieben Tage in der Woche überwacht werden kann und aufgenommene Bilder leichter und länger gespeichert werden können, da Speicherkapazität und Kosten kein Problem mehr darstellen. Noch dazu sind visuelle Überwachungstechnologien heute intelligente Systeme, die automatisiert Gesichter, Objekte wie Nummernschilder und Bewegungen erkennen können. (vgl. Hempel 2008: 87) Der Mensch hinter den Monitoren soll von adaptiven, selbst lernenden Systemen ersetzt oder zumindest unterstützt werden. Wissen diese, was typische Verhältnisse sind, können sie mithilfe von Lernalgorithmen auffälliges und abweichendes Verhalten erkennen und Personen in Archiven zurückverfolgen. (vgl. Krichmayr 2009: 13) Ob es nun aber „besser“ sei, ob einer Person ein wertloser Algorithmus oder ein Mensch zuschaut, sei dahingestellt. Zumindest könnten neue Technologien, die automatisiert und wertfrei überwachen, die Wahrung der Grundrechte verbessern helfen. (vgl. Illetschko/Krichmayr 2009: 13)

Wenn der Datenschutz eingehalten wird, stellt Videoüberwachung kein sonderliches Problem dar, ein solches entsteht eher, wenn die Umsetzung der Möglichkeiten, eine neue Infrastruktur schafft, wie die Verbindung von Video- und Computertechnik, die bereits angestrebt wird (vgl. Hempel 2008: 87f.). Ist eine solche Infrastruktur erst vorhanden, wird auch die Begehrlichkeit eines Missbrauchs gefördert, der bereits durch eine kleine Änderung der Systemeinstellungen geschehen kann, im schlimmsten Falle eine dauerhafte Massenüberwachung. (vgl. Schaar 2007: 64f.) Die Zusammenarbeit mit Datenschutzkommissionen klappt in Österreich teilweise gut. Der Datenschutz kann dadurch erhöht werden, beispielsweise lassen sich Personen in modernen Technologien besser unkenntlich machen. (vgl. Krichmayr 2009: 13, vgl. Illetschko/Krichmayr 2009: 13)

Der Datenschutz fordert eine Zweckbindung von Daten und führte dementsprechend auch viele Vorschriften ein, die aber immer dann angefochten werden, wenn sich die gesammelten Daten für andere wichtige Zwecke eignen. Läuft zum Beispiel ein/e Serienmörder/in frei herum und der Datenschutz wird als Hindernis der Verbrechensaufklärung empfunden, helfen selbst gut begründete Datenschutzargumente wenig, auch wenn das Problem letztendlich gar nicht am Datenschutz liegt. Wird die Zweckbindung partiell gelockert, um z.B. die schwersten Straftaten zu verfolgen, öffnet sich eine Hintertür für zusätzliche Nutzungsmöglichkeiten. Einen Lösungsansatz bieten technische Systeme, die erst gar nicht so viele personenbezogene Daten für einen reibungslosen Ablauf benötigen, anonyme Alternativen sind gefragt, um erst gar nicht in die missliche Lage zu kommen, der Daten Zweck zu entfremden. (vgl. Schaar 2007: 67f.)
Künftig wird es technisch möglich sein, Gesichtserkennungsmethoden mit Videoüberwachungskameras zu verbinden, die PassantInnen anhand ihrer biometrischen Merkmale erkennen. Diese automatisierte, optische Identifikation in Alltagssituationen kann problematisch werden, wenn zum Beispiel die Identitäten der TeilnehmerInnen an einer Demonstration und ihrer WeggefährtInnen gelüftet werden. (vgl. Schaar 2007: 68ff.)

Die hierarchischen Blickbeziehungen, die Überwachungskameras zutage fördern, bilden die Motive für die Gemälde und Arbeiten von Stylianos Schicho.

Abbildung 3: „All inclusive“

Quelle: Stylianos Schicho (2003), „All inclusive“, Acryl auf Leinwand, 2x4 Meter, von: URL: <http://www.stylianosschicho.com/works?gallery_year=2003>

Schicho zeigt hier asymmetrische Blickbeziehungen zwischen einem/r Beobachter/in aus erhöhter Perspektive (wie einer Videokamera) und den damit konfrontierten Menschen. Während die einen irritiert und widerspenstig den Blick erwidern, ergötzen sich die anderen in Ignoranz und körperlicher Fitness, um einem normierten, angepassten Verhalten zu frönen. Die BetrachterInnen werden dabei genau in die problematische Interaktion der Blickbeziehungen, in das Spiel von Widerstand und Kontrollbedürfnis hineingezogen.

3.4.5.2 Handys

Die Nutzung von Mobiltelefonen hat große Auswirkungen auf den Alltag und das Zusammenleben. Sie kommen der Individualisierung und Mobilisierung innerhalb unserer Gesellschaft entgegen und erweitern somit Handlungsspielräume und unterstützen die Aufrechterhaltung von Beziehungen. Mit ihnen lässt sich der Verlust an Nähe zu den wertvollsten, vertrauten Mitmenschen wieder ausgleichen.[14] (vgl. Weber 2008: 286)

Per Handy sind wir heute überall erreichbar. Erreichbar nicht nur für Telefonate, sondern auch für eine punktgenaue Satellitenortung. Damit werden unsere Wege einsehbar für Dritte. Neue Geschäftsmodelle wie die „Location Based Services“ nutzen gerade diese

[14] Hans Geser spricht diesbezüglich vom „Schnuller für Erwachsene“ (Geser 2006: 29).

Möglichkeit, um uns beispielsweise per Sms auf die nächste Tankstelle hinzuweisen. (vgl. Schaar 2007: 13)

Die Speicherkosten für eine digitale flächendeckende und vollständige Aufzeichnung des Telefonverkehrs sind mittlerweile so kostengünstig, dass sie selbst für arme Entwicklungsländer finanzierbar sind. Meist stehen örtliche Geheimdienste dahinter, die so problemlos in die Vergangenheit blicken können. Die USA versucht dabei, möglichst viele internationale Kommunikationsnetze über ihr Territorium zu leiten, um den eigenen Nachrichten- und Geheimdiensten die Daten zu sichern.

Zieht jemand einen Verdacht auf sich, so ist es leicht, eine Verkehrsanalyse seiner Telefonanrufe durchzuführen. Ohne auf den Inhalt zu blicken, ermöglicht sie, herauszufinden, wie, wann und mit wem eine Person kommuniziert. Es lässt sich viel über die Zentralität, Position, Beliebtheit und den sozialen Status von Menschen innerhalb eines sozialen Netzwerks aussagen. (vgl. Weber 2008: 286) DrogendealerInnen sollen beispielsweise eher viele kurze Anrufe von ihren KundInnen, die sie selten kontaktieren, erhalten. Sie selbst wiederum rufen öfters ihre Einkaufsquelle an, so BefürworterInnen der Traffic Analysis. Ein ganzes Kontakt- und Kommunikationsnetzwerk kann somit aufgerollt werden.

Außerdem ist es bereits möglich, mit Spracherkennungssystemen zu arbeiten. Sie errechnen ein Stimmprofil, wenn die Person bereits identifiziert ist, können ansonsten aber automatisiert Merkmale erkennen wie die Sprache, den Dialekt, Alter und Geschlecht und sogar das Erregnungsniveau des/r Sprecher/in. Eine Anfrage an ein solches System könnte lauten: „Gib mir eine Übersicht über die Namen aus allen Telefongesprächen in der letzten Woche, in denen das Stichwort *Demonstration* vorkam, ein Anrufer männlich war, jünger als 30 Jahre, Wiener Dialekt sprach und nervös war.“ (vgl. Rieger 2008: 55-58)

3.4.5.3 Ubiquitous Computing

„Ubiquitous Computing“, also allgegenwärtige Datenverarbeitung bzw. Computereinsatz ist der prägende Begriff seit den 90er Jahren: eine umfassende Informatisierung und Vernetzung fast aller Dinge mit jederzeitiger Verfügbarkeit, Bedienungskomfort und erleichtertem Zugang zu Geräten und Diensten. Fortschritte in der Mikroelektronik und der Kommunikationstechnik könnten Gegenständen ein Wissen über Daten zu ihrem Standort wie auch in Bezug auf Geschehnisse ihrer Vergangenheit ermöglichen und könnten sie über

Funk miteinander kommunizieren lassen. Der Computer solle verschwinden, übrig bliebe nur unscheinbare, aber stetige Datenverarbeitung. „[N]achdem mittlerweile so gut wie alle Computer der Welt daran [ans Internet, Anmerkung D.R.] angeschlossen sind, steht nun also quasi seine Verlängerung bis in die letzten Alltagsgegenstände hinein an!“ (Mattern 2003a: 3)

Die permanente Erreichbarkeit kann natürlich auch negative Folgen haben: Uns entgleitet die Kontrolle, wer genau nun was über uns weiß. Das Recht auf informationelle Selbstbestimmung ist bedroht und der Raum des Privaten, des unbeobachteten und deshalb auch unbefangenen Verhaltens schmilzt, da sich das Potential von Eingriffen in das Private ausdehnt (vgl. Albrecht 2008: 131).

In Alltagsgegenstände eingebaute Mikroprozessoren, die wir an dieser Stelle gar nicht erwarten, können sich vernetzen und Daten austauschen, ohne dass wir eine Kommunikation bemerken. Beispielsweise erfährt eine Mülltonne, welche Materialien in ihr recyclebar sind und gibt die Daten weiter. (vgl. Mattern 2003a: 28) Die Kontrolle geht verloren. Rammert spricht von einer „Aktivierung der Daten“. (Rammert 2007: 24)

Unsere bisher passive technische Umwelt erhält die Fähigkeit, Informationen identifizierend zu sammeln und zu vermitteln. Schlussendlich steht jemand dahinter, der davon profitieren kann. (vgl. Gaycken 2008: 26)

Gefahren wären, dass diejenigen, welche die Kontrolle über die Informationen innehaben, informatisierten Dingen eine Ideologie aufzwingen könnten und eine Abhängigkeit von Systemen, Infrastruktur oder Technik wie dem Internet entstehen könnten. Des Weiteren könnte sich die digitale Kluft vertiefen. Soziale Problemfelder ergeben sich heutzutage weniger aus vertikalen Gesellschaftsverbindungen wie Klassen, sondern aus horizontalen Perspektiven. Es geht darum, „dabei“ und „in“ zu sein. Wer sich etwas nicht leisten kann oder keine Mitgliedschaft tätigen will, kann schnell an den Rand gestellt werden. (vgl. Mattern 2003a: 30f.) Wer nicht über *Facebook* kommuniziert, erhält weniger private Informationen aus seinem Freundeskreis.

Dem Datenschutz kommt beim Ubiquitous Computing enorme Bedeutung zu, um keine Überwachungsinfrastruktur zu schaffen. Würde dieser Versagen ließen sich Profile über Menschen anlegen, die Daten bis in die kleinsten Details verraten. Derzeit ist das Datenschutzrecht auf solche künftigen Technologien nicht vorbereitet. (vgl. ebd.: 31ff.)

Durch die ständige Präsenz, das Aufzeichnen meines Verhaltens und die Möglichkeit, daraus Konsequenzen zu ziehen, kann ein Gefühl der Beobachtung und Unsicherheit entstehen. Andererseits könnte die Weiterentwicklung der Netzwerkkommunikation im Sinne einer allgegenwärtigen Beobachtung durch intelligente, smarte Gegenstände positiv gedeutet werden als allgegenwärtige Assistenz und Betreuung in Form einer virtuellen Bezugsgruppe, also virtuellen PartnerInnen.

3.4.5.4 RFID-Chips

RFID-Chips (Radio Frequency Identification) können gespeicherte Daten mittels Funk übertragen. Mit der passenden Leseeinheit werden diese sichtbar gemacht. RFID-Chips kommen fast überall zum Einsatz, in Reisepässen zur sicheren Erkennung, in Alltagsgegenständen wie CDs zur Zuordnung von Dingen zu Personen, in Fußball-Tickets der FIFA für die Fälschungssicherheit, in Kühen, in Menschen (eine spanische Bar erkennt ihre Stammkundschaft anhand implantierter Chips), vielleicht bald in dementen Menschen und Strafgefangenen. Sie tragen das Potential in sich, die Überwachung individuellen Verhaltens zu ermöglichen und zu vereinfachen. (vgl. Schaar 2007: 49-54)
Die Pharmaindustrie schmiedet gar Pläne, RFID-Chips in papierner Form in Tabletten einzusetzen. Somit kann in Altersheimen leichter überprüft werden, welchen Medikamentenstatus die SeniorInnen haben, dazu werden sie laufend gescannt. (vgl. Gaycken 2008: 26)

3.4.5.5 Location Based Services

Dieselbe Technik, die bei den Location Based Services Handlungen ermöglicht, überwacht zugleich Bewegungsmuster der Handelnden. (vgl. Gottschalk-Mazouz 2008: 213)
Dadurch, dass unserer Gesellschaft Werte wie Individualität, Mobilität, Flexibilität verbunden mit Sicherheit so wichtig wurden, der Einzelne dabei immer erreichbar sein und sich in seiner Umgebung sofort zurechtfinden will, wurden auch Lokalisierungsdienste wichtiger. Der aktuelle Standort wird beispielsweise über das Handy ständig ermittelt, um eine Telefonverbindung aufzubauen. Mobilfunknetze bestehen aus einer Vielzahl partikulärer Funkzellen. Diese haben einen Durchmesser von mehreren hundert Metern bis

zu einigen Kilometern - das hängt von der eingesetzten Technik und der Bebauungsdichte ab. Das Netz muss wissen, in welcher Zelle sich das Gerät befindet, wenn es verwendet werden will. Darum sendet es in eingeschaltetem Zustand auch ständig Bescheide über seine Aktivität. Kommt eine Verbindung zustande wird der Standort beider GesprächsteilnehmerInnen im Verkehrsdatensatz gespeichert, wo er aufgrund der Vorratsdatenspeicherung erstmals ein halbes Jahr verweilen solle, ehe er gelöscht wird. (vgl. Rieger 2008: 57ff.)

Noch genauer können Standorte mittels GPS (Global Positioning System) berechnet werden. Ein Empfangsgerät sendet Signale an Satelliten, die aus der Dauer der Laufzeiten die exakte Ortslage bestimmen. GPS ist ein passives System, das heißt nur das Empfangsgerät erhält die erwünschten Informationen, Dritte können sie nicht aktiv orten. Es sei denn die Daten werden übertragen mittels Mobilfunk beispielsweise. Denn auch Handys sollen mit GPS Funktion ausgestattet werden, um beispielsweise bei einem Notruf gleich die genauen Ortsbestimmungen senden zu können.
Infolgedessen entstanden diese so genannten, neuen Location Based Services-Dienste, die auf Lokalisierungsmechanismen aufbauen. Sie ermitteln den Standort einer Person und können auf Anfrage beispielsweise die nächstgelegene Apotheke, ein Restaurant, eine Tankstelle usw. vorschlagen. Dass damit auch Bewegungsfelder diverser Personen angelegt und mit anderen Angaben zu Profilen verflochten werden können, ist die Kehrseite dieser Services. (vgl. Schaar 2007: 56f.)

3.4.5.6 Pässe mit biometrischen Daten

Die Anschläge vom 11. September 2001 legitimierten Überwachungsmaßnahmen seitens westlicher Staaten. Eine verstärkte Berücksichtigung biometrischer Merkmale, vor allem in Reisedokumenten ist eine Folge dessen. Ausgewertet werden individuelle physiologische Eigenschaften wie Fingerabdruck, Iris, Gesicht oder die genetische Disposition der DNA, und persönliche Verhaltensweisen wie die Stimme, Schreibverhalten und Lippenbewegung zur Identifikation einer Person. Ihr Vorteil besteht darin, dass man sie nicht vergessen kann wie Passwörter, noch kann man sie verlieren wie Schlüssel oder an Dritte weitergeben. (vgl. Kurz 2008: 101f.)

Der Europäische Rat hat 2004 vorgeschrieben, neben Gesichtsphotos auch Fingerabdrücke elektronisch mittels RFID-Chips in Reisepässen und -dokumenten der EU-BürgerInnen aufzunehmen, um diese fälschungssicherer zu machen.[15] Die schnelle Umsetzung sollte schließlich auch der Industrie auf diesem Sektor dienen. KritikerInnen beklagen eine relativ hohe Fehlerquote der Systeme, die kostenintensive Durchführung bei geringem Sicherheitsgewinn und befürchten eine mögliche Entfremdung der Daten, wenn zum Beispiel abgespeicherte Bilder zum Vergleich herangezogen werden, um Personen in Überwachungsvideos zu identifizieren. Neue Begehrlichkeiten werden geweckt, beispielsweise dürfen Behörden zur Verfolgung von Straftaten bereits auf die Daten zugreifen. (vgl. ebd.: 102ff.) Digital gespeicherte Gesichtsbilder beinhalten zusätzliche Informationen, die andere Auswertungsmöglichkeiten zulassen, beispielsweise wenn aus der Beschaffenheit der Iris Verhaltensgewohnheiten wie Alkohol- oder Drogengenuss geschlussfolgert werden. Des Weiteren kann man möglicherweise aus dem Bild auf die Religionszugehörigkeit schließen, aus der Stimme und der Bewegungsweise lassen sich der Gesundheitszustand und psychologische Faktoren wie zum Beispiel die Stimmung ableiten. Manche erfasste Daten können erst in Zukunft bedenklich werden, wenn die Technologie neue Umgangsmöglichkeiten geschaffen haben wird, als mögliches Beispiel: die Forschung findet einen Zusammenhang zwischen Fingerabdrücken und genetisch bedingten Krankheiten. Die bereits gespeicherten Fingerabdrücke wird keine Behörde der Welt freiwillig löschen wollen. (vgl. Schaar 2007: 76ff.)

Das Hauptproblem der gespeicherten biometrischen Daten in „ePässen“ ist, dass sie den Behörden jedes Landes, das man bereist, zur Verfügung stehen und in Datenbänke wandern können, ohne dass wir noch Einfluss darauf bzw. eine Steuerungsmöglichkeit für ihre weitere Verwendung haben. Dabei kann es zu Identitätsdiebstahl, Cross-Matching über Datensätze und zur Erlangung medizinischer Überschussinformation kommen. (vgl. Kurz 2008: 108ff.)

3.4.5.7 Gentests

Keine wissenschaftliche Forschungsrichtung hat einen ähnlichen Einfluss auf die informationelle Selbstbestimmung wie die Ergebnisse der Genetik. Sie befasst sich mit unseren persönlichen Erbinformationen. Das menschliche Genom, also die Struktur der

[15] Die Attentäter von New York und Washington D.C. hatten übrigens gültige Ausweisdokumente und verhielten sich bis zum bekannten Zeitpunkt unauffällig.

Säurekette DNA wurde bereits im Jahr 2000 entschlüsselt. Ein Teil der Struktur enthält Erbinformationen zu Persönlichkeitsmerkmalen und Veranlagungen, ein anderer Teil eben nicht, ist aber bei jedem Menschen einmalig und dient somit der eindeutigen Identifizierung (vgl. Kurz 2008: 110). Letzterer ist es auch, über den sich die Abstammung von den Eltern und die Zuordnung von DNA-Spuren, die an einem Verbrechenstatort gefunden werden, bestimmen lassen. Nun lässt sich anhand einer genetischen Untersuchung des Teils mit Erbinformationen vorhersagen, für welche Krankheiten man anfällig ist, was aber keineswegs bedeutet, dass diese Krankheit mit Gewissheit ausbrechen wird oder zu wissen, wann genau es soweit sein kann, jedoch lässt sich eine erhöhte Wahrscheinlichkeit feststellen. Natürlich spielen auch andere Faktoren wie Lebenswandel, Ernährung und Bewegungshäufigkeit eine wichtige Rolle. Aufgrund dieser Erkenntnisse lässt sich ein individuelles Risikoprofil anlegen, das trotz Unsicherheiten an Aussagekraft gewinnt. Zudem lässt sich ein Gentest heutzutage mittels Biochip leicht, schnell und relativ billig durchführen und elektronisch weiterverarbeiten.

Problematisch wird das Wissen über die Gensequenzen dann, wenn ArbeitgeberInnen und Versicherungen dieses begehren und teilen wollen. ArbeitgeberInnen wollen grundsätzlich effiziente, gesunde Arbeitskräfte einstellen. Die Frage stellt sich, wie viel der/die Arbeitnehmer/in von seinem Wissen mitteilen soll und wie viel der/die Arbeitgeber/in erfahren darf, um „genetische Diskriminierung“ (Schaar 2007: 87) zu vermeiden. Der Druck bezüglich einer Durchführung genetischer Tests nimmt jedenfalls zu. Das Fragerecht der ArbeitgeberInnen umfasst Fragen zur Gesundheit von BewerberInnen, wenn diese für den konkreten Arbeitsplatz relevant sind. Konkret sind es Fragen über mögliche Beeinträchtigung der Arbeitsleistung, Fragen zu akuten und ansteckenden Krankheiten oder geplanten Operationen, aber im Regelfall keine zur Angabe genetischer Dispositionen. Sollte man aber Information zu einer Krankheit haben, die mit über 50prozentiger Wahrscheinlichkeit zu erwarten ist und ihre Auswirkungen bereits nach einem Maßzeitraum von sechs Monaten nach der Einstellung zu erwarten sind und die Arbeitsfähigkeit erheblich einschränken, sollte sie kundgetan werden. Das Problem dabei ist, dass man nur bei wenigen Erbkrankheiten sicher bestimmen kann, dass sie ausbrechen werden, der jeweilige Zeitpunkt aber keineswegs.

Ein fairer Interessenausgleich sollte auch bei den beiden Parteien eines Versicherungsabschlusses angestrebt werden. Einerseits kann ein/e Antragsteller/in, dem/der ein Gentestergebnis vorliegt, vor dem Ausbruch einer prognostizierten, aber geheim

gehaltenen Krankheit noch schnell eine Kranken- oder Lebensversicherung abschließen, andererseits könnten Versicherungen von ihren KundInnen verlangen, einen Gentest vorzuweisen, um eine Versicherung abschließen zu können, nach dem Motto: Wer gefährdet ist, zahlt eine zusätzliche Versicherungsprämie. „Eine generelle Offenbarungspflicht hinsichtlich bereits vorliegender Ergebnisse durchgeführter Gentests würde unverhältnismäßig massiv in das informationelle Selbstbestimmungsrecht eingreifen." (Schaar 2007: 86) Ein möglicher Kompromiss wäre, bei sehr hohen Versicherungssummen das Ergebnis eines möglicherweise negativen Gentests mitzuteilen.

Definitiv kann nachgewiesen werden, dass die DNA-Identitätsfeststellung helfen kann, Verbrechen aufzuklären. Am Tatort aufgefundenes Zellmaterial wird analysiert und mit der DNA von Personen verglichen. Darüber hinausgehend treten Begehrlichkeiten auf, auch die Teile der DNA-Struktur von Verdächtigen verwenden zu dürfen, die Erbgutinformationen wie körperliche Merkmale und psychologisches Profil beinhalten. (vgl. Kurz 2008: 110)

Manche PolitikerInnen und WissenschaftlerInnen fordern nun die Erstellung einer Gen-Datenbank, Restblutproben von Neugeborenen werden immerhin schon seit Jahrzehnten aufbewahrt. Zusätzlich sollte der genetische Code aller Menschen gleich nach der Geburt festgestellt und gespeichert werden, um die Verbrechensaufklärung zu erleichtern, ein sehr brisanter Vorschlag und ein enormer Eingriff in das Recht auf informationelle Selbstbestimmung.

Um dieses heikle Gebiet nicht den Marktkräften zu überlassen, ist die Politik dringend gefordert, „angemessene und klare rechtliche Vorgaben für genetische Untersuchungen" (Schaar 2007: 88) zu erstellen.

3.4.5.8 Internet

Eine ganz neue Dimension eröffnete die Vernetzung der Computer durch das Internet. Angeforderte Informationen, egal aus welcher Sparte, erscheinen heute in Sekundenbruchteilen am Bildschirm. Ende 2007 hatten rund 1,23 Milliarden Menschen Zugang zum World Wide Web, 2010 werden es bereits über 1,5 Milliarden sein (vgl. BITKOM 2007). Das WWW wurde 1989 im Schweizer Forschungszentrum CERN erfunden, es ist ein globaler Marktplatz, der bereits 2005 über ein Volumen von mehr als 11,5 Milliarden Seiten verfügte.

Es birgt aber auch einige Gefahren, unter anderem im Hinblick auf die Beschaffung personenbezogener Daten und den Schutz der Privatsphäre. „Die verbundenen Computersysteme bilden eine globale Informationsinfrastruktur mit einer unüberschaubaren Menge - auch personenbezogener - Inhalte, die prinzipiell miteinander verknüpft werden können, unabhängig vom ursprünglichen Zweck ihrer Speicherung.“ (Schaar 2007: 39)

Ein Prinzip der digitalen Medien überhaupt ist die Personalisierung ihrer NutzerInnen. Etwaige Produkte und Dienstleistungen elektronischer Unternehmen sollen immer besser auf die Bedürfnisse der UserInnen zugeschnitten sein. Die zunehmende Kommerzialisierung des Internets macht es notwendig, dass wir bei unseren Handlungen und Aktivitäten im Netz identifizierbar und verfolgbar werden, um Cyberkriminalität möglichst gut zu unterbinden. Leistungsfähige und feinste Technik wird unsere Anonymität, eine der Formen von Privatsein, durch den Zwang, seine Identität nachzuweisen, (ver)schwinden lassen. Denn der Kampf gegen Terror und organisierte Kriminalität, das Vorgehen gegen Kinderpornographie, die Authentifizierung bei Transaktionen dienen als starke Argumente für das Sammeln möglichst vieler persönlicher Daten, die dann aber weitere Begehrlichkeiten wecken können, wie die Personalisierung von Angeboten, Informationen und Werbung. Digitalisierte Daten sind speicherbar und verwertbar. Leicht lassen sie sich durchsuchen, zusammenführen und auswerten. So dienen sie der wissenschaftlichen Forschung, Verbrechensbekämpfung, Marketing, Wirtschaftsspionage, der Überwachung von BürgerInnen und Angestellten, usw. (vgl. Rötzer 2001: 170ff.)

Das Internet trägt ein erhebliches demokratisches und emanzipatorisches Potential in sich, weil man leicht und kostengünstig oppositionelle Inhalte veröffentlichen kann und dadurch die Meinungsfreiheit gefördert wird. Durch eine Aufhebung der Anonymität zugunsten einer erhöhten Sicherheit im Netz, wie sie wirtschaftliche Unternehmen im Internet fordern, wird sein offenes, demokratisches Wesen eingeschnürt. (vgl. ebd.: 177f.)

Die Kommunikation im Internet folgt anderen Gesetzmäßigkeiten als bisherige Dienste. So kann man sich nie sicher sein, ob Daten, die wir bereitwillig hergeben, nicht von Dritten eingesehen werden. Gezielte Angriffe auf Computer sind über das Internet leichter zu bewerkstelligen. HackerInnen arbeiten mit Hilfe von Viren, Würmern und Trojanern, um sich Passwörter und Kennungen zu sichern und sich so unerwünschten Zugang zu einem fremden Computer oder System zu verschaffen. Dort lagernde oftmals sicherheitsrelevante

Informationen können ihnen für weitere Attacken dienen. Viren sind schadhafte Bestandteile von Programmen und werden bei Öffnen des Wirtsprogramms aktiviert. Würmer und Trojaner sind selbstständig ausführbare Programme. Letztere verstecken die Schadfunktion hinter einem nützlichen Feature wie etwa Datenkomprimierung. Auswirken können sich die Schadprogramme auf die Datenbestände, indem sie diese manipulieren oder löschen. Vorsicht ist dabei vor Programmen geboten, die Aktivitäten von BenutzerInnen unbemerkt überwachen können. Der *Keylogger* ist ein Programm, das alle Tippanschläge am Computer heimlich mitzeichnet und die Daten dann über das Internet an Dritte weitersendet.
Bei jedem Gebrauch des Internets öffnet sich ein Kommunikationskanal, in dem die Daten in beide Richtungen strömen, vom Sender zum Empfänger und umgekehrt. Das ermöglicht zum Beispiel auch ein staatliches Eindringen in persönliche Computer, um diese auf illegale Dateien online zu durchsuchen.
In letzter Zeit wurden auch des Öfteren Fälle bekannt, in denen geschützte Daten wie Passwörter oder Bankdaten durch Fehler und Missstände an die Öffentlichkeit kamen. (vgl. Schaar 2007: 40ff.)

Im Internet wird das Surfverhalten protokolliert, sei es das Versenden einer E-Mail, eine Internetbestellung, ein gewöhnlicher Seitenaufruf oder ein simpler Mausklick. Dies ist technisch deshalb möglich, weil es identifizierbare Datenpakete zu versenden gilt und darum jedem Computer eine IP-Adresse zugeordnet ist. Diese Internet-Protocol-Adresse ist, ähnlich dem Nummernschild eines Autos, eine „Art Kennungsnummer auf Basis einer 32- bzw. 128-stelligen Binärzahl“ (ebd.: 42). Andererseits besitzt auch jede Seite im Web eine eigene IP-Adresse, den so genannten *Uniform Resource Locator* (URL). Somit kann das Besuchen diverser Websites von allen Systemen gespeichert werden, die am Kommunikationsvorgang teilnehmen. Die AnbieterInnen von Webservern können demnach die IP-Adresse, das dort verwendete Betriebssystem, den Browser, den Link, von dem der/die User/in auf die Seite weitergeleitet wurde und dazu genaue Uhrzeitangaben in so genannten Log-Protokollen aufzeichnen.
Des Weiteren setzt beinahe jede/r Anbieter/in von Webangeboten Cookies ein. Das sind kleine Profildateien, die auf den Rechnern der UserInnen abgespeichert werden, „um eine spätere Internet-Nutzung demselben Benutzer zuordnen zu können.“ (Zeger 2009: 97) Diese Dateien zeichnen auf, in welcher Art der/die User/in das Service in Anspruch nahm, bei einer Suchmaschine zum Beispiel, welche Suchbegriffe er/sie bei bisherigen Besuchen

eingab. Diese Informationen lassen sich sehr gut verketten und somit ein Bild über den/die Nutzer/in gewinnen mit seinen/ihren Vorlieben und Interessen. Webshops können das Einkaufsverhalten ihrer KundInnen mit Hilfe von Cookies hervorragend beobachten.
Bei individualisierten Webdiensten, die eine Registrierung erfordern, kann folglich das Verhalten im Web unmittelbar einem Individuum mit Namen, Anschrift, meist auch Details über Zahlungsabwicklungen zugeordnet werden. Das Cookie registriert dann jeden direkten personenbezogenen Mausklick.

Wer im Internet anonym bleiben will, muss selbst einen technischen Aufwand betreiben, zum Beispiel die Verschleierung der IP-Adresse. Aber die Anonymität sollte auch ohne große Eigeninitiative gewährleistet sein, denn sonst machen sich wiederum genau die verdächtig, die nach Anonymität streben. (vgl. Rötzer 2001: 175f.)

3.5 Staatliche Überwachung

3.5.1 Vom Traum, künftige Verbrechen zu verhindern

Wäre es nicht der Traum eines jeden Staates, Gewaltverbrechen zu verhindern, bevor sie passieren, eine Welt, in der MörderInnen der Vergangenheit angehören. Solch ein Zukunftsszenario entwirft zumindest Philip K. Dick in seiner Science-Fiction-Kurzgeschichte *Der Minderheiten-Bericht*. So genannte Präkogs, menschliche Wesen mit einer besonderen Begabung und speziellem Training, dienen einzig dem Zweck, künftige Verbrechen circa zwei Wochen vor ihrem Geschehen vorauszusagen. Die Polizei braucht schließlich nur noch den/die potentielle/n Täter/in abzuholen und zu verhaften. (vgl. Dick 1993a)
Parallelen zu der Realität zeigen sich im Wunsch, Verbrechen wie terroristische Anschläge erst gar nicht passieren zu lassen. Bereits im Vorhinein soll das Denken und Handeln von GesellschaftsfeindInnen ausgeforscht und in seiner Radikalität entschärft werden. Während die Existenz von Präkogs schlichtweg fiktiv bleibt, verhofft man sich real mittels eines anderen Weges seherische Qualitäten: Datensammlungen, Überwachung und „einer Neubewertung von heimlichen und täuschenden Ermittlungspraktiken.“ (Albrecht 2008: 132)
So verschiebt sich der Fokus der Strafverfolgung auf Risikokontrolle und Prävention.

> Dick zeigt, wie durch die vermeintliche Unfehlbarkeit der Verbrechensprävention ein System geschaffen wird, in dem die technologisch gezogene Grenze zwischen Ordnung und Unordnung nahezu nicht mehr angezweifelt werden kann, und er führt uns deutlich vor Augen, wie sehr diese Grenze dann auch zum Schutz jener Übeltäter wird, die es schaffen, sie zu überwinden.
> (Purgathofer 2008: 207)[16]

Wer also den Anschein wahren kann, sich innerhalb der Grenzen zu bewegen, hat wenig zu befürchten, was auch bedeutet, dass Verdächtigte nicht immer zu Recht als solche gelten.

3.5.2 *1984*

Das Sinnbild für staatliche Überwachung ist seit der Entstehung des Buches *1984* von George Orwell schlechthin der *Big Brother*, ein allwissender Staat mit einer absoluten Kontroll- und Überwachungsfunktion. Ausgehend von den totalitären faschistischen und stalinistischen Regimes der Zeit vor und während des zweiten Weltkrieges entwickelt Orwell seine Dystopie in den Jahren 1947/48 und verlegt den Handlungsrahmen in die nahe Zukunft. Ein mächtiger, totalitärer Staat beherrscht mittels effektiver Überwachungstechnologie seine BürgerInnen und vor allem ParteimitgliederInnen. In Privatwohnungen eingebaute Teleschirme, zugleich Sende- und Empfangsgeräte, die im Sinne einer Videokamera die gesamte Wohnfläche abzufilmen vermögen, Mikrophone, die in der freien Natur wie Wanzen funktionieren, Hubschrauber der Gedankenpolizei und ein ausgeklügeltes Spitzelwesen garantieren die perfekte Überwachung und eine Gesellschaft ohne Menschenwürde. (vgl. Orwell 1983)
Ein Vergleich zum Panoptikum, zur totalen Überwachung lässt sich herstellen, denn das Individuum weiß nie, ob es im Moment gerade und wie oft es überhaupt überwacht wird.

> Orwell warnte nicht vor der Technologie an sich, sondern vor der Gefährdung der Demokratie und der Selbstbestimmung durch totalitäre Ideologien und Mächte, die sich der Überwachungstechnik bedienen könnten [...] Demokratie bedeutet stets auch Begrenzung staatlicher Macht, Schutz von Menschenwürde und Privatsphäre.
> (Schaar 2007: 95)

[16] Purgathofer meint hier wohl eher die inhaltlich abgeänderte und erweiterte Verfilmung *Minority Report* von Steven Spielberg, in der das System mutwillig umgangen wird.

Heutzutage hätten wir weit effektivere technische Möglichkeiten, um ein Überwachungssystem zu installieren, informationstechnische Überwachung kann vollautomatisch ablaufen, gering an Personal und Kosten.
So meint Sandro Gaycken auch, dass Orwells „Gedankenverbrecher“ in heutigen Gesellschaften bereits vorzufinden sei. „Er sitzt zu diesem Zeitpunkt in chinesischen und amerikanischen Gefängnissen, interniert auf Basis potentieller Gedanken, die automatisierte ‚Profiling'-Prozesse seinem Internet-Verhalten unterstellt haben.“ (Gaycken 2008: 26)
Auch lässt sich im Vergleich mit heutiger technischer Überwachung feststellen, dass die Mittel gleich blieben bzw. sogar verbessert wurden, die Zwecke aber edler und wohlmeinender zur Herstellung von Sicherheit geändert wurden. (vgl. Ropohl 2008: 266)
Gefeit vor Überwachung sind aber auch Demokratien nicht, viele Menschen sind bereit für ein Mehr an Sicherheit Freiheitsrechte und die Privatsphäre einzuschränken.
Heutzutage verbinden Menschen jedoch ohnehin mit *Big Brother* eher eine Reality-Fernsehshow, die signalisiert, dass die Beobachtung der eingeschlossenen Personen Spaß machen könne und „normal“ sei. Wir alle seien Big Brother.

Ein moderner Staat kann nur durch die Erhebung einer Vielzahl an Daten funktionieren. Er braucht Informationen, dokumentiert und archiviert diese, um eine moderne Bürokratie zu bewerkstelligen und den Staat auf eine objektive Basis zu stellen. Um das Meldewesen einzuführen, um Steuern einheben zu können, um die Verkehrssicherheit aufrecht zu erhalten, um Wahlen zu organisieren, um das Gesundheitswesen zu organisieren, bedurfte und bedarf es einer Menge an Informationen über seine BürgerInnen. Registriernummern wie Telefonnummer, Kontonummer, Versicherungsnummer, Matrikelnummer werden dafür verzeichnet.
Der Staat hat für Ordnung, Sicherheit, Gerechtigkeit, Schutz vor äußeren Bedrohungen, Bildung, Wissenschaft, Medien und Kultur Sorge zu tragen. Dabei wird er von der Judikative, von unabhängigen Gerichten kontrolliert und korrigiert, Recht und Gesetze stehen ihm vor, wie die sogenannten Grundrechte, die in langen Prozessen erstritten wurden und die Bevölkerung schützen sollen. Das deutsche Recht auf informationelle Selbstbestimmung, das aus dem allgemeinen Persönlichkeitsrecht und dem Recht auf Menschenwürde abgeleitet wurde, ist ein solches.

3.5.3 Freiheit vs. Sicherheit

Schwierigkeiten bereitet für den Staat, ein ausgewogenes Verhältnis an größtmöglicher Sicherheit und zugleich größtmögliche Freiheit für seine BürgerInnen zu finden. Einerseits will man die Bevölkerung vor Bedrohungen wie Terrorismus, Kriminalität usw. schützen, andererseits ist ein massiver Eingriff in die Rechte der BürgerInnen, zum Beispiel in den Datenschutz gleichzeitig ein Eingriff in die Freiheit insgesamt. (vgl. Schaar 2007: 95ff.)
So meinte schon Benjamin Franklin: „Wer die Freiheit aufgibt, um Sicherheit zu gewinnen, der wird am Ende beides verlieren.“[17] (Benjamin Franklin, zit. nach Trojanow/Zeh 2009: 11)
In diesem Sinne spricht auch Günter Ropohl über Menschen der globalisierten Informationsgesellschaft: „Befangen von der Illusion, ewig leben zu können, verfehlen sie mit andauernder Endzeitsorge das wirklich gute Leben.“ (Ropohl 2008: 267)

Ropohl unterzieht die Überwachungstechnologie einer ethischen Technikbewertung bzw. Technikfolgen-Abschätzung. Dabei werden die erwarteten „Folgen technischer Neuerungen aufgrund definierter Ziele und Werte“ (Ropohl 2008: 271) beurteilt. (Ropohl bezieht sich auf den Wertkatalog der VDI-Richtlinie 3780 (2000).) *Für* die technische Überwachung sprechen die Unterwerte „Körperliche Unversehrtheit“, „Lebenserhaltung des einzelnen Menschen“ und „Minimierung des Risikos (Schadensumfang und Eintrittswahrscheinlichkeit)“, die dem Wertbereich *Sicherheit* entspringen, „Körperliches Wohlbefinden“ und „Minimierung von unmittelbaren und mittelbaren gesundheitlichen Belastungen“ aus dem Wertebereich *Gesundheit* und „Beherrschbarkeit und Überschaubarkeit“, „Ordnung, Stabilität und Regelhaftigkeit“, „Transparenz und Öffentlichkeit“ und „Gerechtigkeit“ aus dem Wertebereich *Persönlichkeitsentfaltung und Gesellschaftsqualität*. *Gegen* technische Überwachung sprechen die Unterwerte „Psychisches Wohlbefinden“ aus dem Wertebereich *Gesundheit* und „Handlungsfreiheit“, „Informations- und Meinungsfreiheit“, „Privatheit und informationelle Selbstbestimmung“ und „Geborgenheit und soziale Sicherheit“ aus dem Wertebereich *Persönlichkeitsentfaltung und Gesellschaftsqualität*. Schnell wird erkennbar, dass es unweigerlich zu Wertkonflikten kommen muss, weil man nicht alle Werte gleichermaßen erfüllen kann und sie in ihrer völligen Abstraktheit nicht aufzulösen vermag.

[17] Original in Englisch: „Those who would give up essential Liberty to purchase a little temporary Safety, deserve neither Liberty nor Safety.“

Eine andere Illustration dieses Dilemmas ist die Theorie der moralischen Regeln des amerikanischen Philosophen Bernard Gert. Sie stellt eine negative Folgenethik dar, wonach moralische Regeln verbieten, was anderen Menschen vermeidbare Übel zufügen könnte. *Für* die technische Überwachung sprechen die von Ropohl modifizierten Regeln „[Leben] Niemand darf gegen seinen Willen getötet werden." und „[Gesundheit] Niemand darf gegen seinen Willen verletzt, gequält oder anderweitig in seiner Gesundheit geschädigt werden." *Gegen* technische Überwachung sprechen die moralischen Regeln „[Freiheit] Niemand darf in der Selbstbestimmung der persönlichen Lebensführung und in der freien Wahl unter seinen wohlverstandenen Entfaltungsmöglichkeiten beschränkt werden. (Wohlverstandene Entfaltungsmöglichkeiten sind solche, welche die Entfaltungsmöglichkeiten anderer nicht über Gebühr behindern.)" und „[Wahrheit] Niemand darf in seinem Vertrauen zu anderen erschüttert werden. (Vertrauen wird erschüttert durch Täuschung und Betrug, durch Bruch von Vereinbarungen und Versprechen sowie durch Äußerungen wider besseres Wissen.)"
Diese Werte und Regeln gelten nach Ropohl unbedingt und können nicht gegeneinander aufgewogen werden.
Ropohl versucht nun argumentativ und mittels konkretisierender Kriterien herauszufinden, welches nun das größere Übel wäre, das den Menschen zugefügt wird.
Die UrheberInnen von Anschlägen und Attentaten sind TerroristInnen, der Verursacher der Freiheitseinschränkungen der Überwachung ist vor allem der Staat. „Der Staat steht allein vor der Frage, wie viel Freiheit er einschränken darf, um seine Bürger vor einer Lebensbedrohung zu schützen, die von Dritten ausgeht." (Ropohl 2008: 276) Der Staat müsste aber nicht aktiv handeln, sondern könnte auch auf Vorsorgemaßnahmen verzichten. So könnte er von der Gefahrenabwehr ablassen, wenn verfassungsrechtliche Grundprinzipien unterminiert werden. Muss der Staat seine BürgerInnen überhaupt vor allen möglichen Gefahren beschützen? Zu Berühmtheit innerhalb dieses Diskurses brachte es das absurde Beispiel des „Pfützentritts". Was macht ein Staat nach einem Regenguss, um seine BürgerInnen vor dem Treten in eine Pfütze und einer folgenden Beschmutzung zu bewahren? Soll er Warnschilder montieren, die Pfützen absperren oder gar eine Ausgangssperre bei Regenwetter verhängen? Oder überlässt er es der Freiheit der Menschen und bevormundet sie nicht?
Zweitens wäre eine vollkommene Sicherheit nie zu gewährleisten, da immer Fehler auftreten werden und eine Überfülle an Daten schwierig zu verarbeiten ist. Kriminelle Energie wird deshalb immer Wege finden, sich zu verwirklichen. Technische Überwachung kann maximal die Wahrscheinlichkeit eines ohnehin geringen Risikos verringern, sie aber

nicht nullifizieren. Andererseits würde eine technische Überwachung zu einer Vielzahl falscher Verdächtigungen führen, wogegen sich die Einzelnen kaum erwehren können. Eine Untersuchung zeigte, dass im Falle einer Totalüberwachung die Anzahl der zu Unrecht Verdächtigten erheblich größer wäre aufgrund einer unvermeidlichen Fehlerquote als die Zahl der zu Recht Verdächtigten. Dabei wäre die Eintrittswahrscheinlichkeit dieses Übels einer allumfassenden Überwachung sehr hoch, fast mit Gewissheit würde es eintreten und dabei wäre die Zahl der Betroffenen deutlich höher als die der Opfer terroristischer Anschläge. Ropohl fragt, was mehr zähle, das Leben weniger oder die Freiheit aller? Zuletzt der Punkt, wie sich die Dinge eventuell künftig entwickeln könnten, wenn es zu einer Zuspitzung der Ereignisse käme. Würde Terror und Gewalt in unvorhergesehenem Maß zunehmen, dann käme es einer Verfehlung gleich, würden sicherheitsdienliche Überwachungsmaßnahmen unterbleiben. In diesem Fall könnten später noch weitaus schärfere Maßnahmen auftauchen. Das äquivalente Szenario wäre eine Totalüberwachungsinfrastruktur, die in die Hände eines/r Diktators/in fallen würde. Ganz ausschließen kann man selbst in westlichen, demokratischen Ländern nicht, dass eine politische Kehrtwende stattfinden könnte. Ein bereitstehendes Überwachungssystem könnte die Übel ins Unerträgliche heben.
(vgl. ebd.: 270ff.)
Ropohl, der hier deutlich ausspricht, dass er eine totale technische Überwachung mit dem geringen Nutzen, den sie bringt im Gegensatz zu den großen Schäden, die sie anrichtet, für demokratische Rechtsstaaten unangemessen hält, vergisst hier einen wichtigen Punkt: die qualitative Betroffenheit durch Übel. Der Wert der Lebenserhaltung bedingt den der Freiheit, wodurch sein Faktor höher zu bewerten ist. Ein Leben zählt mehr als die Auslebung seiner Freiheiten, die durch totale Überwachung, wie sie Ropohl in unserer Gesellschaft bereits erkennt, zumindest aus meiner bisherigen persönlichen Sicht nicht spürbar eingeschränkt werden. Der Wertkonflikt ist damit aber keineswegs aufgelöst.

In der Kontrollpolitik wird argumentiert, dass der Überwachungstrend rechtspolitisch in Ordnung gehe, weil BürgerInnen ja freiwillig und in ihrem eigenen Interesse einer funktionierenden und nach Möglichkeit auch präventiven Sicherheitslogik zustimmen würden und auch von effektiven Strafverfahren sowie dem Schutz ihres Lebens und ihrer Gesundheit profitieren. Übersehen werden dabei zwanghafte Regeln, nach denen die Zivilgesellschaft in Strafverfolgung und Fragen der Sicherheit einbezogen wird, wie beispielsweise Kontroll- und Mitteilungspflichten von Banken,

FinanzdienstleistungsträgerInnen, NotarInnen und RechtsanwältInnen bei Verdacht auf Geldwäsche und Terrorismusfinanzierung zeigen. (vgl. Albrecht 2008: 133ff.) So fordern viele PolitikerInnen zum größtmöglichen Schutze der Bevölkerung einen Einsatz aller vorhandenen technischen Überwachungseinrichtungen und diffamieren KritikerInnen als Sicherheitsrisiko. Der ehemalige britische Premierminister Tony Blair meinte sinngemäß, der Schutz der Grundrechte sei veraltet und im Zeitalter des Terrorismus nicht mehr zeitgemäß. Es brauchte daher oftmalig Eingriffe der diversen Bundesverfassungsgerichtshöfe, um weiteren überwachungsfördernden Gesetzen Einhalt zu gebieten und an die Grundrechte der demokratischen Verfassung zu erinnern. (vgl. Dix: 153ff.)

3.5.4 9/11

Nach den Anschlägen auf die New Yorker Twin-Towers am 11. September 2001 schlich sich eine Tendenz ein, BürgerInnen als Risikofaktoren, potentielle StraftäterInnen und RegelbrecherInnen zu sehen. Die Privatsphäre wurde eingeengt, unbeobachtete Freiräume, in denen terroristische Pläne geschmiedet werden könnten, minimiert. Der Weg zur Ansammlung von Daten wurde verbreitert. „Die Unbestimmtheit des Feindes findet ihre Antwort in politischen Strategien der Prävention, Vorsorge und Abschreckung des Unvermeidlichen, objektiviert in Sicherheitsanwendungen alltäglicher Überwachung.“ (Hempel 2008: 94) So meinte der US-Präsident George W. Bush in einer folgenschweren Rede über den „Krieg gegen den Terror“ Mitte September 2001: „Wir werden jede uns zur Verfügung stehende Ressource nutzen - jedes Werkzeug der Geheimdienste, jedes Instrument der Strafverfolgung, jeden finanziellen Einfluss und jede erforderliche Kriegswaffe -, um das globale Terrornetzwerk zu sprengen und zu besiegen.“ (Bush 2001)

Die Auswirkungen dieser aggressiven Politik ließen nicht lange auf sich warten. Die geforderte Überwachung hatte bereits im eigenen Land anzusetzen, BürgerInnenrechte wurden damit beschnitten, Polizeibehörden und Geheimdiensten neue Befugnisse erteilt.
Auch verdanken wir ihr staatliche Zugriffe auf die Daten der Fluggäste sowie den Umstand, dass seit dem Jahr 2008 neu ausgestellte Reisepässe EU-weit mit RFID-Funkchips ausgestattet sind, auf denen biometrische Merkmale gespeichert sind, nämlich digitalisierte Passfotos und Fingerabdrücke.

Der internationale Druck auf westliche Regierungen aktivierte ihre gesetzgeberischen Leistungen und innerhalb kürzester Zeit kamen erhebliche Gesetzesänderungen zustande, die aufgrund des Zeitmangels keiner ordentlichen öffentlichen Prüfung standhielten und somit in Grundrechte eingriffen. (vgl. Schaar 2007: 125ff.)

Mittels einer Unmenge an Daten versuchen beispielsweise Behörden, die der Terrorismusbekämpfung dienen, auf Verbrechen präventiv zu antworten. Das Augenmerk wird in das Vorfeld der Gefahrenabwehr und der Strafverfolgung gelegt. Abstrakt, aber utopisch ist dabei die Möglichkeit ein Verbrechen vor seiner Ausführung zu verhindern. Die Datensammelwut bezieht auch BürgerInnen mit ein, die sich nirgendwo schuldig gemacht haben, Risikofaktoren können schließlich überall lauern. Sicherheit gegen Freiheit, so weiten sich Mittel zur Terrorismusbekämpfung von Verdächtigen auch auf friedliebende Menschen aus.

Hempel sieht die Anschläge vom 11. September eher als Vorwand dieser politischen Verschärfungslinie.

> Terroristische Anschläge sind hierfür weniger der Ausgangspunkt als im Allgemeinen behauptet wird. Vielmehr hat eine Neubewertung des Wohlfahrtsstaats im Umgang mit der Kriminalität und der sozialen Kontrolle, wie sie im Zeichen gesellschaftlicher Transformationsprozesse […] beschrieben wird, seit Ende der 1970er Jahre einen Wandel in der Wahrnehmung von Sicherheitsrisiken vorbereitet und unter neo-konservativer und neo-liberaler Perspektive veränderte Risikokalküle und Kontrolltechniken hervorgebracht […]. Zugleich hat sich im Zuge von Globalisierungs- und Transnationalisierungsprozessen herausgestellt, dass globale Vernetzung und Mobilität Gefahren und Risiken bergen, deren Umfang die Ressourcen und Kapazitäten der traditionellen Nationalstaaten, die Sicherheit ihrer Bürger zu gewährleisten, überschreiten. (Hempel 2008: 82)

Da mögliche TäterInnen ebenfalls auf modernste Technologien zugreifen und sich temporär einen Schritt vor den Sicherheitskräften befinden, entspringt zugleich ein Wettringen um die Vorherrschaft der neuen Informations- und Kommunikationssysteme. Die Gewährleistung der Sicherheit und damit die Regulierung und Kontrolle seiner BürgerInnen lassen sich nur noch in internationaler Zusammenarbeit durchsetzen. Der Staat scheut es dabei nicht, Kooperationen in Form von Public-Private-Partnerships einzugehen. So boten nach dem 11. September viele Privatunternehmen für Marketingzwecke akribisch gesammelte Daten dem

US-amerikanischen Justizministerium an, um ihren Beitrag im „Kampf gegen den Terror“ zu leisten. Diese Daten über das Verhalten von US-BürgerInnen sollten Abweichungen von der Norm erkennbar machen und personifizieren. Während Privatunternehmen das ökonomische Risiko tragen, behält sich der Staat das Recht vor, auf die Daten bei Gebrauch zuzugreifen. Die Bevölkerung hat schlussendlich Eingriffe in grundrechtlich zugesicherte Freiheitsrechte zu dulden, denn diese Mehrfachnutzung der Daten hat eine Konfrontation des alltäglichen Handelns mit Gefahrensituationen. Zu löchrig wird die Trennung von Falschparken und Terrorismusbekämpfung in Zeiten wechselhafter Bedrohungen. Zivile Überwachungstechnologien erschließen die Infrastruktur für ihren militärischen Gebrauch. (vgl. Hempel 2008: 82ff.)

Der US-amerikanische Sicherheitsexperte Bruce Schneier kritisiert genau dieses Vorgehen gegen bekannte Gefährdungen, das er „movie plot security“ nennt, die gleichzeitig Erschwernisse für BürgerInnen durch abermalige Reglementierungen alltäglicher Vorgänge mit sich bringen, wie im Flugverkehr üblich.

> The problem with movie plot security is that it only works if we guess right. If we spend billions defending our subways, and the terrorists bomb a bus, we’ve wasted our money. To be sure, defending the subways makes commuting safer. But focusing on subways also has the effect of shifting attacks toward less-defended targets, and the result is that we’re no safer overall.
> (Schneier 2005)

Die aktuelle Debatte um Nacktscanner auf internationalen Flughäfen ist symptomatisch für die von Schneier angesprochene Verfehlung.

3.5.5 Staatliche Behörden

Nachrichtendienste sind verdeckt handelnde, staatliche Organisationen, die dem Schutz der Verfassung dienen und Informationen über feindliche, extremistische Individuen sammeln. Zu ihren Aufgaben zählen weiters Terrorismusbekämpfung und Spionageabwehr. Sie sammeln umfangreiche Datenbestände und versuchen diese bereits im Vorfeld auszumachen.

Sollten ebendiese Daten- und Informationsbestände verschiedener Nachrichten- und Geheimdienste, sowie auch die der Polizei zusammengelegt, verknüpft und für alle Sicherheitsbehörden zugänglich gemacht werden, was von PolitikerInnen bereits gefordert wurden und was auf den ersten Blick nicht unlogisch erscheint, könnte das auch Gefahren mit sich bringen.
Informationen der Nachrichtendienste unterstehen keiner gerichtlichen Überprüfung. Wenn also die Polizei auf solche Daten, die nebenbei bemerkt, nicht immer gesichert sein müssen, zugreift, wären diese Informationen und darauf folgende Aktionen nicht mit vollem Umfang gerichtlich kontrollierbar. Ein Zusammenwachsen der Sicherheitsbehörden könnte ein Eigenleben dieser nach sich ziehen, das schwierig zu durchschauen ist und der demokratischen Steuerung entgleiten könnte. (vgl. Schaar 2007: 152f.)

So kann es auch sehr bedenklich sein, wenn Nachrichtendienste unsere Telekommunikation überwachen und aufzeichnen und Verkehrs- und Standortdaten auf Vorrat mit Fristen von einem halben bis zu zwei Jahren von Kommunikationsdiensten nach EU-Richtlinie zur Verbrechensbekämpfung gespeichert werden müssen, wovon 450 Millionen EU-BürgerInnen betroffen sind. Während der Staat hier intensiv in das Leben seiner Bevölkerung eingreift, das Prinzip der Unschuldsvermutung umkehrt und der freien Entfaltung widerspricht, kann einem/r motivierten Verbrecher/in mit technischem Know-how leicht gelingen, sich den Maßnahmen der Vorratsdatenspeicherung zu entziehen (öffentliche Telefonzellen, ausländische Prepaid-Karten, usw.). (vgl. Engling 2008: 67ff.) Des weiteren ist es bedenklich, wenn staatliches Online-Hacking privater Computer betrieben wird, wenn US-Behörden internationale Geldströme kontrollieren, wenn jemand fälschlicherweise und ohne Rechtsschutz auf einer Anti-Terror-Liste landet, die mit beachtlichen Sanktionen einhergeht, wenn die Polizei und andere Behörden präventiv Daten sammeln, um kriminelle Vergehen erst gar nicht aufkommen zu lassen. Erfolg dabei konnte bisher kaum nachgewiesen werden, dafür aber das Ausforschen „unschuldiger“ Personen.

Verfassungsrechtlich vorgeschriebene Verhältnismäßigkeitsevaluationen dieser neuen Befugnisse blieben großteils aus. Jeder Eingriff in Grundrechte sollte von den GesetzgeberInnen überprüft werden, ob er einen tatsächlichen Sicherheitsgewinn garantieren kann. Ist das nicht der Fall müssen sie die Freiheitseinschränkungen revidieren. In eine solche Kosten-Nutzen-Forschung von Gefahrenabwehr und Strafverfolgung wird derzeit aber kaum investiert. (vgl. Dix 2008: 158f.)

Aber nicht nur die Sicherheitsbehörden sind eifrige DatensammlerInnen, auch die Aufrechterhaltung des Sozialstaates erfordert eine enorme Verarbeitung an teils sensiblen Daten, wie sie beispielsweise Krankenkassen über den Gesundheitszustand der Betroffenen oder Finanzbehörden benötigen, um Steuern umzuverteilen und ihre Hinterziehung zu verhindern.
Auch sollen Verwaltungsabläufe, also die Kommunikation zwischen BürgerInnen, Unternehmen und staatlichen Stellen in den meisten europäischen Ländern großteils auf elektronische Verarbeitungsverfahren, sprich eGovernment umgestellt werden.
Die Gefahr besteht wiederum, dass die BürgerInnendaten zusammengeführt werden, dabei Grundrechte und die Menschenwürde verletzt werden könnten. (vgl. Schaar 2007: 157ff.)

Noch anzumerken bleibt, dass jede/r Ausländer/in, selbst die aus der EU kommenden, verstärkt einem Datenzwang unterliegt. Neben den „gewöhnlichen" Daten, die auch von InländerInnen dokumentiert werden, gibt es zusätzlich noch Ausländerbehörden und -zentralregister, die Informationen sammeln, auf die sehr leicht von anderen Behörden zugegriffen werden kann und sie teilweise in europaweiten Datenbanken speichern. Manche neuen Datensammlungen nehmen im Ausländerzentralregister ihren Probelauf und werden dann auf die inländische Bevölkerung ausgeweitet, wie etwa die Ausweis- und Meldepflicht oder die erste zentrale biometrische Datenbank der EU für Fingerabdrücke von AsylwerberInnen (vgl. Kurz 2008: 102). Bereits der deutsche Bundesdatenschutzbeauftragte Hans Peter Bull stellte 1984 die Frage, warum AusländerInnen „durch besonders umfangreiche Datenerfassung und -auswertung diskriminiert werden" (Bull 1984: 209). Einer Gleichstellung näherte man sich seit damals nicht an, der Umfang wurde geweitet.

3.5.6 Fernmeldegeheimnis

In den Mittelpunkt der präventiven Kriminalitätsbekämpfung wie auch der repressiven Strafverfolgung rückten nach und nach Telekommunikationsdaten und entsprechende Auswertungsstrategien. Als Grundlage dafür dient ein Modell, das der Kommunikation innerhalb einer Transaktionskriminalität hohe Bedeutung beimisst. Anders als bei der individuellen Kriminalität sind kriminelle Netzwerke und Gruppierungen innerhalb des Drogen-, Menschenhandels und des Terrorismus auf ein besonderes Maß an

Informationsaustausch angewiesen, um ihre Organisation, Rekrutierungen, Rechtfertigungen, Propaganda und Planungen abzustimmen. Dabei unterliegen auch sie dem Prinzip von Angebot und Nachfrage. (vgl. Albrecht 2008: 129f.)
Wichtig sind nicht die Kommunikationsinhalte selbst, sondern viel eher Art und Weise, Häufigkeit und Struktur der Kontakte zwischen verdächtigen Personen. Diese Form der Netzwerkanalyse entstand im Militärwesen und wurde auf Verhaltensweisen von TerroristInnen und SerienverbrecherInnen übertragen. Aufgrund einer Handlungsabfolge, die sich standardisieren lässt, wie zum Beispiel bestimmte Telefonanrufe vor dem Start einer Rakete, lässt sich auf deren Folgen schließen. Ohne den Inhalt, den Code oder die Zahlenfolge zu kennen, über die in einem Anruf meist auch gar nicht gesprochen werden, lässt sich so ein Verbindungsnetzwerk erkennen und eine Ereigniswahrscheinlichkeit vorhersagen. (vgl. Lemke 2008: 175)

Elektronische, digitale Kommunikation ist aus unserem Leben nicht mehr wegzudenken - beim Telefonieren, beim Surfen im Internet, wenn wir unser „Second Life“ ausleben. All diese Verbindungen werden auf digitalem Wege vermittelt, und es fallen nebenbei allerhand Daten an, und zwar „wer mit wem wann unter Verwendung welcher technischen Einrichtung kommuniziert.“ (Schaar 2007: 111) Dies ist bei E-Mails genauso der Fall wie bei der Internettelephonie (Voice over IP) oder digital gesteuerten Gebrauchsgegenständen. Was uns nicht aus den Augen verloren gehen darf, ist, dass diese Daten viel über uns verraten und uns kontrollierbar machen. Deshalb ist auch ein festgeschriebenes Fernmeldegeheimnis von unschätzbarem Wert. Es ist eines der „zentralen Schutzrechte der Informationsgesellschaft“ (ebd.: 112). Ohne es wären das Recht auf informationelle Selbstbestimmung und sämtlicher Datenschutz nur Farce. So heißt es auch in Artikel 10a des österreichischen Staatsgrundgesetzes: „Das Fernmeldegeheimnis darf nicht verletzt werden.“ (StGG Art. 10a)
Dieses umfasst nicht nur die Kommunikationsinhalte, sondern auch die näheren Umstände der Kommunikation, also Daten darüber, wer an einem Kommunikationsvorgang beteiligt war, wo und wann er stattfand, ob überhaupt kommuniziert wurde. Es gilt sowohl für Telefongespräche, wie Internetzugänge, wie auch für E-Mail-Kommunikation. (vgl. Schaar 2007: 112)

Somit würde die Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten Eingriffe in ein Grundrecht durch Überwachungshandlungen darstellen, aus internationaler

Perspektive betreffen sie das Persönlichkeitsrecht, aus österreichischer Sicht auch die speziellen Grundrechte des Fernmeldegeheimnisses. (vgl. Albrecht 2008: 129f.).

3.5.7 Staatliche Internetzensur

Politische Aussagen können im Internet schwerwiegende Probleme bereiten. In totalitären oder autokratischen Regimes sind oppositionelle Haltungen nicht gern gesehen. So forderte die chinesische Regierung die Identifikation der UrheberInnen oppositionspolitischer Äußerungen. Der US-Internetdienst Yahoo gab der chinesischen Polizei KundInnendaten, was von Menschenrechtsorganisationen stark kritisiert wurde. Einige politische GegnerInnen wurden daraufhin entschärft und für Jahre ins Gefängnis geworfen.
Die gesamte Provinz Xinjiang wurde monatelang vom Internet abgeschaltet, weil in der Hauptstadt Ürümqi ethnische Unruhen stattfanden. Andererseits werden Blogs mit oppositionellen, unliebsamen Inhalten einfach mit ausgefeilten Firewalls blockiert und gesperrt. (vgl. Erling 2010: 24)
Kooperieren große Online-Unternehmen mit Regierungen wird es für diese leichter die Informationsströme zu leiten und zu manipulieren. Kritische Stimmen wagen sich nicht mehr zu erheben. Ein weiteres Beispiel aus China: IT-Unternehmen gaben den Forderungen der dortigen Regierung nach, die somit Inhalte über Tibet, Menschenrechte und Demokratie zensieren kann, was wiederum 360 Millionen Menschen betrifft, die in China online gehen können und deren Internetzugang China für den wirtschaftlichen Aufschwung benötigt. So drohte der IT-Konzern *Google* mit einem Rückzug aus China mit dem Argument, sich der staatlichen Internetzensur nicht länger beugen zu wollen. Selbst bei *Googles* Ankündigung, die in kurzen Auszügen in einigen Newsportalen wiedergegeben wurde, fehlten die Wörter *freie Meinungsäußerung* und *Überwachung*. (vgl. Erling 2010: 24) Erinnerungen an *1984* werden wach, denn auch im Big Brother-Staat dürfen Worte wie *frei* nicht verwendet werden und werden somit zensuriert.
Eine Überwachung des Netzes wird auch in demokratischen Verhältnissen vollzogen, hier als Mittel, um Rechtswidrigkeiten vorzubeugen. Das Internet ist auch eine Plattform, um Vorbereitungen zu illegalen Handlungen zu unternehmen und diese auszuführen, Stichwort Kinderpornographie, Bombenbaupläne, Online-Betrug. Deshalb ist eine gewisse Kontrolle von Polizei und Justiz notwendig. Das Prinzip der Unschuldsvermutung und der Grundsatz

der Verhältnismäßigkeit sollten dabei aber nicht übergangen werden, wenn präventiv Daten registriert und ausgewertet werden.

3.5.8 Naziregime

Österreich hat Mitte des 20. Jahrhunderts bereits ein schockierendes Zusammentreffen mit einem überwachenden, kontrollierenden Staatsapparat erlebt, der jegliche datenschutzrechtliche Bestimmungen missen ließ. Diese dunklen Flecken der Vergangenheit machten aber bewusst, dass eine mächtige Geheimpolizei, wie es die Gestapo war, unbedingt vermieden werden muss.
Das NS-Regime erkannte bald den Nutzen einer automatisierten Massendatenverarbeitung. Mit Hilfe von 90 Millionen Lochkarten, vom amerikanischen Unternehmen IBM bezogen, konnten sie die Bevölkerung in einer Volkszählung auch auf ihre „rassische“ Abstammung hin erfassen. Weiters diente dieses Verarbeitungssystem den Nazis zur Verwaltung der besetzten Gebiete, zur Bewältigung logistischer Herausforderungen ihrer aggressiven Kriegspolitik und schlussendlich zur Abwicklung des Holocausts und des Euthanasieprogramms.
Auch herrschte eine strenge Hierarchie vor, die beispielsweise mit tausenden freiwilligen Blockwarten und Blockleitern ausgeübt werden konnte, die alles erfahren und sich überall einschalten mussten. (vgl. Coy 2008: 48ff.)

3.6 Wirtschaftliche Überwachung

3.6.1 Wirtschaftliche Interessen

Wirtschaftlich ausgerichtete Unternehmen stehen dem Staat in Bezug auf die Größe der Datensammlung und deren Sensibilität um nichts nach. Unternehmen müssen mit dem harten Wettbewerb Schritt halten und mit einer großen Innovationsbereitschaft aufhorchen lassen können. Dadurch wollen sie ihre KundInnen besser kennen lernen und greifen vermehrt auf Daten zurück, erzeugen und verwerten Daten über das Kaufverhalten, das Bewegungsverhalten von Kaufobjekten, die Gesundheit und Bonität von Menschen. (vgl. Rammert 2007: 19)

Dies ist beispielsweise bei privaten Krankenversicherungsgesellschaften ebenso wie bei Banken der Fall. Der Unterschied in der Qualität der Datenverarbeitung liegt darin, dass öffentliche Behörden zur Erfüllung ihrer Aufgaben über Zwangsmittel verfügen. Dabei tut sich gegenüber den BürgerInnen ein Machtgefälle auf wie es ähnlich zwischen Unternehmen und KundInnen besteht. Der Rahmen für die Datenverarbeitung staatlicher Stellen ist gesetzlich durch das Datenschutzgesetz sehr genau festgelegt, während es für Unternehmen nur allgemeine Grundsätze bereitstellt, der Umfang wird im Einzelfall eher durch Interessensabwägungen ausgemacht. Es ist generell erlaubt, dass ein Unternehmen für die Erfüllung und den Abschluss eines Vertrages Daten seiner KundInnen und MitarbeiterInnen speichert, die es benötigt. Die Grenze dabei ist schwierig zu ziehen, wenn Unternehmen auch sonstige darüber hinausgehende, aber durchaus legitime Interessen wahrnehmen wollen. Müssen KundInnen beispielsweise informiert werden, wenn Informationen über sie eingeholt werden und diese zu einem umfangreichen Profil verknüpft werden?

Unternehmen erhoffen, sich einen kompetitiven, strategischen Vorteil zu verschaffen, indem sie den Blick in alle Teilbereiche schärfen. (vgl. Coy 2008: 47) Forderungen nach besserem Datenschutz werden vorschnell als wirtschaftsfeindlich abgetan, doch könnte ein solcher auch fördernd sein, weil er das Vertrauen der KundInnen und dadurch ein positives Image des Betriebs stärken kann.

In vielen Fällen kommt es zu einer Zusammenarbeit von staatlichen Behörden und privaten Unternehmen, was die Nutzung von Daten anbelangt. Wenn Strafverfolgungsbehörden Telekommunikationsdaten benötigen, müssen sie Unternehmen unweigerlich herausrücken, ob sie es wollen oder nicht. Durch die eingeführte Vorratsdatenspeicherung kann sich die Polizei beispielsweise noch leichter der hilfreichen Quellen bedienen. Die Kooperation funktioniert auch, wenn der Staat Privatunternehmen (z.B. Callcenter oder private Rechenzentren) beauftragt, personenbezogene Daten zu sammeln und zu verarbeiten. Man nennt dies *Outsourcing* oder *Public Private Partnership*. Die Verantwortungsverteilung ist dabei nicht immer rechtlich geklärt. (vgl. Schaar 2007: 179ff.)

Moderne Datenschutzkonzepte versuchen ökonomische Vorteile für die Unternehmen herauszustreichen, wenn sie auf Datenschutz setzen. Der Ruf einer Bank ist umso besser, je weniger Zwischenfälle es bezüglich Datenschutzverletzungen gibt. Es wäre verheerend, wenn sich ein Hacker Zugang zu einem fremden Konto verschaffen kann. Überhaupt rentiert sich die Investition in Datenschutz, weil etwaige Versäumnisse später oft viel teurer zu stehen kommen. Ein anderer Ansatz ist die Vergabe eines Datenschutz-Gütesiegels, das von

einer unabhängigen Prüfstelle vergeben wird und Produkte oder Dienstleistungen bezüglich datenschutzrechtlicher Kriterien qualitativ auszeichnet und das Unternehmen zu Werbezwecken nutzen könnten. (vgl. www.datenschutzzentrum.de/europrise) Die dafür notwendigen rechtlichen Rahmenbedingungen lassen schon lange auf sich warten. Ein alternativer Ansatz, Wirtschaftsunternehmen zur Einhaltung des Datenschutzes anzuhalten, wird in den USA vorgezeigt. Eine Informationsverpflichtung bei Kompromittierung ihrer Daten lässt die Unternehmen um ihren Ruf fürchten und zu verstärkten Sicherheitsmaßnahmen greifen.

Manche Wirtschaftsbereiche sind abhängig vom Anhäufen und Handeln mit personenbezogenen Daten, zum Beispiel Telefonbuchverlage und Auskunfteien. Die Daten stammen teilweise von den Betroffenen selbst, ohne dass sich diese dessen bewusst sind. Preisausschreiben, elektronische Quiz, Befragungen für VerbraucherInnen, usw. dienen oft ausschließlich der Gewinnung von Daten wie Adresse, Interessen, Einkommen, Familienverhältnisse, usw., um sie in weiterer Folge in Personenprofile einzuordnen, die sich auch gut vermarkten lassen. Dabei geht der Trend moderner Werbe- und Marketingstrategien in die Richtung eines individualisierten Marketings im Sinne eines Customer-Relationship-Management. (vgl. ITA 2009: 29) Das bedeutet, dass die interessantesten, lukrativsten KundInnen ausgewählt und Werbung und Dienste auf sie zugeschnitten werden, um eine langfristige Beziehung zu den KundInnen aufrecht zu erhalten. Dazu bedarf es ihrer persönlichen Wünsche und personenbezogenen Daten aller Bereiche, die sich durch die fortschreitende Digitalisierung leichter ermitteln lassen. Die Gefahr der personalisierten, optimierten Werbungen, Angebote und Einkäufe ist im Gegensatz zur herkömmlichen, dass Bedürfnisse gezielter gelenkt werden können und damit das Angebot und die Wahlfreiheit einseitig eingeschränkt werden. (vgl. ebd.)

Marketingunternehmen werben schließlich auch für den Adresshandel mit Daten, die sie aus dem so genannten *Profiling* bezogen: 2830 Adressblöcke und Anreden zu Pfarren und Priestern in Österreich, teilweise mit Zusatzdaten wie Telefon und E-Mail zu 0,60 Euro/Stück. Den Betroffenen bleibt einzig ein Widerspruchsrecht um der Verwendung ihrer Daten entgegenzuwirken. (vgl. Schaar 2007: 188ff.)
Auch Webshops bedienen sich der Daten, die jeder Mausklick und jeder Seitenaufruf auf ihrer Website hinterlässt. Jeder Schritt durch das elektronische Angebot wird gespeichert, Suchanfragen und Kaufabschlüsse, die auf unsere persönlichen Interessen hinweisen,

werden zu einem Profil zusammengetragen und mit Daten aus Telefonverzeichnissen und statistischen Angaben kombiniert. Hier spielen Cookies, IP-Adressen und Log-Ins wiederum eine entscheidende Rolle. Bestellt der/die Besucher/in dann tatsächlich eine Ware, werden die wichtigsten Daten lukriert, Name, Anschrift und Bankverbindung. Clubmitgliedschaften, die exklusive Dienste versprechen und bieten, binden dann den/die Kunden/in und lassen ihn/sie noch genauer kennen lernen. (vgl. ITA 2008: 29ff.)

Elektronischer Werbemüll, genannt Spam soll den VersenderInnen meist einen finanziellen Vorteil verschaffen, darum sind E-Mail-Adressen oftmals Mittelpunkt des Begehrens. Systematisch durchsuchen sie das Netz und scheuen auch nicht vor Phising-Attacken (Abfischen und Ernten von Passwörtern), Viren und Trojanern zurück, um Zugangsdaten oder Kontaktadressen auszuspionieren. Sie bieten dann Viagra oder Rolex-Uhren an, werben für Erotikseiten oder versuchen mit einem Trick, Geldbeträge zu erhalten. Sie beeinträchtigen so die Privatsphäre genauso wie aggressives Telefonmarketing. (vgl. Zeger 2008: 97ff.)

Es ergeben sich Interessenskonflikte zwischen wirtschaftlichen, profitorientierten Unternehmen und den Autonomieinteressen Einzelner. Was auf der einen Seite hohen Profit bringen soll, führt zur „De-Anonymisierung“ bei den anderen. Problemfelder sind, dass die Daten nicht anonym computergestützt verarbeitet und auch weiterverkauft werden. Personen werden identifiziert in Belangen, in denen sie dies nicht wünschen. Beispielsweise kann das „browser-behaviour“ gespeichert werden und wird es auch. Die Frage dabei ist, welche Lebensaspekte der Betroffenen eingeschränkt werden, inwieweit sie in ihrer Freiheitsausübung beschnitten werden. Schwierig wird es aber dann von Verletzungen der Privatheit zu sprechen, wenn Personen freiwillig ihre Privatsphäre beschneiden, neu verhandeln oder verkaufen, um im Gegenzug Vorteile zu erhalten. Dies geschieht beim Online-Kauf mit Kreditkarte genauso wie beim Surfen durch das Internet, währenddessen so manche Cookies am Server abgelegt werden. Das heißt, wir hätten mehr Rechte und Möglichkeiten, unsere Privatheit einzufordern, nehmen diese aber nicht wahr. Es ist aber keineswegs so, dass wir nur arme, den datenhungrigen Unternehmen ausgelieferte „Opfer“ sind, nein, wir sind auch selbst potentielle TäterInnen, wenn wir (vor allem in den USA übliche) „nannycams“ einrichten, Videokameras, die dazu dienen, Kindermädchen oder -jungen zu filmen und auf ihr artiges Verhalten hin zu prüfen. Rössler spricht vom „egalitäre[n] Panoptikon“ (Rössler 2001: 232). Sie warnt auch, vor einer gewissen

Gleichgültigkeit davor und Gewöhnung daran, gewisse Formen von Privatheit nicht mehr als gesichert anzusehen und sie in ihrer Wichtigkeit abzustufen, zu vergessen, wie ein autonomes Leben allererst aussehen kann. (vgl. Rössler 2001: 231ff.)

3.6.2 Bonität

Banken tragen bei der Vergabe von Krediten ein Risiko mit sich. Es kommt vor, dass KreditnehmerInnen einen solchen nicht zurückzahlen können. Dasselbe gilt für andere Branchen, die das Risiko eingehen, dass KundInnen aus welchen Gründen auch immer ihre Rechnungen nicht bezahlen. Um solchen Fällen vorzubeugen, wissen sich wirtschaftliche Unternehmen mit zweierlei Mittel zu helfen. Einerseits wird von vergangenem auf zukünftiges Verhalten geschlossen. Wenn also eine Person einmal artig seine Rechnung beglichen hat, wird erwartet, dass sie dies wieder tun wird, wenn nicht, wird mit ihr wahrscheinlich kein künftiger Vertrag abgeschlossen werden. Andererseits greifen Unternehmen, falls keine bisherigen individuellen Erfahrungen vorliegen, auf bekannte Daten wie Einkommen, Alter, Wohnort zurück und berechnen statistisch Näherungswerte (Score-Werte) zur Kreditwürdigkeit. Ist diese nicht hoch genug, kann es sein, dass eine Kreditvergabe nicht mehr zustande kommt bzw. nur zu erhöhten Zinsen, Waren nur gegen Vorkasse ausgeliefert werden und die persönlichen Daten an eine Auskunftei gesendet werden, die sie im Sektor weiter verbreitet. Klar ist es legitim, dass sich Unternehmen absichern und ihren Fokus auf finanzstarke VertragspartnerInnen legen, aber der Ansatz ist rechtsstaatlich etwas problematisch, wenn solche Informationen nicht nur betriebsintern Verwendung finden, sondern Branchen übergreifend weitergegeben werden. Ein falscher, veralteter Eintrag in die Datenbank kann dann zur Folge haben, dass eine Person einen Handyvertrag nicht gewährt bekommt. (vgl. ITA 2008: 29)

Auskunfteien sammeln die Daten ihrer VertragspartnerInnen und geben ihnen dafür die gewünschten Auskünfte über KundInnen. Sie bekommen beispielsweise Informationen von Banken, die wiederum über ihre Klientel Daten erheben und diese weiterreichen, aber auch Versicherungen, Telekommunikations- und Immobilienunternehmen, der Versandhandel und Zahnärzte/innen sind Teil solcher Auskunftssysteme. Auskunfteien funktionieren wie Warnsysteme, sie ermessen die Bonität von Personen, suchen weitere Informationen und ermitteln die Wahrscheinlichkeit, mit der sie ihre Rechnungen begleichen werden. Der

Mensch wird als Ich-AG angesehen, wird wie ein Unternehmen behandelt, seine Bilanzen und seine Finanzkraft werden ermittelt. Wird ein Risiko gesehen, warnen Auskunfteien ihre GeschäftspartnerInnen, eine Einwilligung der Betroffenen ist hierzu nicht nötig. Ist jemandem beispielsweise ein Konkursverfahren anhängig, wird diese Information gespeichert und weitergegeben. Es liegt dann im Ermessen des Unternehmens, wie darauf reagiert wird, ob man einen Kredit genehmigt, höhere Zinsen verlangt, usw., es ist aber üblich, Score-Werte automatisiert in die Berechnung von Konditionen einzubeziehen. Bei solch brisanten Daten, ist es sehr unangenehm, wenn aufgrund von Verwechslungen oder unzulässigem Meldeverhalten Nachteile entstehen, die Fehlerquote ist nämlich erstaunlich hoch. (vgl. Zeger 2008: 89ff.)

3.6.2.1 Scoring

Scoring-Systeme (score ist englisch und bedeutet übersetzt Punktzahl) berechnen die Kreditwürdigkeit von Personen, wenn keine bisherigen Erfahrungen aufliegen, können vom tatsächlichen Verhalten der Betroffenen aber abweichen.
Sie „errechnen mittels mathematisch-statistischer Verfahren die individuelle Wahrscheinlichkeit für den Eintritt eines Risikos, wobei unterschiedlichste Daten berücksichtigt werden.“ (Schaar 2007: 198) Die Bonität der KundInnen wird somit in eine Bewertungsskala eingetragen, die verschiedene „Rating-Stufen“ umfasst, und schließlich den VertragspartnerInnen der Auskunfteien angeboten.
Das Problem solcher Systeme ist die mangelnde Transparenz. Auskunfteien lassen sich ungern in die Karten schauen und geben kaum Auskunft darüber, wie sie den Score-Wert berechnen und welche Daten genau sie dazu heranziehen. Es kamen aber bereits einige Details ans Tageslicht, die an der Gerechtigkeit der Scoring-Systeme zweifeln lassen. Eines davon nennt sich Geoscoring, im Deutschen Georeferenzierung. Bei dieser Methode schließt man von der Wohnadresse auf die Bonität, versucht mit statistisch unterfütterten Voraussetzungen eine objektivierbare Grundlage zu schaffen. Sie nahm ihren Ursprung in den USA der 20er Jahre. Stadtgebiete, denen man nur eine finanzschwache Bevölkerung zutraute, wurden rot umrandet. Dieses „Redlining“ führte dazu, dass Menschen aus diesen Zonen kein Kredit gewährt wurde mit der Konsequenz, dass diejenigen, die es sich leisten konnten, in besser klassifizierte Gegenden umzogen. Geosoziale Auswirkungen lagen auf der Hand, übrig blieb eine arme Bevölkerung meist zusammengesetzt aus ethnischen

Minderheiten. In weiter Folge beeinflusste die georeferenzierte Risikobewertung so das Stadtbild und führte unter anderem zu Verslumung, auch heutzutage kann es zu negativen Konsequenzen wie Diskriminierung und Ausgrenzung für Menschen und Regionen beitragen. (vgl. ebd.: 198ff.)

Die Gefahr sozialer Diskriminierung besteht auch darin, dass Betroffene trotz eigenen Handelns kaum Einfluss auf negative Bewertungen haben. Sie erfahren in manchen Fällen nur gegen Bezahlung einer Gebühr, in den anderen Fällen gar nicht, das Zustandekommen ihres Score-Wertes, weil der einem Betriebs- und Geschäftsgeheimnis unterliegt. Eine weitere Gefahr besteht wiederum in der Zusammenschaltung verschiedener Systeme, wodurch Betroffenen dann in mehreren Branchen Nachteile entstehen können, weil sie innerhalb der einen nicht vertragsgemäß gehandelt hatten. Klare Regelungen, unter welchen Bedingungen Daten über SchuldnerInnen und deren wirtschaftliche Integrität gesammelt werden dürfen, welchen Qualitätskriterien sie unterliegen und wann sie gelöscht werden müssen, existieren nicht. (vgl. Zeger 2008: 93)

Eine weitere negative Konsequenz der wirtschaftlichen Datenverarbeitung liegt darin, dass mittellose Menschen, die kaum Chancen haben, ihre Interessen durchzusetzen, eine weitere Diskriminierung erfahren. Der „digital gap“, also die Spaltung der Bevölkerung hinsichtlich des Zugangs zu und der Nutzungsmöglichkeiten von elektronischen Diensten nach regionalen, sozialen und altersmäßigen Kriterien wird sich erweitern, wenn der Staat die wirtschaftliche Informationsverarbeitung nicht reguliert. Soziale Gruppen oder einzelne Personen werden benachteiligt, wenn sie nur noch gegen Vorkasse bestimmte Dienstleistungen und Produkte erhalten. So kann es sein, dass jemand keinen Handyvertrag bekommt, wenn er die falsche Adresse oder einen schlechten Score-Wert hat und Strom- und Gasanbieter liefern nur noch gegen Vorzahlung. Solche Prepaid-Modelle für schlecht Beleumundete sind in Großbritannien in Kraft.

3.6.3 UrheberInnenrecht

> [T]he problems of privacy and copyright are exactly the same. With both, there’s a bit of ‘our’ data that ‘we’ve’ lost control over. In the case of copyright, it is the data constituting a copy of our copyrighted work; in the case of privacy, it is the data representing some fact about us. In both cases, the Internet has produced this loss of control: with copyright,

> because the technology enables perfect and free copies of content; with privacy, [...] because the technology enables perpetual and cheap monitoring of behavior.
> (Lessig 2006: 200)

Das Urheberrecht stellt aufgrund Entwicklungen in den letzten Jahren einen erheblichen Eingriff in den Datenschutz dar. Es dient dazu geistiges Eigentum wie Filme, Musikstücke, Computerprogramme und weitere mediale, digital festhaltbare Inhalte zu schützen. Der Vorteil, den die Unterhaltungsindustrien von der einfachen, kostengünstigen Reproduzierbarkeit und elektronischen Vervielfältigung digitalisierter Werke erhalten, erweist sich auch als Nachteil, weil die KonsumentInnen dies genauso gut praktizieren, wie der Hype um Online-Tauschbörsen wie *Napster* und Co zuletzt belegen. Die Antwort auf die Mehrfachverwendung von Seiten der Industrie reicht von straf- und zivilrechtlichen Klagen bis hin zu Digital-Rights-Management-Systemen wie Kopierschutzmaßnahmen oder die persönliche Erfassung der NutzerInnen und ihres Nutzungsverhaltens. Um Musiktitel, Filme und Programme zu erhalten, muss man sich registrieren. Dadurch kann dann bei Verbindung mit dem Internet mittels IP-Adresse von den ServerbetreiberInnen protokolliert und lokalisiert werden, wer zu welchem Zeitpunkt an welchem Ort einen bestimmten Song hört. Die Überwachten nehmen davon meist keine Kenntnis. (vgl. Weber 2008: 284f.)
Ein Kniefall der europäischen Politik vor den Lobbys der Musik-, Film- und Softwarebranche brachte ein Gesetz, das den Rechteinhabern einen generellen Auskunftsanspruch einräumt. So müssen ihnen InternetanbieterInnen auf Anfrage die passenden Namen usw. zu auffällig gewordenen IP-Adressen nennen. Die Vorratsdatenspeicherung von Telekommunikationsdaten kommt ihnen dabei weiter entgegen. (vgl. Albrecht 2008: 131)
DatenschützerInnen fordern aber die Möglichkeit einer anonymen Nutzung digitaler Medien, die Identität sollte nicht auf Servern erfasst sein.

3.6.4 Online-Marketing

Online-Marketing ist die Boom-Branche des Internets. Dabei geht es gar nicht rein um Werbung, sondern um *Tracking* und *Targeting*, was soviel wie *nachspüren* und *treffen* bedeutet. Internet-UserInnen sollen aufgespürt und identifiziert werden und wenn sie ihre Fährte verwischen, gilt es ihre Spur wieder zu finden.

Die Unternehmen brauchen dabei gar keine formale Identität des/der Internetuser/in. Mittels IP-Adressen, Cookies, Browsererkennungsmethoden, identifizierender Links und verknüpfter Inhalte reicht es, für jede/n Benutzer/in ein Online-Pseudonym anzulegen, das er/sie nicht ablegen kann, Dazu werden individualisierte Informationen gespeichert. Das heißt, es ist für das Online-Unternehmen nicht relevant, die UserInnen mit ihrem tatsächlichen Namen zu benennen. Sie geben ihnen Pseudonyme wie 0df4586gk6k49495zt4 ordnen diesen ganz individuelle Interessen usw. zu. Kauft diese Person dann etwas, muss sie ohnehin ihren Namen, Bankdaten, Zustelladresse, die Identität lüften.
Was ein Mensch im Internet anschaut, was er sucht, dafür interessiert er sich auch. (Kaum jemand gibt 20 irreführende Suchanfragen ein, um erst dann die relevante einzugeben.) Diese Interessen können zusätzlich noch glaubhafter ausgemalt werden, weil Anzahl der aufgerufenen Seiten, die Verweildauer und die Intensität einer Suche noch detaillierter verraten, wer sich für was erwärmt. Den UserInnen werden lokale Suchfunktionen, kontextspezifische Werbung, Hilfsprogramme, Toolbars und Plugins angeboten, die auf anderer Seite das Tracking erleichtern sollen. (vgl. Zeger 2009: 96ff.)

Dabei muss erwähnt werden, dass der Markt im Internet nicht auf beliebig viele TeilnehmerInnen aufgeteilt wird, sondern dass ihn weniger als 100 Konzerne beherrschen.

> Der Mythos, das Internet würde dezentral aufgebaut sein und wäre deswegen schwer zu überwachen, hat leider nichts mit der Realität zu tun. Der weltweite IP-Verkehr wird über eine kleine Anzahl von Leitungsanbietern abgewickelt und fließt durch wenige Knotenpunkte. So kann mit vergleichsweise wenigen, aber strategisch gut platzierten Hochleistungsabhörsystemen die Überwachung von immer mehr Kommunikationsverbindungen konzentriert und somit die Kosten gesenkt werden.
> (Rieger 2008: 65)

So fielen nach den Terroranschlägen vom 11. September, als die Schaltzentrale des Telekommunikationsunternehmens *Verizon* beschädigt wurde und wenig später mehrere Internet-Schaltzentralen im Welthandelszentrum zusammenbrachen, Netzwerke nicht nur in New York City aus, sondern weltweit. Aus Kostengründen liefen Schaltkreise über New York City, in Südafrika aber verschwanden sämtliche .za-Websites für Tage aus dem Internet. (vgl. Schulzki-Haddouti 2004: 50f.)
Mutterfirmen und Tochterunternehmen, Webserver und abhängige Webportale, alle sammeln sie Informationssplitter, die untereinander ausgetauscht werden, wobei es gar nicht notwendig ist, die Personendaten wirklich weiterzugeben, man benötigt nur ein

gemeinsames Merkmal, das die UserInnen sicher identifiziert. So arbeitet eine bekannte Blogging- und Website-Plattform unerkannt mit einer erfolgreichen Online-Marketing und -Business-Firma zusammen, das alles unwissentlich unter dem Namen *Yahoo!*. So gehört *Youtube* zu *Google*, *Geocities* und *Flickr* zu *Yahoo!*, *Myspace* zu *Murdoch/Fox* usw.

Mit Hilfe von Data-Mining-Tools wird schließlich versucht, Erkenntnisse über die UserInnen zu gewinnen. Diese funktionieren so, dass sie Ziele weitgehend selbstständig verfolgen können, das heißt „ohne intensive Interaktionen mit dem Benutzer“ (Bodendorf 2006: 46). Dabei generieren sie Hypothesen über mögliche Zusammenhänge, Muster oder Trends, überprüfen sie anhand der Daten und stellen ausschließlich die als gültig erkannten als Ergebnis zurück. Ein häufig angewandtes Verfahren ist das der „Entdeckung von Assoziationsregeln für Elemente eines umfangreichen Datenbestands.“ (ebd.) Tritt beispielsweise ein Ereignis A auf, kann mit Hilfe der Assoziationsregeln festgestellt werden, wie sicher dann das Ereignis B auch zutreffen wird. Empfehlungen bei *Amazon* arbeiten in dieser Weise: Leute, die sich für dieses Produkt entschieden, haben auch das Produkt gekauft.

Auch *Facebook* versucht die Profile und die ungeheure Datensammlung, für die sie schließlich Speicherplatz zur Verfügung stellen, gewinnbringend zu verwerten. 2007 erregte das Unternehmen Aufsehen als es betonte, das System *Facebook Ads* aufzunehmen, das Werbung in die Profile seiner UserInnen einschleust. Die MitgliederInnen können selbst angeben, welche Websites sie gerne ansehen und welche Produkte sie kaufen, ganz nach dem Motto Mark Zuckerbergs, nichts würde die Empfehlung eines/r guten Freundes/in toppen. Doch auch *Myspace* arbeitet mit *Google* zusammen. Es hat dessen Suchfunktion und das Werbesystem *AdSense* integriert und erhält dafür Millionen. (vgl. Zeger 2009: 101ff.)
Übrigens konnten die bekanntesten Social Networks in einer Studie des Fraunhofer Instituts für Sichere Informationstechnologie hinsichtlich des Privatsphärenschutzes nicht überzeugen. (vgl. Fraunhofer Institut (SIT) 2008: 117)

Andererseits sind es die UserInnen selbst, die sich innerhalb eines ganz engen Horizontes in der virtuellen Welt bewegen. Während unseres Surfvorgangs stellen Verlinkungen, Suchmaschinen und Themenportale die Wellen dar, die uns antreiben. Aber meist bewegt man sich sowieso auf dem bekannten Terrain. Man braucht sich nur selbst zu beobachten, immer wieder werden dieselben Websites aufgerufen. Trotz der Millionen Internet-

Angebote bleibt der Aktionsraum erstaunlich klein. Somit lässt sich das Webverhalten auch leichter ausspähen.
Online-TrackerInnen zielen darauf ab, das Verhalten der UserInnen im ökonomischen Sinne zu steuern. Die Effektivität dieser Methoden ist zwar noch nicht sehr hochrangig, aber stehen sie schließlich noch am Anfang. Bessere Identifizierungen und Auswertungsmöglichkeiten lassen die Unternehmen von wunderbaren Zeiten träumen, denn schließlich wird der Pool der UserInnen nicht von staatlichen Grenzen umzäunt. (vgl. Zeger 2009: 104f.)

3.7 Gesellschaftliche Vorteile der Überwachung

Vorteile, die sich die AuftraggeberInnen von ihren Datensammlungen und von einer Überwachung erwarten dürfen, sind hier nicht explizit erwähnt. Für Unternehmen stellen diese natürlich einen Nutzen und Mehrwert dar, auch der Staatsapparat lässt sich mit diesen in seiner Effizienz steigern.

Die Vorteile der Überwachung sind offensichtlich, greifbar und nicht zu leugnen. Personen können sich physisch sicherer fühlen und ihr Eigentum als besser geschützt ansehen. Finanzielle Vorteile können sich ergeben, indem Fehler, Missbrauch und Betrug leichter aufgedeckt und vorgebeugt werden. Dies gilt sowohl für den Staat als auch für den privaten Sektor. Auch die abschreckende Wirkung, die Überwachungsmittel verbreiten, kann als symbolischer, moralischer Gewinn gesehen werden. (vgl. Clarke 1987)
Ähnlich beschreibt das Gottschalk-Mazouz. Zuerst erfahren wir ein Sicherheitsgefühl. Wir können uns an bestimmte Orte trauen, weil sie beispielsweise videoüberwacht sind, müssen nicht ständig auf Bedrohungen reagieren und gewinnen deshalb Zeit und Sicherheit für autonome Entscheidungen. Dann ermöglicht sie uns eine Stabilität in unseren Erwartungen, wir können von anderen erwarten, dass sie Spielregeln und Gesetze einhalten, also korrekt handeln. Sie kann einen gemeinsamen Hintergrundkonsens bei den Überwachten schaffen, wenn diese beispielsweise angenommen oder tatsächlich mit den Zielen der Überwachung einverstanden sind. Gottschalk-Mazouz sieht hier Ähnlichkeiten bei Überwachung, Recht und Moral in Bezug auf die Internalisierung von Werten und Normen. Überwachung kann weiters Verantwortung abnehmen und damit Personen entlasten. Manche Menschen fühlen sich wohl dabei von einer höheren Instanz, wie dem/der Vorgesetzten überwacht zu werden,

da sie möglicherweise korrigierend eingreift und sagt, was man falsch macht. Überwachung scheint auch einen Einfluss auf die Identitätsbildung von Jugendlichen zu haben. „[I]n einer Art reziproker juveniler Überwachungskultur“ (Gottschalk-Mazouz 2008: 215) stellen sie sich selbst mittels Bild, Ton, Film und Wort öffentlich zur Schau und konsumieren zugleich die Zurschaustellung anderer und reagieren darauf. Sie geben ihre Privatheit preis, um andere zu beeindrucken, einem eitlen Narzissmus zu frönen, sich vom Selbst zu befreien oder aus vielen anderen möglichen Gründen. Überwachung wird mehr und mehr normal, sowohl aktiv zu überwachen oder passiv überwacht zu werden. Damit steigen soziale und technische Zwänge, sich seinen Mitmenschen in unseren Handlungen und der Verwendung technischer Artefakte anzupassen und somit potentielle und reale technisierte Überwachung zu akzeptieren. (vgl. ebd.: 214ff.)

3.8 Gefahren der Überwachung

Viele Gefahren wurden bereits in anderen Kapiteln zu den jeweiligen, dort angesprochenen Aspekten passend diskutiert. Hier seien überblicksartig nochmals die wichtigsten Gefahren angeführt.

Datenschutz hat in Deutschland seit 1983 den Status eines Grundrechts. Damals kam das deutsche Bundesverfassungsgericht zu seinem berühmten, oft zitierten Volkszählungsurteil. Es stellte unter anderem fest:

> Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.
>
> (zitiert nach Schulzki-Haddouti 2004: 159)

Gelangen Menschen, seien es PassantInnen oder KundInnen, in den Umstand des Wissens, dass über sie Daten gesammelt und weiterverarbeitet werden, kann und wird dies zu einer Beeinträchtigung ihres Verhaltens, ihres Denkens und Empfindens führen. Die Daten erhalten eine Macht über Gedanken und Äußerungen. Die Freiheit des/r Einzelnen wird gehemmt. (vgl. Rammert 2007: 18 und Albrecht 2008: 132)

Eine weitere Gefahr ist, dass das Verfügen über ein System, das auf hoher Interdependenz basiert, mit strategischen Vorteilen verbunden ist. Wer sich Zugang und Kontrolle über das System verschafft, sich beispielsweise einhackt, kann Informationsströme dirigieren, Tätigkeiten blockieren oder erzwingen und so schließlich andere zu einem gewissen Grad kontrollieren. (vgl. Gottschalk-Mazouz 2008: 218ff.)

Des Weiteren gerät man in der „elektronischen Erfassungsgesellschaft“ (Schaar 2007: 14) leicht in Verdacht, gegen gewisse Gesetze verstoßen zu haben. Zu beweisen gilt dann die eigene Unschuld. Bei der Verwendung des Internets kann dies zum Beispiel sein, dass wir bezeugen müssen, dass wir keine urheberrechtlich geschützten Werke aus dem Netz downgeloaded haben oder dass wir zwecks Forschungsinteresse auf rechtsextremen Seiten gestöbert haben und nicht wegen der politischen Übereinstimmung.

Eine Zusammenfassung wirklicher und potentieller Gefahren der Datenüberwachung bietet Clarke:
Bei einer Überwachung einzelner Personen:

- Fehlidentifikation (Wenn Daten einer falschen Person zugeordnet werden)
- Schlechte Qualität der verwendeten Daten
- Verwendung von Daten außerhalb ihres ursprünglichen Zusammenhangs und daraus resultierende Gefahr von Fehlinterpretationen
- Qualitativ schlechte Entscheidungen
- Fehlendes Wissen der Betroffenen von der Überwachung und von Datenflüssen
- Fehlende Zustimmung der Betroffenen
- Aufnahme in schwarze Listen
- Verweigerung der Löschung oder Korrektur

Bei einer Massenüberwachung von Personengruppen oder der gesamten Bevölkerung:

- Risiken für die Betroffenen:

- Willkür
- Verknüpfung von Daten außerhalb ihrer ursprünglichen Zusammenhänge (und daraus resultierende Gefahr von Fehlinterpretationen)
- Komplexität und Missverständlichkeit von Daten (aus unterschiedlichen Quellen)
- Hexenjagden, indem aus bestimmten statistischen Wahrscheinlichkeiten Schlüsse abgeleitet werden, die nicht immer zutreffen
- Vorab-Diskriminierung und Schuldvorhersage
- Manipulation durch gezielt selektive Werbung
- Umkehr der Beweislast
- Verdeckte Überwachungsoperationen
- Anschuldigungen von Unbekannten und unbekannte BeschuldigerInnen
- Verweigerung eines ordentlichen, rechtsstaatlichen Verfahrens

o Risiken für die Gesellschaft:

- Vorherrschendes Klima des Misstrauens
- Feindliche Beziehungen, Gegnerschaft
- Konzentration der Strafverfolgung auf leicht ermittelbare und beweisbare Straftaten (anstatt auf professionelle und organisierte Kriminalität)
- Ungleicher Gesetzesvollzug
- Verlust an Achtung für das Gesetz und die Vollzugsbehörden
- Individuelle Handlungen verlieren an Bedeutung
- Verlust an Eigenständigkeit und Selbstbestimmung
- Herabmachung der Eigenständigkeit und Originalität
- Verstärkung der Tendenz, sich aus der offiziellen Gesellschaft auszuklinken
- Schwächung der moralischen Verbundenheit der Gesellschaft
- Destabilisierung der Ausgewogenheit der strategischen Machtverhältnisse
- Repressives Potenzial für eine totalitäre Regierung

(Clarke 1987)

3.8.1 Gefahren in Social Networks

Zeger sieht die Gefahren der Social Communities nicht im Exhibitionismus oder Daten-Striptease und den unanständigen Meinungen der TeilnehmerInnen, sondern woanders. PlattformbetreiberInnen haben eine Art von Zensur- und Sanktionsmacht. Sie stellen Geschäftsbedingungen bereit, die sie einseitig abändern können. So können Foren kostenpflichtig werden, ihre formalen Regeln überwacht, bestimmte Meinungen und Aussagen gelöscht, UserInnen von den BetreiberInnen gar ausgeschlossen werden. Auf *Myspace* wurde beispielsweise die religionskritische „Atheist and Agnostic Group“ zuerst gänzlich gelöscht und erst später nach Protesten wieder hergestellt, wobei viele MitgliederInnen ausgesperrt blieben.
Online-Diensten wird eine gewisse Privatsphäre anvertraut. Diese kann von Personen und Unternehmen aber hintergangen werden. Nutzt man die Daten dort für andere Zwecke als der vorgesehenen, so tritt ein Fall von Missbrauch ein. Wer andere ausspäht, zum Beispiel ArbeitgeberInnen, Kreditinstitute, WohnungsnachbarInnen oder zu manipulieren versucht, Werbe- und Marketingunternehmen eventuell, missbraucht fremde Daten.
Manchmal werden Menschen wohl unbeabsichtigt gegen ihren Willen in die Datenmaschinerie hineingezogen. Wer Freundschaftswerbungen oder Weiterempfehlungen ausschickt, gibt Daten von anderen meist ohne deren Zustimmung und Wissen her.
Eine selbsternannte Gattung von Cybercops setzt sich selbst als Ziel, „illegales“ Verhalten im Web aufzudecken, wie immer sie illegal dann auch definieren. Das können anstößige Bilder sein, unerwünschte Meinungen, Beleidigungen aller Art, Spam-Aktivitäten, usw. Diesen Cops stehen viele geeignete Methoden zur Verfügung, dieses Verhalten zu verhindern, wie zum Beispiel Sperren der IP-Adresse, Blockieren ganzer Netzwerke, Angriffe mit Würmern und Viren oder Identitätsdiebstahl. Überwachung wird in Communities normal. Auf großen Plattformen gibt es meist Links mit der Aufforderung, Unerwünschtes zu melden. Sie versuchen damit, mögliche Eingriffe von Seite der Behörden und der Politik zu umgehen. (vgl. Zeger 2009: 61ff.)

3.9 Ausweg, Besserung, Lösungsvorschläge

Gaycken vergleicht die DatenschutzaktivistInnen mit Fachärzten, denen man auf keinen Fall hypochondrisches Verhalten unterstellen darf. Sie sind SpezialistInnen, die bereits

wahrnehmen, was in Raum und Zeit noch weit entfernt liegt und die ein Bewusstsein schaffen sollen, in das die Öffentlichkeit Einsicht nehmen kann. Eine explizite Politisierung kann erst dann stattfinden. (vgl. Gaycken 2008: 27)

Ein solcher Aktivist ist Peter Schaar. Er fordert ein wachsendes Bewusstwerden der Gefahren von Überwachung und Datenmissbrauch zum Schutze der Privatsphäre. Da einzelne Gesetzesanträge und Novellierungen mit dem Fortschritt an Technik und Technologien nicht Schritt halten können, fordert er eine globale Ethik des Datenschutzes innerhalb des Informationszeitalters und einen verantwortungsbewussten Umgang mit seinen technischen Möglichkeiten, „ethische Grundsatzentscheidungen darüber, wie unsere Gesellschaft mit den Techniken und den dabei entstehenden persönlichen Datenspuren umgehen will." (Schaar 2007: 218) Versuche dazu wurden schon gemacht, wie in der *Erklärung von Montreux*, auf der 27. Internationalen Datenschutzkonferenz 2005, ihre Anerkennung reicht über einen gewissen Kreis von Gleichgesinnten kaum hinaus. (vgl. Schaar 2007: 217ff.)
So fordert auch Philippe Quéau, Direktor der UNESCO-Abteilung für Information und Informatik eine philosophische Ethik für die globale Informationsgesellschaft, die die Grundlage für eine Politik auf metanationaler Ebene legt, um dann die Früchte einer Ökonomie des Immateriellen zu ernten. Denn wie er es beschreibt: „Wir befinden uns in einer Welt ohne Steuermann - in den Händen von blinden, irrationalen Kräften, gesteuert von ‚unsichtbaren Händen' ohne Gehirn und Herz mit sehr kurzfristigen Zielen." (Quéau 1998)

Schaar verlangt, dass bereits bei der Herstellung moderner technischer Geräte und Technologien diese grundrechtskonform gestaltet werden. Datensparsamkeit und -vermeidung sollen gewährleistet werden. Den NutzerInnen soll ein Höchstmaß an Anonymität zugestanden, personenbezogene Daten erst gar nicht erfasst werden. In der Praxis ist aber eher das Gegenteil der Fall, alle Möglichkeiten von Verarbeitungssystemen werden ausgelotet, eher erwartet man sich Vorteile von zusätzlichen, vorerst gar nicht benötigten, aber leicht zu speichernden Daten. Umfassender und ausreichender Datenschutz kann nur erreicht werden, wenn eine angemessene Technik und IT-Sicherheitsmaßnahmen zur Unterstützung herangezogen werden können. Der Datenschutz sollte dabei schon im Vorhinein in die Planung und das Design der IT eingepflanzt werden. Nachbesserungen führen zu einem weitaus schlechteren und meist auch kostenintensiveren Ergebnis. Eine

Verbindung oder Mehrfachnutzung von Datenbeständen, die zu verschiedenen Zwecken generiert wurden, sollte nur ausschließlich und unter genau geregelten und kontrollierten Bestimmungen erfolgen können. Außerdem hätten HerstellerInnen für BenutzerInnenfreundlichkeit und Transparenz bezüglich Möglichkeiten und Konsequenzen ihrer technischen Produkte Sorge zu tragen. (vgl. Schaar 2007: 220ff.) Der Datenschutz will den technologischen Fortschritt innerhalb der Informationsgesellschaft gar nicht beschränken oder aufhalten, aber er will ihn mitbestimmen und prägen, um nicht in einer Überwachungsgesellschaft zu landen, denn „[d]er Mensch ist Subjekt, nicht Objekt der Information." (ebd.: 230) Doch auch der Datenschutz selbst muss dynamisch bleiben und sich weiterentwickeln.

Auch Gaycken fordert technische Gegenmaßnahmen, da soziale Regulierungen keine fixen, unabänderlichen Größen sind. Gehandelt werden muss sofort, bevor sich negative Dynamiken und Konsequenzen vollends entfalten können. Eine zentralisierte, geistige Kontrolle kann eine Bedrohung für Menschenrechte im neuen technischen Zeitalter werden. Die Überwachungstechnologie „bietet so entsprechend gesonnenen und ausgestatteten Akteuren die attraktive Option der Kontrolle über die erste Grundlage jeder Kritik an Gewalt und Unrecht: den menschlichen Geist." (Gaycken 2008: 42) Ähnlich wie das natürliche Klima muss man auch das geistige Klima präventiv schützen, weil deutliche Eingriffe im Nachhinein viel schwieriger zu beheben sind, auch wenn ihre Auswirkungen nicht ganz so klar auf der Hand liegen. Geistige Freiheit ist eine kulturelle Errungenschaft und Voraussetzung für Demokratie und Gerechtigkeit, sie durchzieht unsere Ausformungen von Politik, Wissenschaft, Wissen, Kultur, Individualität und Gemeinschaft und bedarf deshalb besonderer Achtung. (vgl. ebd.: 42f.)

Überhaupt weg von der technischen Überwachung will dagegen Dix. Es wird vonseiten der PolitikerInnen viel zu selten angedacht, den Fokus weg von den technischen Möglichkeiten von Überwachung zur Sicherheitserhöhung auf die wirklichen Ursachen von Terrorismus, Kriminalität usw. zu legen. Finanzielle Investitionen könnten auch in die Islamwissenschaften zur Erforschung der Wurzeln des fundamentalistischen Terrors fließen, menschliche Intelligenz könnte anstatt technischer gefördert werden. (vgl. Dix 2008: 156f.)

Entscheidend für die Zukunft des Datenschutzes wird auch die Adaption und Modernisierung des zugehörigen Rechts sein. Das derzeitige ist kompliziert verfasst, in

Einzelgesetze zerstückelt, schwierig zu vereinbaren und hinkt dem gesellschaftlichen und technologischen Fortschritt hinterher. Im Idealfall sollte es aber „Richtmarken für die Zukunft der Informationsgesellschaft“ (Schaar 2007: 226) setzen.
Wirtschaftsunternehmen gelingt es leicht, rechtliche Bestimmungen zu umgehen, indem sie sich die Einwilligungen der Betroffenen bei Vertragsabschluss holen. Das täuscht Freiwilligkeit und Eigenverantwortung vor, aus Mangel an Alternativen unterliegen die VerbraucherInnen aber einem gewissen Zwang, Informationen preiszugeben, wenn sie beispielsweise den Kredit oder Job haben wollen. Des Weiteren sind Datenschutzverstöße schwer zu ahnden und die Bußgelder selbst für schwere Vergehen sind im Vergleich zu Kartellrechtsverstößen Peanuts, was jene Rechtsbrüche zu Kavaliersdelikten degradiert.

Wichtig ist auch, dass ein sinnvolles Datenschutzrecht global gilt, weil elektronische Datenverarbeitung in andere Länder ausgelagert wird, wo sie dann dortigem Recht unterliegt. Innerhalb der EU-Mitgliedstaaten ist das Niveau des Datenschutzes relativiert zu anderen Ländern (außer der Schweiz, Kanada und Argentinien) hoch. In außereuropäischen Ländern genießt man den Vorteil, dass die Lohnkosten meist niedriger sind, dafür erlauben sich staatliche Stellen, Zugriffe auf die Daten zu fordern und erhalten diese auch, wie das Beispiel China verdeutlicht.
Die Relevanz einer globalen Ethik erklärt sich auch bei der internationalen Zusammenarbeit von Polizeibehörden und Nachrichtendiensten. Was in dem einen Staat als rechtens gilt, wird im anderen als illegal angesehen. So kann es sehr problematisch sein, wenn Daten weitergereicht werden, die dann der Verfolgung politischer Delikte dienen. (vgl. ebd.: 232ff.)
In der 27. Internationalen Datenschutzkonferenz 2005 in Montreux wurde betont, „dass das Recht auf Datenschutz und den Schutz der Privatsphäre in einer demokratischen Gesellschaft unabdingbare Voraussetzung für die Gewährleistung der Rechte der Personen, des freien Informationsverkehrs und einer offenen Marktwirtschaft“ sei. Es sei ein „grundlegendes Menschenrecht“ (27th International Conference of Data Protection and Privacy Commissioners o.A. 2005: 2) und solle auf globaler Ebene durchgesetzt werden.

Karsten Weber spricht in Bezug auf John Rawls davon, dass die verschiedenen moralischen Überzeugungen von Menschen in einer pluralistischen Gesellschaft (verschiedene Nationen, Kulturen, Religionen,…) wie in der Mathematik einen gemeinsamen Teiler aufweisen und zu einem „overlapping consensus“ (Weber 2008: 298) führen, ohne dabei auf eigene

moralische Vorstellungen verzichten zu müssen. Dieser Konsens soll so klein wie möglich gehalten werden, nur das Zusammenleben der BürgerInnen in politischem Sinne betreffen. Auf diesen Bereich sollte durch staatliche Regelungen Einfluss genommen werden. Der restliche Raum sollte aber so unangetastet wie möglich bleiben, die Freiheit darin größtmöglich sein, was auch den Umgang mit Informationen betrifft. Eine liberale Gesellschaftsform weist somit den BürgerInnen ein hohes Maß an individueller Gestaltung und daran anschließend auch individueller Verantwortung zu. (vgl. Weber 2008: 298)

3.10 Zwischenfazit

Überwachung wird in dieser Arbeit definiert als das Sammeln und Verarbeiten von personenbezogenen Daten, um Einfluss zu nehmen auf künftige Ereignisse, die diejenigen betreffen, deren Daten erhoben wurden. Infolgedessen ließe sich unsere Gesellschaft vielleicht sogar als Überwachungsgesellschaft ausmachen - obwohl mit solchen Begriffen eher sorgfältig umzugehen ist - denn nach Gottschalk-Mazouz ist Überwachung in unserer Gesellschaft bereits unter anderem allseitig, automatisiert, permanent und integriert. Auf jeden Fall herrscht in der menschlichen Zivilisation eine Urangst vor einer allgemeinen Unordnung und vor unkontrollierten Bewegungen, die als Bedrohungen angesehen werden, wie das Beispiel der verpesteten Stadt zeigt. So konnte sich im Übergang zu den modernen Gesellschaften eine Disziplinarmacht durchsetzen, die sich auf alle Individuen ausstreckt und nur verwoben agieren kann. Ihre erfolgversprechenden, einfachen Mittel sind eine hierarchisierende Überwachung, normierende Sanktionen und die Verfahren der Prüfung, wo die beiden ersteren am besten kombiniert sind. Mit ihnen gelingt es, die Individuen kontrollierbar, vergleichbar zu machen, zu züchtigen, zu dressieren, zu bestrafen, wenn das Recht nicht greift. Das Licht, früher den Mächtigen gewährt, wird nunmehr auf die Individuen gelenkt, um sie dokumentierbar und angreifbar zu machen. So lassen sie sich besser korrigieren, normalisieren und einer am Durchschnitt gemessenen Norm anpassen. Dieser Konformitätsdruck breitet sich schließlich selbst dann aus, wenn die ÜberwacherInnen völlig in den Hintergrund rücken. Das Individuum problematisiert und diszipliniert sich selbst, passt sich an, um in der Gesellschaft angesehen zu sein. Dabei wirkt die Disziplinarmacht nicht zwingend repressiv, ganz im Gegenteil konnte sie sich nur deshalb etablieren, weil sie stets auf Produktivität abzielt. Sie treibt an, steigert Leistungen, beispielweise in ökonomischen, pädagogischen oder medizinischen Funktionen. Sie ist es,

die das Wissen erst hervorbringt. Die Wissenschaften vom Menschen entstanden, um den Menschen und sein Verhalten besser kontrollieren, objektivieren und normalisieren zu können. Seinen idealen Realisierungsort hat dieser Machtmechanismus in der Architektur des Panoptikums gefunden. Von diesem abstrakten Ort dehnt sich der Panoptismus auf den gesamten Gesellschaftskörper aus.

Überwachung ist als technisiertes Handeln immer auf eine Technologie, gewisse technische Artefakte oder bestimmte Medien angewiesen. Die Überwachungstechnologie unterstützt den Menschen bei geistig-rezeptiven Fähigkeiten. Das Problem an ihr ist, dass sie eine missbrauchstendenziöse Technologie darstellt, weil sie nur einigen auf Kosten von vielen anderen hilft. Als Beispiel dienen hier Videokameras. Doch auch Handys mit Location Based Services, RFID-Chips, Ubiquitous Computing oder das Internet bieten datenschutzrechtliche Schwierigkeiten.

Der Staat hat die Aufgabe, seine BürgerInnen vor Gefahren zu beschützen. Auf der anderen Seite haben sich diese Freiheitsrechte erkämpft, die der Staat zu respektieren hat. Diese schwierige Balance, Freiheit auf der einen Seite, Sicherheit auf der anderen, hat der Staat zu halten. Seit dem 11. September 2001 war diese aber einem Ungleichgewicht mit Hang zur Überwachung gewichen. Was in Demokratien schon für erhebliche Schwierigkeiten sorgt, kann sich in Diktaturen besonders gravierend auswirken.

Wirtschaftliche orientierte Unternehmen stehen den Staaten in Bezug auf Datensammlungen um nichts nach. Sie wollen genau darüber informiert sein, wie ihre und eventuell neue KundInnen ticken und häufen deshalb auch Berge von Daten für werbe- und marketingtechnische Zwecke an.

Die gesellschaftlichen Vorteile der Überwachung liegen vor allem im erhöhten kollektiven Sicherheitsgefühl, andererseits schränkt sie unsere Verhaltensweisen und damit unsere Freiheiten ein, sie widerspricht einem freiheitlichen, demokratischen Gemeinwesen. Für den/die Einzelnen und die Gesellschaft weist sie noch weit mehr (mögliche) Folgen und Gefahren auf. Im Web 2.0 liegen diese auch in der Sanktions- und Zensurmacht der BetreiberInnen.

Um solche Gefahren zu vermeiden, wäre eine globale Ethik in Bezug auf Datenschutz wünschenswert. Wenn schon technische Geräte als hilfreich für die Gesellschaft angesehen werden, so sollte zumindest der Datenschutz bereits in das Design der Produkte implementiert werden.

4. Empirische Untersuchung

Um meine Hypothesen empirisch überprüfen zu können, habe ich mich für die Methoden der problemzentrierten Leitfadeninterviews, der wörtlichen Transkription und eine interpretative Auswertungsstrategie für leitfadenorientierte Interviews von Meuser und Nagel entschieden.

4.1 Konkretisierung des Forschungsinteresses

Das Ziel der vorliegenden empirischen Arbeit ist, das Potential von Überwachungsmöglichkeiten, die freiwillig hergegeben Daten betreffen, zu ergründen, was sich in der zentralen Fragestellung ausdrückt:

Lassen die Daten, die wir freiwillig im Internet hinterlassen, spezifischere Formen von Überwachung zu?

Dass Daten vorhanden sind, unter anderem deshalb weil wir sie auch freiwillig hergeben, konnte gezeigt werden. Die Aspekte, die nun im Vordergrund stehen, betreffen die Dimension der Überwachung. Es konnte auch schon gezeigt werden, dass der Staat, wirtschaftliche Unternehmen, Privatpersonen, die Wissenschaften usw. Daten sammeln, um für sich einen Vorteil herauszuholen. Nun soll den Fragen nachgegangen werden, was das Spezifische an den freiwillig hergegebenen Daten ist, wem sie nützen können, wofür sie genutzt werden und schlussendlich welche Vorteile, Nachteile und Gefahren mit diesen verbunden sind.

Um diese Fragen beantworten zu versuchen, habe ich neben einer intensiven Literaturanalyse, ExpertInnen aus verschiedenen gesellschaftlichen Tätigkeitsfeldern zu Interviews gebeten, um ihre Erfahrungen, ihr Wissen und ihre Expertise teilen zu können. Aus diesen qualitativen Befragungen leitete ich Indikatoren ab, die mit den wissenschaftlichen Inhalten der Literatur verwoben, zu einer Charakterisierung dieser spezifischen Überwachungsformen führen.

Im Zuge der Auseinandersetzung mit den theoretischen Aspekten der vorliegenden Arbeit ergaben sich folgende Forschungsfragen, die durch die empirische Untersuchung geklärt werden sollten:

FF 1: Tragen freiwillig veröffentlichte, sensible Daten zu einem digitalen Fußabdruck bei?

FF 2: Macht es einen Unterschied, ob wir Daten freiwillig hergeben oder gibt es ohnehin anderweitige Methoden der Datenerhebung?

FF 3: Wer nutzt beispielsweise Social Networks zu Überwachungszwecken?

FF 4: Wird Überwachung im Web 2.0 eher personalisiert, das heißt für einzelne Privatpersonen ermöglicht?

FF 5: Welche Vorteile liegen in der Entwicklung hin zu mehr Überwachung?

FF 6: Welche Gefahren gehen von einer Überwachung aus?

Des Weiteren ergaben sich unter anderem aus diesen Fragestellungen heraus folgende Forschungshypothesen, die nach der Darlegung der empirischen Untersuchung zu überprüfen, bewerten und interpretieren sind.

Hypothese 1: Wir hinterlassen auf unseren Wegen durch das Web „digitale Fußabdrücke".

Hypothese 2: Daten im Netz werden von unternehmerischer und staatlicher Seite gespeichert und die riesigen Datenmengen weiterverarbeitet.

Hypothese 3: Diese Weiterverarbeitung geschieht zielgerichtet und ohne unser Wissen.

Hypothese 4: Die freiwillige Preisgabe von Daten im Internet ist nur ein Tropfen auf dem heißen Stein in Bezug auf Überwachungsformen. Der Staat, Unternehmen und die Wissenschaften greifen auf andere Möglichkeiten der Datenerhebung zurück und generieren Daten selbst.

Hypothese 5: Überwachung wird personalisiert und dezentralisiert. Einzelne Personen, wie Firmenchefs/innen, LehrerInnen, DirektorInnen, usw. nutzen die freiwillige Preisgabe dieser Daten zu persönlichen Überwachungszwecken.

Hypothese 6: Überwachung führt zu gesellschaftlich angepasstem Verhalten.

4.2 Methodische Vorgangsweise

4.2.1 Die Wahl des ExpertInneninterviews als bevorzugte wissenschaftliche Methode

Da es in meinem Forschungsinteresse liegt, ein bestimmtes Wissen über die Thematik der Überwachung, der Privatsphäre im Web 2.0 zu generieren, schienen mir ExpertInnen, die auf diesem Gebiet besonderes Wissen bereitstellen könnten, für die Überprüfung meiner Hypothesen als besonders hilfreich. Dabei sollte nicht die Person selbst in den Mittelpunkt rücken, sondern allein ihr Wissen. „*Experten sind Menschen, die ein besonderes Wissen über soziale Sachverhalte besitzen, und Experteninterviews sind eine Methode, dieses Wissen zu erschließen.*“ (Gläser/Laudel 2004: 10)

Nach der Recherche und der Analyse zutreffender Literatur schien es mir sinnvoll wie schon Max Weber schrieb, den Ablauf und die Wirkungen von sozialem Handeln ursächlich zu erklären. (vgl. ebd.: 23) Dafür schien mir eine standardisierte quantitative Methode, die sich vor allem in Zahlen, Häufigkeiten und Statistiken ausdrückt, nicht so zielführend zu sein als eine qualitative Methode, die verbal Sachverhalte zu beschreiben, Kausalzusammenhänge zu identifizieren und zu verallgemeinern versucht. (vgl. ebd.: 24f.)
Denn Ziel meiner Interviews war es, Meinungen und Schlüsse, die sich bei mir nach der Literaturanalyse abgelegt hatten, zu überprüfen, auf übersehene Aspekte aufmerksam zu werden, eventuell neue Horizonte zu erschließen, Hintergründe zu erkennen, die theoretische Literatur anhand praktischer Beispiele zu beleben, andere Blickwinkel zu verstehen. Dazu benötigte ich das besondere Wissen der ExpertInnen, der „’Zeugen der uns interessierenden Prozesse’“ (ebd.: 10), die aufgrund ihrer Ausbildung und ihres beruflichen Werdegangs näher zu dem Thema standen als ich selbst, die aufgrund der Institution oder Organisation, in der sie tätig sind, von praktischen Fallbeispielen berichten können oder juristische Aspekte und psychologische Elemente einbringen können, die aufgrund ihrer

längeren Auseinandersetzung mit dem Themengebiet einen Wissensvorsprung zu mir haben und exaktere Aussagen treffen können, die es mir aufgrund ihrer Professionalität und Eloquenz einfacher machen an die gewünschten Daten zu gelangen als eine ungefilterte Öffentlichkeit.

Das Wissen der ExpertInnen lässt sich analytisch differenzieren.
Zum einen das ‚technische' Wissen, das sich vom Alltagswissen an Systematik und inhaltlicher Spezifität am ehesten unterscheidet, da es sich „durch die Herstellbarkeit und Verfügung über Operationen und Regelabläufe, fachspezifische Anwendungsroutinen, bürokratische Kompetenzen usw. charakterisiert." (Bogner/Menz 2005: 43)
Zweitens das Prozesswissen als praktisches Erfahrungswissen, das sich auf Handlungsabläufe, Interaktionsroutinen, Konstellationen und Ereignisse bezieht, die die ExpertInnen aufgrund ihrer persönlichen Involvierung und dem eigenen Handlungskontext besitzen.
Drittens das Deutungswissen, das mehr subjektive Relevanzen, Sichtweisen, Interpretation, Regeln der ExpertInnen aufweist. Ein heterogenes Wissensfeld der „Ideen und Ideologien", der „Sinnentwürfe und Erklärungsmuster" (ebd.: 44) wird damit beschritten. Erst mittels der Datenerhebung und der -auswertung wird ein Deutungswissen vom Forscher selbst produziert.
(vgl. ebd.: 43f.)
Die drei Wissenstypen verschmelzen ineinander, ihre Trennung ist sehr analytisch. In meinen Interviews werden alle drei Formen durchaus automatisch abgefragt.

Zuletzt gibt es noch subjektive, charakterliche Vorzüge, die mich die Methode des Interviews wählen ließen. Ich schätze den Dialog und mich als guten Zuhörer.

4.2.2 Zum ExpertInnenbegriff

ExpertInnen sollen selbst Teil des Handlungsfeldes sein, das den Forschungsgegenstand ausmacht. Das schränkt den AdressatInnenkreis von ExpertInneninterviews nicht unbedingt ein. Ganz im Gegenteil kommen Personen aus allen Branchen dafür in Frage. Den ExpertInnenstatus verleiht im Grunde der/die Interviewer/in, wenn er/sie Personen befragt, die für die Abwicklung eines jeweiligen Forschungsinteresses Hilfe leisten können.

Nach Meuser und Nagel kann als ExpertIn angesprochen werden,

> - wer in irgendeiner Weise Verantwortung trägt für den Entwurf, die Implementierung oder
> die Kontrolle einer Problemlösung oder
> - wer über einen privilegierten Zugang zu Informationen über Personengruppen oder Entscheidungsprozesse verfügt.
> (Meuser/Nagel 2005: 73)

Meist gilt es, mehrere ExpertInnen zu befragen, da verschiedene Personen aufgrund ihrer spezifischen Stellungen, die sie einnehmen, jeweils über andere Informationen verfügen. (vgl. Gläser/Laudel 2004: 113) Andererseits sind mehrere InterviewpartnerInnen geeigneter, um Informationen abzusichern, mehrere Quellen bedeuten empirisch eher abgesicherte Ergebnisse.
Die genaue Zahl kann aber nicht definitiv genannt werden, da sie auch vom Aufwand, der Bereitschaft der ExpertInnen, von der Thematik usw. abhängt. Es können auch wenige zentrale AkteurInnen ausreichen, um das Forschungsgebiet ergiebig zu durchleuchten. (vgl. ebd.: 102)

4.2.3 Auswahl der ExpertInnen

Schon im Rahmen meiner Literaturrecherche fielen Namen, die folglich als Kontaktpersonen für meine Interviews gelten konnten. Zum einen waren das BuchautorInnen, die bereits selbst über die relevante Thematik geschrieben hatten und ExpertInnen, die in der Literatur oft Erwähnung gefunden hatten oder mir von Fachkundigen empfohlen worden waren. Des Weiteren schrieb ich JournalistInnen an, die in IT-Kreisen schon Bekanntheit erreicht hatten. Zum dritten ersuchte ich WissenschaftlerInnen aus den Fächern Publizistik- und Kommunikationswissenschaften, Psychologie und Informatik um ein Interview. Zum vierten probierte ich mein Glück bei Institutionen bzw. Vereinen wie der Datenschutzkommission, der ARGE Daten oder der Arbeiterkammer, deren MitarbeiterInnen mir mit juristischen Erwägungen weiterhelfen sollten.
Diesen Personenkreis zählte ich zu FachexpertInnen, die mir bei der Überprüfung meiner Hypothesen zur Seite stehen sollten und sich auch tatsächlich als kompetente

InterviewpartnerInnen und Antriebskraft herausstellten. Der Kreis wäre wahrscheinlich noch viel weiter zu ziehen gewesen, aber für meine Anfragen hatte ich eine Auswahl zu treffen.

Zuerst schrieb ich die Personen per Mail an. Nachdem ich einige Absagen erhalten hatte und diese Art der Kommunikation eher einseitig verlaufen war, ich also wenige Antwortmails bekommen hatte, rief ich die Personen an. Dies war die weit erfolgreichere Methode. Die ExpertInnen wussten bereits über meine Anfragen Bescheid, hatten die Priorität meiner Mail nur etwas nach hinten verschoben, und waren auch gewillt ein Interview durchzuführen. Die Wahl des Datums und des Orts für das Gespräch überließ ich den ExpertInnen.

Folgende Personen erklärten sich für ein Interview bereit:

König, Gregor: LL.M., Mitarbeiter bei der Österreichischen Datenschutzkommission
Möchel, Erich: investigativer Journalist, Redakteur der *Futurezone*, IT-Nachrichtenportal des ORFs
Reischl, Gerald: Redakteur des *Kuriers*, mehrfacher Buchautor (u.a.: *Die Google-Falle*)
Zeglovits, Wolfgang: Psychologe und Medienanthropologe, Geschäftsführer der *datenwerk innovationsagentur*, Lehrbeauftragter am Institut Publizistik- und Kommunikationsforschung
Zimmer, Daniela: Arbeiterkammer-Expertin für Konsumentenschutz und moderne Medien, Schwerpunkt: Telekom- und Internetrecht, Mitglied der Datenschutzkommission, Ersatzmitglied im österreichischen Datenschutzrat
Anonyme Person: (Ein sechstes Interview, das ich leider nicht aufzeichnen durfte, fand zusätzlich statt. Da es mir nicht möglich war, zugleich sinnvoll mitzuschreiben, aufzupassen und Fragen zu stellen, berücksichtige ich dieses nicht weiter. Das Interview diente ohnehin eher dafür, zusätzliche Literatur und weitere ExpertInnen zu erfahren. Da ich dann auch noch vergaß zu fragen, ob ich den Namen des/der Experten/in angeben dürfe, beschreibe ich diese/n als anonym.)

4.2.4 Das ExpertInneninterview

In den vorangegangen Kapiteln wurden die Grundlagen für diese Arbeit gelegt, die Begriffe und Themenfelder der Daten, der Privatheit, der Überwachung und der

Disziplinargesellschaft theoretisch eingebettet. Die Methode des empirischen Teils der Arbeit beruht nun auf der Verfahrensweise einer qualitativen Befragung von ExpertInnen, einer Technik qualitativer Analyse. Mit dieser sollen fachkundige Aussagen bezüglich Erfahrungen und praktischer Auseinandersetzung zum Themenfeld der Überwachung gewonnen werden, die dann im Anschluss mit den Anführungen im theoretischen Teil verglichen werden, Gemeinsamkeiten und Unterschiede sollen herausgearbeitet werden.

In Rahmen meiner Arbeit hat sich das problemzentrierte, leitfadengestützte ExpertInneninterview als profitable Datenerhebungstechnik für die wissenschaftliche Erkenntnisgewinnung durchgesetzt. Dabei soll an gesellschaftlichen Problemstellungen angesetzt werden und subjektive Bedeutungen von Personen übermittelt werden, die sich durch eine Beobachtung kaum erforschen ließen. Viele verschiedene Arten und Namen für Interviewtechniken kursieren in der Sozialforschung, unter dem Begriff problemzentriertes Interview sollen alle Formen der offenen, halbstrukturierten Befragung zusammengefasst werden. Der/Die Interviewte hat dabei keine Antwortvorgaben, kann also frei antworten. Die soll einem offenen Gespräch möglichst nahe kommen, in dem eine Vertrauenssituation aufgebaut werden kann. Der Fragenkatalog ist ebenfalls nicht starr und kann sich deshalb der Interviewsituation anpassen. Natürlich bringt der/die Interviewer/in eine gewisse Problemstellung mit ein, auf die sich die Fragen beziehen. Gewisse Vorarbeiten, Recherchen und eine Analyse der Problemstellung sind deshalb Voraussetzung. Diese spiegeln sich im Interviewleitfaden wider. (vgl. Mayring 2002: 66f.)

Der Unterschied zwischen ExpertInneninterviews und anderen Formen offener Interviews liegt laut Meuser und Nagel darin, dass bei ersteren nicht die Gesamtperson den Gegenstand der Analyse bildet, sondern der organisatorische und institutionelle Kontext und Zusammenhang in den Mittelpunkt rückt. (vgl. Meuser/Nagel 2005: 72f.) Somit sind nur bestimmte Aspekte individueller Erfahrungen von Relevanz, nicht die befragte Person selbst soll ausgekundschaftet, sondern ihr ExpertInnenwissen erhoben werden.

4.3 Die Datenerhebung

4.3.1 Der Interviewleitfaden

Der Leitfaden dient dazu, einzelne Thematiken und die zentralen Aspekte des Untersuchungsproblems, das bereits konkretisiert und analysiert sein sollte, in einer vernünftigen Reihenfolge zu gliedern. Das genaue Ausformulieren der Fragen und Anregungen, sowie eventuelle Alternativen ist durchaus erwünscht. (vgl. Mayring 2002: 69) Um aber eine offene Gesprächsführung zu gewährleisten und dem „Prinzip der Offenheit" (vgl. Flick/von Kardorff/Steinke 2003a: 23) zu entsprechen, sollte der Gesprächsleitfaden nicht starr und vollkommen standardisiert sein. Er hat den Zweck, die vorangegangene Recherche und Arbeit in ein Formular zu gießen, das zugleich dem/der Forscher/in ein den ExpertInnen nahezu ebenbürtiges Maß an Kompetenz bescheinigt. Zusätzlich regelt er das Gespräch, um sich nicht in Wegen zu verlieren, die zu weit vom eigentlichen Thema bzw. Forschungsinteresse wegführen. (vgl. Meuser/Nagel 2005: 77 f.)
Bei der Anwendung ist zu beachten, dass der Leitfaden nicht als zwingendes, striktes Ablaufmodell der Befragung bzw. des Diskurses verwendet wird, sondern vielmehr als Orientierungsrahmen und Gedächtnisstütze für den/die Interviewer/in dient. (vgl. Lamnek 2005: 367) Innerhalb seines Rahmens kann man sich flexibel bewegen, er ist abänderbar, wenn es die Antworten erfordern, wenn es erforderlich ist, intensiver nachzufragen oder manchmal ganz unspezifisch, um die Befragten frei artikulieren zu lassen, Fragen sind vorzuziehen oder hintanzustellen, wenn es der Diskursverlauf so verlangt. (vgl. Hopf 2003: 358) So entsteht ein gutes Gespräch dann, wenn der/die Experte/in dazu animiert wird, sich verschiedenster Darstellungsformen zu bedienen, wenn er/sie „berichtet, typisiert, rekonstruiert, interpretiert, kommentiert und exemplifiziert." (Meuser/Nagel 2005: 79)

Einen weiteren großen Vorteil bietet die Verwendung eines Leitfadens, der dann doch eine leichtere Form der Strukturierung mit sich bringt und zwar dann, wenn es um die Auswertung der Interviews geht: ihre Vergleichbarkeit. Denn das Material kann auf die Leitfragen bezogen werden und ist damit leichter bearbeitbar. (vgl. Mayring 2002: 70) Der Leitfaden schneidet ein gewisses Themenspektrum aus der Breite des Wissenshorizonts des/r Experten/in heraus und behält diese dann im Fokus des Interviews. (vgl. Meuser/Nagel 2005: 81f.)

Der Leitfaden meiner Interviews ist so aufgebaut, dass zu Beginn, nachdem ich die ExpertInnen gefragt habe, ob ich das Interview aufzeichnen dürfe und ich sie namentlich oder anonym erwähnen solle, eine einfache Einstiegsfrage gewählt wird, die von den ExpertInnen ganz leicht zu beantworten ist, um eine eventuelle Scheu vor dem Gespräch zu nehmen. Dies ist in meinem Fall die Frage, eher Bitte, sich vorzustellen und den jeweiligen Arbeits- bzw. Forschungsschwerpunkt zu beschreiben. Danach folgen Fragen zu den Blöcken Daten und Privatsphäre, um dann intensiv das Thema der Überwachung zu erörtern. Die Fragen sind einfach, neutral und klar formuliert. Um schlussendlich einen versöhnlichen Abschied zu gewähren, ist die letzte Frage nach der Dankaussprechung, ob die ExpertInnen von sich aus noch wichtige Aspekte benennen wollen, die ihrer Meinung nach zu wenig berücksichtigt worden seien.
Außerdem variiert der Leitfaden von Interview zu Interview, von ExpertIn zu ExpertIn ein bisschen. Je nachdem, welches Wissen von dem/der Interviewpartner/in erwartet wird, fallen die Fragen etwas anders aus. Hat sich eine Frage in einer bestimmten Form nicht bewährt, kann sie auch weggelassen oder geändert werden. (vgl. auch Gläser/Laudel 2004: 138ff.)

(Der Gesprächsleitfaden befindet sich im Anhang.)

4.3.2 Durchführung der Datenerhebung

Die Interviews fanden alle im Großraum Wien in der Zeitspanne von 5. Februar bis 4. März 2010 statt. Über den Ort, das Datum und die genaue Uhrzeit der Treffen entschieden die GesprächspartnerInnen. Alle Interviews fanden in Besprechungszimmer oder Büros statt. Als eingeplante Dauer waren 45 bis 60 Minuten eingeplant, hatte sich aber ganz nach der zeitlichen Verfügbarkeit der ExpertInnen zu richten. Ein Interview weicht mit 22 Minuten etwas von der Länge der anderen ab, Frau Zimmer hatte aus beruflichen Termingründen nicht länger Zeit.
Alle InterviewpartnerInnen hatte ich anfangs per Mail angeschrieben und ihnen meine Situation, mein Forschungsinteresse sowie das Interesse an der jeweiligen Person offen gelegt. Spätestens nach dem Telefonanruf ein bis zwei Wochen später erklärten sich die ExpertInnen bereit, ein Interview abzuhalten. Wenn es erwünscht war, sandte ich ihnen zuvor noch einen oberflächlichen Schwerpunktkatalog der anzusprechenden Themen zu,

damit sich die ExpertInnen inhaltlich auf die Themenkomplexe vorbereiten konnten. Eine genaue Ausformulierung der Fragen behielt ich mir für das Interview vor, um es authentisch geschehen zu lassen und eine Verzerrung der Empirie auszuschließen. (vgl. auch ebd.: 154f.)
Die ExpertInnen stimmten allesamt meiner Bitte zu, das Interview für eine leichtere Transkription aufzeichnen zu dürfen.

4.4 Datenaufbereitung

Das Material der Datenerhebung muss für eine Auswertung sauber, dem Gegenstand angemessen aufbereitet werden, ein Punkt der oftmals vernachlässigt wird. Zum Zwecke der Vergleichbarkeit wählte ich als Protokollierungstechnik die wörtliche Transkription. Diese soll als Basis für den Vergleich von Textstellen und für ausführliche Interpretationen dienen. Einzelne Aussagen können in ihrem Kontext angesehen werden. Die teils dialektisch gefärbten Reden übertrug ich in normales Schriftdeutsch, Satzbaufehler wurden großteils behoben, da die inhaltlich-thematische Ebene im Vordergrund steht. (vgl. Mayring 2002: 85) Da es um das gemeinsam geteilte Wissen geht, ist ein zu aufwendiges Notationssystem nicht zielführend. Pausen, Stimmlagen und sonstige nonverbale Elemente werden bei der Transkription ausgespart. (vgl. Meuser/Nagel 2005: 83).

(Die Transkripte befinden sich im Anhang.)

4.5 Die Auswertungsmethode

Jedes einzelne Interviewprotokoll ist als spezielle Form der Interaktion und Kommunikation einmalig und unverwechselbar an Inhalt und Form. Nun gilt es, die Texte zu vergleichen, das Repräsentative aus den ExpertInneninterviews herauszufiltern und die Gewinnung von Aussagen für andere nachvollziehbar zu machen. Ziel ist es, aus den verschiedenen Interviews das „Überindividuell-Gemeinsame herauszuarbeiten, Aussagen über Repräsentatives, über gemeinsam geteilte Wissensbestände, Relevanzstrukturen, Wirklichkeitskonstruktionen, Interpretationen und Deutungsmuster zu treffen.“ (Meuser/Nagel 2005: 80)

Als Vorlage für die nicht-standardisierte Auswertung des Datenmaterials ziehe ich folglich eine interpretative Auswertungsstrategie für leitfadenorientierte ExpertInneninterviews von Meuser und Nagel heran. Diese ist als Modellvorschlag zu verstehen, kann und sollte flexibel den jeweiligen Untersuchungsbedingungen angepasst werden.
Grundsätzlich gilt, dass sie sich an thematischen Einheiten orientiert, an Passagen, die inhaltlich zusammengehören, wenn sie auch über den ganzen Text verstreut sind. Die Sequenzialität der Äußerungen im Interview rückt hingegen aus dem Blickfeld. (vgl. ebd.: 81)

Meuser und Nagel schlagen sechs Stufen für ihre interpretative Auswertung vor:

1. Transkription

Den ersten Schritt des Modells habe ich bereits im vorangehenden Kapitel als Aufbereitungsmethode beschrieben.

2. Paraphrase

Die Paraphrase ist ein erster Schritt zum Verdichten des Textmaterials. Es geht darum, den transkribierten Text getreu in eigene Worte zu fassen, wobei nur das zu paraphrasieren ist, was in Hinblick auf die leitenden Forschungsfragen und auf die Bewertung der Hypothesen von Belang ist. Dabei ist der Chronologie des Gesprächsverlaufs zu folgen. Entscheidend ist bei dieser Vorgehensweise, den Inhalt nicht zu verzerren und keine Informationen zu verschenken. (vgl. ebd.: 83f.)

3. Überschriften

Als nächsten Schritt ordnet man den paraphrasierten Passagen Überschriften zu, der Terminologie der Interviewten folgend. Es ist erlaubt und notwendig, die Reihenfolge des Textes zu zerreißen. Auch können manche Passagen mehreren Überschriften zugeordnet werden, wenn es die Thematik verlangt. Sind Passagen gleich oder ähnlich, werden sie unter eine Hauptüberschrift subsumiert. Eine Übersicht über den Text wird geschaffen, man bewegt sich aber noch innerhalb des einzelnen Interviews. (vgl. ebd.: 85f.)

4. Thematischer Vergleich

Die Interviews werden ab diesem Schritt miteinander verknüpft. Thematisch vergleichbare Textpassagen aus den verschiedenen Interviews werden in Kategorien mit Überschriften geteilt. Die Überschriften werden vereinheitlicht, was eine notwendige Reduktion von Terminologie und Redundanz bedeutet. Die Kategorienbildung soll textnah bleiben und soziologisch-wissenschaftliche Begriffe noch aussparen. Gemeinsamkeiten in den Aussagen der Interviewten sind herauszuarbeiten, genauso wie Abweichungen, Widersprüche und Unterschiede festzuhalten. (vgl. ebd.: 86ff.)

5. Soziologische Konzeptualisierung

Das Gemeinsame der verschiedenen Interviews wird herausgearbeitet und mit wissenschaftlicher Terminologie versehen. Die Kategorien werden mit soziologischen Begriffen betitelt, die allgemeine Geltung beanspruchen und zusammengefasst. Dies soll einen Anschluss der Interpretationen an bestehende Theorien und an allgemeine disziplinäre Diskussionen befördern. Das Material wird dabei systematisiert. Die Generalisierung bleibt noch auf das vorliegende empirische Material begrenzt. (vgl. ebd.: 88f.)

6. Theoretische Generalisierung

In dieser Phase werden die Begründungen und Zusammenhänge der Kategorien systematisch aufgerollt. Sinnzusammenhänge der Empirie werden mit Hilfe der analytischen Vorarbeit interpretiert, generalisiert und zu Typologien und Theorien verknüpft. Folglich wird Empirie und Theorie miteinander konfrontiert und verglichen, die theoretischen Konzepte dabei können inadäquat sein, müssen falsifiziert werden oder passen.
Alle Stufen sollten Schritt für Schritt durchlaufen werden, stets sollte nachkontrolliert und nachgebessert werden. (vgl. ebd.: 89ff.)

4.6 Auswertung

Die folgenden Kapitel umfassen die Ergebnisse der Auswertung, die durch die zuvor beschriebenen und vorangegangenen Auswertungsschritte gewonnen werden konnten. Die ExpertInnenaussagen zu den bestimmten Aspekten wurden gegenübergestellt, um die aus den Interviews gewonnenen Erkenntnisse zu vergleichen, zu verdichten, Gemeinsamkeiten und Unterschiedlichkeiten, sowie Verallgemeinerungen und Deutungsmuster zum Thema

der vorliegenden Arbeit zu erhalten. Der Vergleich mit theoretischen Aspekten der Literaturanalyse geschieht in den Fazits und bei der Beantwortung der Forschungsfragen.

4.6.1 Charakterisierung von Privatsphäre und sensiblen Daten aus ExpertInnensicht

Der erste Block umfasst das Wissen, Perspektiven, Meinungen, Aussagen, Interpretationsweisen, Beispiele der ExpertInnen hinsichtlich Fragen zu den Themenkomplexen der Daten und der Privatsphäre. Die Dimension der Überwachung steht hier noch nicht explizit im Raum, eher werden grundsätzliche Bedingungen erörtert, die einer Überwachung und Verwendung unserer Daten vorangehen.
Vielleicht auch aufgrund der sehr allgemein gehaltenen Fragen, ließen sich in den Aussagen und Ansichten der ExpertInnen kaum Widersprüche entdecken. Sie ergänzen sich in ihren Antworten vielmehr auf technischer, juristischer, praktischer und psychologischer Ebene.

- **Sensible Daten**

Während aus juristischer Sichtweise, die Frage, welche Daten als sensibel zu gelten haben, ganz klar geklärt werden kann, beziehen die Experten mit anderem Ausbildungshintergrund den Kontext der Daten und individuelle Sensibilitätsschwellen mit ein.

Gregor König (GK) erklärt, dass Personen oft Daten als sensibel bezeichnen und ansehen, die sie aus subjektiver Sicht als sensibel erachten wie zum Beispiel Bankdaten, was auch verständlich ist. In unserem Rechtssystem definiert das Datenschutzgesetz sensible Daten aber ganz genau, was bedeutet, dass eben nur diese Typen von personenbezogenen Daten als sensibel gelten. Diese sind beispielsweise Gesundheitsdaten, Daten über die ethnische und rassische Herkunft, über die Gewerkschaftszugehörigkeit, über die Religion, über die Sexualität, jedoch nicht, gegen landläufiger Meinungen, Bank- und Kontodaten. Sensible Daten sind vom Gesetz genau definiert und sind nichts, was im subjektiven Ermessen oder Betrachten des Einzelnen liegt. (siehe Interview mit Gregor König: Frage 2, kurz GK 2)
Wolfgang Zelgovits (WZ) erklärt, dass einzelne Daten an sich nicht sensibel sind. Sie werden erst in ihrem Kontext, in der Verbindung mit anderen Daten, die zugleich

rückführbar sind auf eine Person, sensibel; dann, wenn ein Informationsbild über eine Person entsteht.

Wenn Daten personenbezogen gesammelt und zusammengeführt werden können und dadurch ein Personenbild entsteht, dann sind sie sensibel, was bedeutet, dass die Daten potentiell missbrauchsmöglich sind oder systematisch zu einer Benachteiligung führen können. Gesundheitsdaten sind ein Beispiel, die Auswirkungen auf Beruf und Versicherungsverträge haben können. Auch Daten über religiöse Motive können zu einer wie auch immer gearteten Verfolgung führen. Sie sind deshalb auch genau geschützt wie auch Daten über Straffälligkeiten. Wird das Bild, das eine Person gerne nach außen präsentieren würde, so weit untergraben, dass die Person dadurch Schaden erleidet, können sie als sensibel bezeichnet werden. (WZ 2, 3)

Gerald Reischl (GR) meint hierzu, dass es aber auch eine Definitionssache ist, welche Daten als sensibel gelten. Für jede/n sind Daten anders sensibel. Manche denken, es kann ruhig jeder alles über sie wissen, weil sie nichts zu verbergen haben, sie sich für brave BürgerInnen halten und denken, es wird ihnen deswegen auch nichts passieren, andere wollen das wiederum gar nicht. (GR 2)

Erich Möchel (EM) denkt ähnlich, dass es immer ganz auf die Umgebung drauf ankommt, wem man irgendwelche Daten gibt. Gesundheitsdaten gibt man am besten alle seinem Arzt, während man in anderen Umgebungen wesentlich restriktiver sein muss. Sensibilität ist für jeden Menschen anders anzusetzen, das zeichnet sich auch im Umgang von Personen mit relativ heiklen Themen ab. Manche bewältigen Situationen, indem sie an die Öffentlichkeit gehen, andere schweigen darüber. Damit ist man in der Individualität des Menschen und weil eben nicht alle gleich sind, muss man die Sensibilitätsschwelle sehr niedrig ansetzen, damit auch die Empfindlichsten geschützt sind. Manchen Daten sieht man auch gar nicht an, dass sie sensibel sind, weil sie erst in ihrer Verknüpfung sensibel werden. Werden kleine Datenmengen miteinander vernetzt, kann dies sehr problematisch werden. (EM 2)

- **Rechtlicher Schutz der Daten**

Die zwei dazu befragten Experten geben als rechtlichen Schutz für Daten primär das Datenschutzgesetz an. Daneben gibt es noch Rechtsansprüche aus anderen Gesetzen und Richtlinien als eine Art freiwilliger Selbstkontrolle.

Neben dem Datenschutzrecht, das ein im Verfassungsrang stehendes Recht ist, ein Grundrecht auf Datenschutz darstellt und sowohl normale Daten schützt, wie sensible besonders, existieren auch noch Rechtsansprüche aus anderen Gesetzen parallel, wie das Bankgeheimnis, die ärztliche Schweigepflicht. Das Datenschutzrecht sticht hier kein anderes Rechtsgebiet oder Gesetz aus. (GK 3) Wo es beispielsweise um strafrechtlich relevante Daten geht, regeln das Sicherheitspolizeigesetz und die Strafprozessordnung genau, welche Datenanwendungen staatliche Behörden betreiben dürfen und was sie machen dürfen. (GK 15)
So sagt auch WZ, dass neben dem Datenschutzgesetz Daten durch spezielle, verstärkte Schutzmechanismen vor allem für Institutionen (staatlicher Seite) rechtlich geschützt werden. Zusätzlich gibt es auch eine Art freiwilliger Selbstkontrolle, wie zum Beispiel die *ESOMAR*-Richtlinien [*European Society for Opinion and Marketing Research*, Anmerkung D.R.] in der Markt- und Meinungsforschung, die Regeln definieren, um eine Missbrauchschance möglichst klein zu halten. (WZ 4)

- **Gründe für die Preisgabe an Daten**

Die ExpertInnen sehen die Gründe, für die Preisgabe sensibler, heikler Daten, vorrangig in der fehlenden Kompetenz im Umgang mit dem Medium Internet und im sozialen Druck zur Selbstdarstellung, der aus deren Normalisierung hervorgeht.

Die junge Generation, die in der IT-Ära aufgewachsen ist, stellt die Freiheit, alles über sich veröffentlichen zu dürfen, höher als die Privatsphäre. Es erfüllt sie mit Stolz, Fotos und private Daten online zu stellen und sie sehen sich als Teil der Gesellschaft, sprich es zählt das Argument, dass es andere genauso machen. (GR 3)
So meint auch Daniela Zimmer (DZ), dass laut Motivforschung UserInnen einem Trend folgen, stark in Medien präsentiert zu sein, und einem gewissen Druck unter Jugendlichen nachgeben, zu einer bestimmten Peer Group zu gehören, wenn sie heikle Daten, die ein gutes Personenprofil ermöglichen, freiwillig ins Netz stellen. (DZ 2)
Auch die Unerfahrenheit mit dem Medium Internet ist ein Grund für das Preisgeben von Daten. Wir haben noch nicht den Erfahrungsschatz, das Tacit Knowledge erworben, dass uns Daten im Internet überdauern, dass sie gespeichert und abrufbar bleiben und nicht mehr bewusst gelöscht werden können, dass sie eventuell mit anderen Daten zu einem Gesamtbild

über uns zusammengeführt werden und nicht wie im analogen Leben nach dem Ausrufen wieder in Vergessenheit geraten oder dementierbar sind. Die potentielle Verknüpfung der Daten ist uns emotional und teilweise auch kognitiv noch nicht nachvollziehbar, weil uns auch die Vorstellungskraft fehlt, welche unglaubliche Rechenleistung in der Infrastruktur des Internets liegt. (WZ 5) Andererseits ist aber interessant zu beobachten, dass wir manche bereits verfügbare Daten, die uns Qualität bescheinigen, scheinbar trotzdem nicht veröffentlichen, ein hoher IQ beispielsweise. (WZ 10)

Personen allgemein und insbesondere Jugendlichen ist die Tragweite der Handlungen nicht bewusst. Sie wollen etwas, auch Nacktvideos beispielsweise FreundInnen zeigen oder in ihrem Freundeskreis publik machen und beachten dabei zu wenig, was mit solchen Daten alles passieren kann oder dass eben so ein Video schließlich ganz woanders auftauchen kann. Vergessen wird, dass das Internet nichts „vergisst". Die Datenschutzkommission hat sich unter anderem mit einer Initiative und einer Broschüre ganz verschrieben, Jugendliche über die Gefahren der Preisgabe von Daten aufzuklären, um sie ins Bewusstsein zu rufen, denn, so ist GK überzeugt: Wüssten die Leute, was mit den Daten alles passieren kann, so würden sie sie nicht so leichtsinnig hergeben. (GK 4)

Leute, die ihre Daten freiwillig im Web preisgeben, streben vor allem nach sozialer Anerkennung und leben noch in einem anderen Medienzeitalter, nämlich dem Fernsehen. Dort stellen sich Menschen in Privatkanälen vorrangig öffentlich, oft selbst demütigend zur Schau, weil erstens schon alles im Fernsehen vorkommt und ihnen zweitens etwas fehlt, wenn sie nicht einmal im Fernsehen zu sehen waren. Auch das Verhalten in *Facebook* und Co entspricht dem Fernsehzeitalter. Doch Fernsehen gilt im Gegensatz zum Informationsmedium Internet als flüchtig. Eine Sendung ist vorbei, wenn man das Gerät ausschaltet. Nicht so im Internet, der *Google*-Cash ist nachhaltig und reich gefüllt. (EM 3, 4)

- **Digitaler Fußabdruck**

Alle InterviewpartnerInnen sind sich einig, dass wir digitale Spuren im Internet hinterlassen, wie man diese dann genau bezeichnet, variiert.

Die Frage, ob wir im Netz einen digitalen Fußabdruck hinterlassen hält GK für eine gesellschaftspolitische, in welcher Gesellschaft wir leben und welche technischen Möglichkeiten es gibt, Daten zusammenzuführen. 1995 wurde von der EU eine

Datenschutzrichtlinie erlassen, die im Jahr 2000 in Österreich mit dem Datenschutzgesetz umgesetzt worden ist. In der damaligen Landschaft ging man von einzelnen Datenbanken aus, die gemeldet werden mussten, die leicht zu überprüfen sein sollten. Heutzutage kommt es aber zur totalen Vernetzung. Man weiß nicht genau, wo Daten tatsächlich verarbeitet werden und was genau mit den Daten passiert. (GK 6) Daten machen nicht vor den Grenzen Halt. (GK 1) Die technischen Möglichkeiten gingen in die Richtung und lassen es mitunter zu, Profile von Personen anzulegen bzw. einen Fußabdruck anzufertigen, was eine Gefahr darstellt und als solche eine Herausforderung für GesetzgeberInnen und Behörden ist, Datensicherheitsmaßnahmen einerseits und eine Zweckbindung der Daten andererseits zu gewähren. (GK 6)

Mit Sicherheit tragen Daten, die wir ins Netz eintragen, so DZ, zu einem digitalen Fußabdruck bei, der für viele sichtbar wird. Wie eine Studie der EU anlässlich des Datenschutztages 2010 gezeigt hat, haben 60 Prozent der Social Network-UserInnen die Voreinstellungen so gewählt, dass die gesamte Internetgemeinde darauf Zugriff hat. Der/Die Durchschnittsnutzer/in beschäftigt sich also mit solchen Sicherheitseinstellungen eher nicht. (DZ 3)

Egal, ob man es digitalen Fußabdruck oder Fingerabdruck nennt, - WZ würde ihn eher als digitalen Klon beschreiben, der über die Selbstbeschreibung der Person hinausgeht und auch das soziale Netzwerk, die Aufenthaltsverortung und benutzte Kanäle, sowohl online als offline, mit einbezieht (WZ 9) - die digitale Spur, die wir hinterlassen, erlangt erst dann einen Wert, wenn man eine Abgleichsmöglichkeit dazu vorfindet, sprich das Wissen bzw. einen Vergleich hat, ob diese Spur zu einer Person passt.

Die Angabe und Speicherung von Daten gibt es dabei schon seit langer Zeit beispielsweise in Tauf- und Geburtsurkundenbüchern, und im Nachhinein war die Spur auch relativ leicht zu den Ursprungs- und Erstaufzeichnungen rückverfolgbar, wenn auch nicht in präventivem Sinne. Unterschätzt wird von den Leuten aber die Möglichkeit, dass dieser Datenabgleich nun im digitalen Zeitalter von weitaus mehr Menschen, im Grunde von jeder beliebigen Person und um soviel einfacher durchgeführt werden kann. (WZ 6)

Alles, was im Netz verbreitet wird, bleibt auch drinnen. Der Vergleich mit einer Schultafel ist nahe liegend, nur dass auf dieser Tafel nichts gelöscht werden kann. Man hat kaum eine Chance, das herauszubekommen, zum Beispiel ein Video, weil es leicht herunter geladen und weiterverbreitet werden kann. GR weiß in seiner Karriere nur von einem Video, das er kein zweites Mal gefunden hat. Einem japanischen Hersteller ist es scheinbar gelungen,

unvorteilhaftes Bildmaterial, das zeigte, wie bei einer Präsentation ein Notebook in Flammen aufging, vollständig aus dem Netz zu nehmen. (GR 6)
EM würde eher von einem digitalen Fingerabdruck anstatt eines Fußabdrucks sprechen. Dass wir aber unzählige digitale Spuren hinterlassen, steht außer Frage. Als Beispiel dient *Google*. Ihr Programm *Google Ananytics* wird von den meisten österreichischen Tageszeitungen verwendet (nicht der *ORF* und nicht der *Kurier*) und über dieses Programm erhält *Google*, sämtliche Clickstreams. Sprich die Algorithmen von *Google* registrieren, welche/r Österreicher/in in welcher Reihenfolge welche Nachrichten an welchem Tag konsumiert, wann er/sie nicht liest. *Google* kann also Interessensprofile von jedem/r Einzelnen anlegen und sie mit einer IP-Adresse bzw. mit Cookies als Eigenerkennung des betreffenden Browsers verknüpfen. Bei *Google* laufen diesen Daten aus allen Ecken und Enden zusammen und das ist eine Gefahr, wenn ein Unternehmen zuviel davon besitzt. (EM 5)
Um die digitale Spur zur Sonnenseite wandern zu lassen, gibt es Reputationsunternehmen, die gegen Bezahlung versuchen, einen Ruf im Internet wieder herzustellen. Sie gehen so vor, dass sie zuerst jemandem zeigen, was im Internet alles über diese Person gefunden werden kann und man selbst bestimmt dann, welche Informationen und Links man gelöscht haben will. Auch das Businessmodell der Suchmaschine *123people* funktioniert so, dass sie eng an diese Reputationsfirmen gekoppelt sind. Zuerst sieht man, was über eine Person selbst zu finden ist, zugleich wird eine Werbung für einen Online-Schutzdienst geschaltet, mit dem die Suchmaschine kooperiert. (GR 7)

- **Personenbezogene Datenspuren**

Laut Recht sind Daten erst geschützt, wenn sie personenbezogen sind. Der Name ist im Web aber nicht allzu schwer zu eruieren, wobei DatensammlerInnen nicht unmittelbar auf Namen angewiesen sind, um Profile zu erstellen.

Datenschutzrechtlich sind Daten nur dann relevant, wenn sie personenbezogen sind, weil es an ebensolche anknüpft und dafür muss eine Person zumindest bestimmbar sein. Rein statistische Daten sind aus datenschutzrechtlicher Sicht unproblematisch. Das bedeutet aber nicht, dass der Name zwingend vorliegen muss, sondern auch Bilddaten können die Identität einer Person, zum Beispiel in einem Betrieb, wo man die Gesichter kennt, verraten, wie die

neuen Regelungen zur Videoüberwachung besagen. Sofern eben diese Datensätze für Unternehmen auf eine bestimmte Person hinweisen, ohne dass auch ein Name genannt ist, sind es personenbezogene Daten. (GK 7)

Irgendwann im Laufe des Internetsurfens gibt man irgendwo seinen Namen ein. Das Problem dabei ist, dass man Unternehmen damit die Gelegenheit gibt, die Daten dann zu verknüpfen. Als Beispiel dient *Google*, das ja ein eifriger Datensammler ist. *Google* hat mehr als 150 Dienste, Services und Geschäftsfelder. Sollte hier einmal irgendwo ein Name fallen, so ist GR überzeugt, wird der von *Googles* Data-Mining-System aufgesogen und ins Profil aufgenommen. (GR 8)

Anhand eines Beispiels aus dem populärwissenschaftlichen Magazin *Wired* zeigt WZ, dass die Geheimhaltung von Name und Daten schwierig ist. So war es für einen Redakteur unmöglich, länger als vier Wochen unterzutauchen. Das Magazin bot demjenigen eine Erfolgsprämie, der beweisen konnte, dass er nicht verschwunden sein konnte. Eine Community bildete sich heraus, die vor allem im Internet nach seinen personenbezogenen Daten suchte, und sie auch großteils legal bezog, zum Beispiel Kontoverbindungsdaten. Trotz eines Informationsvorsprungs (da er mitlesen konnte, wie sich die Communitiy organisierte) und diverser Methoden, seine Identität zu verschleiern, konnte der Mann leicht aufgespürt werden. (WZ 7, 8)

EM meint, dass der Name für Unternehmen gar nicht so wichtig wäre, weil es Ersatz dafür gäbe. Unternehmen brauchen nur einmal die IP-Adresse, dann haben sie die viel eindeutigeren Browsererkennungsmethoden oder das NutzerInnenverhalten bestimmt den Identifizierungsvorgang. (EM 5) Somit kann *Google* leicht behaupten, sie würden keine Namen und IP-Adressen sammeln, weil alleine die Browserkonfiguration die KundInnen verrät. (EM 14)

- **Künftige Daten: Prognosen darüber, welche Daten noch kommen könnten**

Die vier Experten sind sich einig, dass nicht mehr viele Daten hinzukommen können, weil schon so gut wie alles vorhanden ist, biometrische Daten, auch zur DNA, Daten, über die Bonität eines Menschen, usw. Die Zukunft geht deshalb eher in die Richtung, die Daten qualitativ aufzuwerten.

Ein Mehr an Daten geht kaum noch, weil schon alles da ist, dafür ist eine Perfektionierung der Daten möglich, zum Beispiel eine Aufwertung an semantischem Gehalt oder zutreffende Gesichtserkennung von Bildverfahren, die in handelsüblichen Softwarelösungen eingesetzt sind. Es wird nicht darum gehen, neue Daten zu generieren, sondern darum, Erkennungsverfahren einerseits zu verbessern und andererseits die quantitativen Daten zu einem digitalen Klon zusammenzusetzen. (WZ 9) Ein Beispiel dafür wären, Kameras, die bereits erkennen, dass sich vor ihrer Linse ein Mensch befindet und was er macht, also einfache Verhaltensmuster erfassen. Auch gibt es Bestrebungen in die Richtung, Videoaufnahmen mit Personalfotos aus einer Datenbank abzugleichen. Was hier technisch schon möglich ist, also der automatisierte Bildabgleich, ist in der Datenschutzgesetz-Novelle aber explizit verboten worden. (GK 19)

Im Grunde wird schon alles an Daten ins Netz gestellt, so auch EM. Das Geschäftsmodell von *23andme*, eine Firma, die unter anderem der Frau von *Google*-Gründer Sergej Brin gehört, ist es, Leute aufzufordern, DNA-Proben für ca. 200 Dollar an sie zu schicken, um sie auswerten zu lassen und festzustellen, mit wem sie alle über mehrere Ecken verwandt sind. In unserem Strafrecht dürfen DNA-Proben nur als Identifikationsmittel zur Aufklärung schwerer Verbrechen genommen werden, obwohl die Schwelle bereits sinkt, weil diese Analysen billiger und häufiger werden. Aber die Leute machen das freiwillig. (EM 6) Von einem Vorstand von *23andme* wurde auch schon vorgeschlagen, eine DNA-Komponente in ein soziales Netzwerk zu integrieren, um Menschen mit genetischen Übereinstimmungen zusammenzuführen. (GR 12)

Mit den technologischen Verbesserungen erhalten wir zweifelsohne Vorteile in irgendeiner Richtung. Der Nachteil aber ist, dass immer mehr Daten dadurch generiert werden. Was derzeit stark im Kommen ist, sind biometrische Daten, in denen man sich vor allem Vorteile in Sicherheitsaspekten erhofft. Für diese gibt es aber hohe Verwendungsbeschränkungen bzw. gibt es nur ganz bestimmte Gründe, warum und wann man diese Daten überhaupt verwenden und weiterverarbeiten darf.

Auch Daten über die Bonität eines Menschen sind in den letzten Jahren stark hervorgekommen. Bonitätsprüfungen sind mittlerweile bei jedem Kauf auf Raten üblich. Diese bergen aber Probleme der Interessensabwägung in sich. Aufgabe der Behörde ist es, in Verhältnismäßigkeitsprüfungen die legitimen Interessen eines/r Gläubigers/in mit dem Geheimhaltungsinteresse des/r Schuldners/in an seinen/ihren Daten abzuwägen, was als Einzelfallprüfungen nicht immer einfach ist. Es gilt aber, dass Kreditauskunfteien von der Gewerbeordnung anerkannte Gewerbe sind. (GK 8)

- **Wichtigkeit der Privatsphäre**

Die ExpertInnen stimmen überein, dass das Ansehen der Privatsphäre und die Wertschätzung von Daten bröckeln. WZ sieht sie aber als soziales Konstrukt, das zwar Veränderungen ausgesetzt ist, man aber nicht unbedingt gegen den Willen der Betroffenen erhalten und durchsetzen muss.

Für die Jugendlichen, die in der heutigen Zeit sozialisiert wurden, verliert die Privatsphäre an Bedeutung, weil so viele so vieles über sich preisgeben. Anders sieht das zum Beispiel die Großelterngeneration, die den Weltkrieg hautnah erfahren hat und mit Spionage konfrontiert war. Unser Gehirn funktioniert so, dass man das, was man nicht wahrnimmt, für jemanden auch nicht existiert. Das lässt sich auch auf die nichtsichtbaren Gefahren im Internet übertragen. Solange den Personen nichts Nachteiliges widerfahren ist, solange gilt die Preisgabe der Daten als ungefährlich. Offenbar ist den Jugendlichen diesbezüglich noch wenig Unangenehmes passiert. (GR 4)
GK denkt ähnlich, dass es zu einer gesellschaftlichen Veränderung in der Bewertung von Privatsphäre gekommen ist, weil man heute einfach mehr ausplaudert als früher. Das muss nichts Negatives bedeuten, Vorsicht ist jedoch geboten, nicht jegliches Maß im Umgang mit Daten fallen zu lassen. Bei einer Umfrage würde wohl trotzdem ein Großteil der Leute sagen, dass ihnen ihre Privatsphäre wichtig ist. Aber sie scheint sich gesellschaftlich zu ändern. Vor allem sind den Leuten die Konsequenzen in den elektronischen Medien nicht ganz bewusst, weil sie nicht unmittelbar Auswirkungen auf die gesetzten Ursachen hin erfahren. Sie glauben die Daten wären nur dort, wo man sie hintransportiert hätte. (GK 21)
Auch EM meint, dass UserInnen völlig unterschätzen, wie wertvoll ihre Datensätze sind und dass mit diesen inzwischen ein Riesenhandel betrieben wird. Leute können selbst mit den Kommunikationsmedien im Internet, nur soweit umgehen, dass sie eine Kommunikation zusammenbringen. Unter welchen Umständen sie geschieht, wer da noch dabei sein könnte, den man weder sieht noch hört, darüber machen sie sich keine Gedanken. Dieser sorglose Umgang und dieses Nichtwissen und Nichtwissen-Wollen ermöglicht aber gerade große Gefahren und Nachteile. Beispielsweise, wenn aus Sorglosigkeit dazu eingeladen wird, einen Rechner zu kidnappen, auf dem dann Kinderpornographie gehostet wird oder wenn man auf Attacken mittels Phising-Websites oder Spam-Mails hereinfällt oder wenn man

Mail-Systeme falsch verwendet. Manche Leute zeigen irrationales Verhalten, indem sie über solche Gefahren gar nicht aufgeklärt werden wollen, weil sie so weiter tun wollen wie bisher. Richtiger und sicherer Umgang mit Internet-Tools ist selten. (EM 7)
DZ sieht die Wichtigkeit der Privatsphäre unterminiert, wenn sie, wie bereits zuvor erwähnt, die Studie der EU anführt, die belegt, dass UserInnen kaum auf die Privacy-Einstellung in Social Networks achten. (DZ 3)
Gründe dafür, die Einstellungen so zu wählen, dass jede/r Zugang zu ihren Profilen hat, liegen nach GK einerseits daran, dass die Leute nicht besser Bescheid wissen bzw. darüber aufgeklärt wurden und andererseits daran, dass es ihnen egal ist, wer die Profile betrachten kann. (GK 13)
Etwas anders sieht das WZ. Er fürchtet, dass Privatsphäre ein soziales Konstrukt ist und erklärt das mit den extremen Unterschieden im Umgang mit Privatsphäre bereits in den europäischen Nationalkulturen, zum Beispiel wie viele Einblicksmöglichkeiten Europäer in ihre eigene vier Wände bieten. Was in Holland gang und gäbe ist, wäre in Osteuropa undenkbar. Ein anderes Beispiel wäre der Umgang mit Gehalts- und Steuerdaten in Schweden und Österreich. Während diese in Schweden zu einzelnen Personen ganz leicht herauszufinden sind, tritt man hierzulande einer Person sehr nahe, wenn man sie nach dem Gehalt fragt.
Auf der anderen Seite hält WZ selbst die Privatsphäre für wichtig. Sie bietet einen Rückzugsbereich, der kulturell, politisch und gesellschaftlich geformt ist. Ändert sich der Kontext bzw. Konsens, was in einer Gesellschaft als Privatsphäre zu gelten hat, führt das zu großer Verunsicherung, weil unsere Person Veränderungen ausgesetzt ist. (WZ 11)
Dennoch hält WZ Forderungen nach mehr Datenschutz gegen den Willen der Betroffenen für unangebracht. Eine schwierige Frage selbst für die *ARGE Daten* ist, was nun genau schützenswert sei und was nicht, wenn doch Personen die Daten freiwillig hergeben. Hier zerbröckelt ungewollt das Paradigma, dass Privatsphäre unbedingt geachtet und erhalten werden muss. (WZ 13)

- **Wert von Daten**

EM und GK sprechen den pekuniären Wert an, der in den Datensammlungen liegt.

Datensätze können extrem wertvoll sein, wie auch das Beispiel der Steuerdaten-CD in Liechtenstein und der Schweiz beweist. Für die Daten wird viel Geld hingeblättert, weil man aus ihnen noch viel mehr lukrieren kann. Auch die Daten, die bei *23andme* generiert werden, sind Sprengstoff bzw. extrem wertvoll, da sie Neigungen zu Krankheiten bergen, und zwar kombiniert mit Name, Adresse und Bankverbindung, weil man für den Dienst ja zahlen musste. (EM 6)
Datensätze stellen im Wirtschaftsleben, gerade für Marketingzwecke einen pekuniären Wert dar, der umso höher ist, je genauer, echter, richtiger die Datensätze zutreffen und werden sogar gehandelt. Darum versuchen Unternehmen auch vollständige Bilder ihrer KundInnen zu erhalten. So geschehen Gewinnspiele fast nie ohne Gegenleistung. Die Gegenleistung sind die Daten, die für die Unternehmen eben auch einen Wert haben. (GK 17)

- **Möglichkeiten in der Datenverarbeitung und -auswertung**

Die ExpertInnen gehen damit konform, dass die Auswertung der Daten automatisiert mittels Algorithmen abläuft. Mit diesen ist selbst eine Datenflut zu besänftigen. Der Mensch bildet schließlich das Ende der Kette und misst den Daten Bedeutung bei. Von rechtlicher Seite her nimmt die Zustimmung der Betroffenen zur Datenerhebung und -verarbeitung eine wichtige Stellung ein. Einmal rechtmäßig veröffentlichte Daten unterliegen keiner Zweckbindung.

Nach dem österreichischen Datenschutzgesetz ist es so, dass allgemeine verfügbare Daten, sofern sie rechtmäßig veröffentlicht worden sind, nicht mehr unter dem Schutz des Grundrechts stehen. Das heißt, einmal rechtmäßig veröffentlichte Daten dürfen grundsätzlich für andere Zwecke weiterverarbeitet werden. Beispielsweise dürfen Daten aus dem Telefonbuch für Marketingzwecke gebraucht werden, obwohl das nicht der ursprüngliche Zweck der Speicherung war. Gedanken in Richtung einer Reformierung, veröffentlichte Daten an den ursprünglichen Verwendungszweck zu knüpfen, wurden schon getätigt, derweilen aber noch nicht umgesetzt. (GK 4)
Ein Service, wie beispielsweise das der Gentests bei *23andme* ist legal, solange die Betroffenen ihre ordentliche Zustimmung für die Erhebung und Verarbeitung der Daten geben. Das drückt ein Grundsatz im Datenschutzrecht aus, der in Deutschland sehr treffend *Informationelles Selbstbestimmungsrecht* heißt. Unternehmen, die ihren Standort außerhalb

Österreichs haben, wie zum Beispiel *Google* und *23andme*, liegen aber nicht im Zuständigkeitsbereich der Datenschutzkommission.

Zwei Dinge sind dabei oft problematisch: Zum einen sind die Zustimmungserklärungen oftmals nicht sauber ausgeführt oder sie werden einfach übergangen, was aber rechtswidrig ist. Zum anderen sind die Zustimmungen anders als im Vertragsrecht jederzeit widerruflich. Sobald widerrufen wird, ist die Verwendung von Daten für einen bestimmten Zweck nicht mehr erlaubt. Solange sich solche Phänomene auf die Zustimmungen der KundInnen stützen, sind sie datenschutzrechtlich nicht problematisch. Problematisch wird es dann, wenn Unternehmen auf Daten zugreifen, ohne die Betroffenen zu informieren oder ihre Zustimmung erhalten zu haben. (GK 9)

Datenauswertungen, bei denen es um Quantifizierungen geht oder bei denen eine genaue Hypothese vorliegt, laufen dann automatisch ab. Das ist im Grunde Statistik. Für eine Bedeutungsauswertung braucht man Menschen dahinter. (WZ 23)

Im Hintergrund laufende Algorithmen sind immer vom Menschen programmiert und das Bedrohliche daran ist, dass sie meist schlecht programmiert sind. Es gibt keine Alternative und keinen Ausschaltknopf für das, was einem ständig vorgeschlagen wird und zugleich geben sie eine gewisse Richtung vor, in die man vielleicht nicht will und was zu Langeweile führt und eine/n dann aus dem Angebot aussteigen lässt.

Beim Musikportal *Last.fm* beispielsweise bekommt man ein tolles Musikprogramm zusammengestellt, das genau zum persönlichen Musikgeschmack passt, wenn man sich die Mühe macht, die Titel zu bewerten. Der Nachteil ist, man bleibt in diesen Bahnen und entdeckt nichts Neues.

Es gibt aber auch schon Programme, die aus reinen, unstrukturierten Daten, Trends vorschlagen. Letztendlich muss aber der Mensch diese Trends bewerten. (WZ 24)

Monster hat als Privatanbieter den Vorteil gegenüber dem *AMS*, mit Hilfe von Algorithmen aufgrund von einigen persönlichen Daten einen recht guten Index ausrechnen zu können, wie hoch die Employability ist. Dafür reichen bestimmte Kernwerte und Kernaussagen, auf deren Basis ein Modell der Berufslaufbahn entwickelt wird. Dabei ist es hier unnötig, über manche sensible Daten Bescheid zu wissen, zum Beispiel wie die sexuelle Orientierung der Person aussieht. (WZ 25)

Dem würde EM zustimmen. Algorithmen werten die Unmengen an Daten aus. Menschen stehen am Ende der Datenkette. Die nehmen, was der Computer ausspuckt. (EM 14)

Die Auswertungsmöglichkeiten für Daten sind unbegrenzt. Man kann alle möglichen Fragen an genaue Datensätze stellen. Man kann sie jeweils für andere Produktlinien und Firmen

zweitverwerten, drittverwerten, viertverwerten, verschiedene Teile aus diesen Datensätzen nehmen, usw. Der Vermarktbarkeit sind keine Grenzen gesetzt. Das Argument, dass es ohnehin zu viele Daten seien und man nicht alle auswerten könne, ist Humbug. Allein für *Linux* gibt es zehn verschiedene Open Source Data-Mining-Tools, die trivial zu handhaben sind. Das Schwierige ist, die richtigen Fragen an die Daten zu stellen, was man eigentlich wissen will, sonst werden die Ergebnisse zufällig. (EM 15)

DZ sieht genau diese Hürde im Umgang mit Daten. Es besteht die Schwierigkeit, die Masse an Daten so strukturiert auszuwerten, dass aussagekräftiges Material entsteht. Vor diesem Hintergrund kann man sagen, gibt es eine Barriere, nicht einfach aufs Gutdünken hin, Foren usw. zu durchpflügen. (DZ 10)

Hat man aber die Suchkriterien definiert, besteht für GR kein Zweifel, eine Datenflut zu bewältigen. Die Auswertung bei *Google* läuft sicherlich größtenteils automatisiert ab. Wer bezweifelt, dass so ein großer Datenwulst analysiert werden kann, soll sich vor Augen halten, dass *Google* es schafft, in Sekundenbruchteilen eine millionenfache Trefferliste für einen Suchbegriff darzustellen. Warum sollten sie es als größter Data-Mining-Experte auf dem Globus nicht schaffen, die eigene Datenbank nach gewissen Suchkriterien zu durchforsten und zu sortieren. (GR 11) Fehlen diese Suchkriterien, haben die DatensammlerInnen aber nicht viel von der Datensammlung, dann können sie aus diesen Daten keine Informationen herausfiltern. (GR 26)

Die Auswertung der Daten, vor allem bei reinen Datenbankfeldern, geschieht fast ausschließlich elektronisch und automatisiert. Händische Auswertung im Breitenfeld, und jetzt nicht an der technologischen Spitze, geschieht noch bei Videoüberwachungsanlagen. Da muss noch ein Mensch kontrollieren, ob ein abweichendes Verhalten gegeben ist oder bestimmte Personen zu sehen sind. Künftig werden Bilddaten aber wohl auch automatisiert bearbeitet werden können. Der Mensch wird dann nur noch die Sequenzen zu bewerten bekommen, in denen Abweichungen vom Normalfall auftreten. (GK 18)

Mit solchen Daten ist es schließlich auch leicht, Prognosen über die Zukunft zu erstellen, denn die sind Teil der Profile. Sie besagen, was man heute mit hoher Wahrscheinlichkeit tun wird, weil man es immer so macht. Je nachdem welche Anforderungen man an das System stellt, können abweichende Verhaltensmuster festgestellt und Alarm geschlagen werden. Wenn jemand beispielsweise jährlich nach Griechenland auf Urlaub fährt, aber dieses Jahr nicht, kann das System das bemerken und das geht sehr wohl in die Zukunft. Anhand der Mobilfunkdaten kann man das beispielsweise leicht erkennen. (EM 16)

4.6.1.1 Zwischenfazit

Die Aspekte zum digitalen Fußabdruck behalte ich mir für die Beantwortung der Forschungsfragen vor, um mich nicht zu wiederholen.

Sensible Daten sind vom Recht genau definiert und nur als solche vom Datenschutzrecht als besonders schutzwürdig beachtet. Dennoch macht die Sichtweise der ExpertInnen Sinn, dass es individuelle Unterschiede gibt, welche Daten als sensibel erachtet werden und welche nicht. Dies drückt sich besonders im Umgang mit diesen Daten aus, der eine will sie in der Öffentlichkeit angesprochen wissen, die andere behält sie für sich. Daraus sollte folgen, dass die rechtliche Schwelle für Datenschutz sehr tief anzusetzen ist, sodass trotz individueller Differenzen das Schutzniveau für jede/n als ausreichend empfunden werden kann. Denn so betont auch der deutsche Bundesbeauftragte für Datenschutz und Informationsfreiheit Peter Schaar, dass es Daten, die nicht schutzbedürftig sind, eigentlich nicht gibt. In fremdem Kontext können sie heikle Angelegenheiten beschreiben und Persönlichkeitsrechte verletzen. Neben dem Datenschutzrecht und Rechtsansprüchen aus anderen Gesetzen, können dabei Richtlinien helfen, die als eine Art freiwilliger Selbstkontrolle fungieren, so meine InterviewpartnerInnen.

Doch welche Gründe sehen die ExpertInnen für die freiwillige Preisgabe heikler Daten? Aus ExpertInnensicht fehlt den UserInnen die Medienkompetenz hinsichtlich des Internets. Es hat sich noch kein Erfahrungsschatz ausbilden können, der auf die Gefahren hinweist und klarstellt, dass das Internet kein flüchtiges Medium wie das Fernsehen ist. Außerdem herrscht ein Druck zur Selbstdarstellung nach dem Motto „Wenn es jede/r macht, mache ich es auch.“ Dabei entsteht ein halböffentlicher Raum oder wie es Zeger nennt, ein Bereich „schwacher Öffentlichkeit“.

An quantitativem Umfang lässt sich die Preisgabe von Daten kaum mehr vergrößern, künftig wird im Vordergrund stehen, die Daten zu perfektionieren. Da von DNA-Daten, anderen biometrischen Daten bis zu Daten über die Bonität eines Menschen alles vorhanden ist, gilt es, sie qualitativ an semantischem Gehalt aufzuwerten.

Das Ansehen der Privatsphäre wird von den NutzerInnen ebenso unterschätzt wie der pekuniäre Wert ihrer Daten, der umso höher ist, je genauer, richtiger, echter die Daten sind.

Die unheilvollen Konsequenzen der geringen Wertschätzung an Daten sind ihnen dabei nicht gänzlich bewusst. Überhaupt fehlen ihnen des Öfteren das Wissen und der Wille zum Wissen, Internet-Tools richtig und sicher zu verwenden. Das beweist auch die Studie, dass der Großteil der Social Networks-TeilnehmerInnen die Möglichkeiten, die Privacy-Einstellungen zu ändern, ignoriert. Einen anderen Aspekt bringt WZ ein, wenn er fragt, ob Privatsphäre schützenswert ist, wenn UserInnen sie bereitwillig aufgeben. Es schleicht sich das Gefühl ein, dass ein Paradigma zerstört wird und zwar, „dass es hier irgendwas wie Privatsphäre gibt und man unbedingt darauf schauen muss, dass die geachtet wird und hält.“ Dass das, was als Privatheit angesehen wird, kulturellen Vorverständnissen und einem zeitlichen Wandel unterliegt, rechtfertigt meiner Meinung nach noch nicht die Bezeichnung der Privatsphäre als soziales Konstrukt wie sie WZ ins Feld führt. Dies würde auch der Definition von Beate Rössler widersprechen, die Privatheit als Schutz vor unerwünschtem Zutritt anderer betrachtet. Selbst wenn das Zugangstor gesellschaftlich gesehen weiter geöffnet wird, gibt es immer noch einen Rest an Privatheit, den der/die Einzelne gewahrt wissen will. Doch ich stimme zu, dass es in der Hand des/der Einzelnen liegen sollte, um diese Privatheit zu kämpfen. Auf die Gefahren sollte man hinweisen, den Individuen aber nicht dreinreden, wie sie es handhaben sollten.

Sind Daten einmal rechtmäßig veröffentlicht, dürfen sie grundsätzlich für andere Zwecke verwendet werden. Die fehlende Zweckbindung im Gesetz erlaubt es dann Marketingunternehmen zum Beispiel auf Daten aus Telefonbüchern zurückzugreifen. Ansonsten brauchen Unternehmen die Zustimmung der Betroffenen, um Daten zu erheben und zu verarbeiten. Letzteres geschieht automatisiert mittels Algorithmen, so die ExpertInnen, was bedeutet, dass auch mit einer großen Menge an Daten umzugehen verstanden wird. Der Mensch steht am Ende dieses Prozesses und misst ihnen schließlich Sinn und Bedeutung bei. Stellt man also die richtigen Fragen an Datensätze, kann man die entscheidenden Informationen leicht herausfiltern. Daten lassen sich je nach Anfrage vielfach verwerten. Es lassen sich auch Wahrscheinlichkeiten über künftige Ereignisse bestimmen. Schlussendlich ist es auf SammlerInnenseite meist gar nicht so wichtig, jetzt speziell über sensible Daten wie die sexuelle Präferenz Bescheid zu wissen, Beziehungsnetzwerke sagen grundsätzlich mehr über eine Person aus.

4.6.2 Charakterisierung von Überwachung aus ExpertInnensicht

Dieser Block behandelt die Aussagen der InterviewpartnerInnen zum großen Themenfeld der Überwachung hinsichtlich Vorteilen, Gefahren, staatlicher, wirtschaftlicher, individueller Überwachung freiwillig veröffentlichter Daten, sowie Verbesserungsvorschlägen, streicht wiederum Unterschiedlichkeiten und Überschneidungen heraus.

- **Methoden der Datenerhebung**

Die ExpertInnen vertreten unter diesem Punkt die ähnlichen Meinungen, dass öffentlich bereitgestellte, freiwillig hergegebene Daten sehr wohl, neben spezielleren Methoden der Datenerhebung seitens Wirtschaft und Staat, der Informationsgewinnung dienen.

Es gibt einerseits die willkürliche Transparenz im Internet, die eine bewusste Preisgabe von Daten in Social Networks beschreibt. GR nennt dies *Datenstriptease-Phänomen*. Auf der anderen Seite gibt es die unwillkürliche Transparenz im Internet, die unbewusst durch Suchmaschinen und diverse dubiose Dienste entsteht, das *Google-Phänomen*. Beide zusammen ergeben den gläsernen Menschen und dürfen gemeinsam als gegenwärtiges Problem nicht unterschätzt werden. (GR 14)

Freiwillig hergegebene Daten ergänzen sich optimal mit anderen Methoden der Datenerhebung. Gewisse Sachen können wir nur selbst von uns weitergeben, weil die nirgends aktennotorisch sind, die weiß niemand anderer, außer man erzählt es. Und diese können prima in bestehende Profile integriert werden, die man aus eigenen Datensätzen angefertigt hat. Ein/e Netzbetreier/in weiß beispielsweise, wer wie oft wohin telefoniert, wie oft ins Ausland, welche Nummern, usw. und kann mit diesen Daten ein Profil erstellen und will dadurch ihr Geschäft optimieren. Aber er/sie weiß nicht über die Internetinteressen und andere interessante Daten der Person Bescheid. Würde man bei dem/r selben Anbieter/in sowohl telefonieren, als auch internetsurfen, so ließen sich diese Daten schon wieder einfach verbinden. (EM 8)

Unternehmen sind sicherlich auf die Freiwilligkeit von KundInnen und deren bereitwillig hergegebenen Daten angewiesen. Unternehmen benötigen für die Vertragserfüllung gewisse Daten von KundInnen, für die sie auch verwendet werden dürfen. Will ein Unternehmen die

Daten aber anderweitig, zum Beispiel für Marketingzwecke verwenden, braucht sie wiederum einen Rechtfertigungsgrund im Datenschutzgesetz, den letztendlich nur die Zustimmung liefert, die jederzeit widerruflich ist. Gerade bei Marketingzwecken sind es also Daten, die freiwillig von den KundInnen preisgegeben wurden in irgendeiner Form. Bei Gewinnspielen gibt es oft zusätzlich eine Zustimmungserklärung, die man unterzeichnen muss und in der auch stand, dass diese Daten für Marketingzwecke verwendet werden dürfen.

Der Staat hat aufgrund gesetzlicher Vorschriften gewisse Befugnisse, Daten zu erheben, aber nur für gesetzlich vorgeschriebene Zwecke. Daten im Melderegister oder Daten bei den Sozialversicherungen dürfen nur gegen eine Rechtfertigung, für andere als die bestimmten Zwecke verwendet werden. Die hat der Staat genauso wenig wie Unternehmen.

Die Gefahr droht eher von Unternehmen, die Daten beispielsweise für Marketingzwecke heranziehen, wo sie keine Zustimmung vorweisen können. Das sind die schwarzen Schafe. (GK 11)

Nachrichtendienste und Marketingfirmen können die öffentlichen Daten auf jeden Fall gut gebrauchen. Sie sind NutznießerInnen dieser Freigiebigkeit und der Möglichkeiten im Netz. (WZ 13)

Auch DZ denkt, dass öffentlich preisgegebene Daten eine Rolle insbesondere für Unternehmen spielen. Wenn es um die kommerzielle Nutzung geht, versucht die Wirtschaft sicher Breschen zu schlagen in die Netzwerke in unterschiedlichster Form, beispielsweise als DrittanbieterInnen oder dass sie mittels Applikationen direkten Zugang zu NutzerInnen-Daten erhalten. (DZ 4)

- **Technischer Rüstungskampf**

Zwei der Experten stimmen überein, dass im Netz ein technischer Rüstungskampf um Überwachung und Verschleierung vorherrscht. GR sieht das nicht so, behält für das Statement aber nur die relativ wirkungslosen Verschleierungsdiensten für IP-Adressen im Auge.

Es gibt einen technischen Rüstungskampf im Netz, aber es ist schwieriger etwas zu verschleiern, als es derzeit leichter ist, etwas herauszufinden. Auch das *TOR*-Network lässt sich umgehen, wenn man weiß wie. Wenn man einen Fehler macht, kann man schnell

aufgedeckt werden. Für die Gegenseite gilt, wenn man einmal Daten nicht gesammelt hat, macht das nichts, es ergeben sich noch viele Chancen. (WZ 26)
Man kann im Internet von einem technischen Rüstungskampf sprechen, denn was die eine Seite an Überwachungstechnik dazubekommt, kriegt die andere Seite an Waffen in die Hände. (EM 19)
GR sieht eher keinen technischen Rüstungskampf im Netz, weil die Verschleierungsdienste zwar Daten sammelnden Privatunternehmen ein Schnippchen schlagen, indem die IP-Adresse verschleiert wird, Narrenfreiheit garantieren sie aber noch lange nicht, da sich auch Verschleierungsdienste an Gesetze halten müssen. Vor den Behörden schützen sie nicht, denn nach einer eventuell begangenen Straftat müssen die Verschleierungsdienste die korrekten Daten sehr wohl den Behörden übermitteln. (GR 21)

- **Motive und Nutzen staatlicher Überwachung**

EM und WZ bezweifeln beide, dass staatliche Überwachungsmittel die erhofften Sicherheitseffekte auslösen.

Die Motive hinter staatlicher Überwachung sehen so aus: Man probiert etwas, sieht, dass einem die großen Fische nicht ins Netz gehen und sagt dann, jetzt, wo wir es haben, sollten wir es auch gebrauchen. Wenn es sein muss, für andere Dinge. Beispielsweise geschieht ein Terroranschlag. Stimmen werden laut, die mehr Überwachung fordern. Die EU handelt und gibt eine Richtlinie heraus, die eher breit formuliert wird wie bei der Vorratsdatenspeicherung. Bei der Umsetzung in nationale Gesetze will man plötzlich die FilesharerInnen mit einbeziehen. Eingeführt nur für Fälle von Schwerverbrechen und Terrorismus, zieht man auf einmal Delikte heran, die gerade mit einem halben Jahr bedingt bestraft werden, also die Schwelle soll unter ein Jahr sinken. Die Freiheit verschwindet scheibchenweise wie eine Salami, aber schnell. (EM 11)
Anscheinend bringt dem Staat die Überwachung seiner BürgerInnen nicht viel, denn ansonsten hätte es in den USA im Dezember letzten Jahres mit dem Flug nach Detroit nicht beinahe wieder einen Anschlag gegeben. Jedoch gelingt es dem britischen Geheimdienst offenbar öfters, manch versuchte Anschläge zu vereiteln, wobei es hier eigentlich weniger um klassische Informationsarbeit und um die Verarbeitung elektronischer Daten geht. Auf

der anderen Seite hat London mit einer Form der hohen Jugendkriminalität zu kämpfen und die ist auch mit Überwachung nicht in den Griff zu kriegen. (WZ 15, 16)

PolitikerInnen verzapfen immer wieder populistischen Schwachsinn, „Stopptafeln gegen Kinderpornographie“ ist so eine Sache und das tun sie erstens, weil sie es nicht besser wissen, zweitens weil sie trotz besseren Wissens, dass es sich um einen technischen Blödsinn handelt, mit dem Argument ein anderes Ziel verfolgen oder die Linie, es vor anderen Parteien auszusprechen. (EM 21)

Doch das Momentum der Überwachungswelle scheint sich wieder etwas zu verflachen, sie hat nicht mehr so eine Dynamik. Auch in der Politik wird langsam umgedacht, weil die Überwachungstechnik teuer ist und nicht viel bringt. Verwendet jemand beispielsweise eine Virtual Private Network-Verbindung als Kommunikationsmedium, was bei durchschnittlichen Firmen üblich ist, weil sie sonst anfällig gegen HackerInnen wären und vertrauliche Firmendaten auf dem Spiel stünden, so können eine solche Verschlüsselung selbst Geheimdienste nicht in Echtzeit knacken. Das haben alle namhaften KryptographInnen der Welt bestätigt. Und natürlich benutzen auch klügere VerbrecherInnen und TerroristInnen solche VPN-Verbindungen. Und somit sind Maßnahmen wie die Vorratsdatenspeicherung nur gegen Eierdiebe, also FilesharerInnen gerichtet. Dahinter steht die Musikindustrie, nur dafür sah sie der/die Gesetzgeber/in nicht vor. Für Urheberrechtsinteressen eine Generalüberwachung der gesamten Bevölkerung zu machen, würde der Angemessenheit und Ausgewogenheit, von der JuristInnen sprechen, deutlich widersprechen. (EM 17, 18)

Die Argumente, mit mehr Überwachung, wären bestimmte Fälle nicht passiert, weist EM als unbewiesene Behauptungen zurück. Beispielsweise sind Banken die Orte, die am stärksten und längsten mit Videoüberwachung besehen wurden, die Zahl der Einbrüche stieg trotzdem.

In London, wo am meisten Videoüberwachungssysteme betrieben werden, wird mittlerweile an Softwarelösungen geforscht, die die BeamtInnen bei der Betrachtung der vielen Bildschirme entlasten. Ansonsten müsste man zu viele BeamtInnen einsetzen, um die Überwachungssysteme effizienter zu machen, was die Kosten aber immens in die Höhe treibt. Auch die *Wiener Linien* haben keine Kosten gescheut ein Kamerasystem zu installieren. Aufgerechnet mit den Kosten von Vandalismusschäden müsste dieses 25 Jahre problemlos laufen, um die Kosten wieder einzuspielen. Um Vandalismusschäden zu verringern, würden jedoch Leute, die den Wagen kehren und damit Präsenz zeigen, viel eher

helfen als Videoüberwachung, die nicht von gruppendynamischen Effekten abzuhalten vermag. (EM 10)
Überwachung bringt nicht mehr Sicherheit, denn die Videoüberwachungssysteme in London konnten die Anschläge auch nicht verhindern, später war es lediglich leichter die Verbrechen aufzuklären. (EM 20)

- **Vorratsdatenspeicherung**

Die vier Experten, die die Vorratsdatenspeicherung ansprechen, übereinstimmen darin, dass die Funktion der Vorratsdatenspeicherung sein solle, Daten präventiv bereitzustellen. Ihre Sinnhaftigkeit wird hinterfragt.

Bei der Vorratsdatenspeicherung werden Daten für einen Fall gespeichert, der noch nicht eingetreten ist. Falls jemand einmal kriminell wird, reserviert man sich gleich die Daten, um nachher leichter feststellen zu können, was da genau geschehen ist und wie es dazu kommen konnte. GR hält das für einen Eingriff in die Privatsphäre und in die Freiheit des Menschen. (GR 19)
Um überhaupt einen Informationswert zu generieren, muss der Staat seine Profilsuche genau definieren, worauf er die dazupassenden Daten dann semantisch auswerten kann, das gilt auch für die Vorratsdatenspeicherung. Die Vorratsdatenspeicherung funktioniert nach dem Schema, viele Heuhaufen anzulegen, damit man überhaupt erst suchen kann, weil man mittlerweile befähigt ist, eine Nadel darin zu finden. (WZ 14)
Die Ansicht, Verbrechen präventiv zu bekämpfen und eventuell vor der Tat zu erkennen, folgt der Maxime der Sicherheitsmaximierung. Die Umsetzung führt dann aber zu Generalüberwachung, zum Generalverdacht aller BürgerInnen und zu Freiheitseinschränkungen. In einem demokratischen System, wie wir es jetzt noch kennen, hat jede/r das Recht, nicht die Pflicht, aber das Recht, ein Verbrechen zu begehen. Wer jemanden präventiv einsperrt, nimmt diesem das Recht, ein Verbrechen zu begehen und zugleich das Recht zur willentlichen Entscheidung, die Straftat doch nicht zu begehen. (WZ 17, 18)
Der Datenschutzansatz wandelt sich in Richtung Vorratsdatenspeicherung nach dem Grundsatz, alle wären potentiell Verdächtige und darum werden alle Daten vorerst gespeichert, weil man sie einmal brauchen könnte. Es wird aber gerade auf europäischer

Ebene diskutiert, ob man die Richtlinie der Vorratsdatenspeicherung nicht zurücknehmen will, aufgrund derer, die Staaten verpflichtet sind, diese umzusetzen. (GK 15)
Klügere VerbrecherInnen und TerroristInnen, gegen die die Vorratsdatenspeicherung gerichtet ist, könnten eine solche leicht austricksen. (EM 18)

- **Staatlicher Zugriff auf freiwillig veröffentlichte Daten**

Ob der Staat, seine Behörden und Nachrichtendienste öffentliche Profildaten in Betracht ziehen, ist auf jeden Fall denkmöglich. Rechtlicherseits gibt es zwar genaue Vorgaben, wie weit sie gehen dürfen, die ExpertInnen befinden derartige Zugriffe zur Informationsgewinnung aber als durchaus vorstellbar.

Dass der Staat auf freiwillig hergegebene Daten zurückgreift, sieht DZ vorderhand als die geringere Gefahr, als dass Unternehmen das als Chance sehen, zielgruppenspezifisch zu werben oder kostengünstig Informationen über Kauf- oder Verhaltenvorlieben zu generieren. Bei einer internationalen Konferenz wurde aber einmal behauptet, dass sich in Belgien FinanzbeamtInnen in eine Forumsgruppe zum Thema Steuertricks und -tipps eingeschleust und diese Informationen für Steuerverfahren gewonnen hätten. Denkbar ist es also sehr wohl, dass solche Daten nutzbar gemacht und missbraucht werden könnten. (DZ 5)
Der Staat kann grundsätzlich auf freiwillig hergegebene Daten, die ja schließlich verfügbar sind, zugreifen. Nur ist die Zulässigkeit einer solchen Maßnahme nicht gegeben, weil auch der Staat für die jeweilige Datenverwendung eine rechtliche Grundlage braucht, so wie bei Privaten eine Verhältnismäßigkeitsprüfung einen Rechtfertigungsgrund erbringen kann. Staatlicherseits müssen für eine ordnungsgemäße Grundlage die Zwecke genau definiert sein. Auch Sicherheitsbehörden unterliegen, wo es um strafrechtlich relevante Daten geht, dem Sicherheitspolizeigesetz und der Strafprozessordnung, die genau regeln, welche Datenanwendungen sie betreiben dürfen und was sie machen dürfen. Eine allgemeine Datenbank, in der man von jedem/r österreichischen Staatsbürger/in alles zusammenfassen könnte, wäre nicht zulässig. (GK 15) Also greift der Staat grundsätzlich eher nicht auf Social Network-Profile zurück. Wenn aber Strafverfolgungsbehörden einen bestimmten Sachverhalt prüfen, ein bestimmtes oder mögliches strafrechtliches Vergehen, dann kann sich GK schon vorstellen, dass sie auf solche Profile und veröffentlichten Daten zugreifen.

Wahrscheinlich sind Strafverdächtige aber wohl eher nicht in Social Networks zu finden. (GK 16)

Alle, von den Geheimdiensten bis hin zum investigativen Journalisten Erich Möchel, verwenden Social Networks zu Überwachungszwecken, um Details über Personen seines Interesses und ihre Affilitationen zu erfahren. Beispielsweise gab es bei der *NSA* in den letzten Jahren Veranstaltungen mit dem Fokus, Intelligence aus Public Intelligence zu gewinnen. Damit meinen sie Social Networks, weil die Leute dort ja Unmengen an Daten preisgeben. Was hier der/die Einzelne kann, können Nachrichtendienste automatisiert. (EM 10)

Geheimdienste müssen die Daten nicht mehr mühsam zusammensuchen und Daten aus verschiedenen Quellen verknüpfen, sondern können auf fertige Profile zurückgreifen. Die Erstellung von Profilen fällt somit leichter. (WZ 12)

Die Veränderung zu früher ist, dass es heutzutage leichter ist, allein mit Abfragen in öffentlich zugänglichen Internetdatenbanken ein Profil einer gesuchten Person zu erstellen. Auch die Informationsdienste, die nicht umsonst so heißen, erleichtern ihre Arbeit, indem sie auf öffentlich zugängliche Daten und veröffentlichte Profile zurückgreifen. Wenn aber sogar der/die Privatuser/in bereits Dienste wie *Google Maps* benutzen kann, bleibt den Geheimdiensten nicht mehr viel Informationsvorsprung. So gesehen haben sie nicht viele andere Zugangsmöglichkeiten als öffentlich zugängliche Daten. Sie haben ansonsten noch Sozialversicherungsdaten, die nicht soviel hergeben, die Vorratsdatenspeicherung ist noch nicht eingeführt und sie haben Überwachungsdaten, aber dafür müssen sie schon die Nadel im Heuhaufen definiert haben, die sie suchen. (WZ 14)

GR kann nur mutmaßen, aber er denkt, dass *Google* sehr wohl mit westlichen Staaten kooperiert, was dazu führt, dass diese Einblick in Profile erhalten. In den USA sind Unternehmen aufgrund des *Patriot Acts* ohnehin verpflichtet, Daten im Kampf gegen den Terrorismus bereitzustellen. (GR 18)

GR sieht viele Große Brüder in der globalen Gesellschaft von Staaten bis Privatunternehmen, die mitunter auch kooperieren und sich Informationen gegenseitig zuschieben. China, Vietnam und Myanmar wären in Asien richtiggehende Big Brother-Staaten. Als Größten Bruder bezeichnet er aber die USA aus dem einfachen Grund, dass die meisten IT-Unternehmen dort angesiedelt sind und sich die Amerikaner, vor allem die Geheimdienste aufgrund des *Patriot Acts* eben Zugang zu ihren Datensammlungen, -netzen und -banken verschaffen können. (GR 25)

- **Motive und Nutzen wirtschaftlicher Überwachung**

Drei der ExpertInnen stimmen einhellig überein, dass wirtschaftliche Unternehmen Daten sammeln, um das Marketing zu optimieren und Profit daraus zu schlagen.

Die Unternehmen möchten möglichst viel über ihre KundInnen wissen, um ihnen mehr verkaufen zu können, der Ausdruck dafür lautet Business Intelligence. Und das Geschäftsmodell der Web 2.0-Plattform-BetreiberInnen ist ohnehin, im Gegenzug für Speicherplatz Profile zu erhalten. Die dienen dann rein der Vermarktung. Man kann Inserate ganz gezielt für Zielgruppen schalten, welches Alter, welche Stellung, welche Interessen. Je genauer man die Zielgruppe einschränkt, desto mehr kostet es bei *Google*. Man kann mit einer Kampagne schließlich genau auf eine Gruppe zielen und sie anderen vorenthalten, denn wenn die das sähen, könnte vielleicht sogar ein nachteiliger Effekt entstehen. Die Zielgruppen lassen sich genau runtersegmentieren, rückvergleichen usw. Mit diesen Methoden lässt sich der gesamte Verkauf optimieren. (EM 12, 13)
Unternehmen nutzen die Daten zum Kennen lernen ihrer Zielgruppe, zur genaueren Definierung ihrer Bedürfnisse, zur Steuerung der Zielgruppe. Das alles dient dem Zweck des besseren Marketings und der Verkaufsförderung eines Produkts oder der Bekanntmachung. Da sind sie sogar noch interessierter an Daten über viele Zielgruppen hinweg als Nachrichtendienste. Wo staatliche Stellen eher an den Extremen interessiert sind, also an kriminellen oder einflussreichen Leuten, sind Firmen und Marketingabteilungen an allen Daten interessiert, weil sie überall eine potentielle Zielgruppe, einen potentiellen Markt, eine Kauflandschaft wittern. (WZ 19)
Das Geschäftsmodell *Googles* besteht darin, Werbefläche zu verkaufen. Mit Werbeanzeigen bei *AdWords* verdient *Google* pro Click, der auf diese Anzeigen gesetzt wird. Umso besser *Google* jemanden kennt, über seine Interessen, über das Suchverhalten, usw. Bescheid weiß, desto genauer kann es Werbung platzieren und damit steigen die Erfolgschancen, dass die Werbung angeschaut wird. Ziel von *Google* ist es, die semantischen Hintergründe einer Suche zu kennen und genau zu wissen, warum ein bestimmter Suchbegriff eingegeben wurde und somit seinen Zweck zu bestimmen. (GR 9)
Die Suchmaschine *Googles* ist nur ein Mittel zum Zweck. Ihr Kerngeschäft ist es, größter Online-Distributor von suchbezogener Werbung und Bannerwerbung zu sein. Dabei braucht *Google* auch gar nicht zwingend den Namen der Personen und WerbungsschauerInnen.
(EM 5)

Natürlich weiß genausogut *Last.fm* über den Musikgeschmack der UserInnen Bescheid, so wie *Amazon* über den Lesegeschmack Bescheid weiß oder KabelbetreiberInnen, wer oder welcher Haushalt sich was im Fernsehen ansieht. Und umso zielgerichteter und passender kann Werbung dann geschaltet werden. Die Zukunft geht ganz in diese Richtung. (GR 20)
Im *Gmail*-Account treffen die Werbeanzeigen überraschend genau auf die Bedürfnisse zu, die sich aus dem Mail heraus ableiten lassen. (WZ 21)

- **Zugriff auf freiwillig veröffentlichte Daten seitens wirtschaftlicher Unternehmen**

Unternehmen versuchen, so die ExpertInnen, sicherlich in irgendeiner Art, etwas aus den veröffentlichten Daten für sich herauszuholen.

Wenn es um die kommerzielle Nutzung geht, versucht die Wirtschaft sicher Breschen zu schlagen in die Netzwerke in unterschiedlichster Form, beispielsweise als DrittanbieterInnen oder dass sie mittels Applikationen direkten Zugang zu NutzerInnen-Daten erhalten. FirmenvertreterInnen werden in Netzwerkgruppen geschleust, wo sie sich als DurchschnittsuserIn ausgebend gezielt Stimmung für ein Produkt machen können, bei großen Foren zahlt sich das sicherlich aus. Beispielsweise für PharmavertreterInnen, die in elektronischen Selbsthilfegruppen für bestimmte Arzneimittelprodukte werben. (DZ 4)
Oftmals entscheidet nicht die Menge der Daten, sondern die Verbindung einzelner Parameter darüber, dass wir zu einem erwünschten Ergebnis kommen. Manchmal sind soziodemographische Daten relevant, manchmal sind Wohnadressen relevant, und manchmal braucht man gar nicht wissen, wer die Person ist, sondern es reicht aus zu wissen, welche Kontakte, Beziehungen, Verbindungen bzw. in welchem Netzwerk die Person verkehrt. Von einer Person in einem Beziehungsgeflecht kann man mit Hilfe von mathematisch-netzwerktheoretischen Modellen dann relativ leicht Schlüsse auf die nächste ziehen. Und dafür sind Social Networks ideal. Werden einer Person in *Facebook* FreundInnen vorgeschlagen, so braucht der Algorithmus dahinter keine Angaben über Interessen oder wer welche Seiten besucht, es reicht ihm, einen Vergleich der Beziehungsgeflechte der beiden potentiellen FreundInnen zu haben. Das heißt die Verbindungsstrukturen sagen in *Facebook* viel mehr aus, als es irgendwelche Angaben zur

sexuellen Präferenz oder Beschreibungen tun können, ob wir dort sind, um zu flirten oder Geschäfte zu treiben. (WZ 21, 22)
Unternehmen greifen auf solche veröffentlichten Daten zurück bzw. versuchen Zustimmung für die Verwendung von Daten zu bekommen, weil sie für Marketingzwecke sehr gut geeignet sind. Sie wollen echte und richtige Datensätze und vollständige Bilder ihrer KundInnen, die für sie einen großen Wert darstellen. (GK 17)
So ist es das Geschäftsmodell der Personensuchmaschine *123people*, Daten zu einem Namenspaar zusammenzutragen und dabei alle verfügbaren Quellen im Internet zu durchkämmen. Wer einen ungewöhnlichen Namen trägt, dessen Profil kann relativ genau bestimmt werden. (WZ 13)
123people praktiziert im Grunde genommen nichts Rechtswidriges, sondern es werden veröffentlichte Daten, einerseits von der Person selbst veröffentlicht, andererseits beispielsweise in offiziellen Telefonbüchern, in Echtzeitsuche zu einem bestimmten Namenspaar strukturiert zusammengetragen. (GK 6)
Auch Adressverlage, die mit Adressen handeln, sowie auch Direktmarketingunternehmen, die persönlich adressierte Werbepost versenden, praktizieren nichts Rechtswidriges und sind in der Gewerbeordnung definierte Gewerbe. In diesen Branchen gibt es oftmals schwarze Schafe, prozentuell gesehen wahrscheinlich mehr, weil nicht mit Gütern, sondern mit Daten gehandelt wird, und da lässt sich mehr Schindluder treiben. (GK 5)

- **Anwendungsfelder von Überwachung für Einzelne**

Zwar ist es potentiell auch für Private möglich, mittels Internet Überwachung auszuüben und nötige Informationen über Personen aus dem Web zu ziehen sowieso, wie ArbeitgeberInnen als oft genanntes Beispiel, das gerne machen, darüber, ob man das nun als Überwachung oder Verlust von Privatsphäre bezeichnen kann, kongruieren die Ansichten der ExpertInnen nicht.

Im Prinzip kann jede/r, jede Behörde, jeder Geheimdienst Social Networks zu Überwachungszwecken nutzen. Je mehr jemand über sich preisgibt, desto mehr weiß man auch über die Person, desto besser kann man sie einschätzen. Hat jemand Zugang zu den *Facebook*-Daten einer Person und sieht sich die Fotos, Infos, FreundInnen und Gruppen an, so weiß der/die, ob die Person raucht, welche politische Einstellung sie vertritt und welcher

Religion sie angehörig ist. (GR 17) Sobald man in *Facebook* jemandes FreundIn ist, kann man auch nachsehen, was er/sie macht, was aber natürlich davon abhängt, wie vollständig diese/r sein/ihr Profil ausfüllt. (GR 22)

GK würde die Möglichkeit der Zugriffe auf diverse Profile nicht Überwachung nennen, weil dafür ein bestimmter Wille dahinter stehen müsste, um das fortlaufend systematisch zu betreiben, was bei typischen Social Network-UserInnen eher nicht der Fall sein dürfte. Eher würde er das als Verlust an Privatsphäre beschreiben, weil man für FreundInnen oder für einen oft unbestimmten Kreis an Menschen einfach öffentlicher wird. (GK 20)

So meint auch WZ, dass heute Informationen leichter über uns zu finden sind. Wir sind durch das Web 2.0 zu halböffentlichen Menschen geworden. Zum einen geben wir hier Daten preis und stellen uns selbst dar, zum anderen zeigen dieselben Medienunternehmen in anderen Sendeformaten Halbprominente, die nicht aufgrund dessen Berühmtheit erlangten, was sie geleistet haben, sondern schlicht wie sie sich darstellen in dieser Teilöffentlichkeit. (WZ 27)

Ein Datenabgleich kann nun im digitalen Zeitalter von weitaus mehr Menschen, im Grunde von jeder beliebigen Person und um vieles einfacher durchgeführt werden als zuvor. (WZ 6) Die Institutionen tun sich zwar mittlerweile leichter, Profile zu erstellen, aber ihr Informationsvorsprung zur restlichen Bevölkerung bezüglich einer generellen Überwachung schmilzt, denn wenn sogar der/die Privatuser/in bereits auf Dienste wie *Google Maps* zurückgreifen kann, bleibt den Geheimdiensten nicht mehr viel Informationsvorsprung. (WZ 14) WZ gibt auch, das vorher erwähnte Beispiel an, in der Privatpersonen durch Informationen aus dem Netz leicht der Spur einer untergetauchten Person folgen konnten. (WZ 7, 8)

Heutzutage arbeiten selbst die Geheimdienste nicht mehr mit speziellen Geräten, sondern verwenden Massenware, die sie einfach anders konfigurieren. Die Überwachung ist bereits in die Netze integriert, wobei sich der technische Abstand zwischen Geheimdiensten und UserInnen verringert hat. Der technische Fortschritt spielt nicht allein denen in die Hände, die ihn nur ausnützen, um weitere Überwachungsmethoden einzufordern.

EM gibt weiters ein Beispiel an, das anzeigt, wie der/die Einzelne Social Networks zur Informationsgewinnung nutzen kann. Er er selbst hat diese verwendet, um mehr über die MitarbeiterInnen einer Firma herauszufinden, über die das US-amerikanische *Space and Naval Warfare Center* das *European Telecom Standars Institute* sponsert und fördert, Standards für die Vorratsdatenspeicherung umzusetzen. Auf ihrer Firmenhomepage gaben sie sich schweigsam, dort war nicht viel über die MitarbeiterInnen herauszufinden, im Social

Network *Xing* konnte EM eine Auflistung der Angestellten auf einen Schlag finden. (EM 10)
Interessiert sind viele an den Daten, vor allem Personalchefs/innen, denn zwei von drei lassen ihre BewerberInnen googeln, jede/r dritte sucht in einen Social Network nach ihnen. Die Hälfte davon findet Urlaubs- und Partyfotos, die ja gerne ausgestellt werden, nicht sehr amüsant, Kommentare finden drei von vieren nicht angebracht. Für manche Berufsgruppen ist es deshalb auch völlig tabu, sich in einem Social Network zu präsentieren, zum Beispiel für AnwältInnen. Für diese kann ein Foto auf dem sie mit einem Gläschen Alkohol zu sehen sind, rufschädigend sein, darum ist die Teilnahme an einem Network wie *Facebook* für sie sehr bedenklich, eventuell sind sie in seriöseren Netzwerken wie *Xing* vertreten. (GR 15)
Es ist ein oft beschriebenes Fallbeispiel, dass ArbeitgeberInnen im Zuge des Recruitings, so weit eben öffentlich zugänglich, auf solche Daten zurückgreifen. DZ sieht das als Verantwortungsmix aus beiden Seiten. Zum einen sollten die UserInnen ihre Sicherheitseinstellungen verschärfen, zum anderen sollten NetzwerkbetreiberInnen die Sicherheitsanforderungen so definieren, dass sie von DurchschnittsverbraucherInnen leicht verstanden und genutzt werden können, also nicht zu komplex und nicht zu unübersichtlich. (DZ 6)

- **Vorteile der Überwachung bzw. der Datensammlungen**

Auch wenn die Datensammlungen für die AuftraggeberInnen offenkundige Vorteile bieten, gesellschaftliche Vorteile im Überwachen und Datensammeln sehen die ExpertInnen nicht.

In puncto Social Networks liegen die Vorteile dieser Erfolgsgeschichte auf der Hand, sich unkompliziert austauschen können, im Netz rudeln, lange nicht gesehene Menschen wieder finden.
Allgemeiner erhalten AuftraggeberInnen einen Mehrwert und Nutzen durch die Datensammlungen und -banken, die leicht vernetzbar und leicht zu befüllen sind, ob das jetzt der Staat ist, der glaubt seinen Aufgaben effizienter nachkommen zu können und dem dies zum Teil auch gelingt oder ob es die Wirtschaft ist, die KundInnen besser katalogisieren und einordnen kann. Somit sind der Nutzen und der daraus resultierende, berechtigte Zweck auf dieser Seite leicht abzustecken. Die Frage ist aber, wie es um die Geheimhaltungsinteressen der Betroffenen steht. Was mehr wiegt, Effizienz- und

Einsparungsinteressen einerseits oder Geheimhaltungsinteressen andererseits, kann nur als gesellschaftliche Frage gestellt werden, die nur vor dem Werthintergrund dieser Gesellschaft und kaum objektiv beantwortet werden kann. Selbst im europäischen Kontext gibt es einen einheitlichen Datenschutzrahmen und einheitliche -richtlinien, dennoch interpretieren die einzelnen Mitgliedstaaten je nach datenschutzrechtlicher Tradition diese völlig unterschiedlich. Im liberalen England wird vieles salopper formuliert als beispielsweise in Deutschland, das diesbezüglich schlimme historische Erfahrungen gemacht hat. (DZ 7)

Ob Vorteile in der ständigen Datenerhebung liegen, hängt vom bestimmten Kontext ab. Es gibt dabei immer zwei Seiten einer Medaille. Wenn Gesundheitsdaten auf einer Chipkarte gespeichert werden, hat das den Vorteil, dass der/die behandelnde Arzt/Ärztin sich sofort ein Bild über den Gesundheitszustand machen kann. Die Kehrseite ist immer die bestehende Gefahr von Missbrauch, keine Daten der Welt lassen sich zu hundert Prozent schützen. Ob man das haben will oder nicht, muss in einer gesellschaftspolitischen Diskussion erörtert werden, der/die Gesetzgeber/in hat dann die Aufgabe das so zu gestalten, dass die Missbrauchsmöglichkeit minimiert wird. Grundsätzlich lässt sich sagen, an der modernen Datenerhebung und -verarbeitung wäre nicht viel Positives dran. Die Gesellschaft war auch zuvor „lebensfähig“. (GK 23)

WZ sieht keine Vorteile in der Entwicklung hin zu mehr Überwachung. Das Ausnützen der Rechenleistung der Computer und ihre Vernetzung lässt uns in eine Überwachung rutschen, wogegen man kaum etwas ausrichten kann. Sie führt eher weg von einer freieren, offeneren Gesellschaft. (WZ 28)

Dass mit genaueren Daten, Produkte oder Dienstleistungen individualisiert, schließlich Bedürfnisse besser befriedigt werden könnten, verneint WZ. In der Psychologie setzt man ein eingeschränktes Feld an Bedürfnissen voraus, die relativ einfach abgedeckt und befriedigt sind. Marketingfirmen hingegen gehen davon aus, dass man Bedürfnisse schaffen kann. Solche wären aber eher als Sehnsüchte und interessensgeleitete Lüste zu bezeichnen. Eventuell können mit den umfangreichen Datensammlungen Sehnsüchte besser generiert und befriedigt werden. (WZ 29)

Große gesellschaftliche Vorteile in den Datensammlungen sieht auch GR nicht. Eventuell könnten damit manche Dienste besser entwickelt werden, wobei alles immer ein Pro und ein Contra beinhaltet. *Google Flu* kann zum Beispiel durch gehäufte Suchanfragen ein bis zwei Wochen vor dem Eintritt eine Grippeepidemie prognostizieren. Dadurch können sich ÄrztInnen, Spitäler, die Pharmaindustrie bereits darauf vorbereiten. Andererseits kann *Google* mit diesem Wissen die Click-Preise für Medikamentenwerbungen hinaufsetzen.

Genauso ist es, wenn sich viele Leute per Suchanfragen für einen bestimmten Stadtteil interessieren. Die Stadtverwaltung kann in diesen Teil investieren und Entwicklungen voran-, ImmobilienmaklerInnen können die Preise hinauftreiben. (GR 23)
Vorteile in der Entwicklung hin zu mehr Überwachung sieht EM im Wachsen der Opposition. Mittlerweile gab es Demos zur Vorratsdatenspeicherung, die halbe österreichische Republik ist gegen sie und kaum jemand traut sich noch zu sagen, dass er dafür ist, weil die Pseudoargumente als solche entlarvt wurden. (EM 21)

- **Verschiebung der Toleranzgrenze**

Die beiden dazu befragten Experten, denken nicht, dass es aufgrund der wiederkehrenden Preisgabe von Daten zu einer Erweiterung der Toleranzgrenze hinsichtlich heikler, eventuell peinlicher Daten kommt.

Von einer Verschiebung der Toleranzgrenzen in Bezug auf Dummheiten und Peinlichkeiten im Netz lässt sich eher nicht sprechen. Zu sehr hängt es von dem/r Einzelnen ab, wie sehr er/sie solches Verhalten bewertet. Sieht ein/e Arbeitgeber/in etwaige Fotos, die außerhalb seiner/ihrer Toleranzgrenzen liegen, wird der/die Betroffenen schlichtweg Pech haben. Jenem/r kann man aber keinen Vorwurf machen, die Fotos gesehen zu haben.
Gesamtgesellschaftlich ist das ein bisschen anders, wenn man sich ansieht, dass H. C. Strache kaum Konsequenzen zu befürchten hat, wenn aufgedeckt wird, dass er an einer rechtsradikalen Wehrsportübung teilgenommen hat, wobei man das nicht am Einzelfall festmachen kann. (WZ 31)
Eine Gewöhnung oder Toleranzbereitschaft für Partyfotos im Netz sieht GR eher nicht, vor allem nicht in Berufen und Schichten, wo sich solche Dinge nicht geziemen. (GR 16)

- **Gesellschaftliche Gefahren von Überwachung durch die Verwendung von Daten**

Die ExpertInnen sehen die Gefahren einer Überwachung für eine Gesellschaft allererst in den Freiheitseinschränkungen, die sich dadurch zwangsläufig ergeben. Man kann nie garantieren, dass Datensammlungen nicht für unehrenhafte Zwecke missbraucht werden, so

gab es natürlich schon obligate Datenskandale. In Diktaturen soll Überwachung kritische Stimmen und oppositionelle Verbindungen unterdrücken.

Eine große Gefahr ist, dass die IT Tür und Tor zur totalen Überwachungsgesellschaft öffnet. Jeder Schritt wird beobachtet, das Handy ist eine Art Peilsender, Videokameras verfolgen uns auf Schritt und Tritt. Außerdem gibt es Absichten zur Vernetzung aller Videokameras. (GR 24)

Die Folgen von zuviel Überwachung wurden im klassischen Volkszählungsurteil des Deutschen Bundesgerichtshofes[18] aufgezeigt. Allein das Gefühl, überwacht zu werden, wirkt verhaltensändernd. Der Gerichtshof führte aus, dass dies für eine westliche, demokratische Gesellschaft, die sich in Freiheit entwickeln will, kontraproduktiv sei. Die Gefahr liegt darin, dass man technische Möglichkeiten, wie es eben in der Natur der Sache liegt, auch vollständig ausschöpfen will. Datenschutz soll hier ausgleichend wirken. Trotz Regulierungen treten aber immer Vollzugsdefizite auf. (DZ 8)

Ähnlich spricht WZ, dass eine der gefährlichsten Auswirkungen der Überwachung ist, dass der/die Einzelne sich nicht frei in der Gesellschaft entfalten kann und dass gewisse persönliche Freiheiten, die in bestimmten modernen Gesellschaften hart erkämpft wurden, wieder langsam verloren gehen. (WZ 30)

Die größten Gefahren der Datensammlungen sieht GK im Abgleich und dem Zusammenführen der Daten. Wird eine Datenbank, die qualitativ gute Daten für einen bestimmten Zweck speichert, mit einer anderen Datenbank, die Daten für einen anderen Zweck speichert, zusammengeführt, um daraus neue Daten zu generieren, kann das eine Gefahr darstellen. Dieses Abgleichen von Daten passiert teilweise jetzt schon, wenn man sich die Fluggastdaten, Bankdaten, SWIFT ansieht oder was mit den Vorratsdaten geschehen soll. Problematisch ist das dann deshalb, weil man eine Missbrauchsmöglichkeit nie gänzlich ausschließen kann. (GK 24)

Die Gefahr, wenn eine/r zuviel weiß, also zu viele Daten über jemanden hat, so beschreibt es EM, ist, dass er/sie die Person leicht erpressen kann. Einerseits auf freundlich, indem er/sie versucht, der Person ein Produkt oder etwas anderes anzudrehen. Oder der gefährlichere Fall, und der ist in letzter Zeit auch oft eingetreten, die Daten gehen verloren und tauchen woanders in der Hand eines/r Unbefugten wieder auf, kopiert und dupliziert. Und dann wird versucht, daraus Kapital zu schlagen, beispielsweise mittels Erpressung. Beispiele sind die Telefonverkehrsdaten der *Telekom Italia*, die gestohlen und teuer weiterverkauft worden

[18] Gemeint ist eigentlich das Bundesverfassungsgericht, ebenfalls in Karlsruhe ansässig.

sind, was mit dem Tod des Netzwerk-Security-Chefs endete oder ein ähnlicher Fall in Griechenland. Das sind keine Ausnahmefälle, sondern das ist die Regel, dass Daten verschwinden. Als harmloseste Variante verkaufen SpammerInnen dann diese Datensätze, beispielsweise ein Verzeichnis aller ÄrztInnen im Staat Kentucky mit Name, Adresse, Sozialversicherungsnummer usw. für Marketingzwecke. Daten der *Deutschen Telekom* tauchten in Holland wieder auf, sie hatten einen gerechneten Wert von 50 Millionen Euro jährlich. Die großen Datensammlungen rufen einfach auch EinbrecherInnen auf den Plan. Daten lassen sich relativ leicht anonym verwerten, da man sie virtuell verschieben kann, man kann sie deponieren und gegen Passwort zugänglich machen. Von MitarbeiterInnen selbst geht da natürlich auch eine große Gefahr aus, die Daten abzuziehen. (EM 9)

Wir haben noch nicht den Umgang und die Norm gefunden im Umgang mit dem Thema Internet. Das ist eine Gefahr, weil wir die Grenzen sowohl im Positiven wie auch im Negativen noch nicht kennen und erst ausloten müssen. Manchmal ist es zwar nur die Angst vor dem Problem, die das Problem ist, aber doch hat jede Hochtechnologie seine entsprechenden Katastrophen vorzuweisen, sei es beispielsweise Tschernobyl in der Atomtechnologie. Das Internet wird zwar keine globale Katastrophe auslösen, Zwischenfälle haben sich aber auch hier schon ereignet. Datenfehler, Datendiebstähle, Datenveröffentlichungen, die nicht hätten geschehen sollen, Datensupergaus wie die verlorenen Zugriffsdaten zu Kreditkartenkonten beim britischen Geheimdienst, Manipulationsversuche und Hacks, mitunter auf gesamte Staaten wie auf einen baltischen Staat, ließen sich als solche beschreiben. Im Vergleich dazu liegt in den Biotechnologien aber mehr lebensbedrohliches Potential, da das Internet im Gegensatz dazu relativ viel Transparenz aufzuweisen hat. (WZ 30, 33)

WZ sieht die Gefahren ohnehin nicht in den Datensammlungen selbst, sondern im Missbrauch der Daten. Die *BigBrother*-Awards werden eher denjenigen verliehen, die problematische Konsequenzen aus einer Datensammlung oder gar Datenmissbrauch zu verantworten haben und weniger oft denjenigen, die „lediglich“ Daten sammeln. (WZ 13)

China und der Iran sind schlimme Beispiele dafür, wie eine Diktatur Inhalte im Web überwachen und zensurieren kann. Das erschwert die Möglichkeit sich als Opposition formieren und organisieren zu können. Denn DiktatorInnen behalten sich Privilegien vor, zu kontrollieren, wer sich was im Web ansieht, wer sich welche Nachrichten, E-Mails und Sms zuschickt, Wort-Scanner werden in das Medium integriert. Es ist deshalb schwierig eine Diktatur zu stürzen, weil die Machthabenden die Informationen früher erhalten, als den

Aufständischen recht ist. Die Aufstände auf den Philippinen vor einigen Jahren sind beispielsweise per Sms organisiert worden.
In Weißrussland sind dieses Jahr Wahlen. Bereits im Vorfeld wurden dort die Internetkontrollen verschärft und der Internetzugang eingegrenzt. Die Opposition, die sowieso nur im Netz agieren könnte, weil sie öffentlich nicht auftreten darf, ist somit sogar dieser Alternative beraubt. (GR 28)

- **Gefahren der Überwachung durch die Verwendung von Daten für Einzelne**

Unmittelbare Nachteile für Einzelne durch die Preisgabe heikler Daten wirken sich vorwiegend an der Arbeitsstelle aus, so die InterviewpartnerInnen.

Soziale Netzwerke gefährden die Privatsphäre. GR nennt einige Beispiele vor allem aus *Facebook*, wo ArbeitnehmerInnen oder Menschen Nachteile erfahren haben, weil sie zu offenherzig preisgaben, dass sie beispielsweise ihre Arbeit oder ihre/n Chef/in nicht leiden können. (GR 5)
Mit solchen Social Network-Fällen ist die Datenschutzkommission aber selten konfrontiert, sie beschränken sich eher auf Anfragen. Erstens, weil sie einer gerichtlichen Zuständigkeit unterlägen. Zweitens, weil die meisten BetreiberInnen von Social Networks nicht in Österreich angesiedelt sind und für solche Fälle die Datenschutzbehörde des jeweiligen Landes zuständig wäre. Drittens, weil die UserInnen der Social Networks nicht gut genug über rechtliche Möglichkeiten aufgeklärt sind. (GK 14)
Ob sich Daten in und aus Social Networks zweckentfremden lassen, hängt einerseits von den Datensicherheitsmaßnahmen eines Unternehmens, also BetreiberInnen eines Social Networks und andererseits von den Privacy-Einstellungen der UserInnen, ab. Diese lassen sich so einstellen, dass Profile nicht von Suchmaschinen durchsuchbar sind und der Informationskanal nur zu den interessierenden FreundInnen im Netzwerk geöffnet wird. (GK 12)
Es liegt also vor allem in der Verantwortung der einzelnen Person, so auch WZ, zu bestimmen, wie man mit Social Networks umgeht und wie viel man preisgeben möchte. Missbrauch entsteht, wo gegen den Willen der Betroffenen, Daten erhoben werden. Ein Beispiel wäre in *Facebook*. Dort kann man eine/n Freund/in einladen, doch Teil der *Facebook*-Gemeinde zu werden und kann veröffentlichen, dass man diese Person bereits

eingeladen hat. Andere MitgliederInnen können diese dann bestärken, einzusteigen. Bei diesen Vorgängen lassen sich vonseiten *Facebooks* bereits viele Profildaten über diese Person, die nicht daran teilnehmen will, lukrieren. (WZ 13)
In *Facebook* wird man als UserIn beispielsweise aufgefordert, die Zugangsdaten des persönlichen Web-Mail-Accounts, also UserInname und Passwort oder sein Adressbuch bereitzustellen. Damit kann man aber auch Dritte gefährden, weil deren Daten dann miteinbezogen werden. Schließlich ist das auch arbeitsrechtlich relevant, denn gibt man die Zugangsdaten zum Firmen-Mail-Account preis, kann das ein fristloser Kündigungsgrund sein. Somit verleiten die Web 2.0-BetreiberInnen die Menschen zu gefährlichen Handlungen. Wobei die Leute oft nicht wissen, was sie tun, denn man würde ja auch nicht dem nächstbesten Unternehmen sein schriftliches Adressbuch in die Hand drücken, um bessere Produkte zu erhalten. Schön langsam setzt sich aber die Erkenntnis auch bei den UserInnen durch, dass umfangreiche Profile Gefahren bergen, weil sie mittlerweile öfter hören, dass jemand deswegen einen Job verloren oder nicht bekommen hat. (EM 20)

- **Beweislastumkehr**

Die zwei dazu befragten ExpertInnen meinen, dass es zur Beweislastumkehr bzw. zu einer Ironiefreiheit durch unendliche Datensammlungen kommt.

Durch die vielen Datensammlungen kommt es zur Beweislastumkehr, man muss sich rechtfertigen für etwas, was gar nicht schlecht gemeint war. Bestellt sich jemand *Mein Kampf* von Hitler, steht selbst der/die interessierte Forscher/in unter Argumentationszwang. Manchen scheint das egal zu sein, sie hätten nichts zu verbergen und könnten sich auch leicht rechtfertigen. Trotzdem kann es negative Auswirkungen haben, vor allem wiederum bei der Arbeitsplatzsuche, ebenso wenn der/die Arbeitgeber/in einen DNA-Test verlangt, um zu sehen, wie es um die Gene des/r Betroffenen bestellt ist. (GR 27)
Eine Entwicklung im Netz ist auch, dass es zu einer gewissen Ironiefreiheit kommt. Wer etwas Ironisches ins Netz stellt, muss damit rechnen, dass das aus dem Kontext herausgerissen wird und vielleicht Jahre später zum Vorwurf gemacht wird. Parallel besteht aber die Entwicklung, dass sich die Gesetze der Soaps von fiktionalen Serien in den Medien auf die Gesellschaft übertragen, und folglich nichts mehr sonderlich ernst genommen wird. Vor allem in der Politik reicht das Setzen einer neuen Aktivität aus, um vergangene

Fehltritte aus der Aufmerksamkeitsspanne der Öffentlichkeit zu hieven. Besondere Auswirkungen hat man keine zu befürchten. (WZ 30)

- **Vorschläge für einen künftigen, verbesserten Umgang mit Überwachung und Datenschutz**

Die Überwachungswelle scheint wieder etwas zu verflachen, trotzdem warten große Herausforderungen. Neben einem Rechtssystem mit sensibler, niedriger Schwelle könnten bereits technische Datenschutzmaßnahmen in die Systeme implementiert werden. Oder man würde wieder mehr auf den altbewährten Human Factor setzen.

GK würde nach wie vor von einer Informations- anstatt einer Überwachungsgesellschaft sprechen. Aber es hat Veränderungen in den letzten zehn, zwanzig Jahren gegeben. Wir legen mehr, also sehr viel Wert auf Informationen, wollen trotzdem noch Privatsphäre respektiert wissen. Tendenzen in Richtung Überwachungsgesellschaft gibt es aber, wenn man als Beispiel London betrachtet, wo tausende Videokameras auf der Straße vom Staat betrieben werden, was in Österreich in der Art nie Thema war. Auch Vorratsdatenspeicherungsrichtlinien und Fluggastdaten sind solche Tendenzen, die als Folge der Terroranschläge von den USA auf uns herüberschwappten, eben mehr Daten zu speichern, um sie vorrätig zu haben, sie in irgendeiner Form bereitzuhalten. Von diesem Kurs weicht man in Europa aber wieder etwas ab, der Datenschutz bekommt tendenziell wieder mehr Aufschwung. (GK 22)
Die UserInnen sollten sich mehr wehren, meint EM. Im Big Brother-Staat sind wir aber noch nicht angelangt, weil auch eine Gegenbewegung auszumachen ist. In einer Gesellschaft hat es noch niemals eine Welle gegeben, die ungebrochen weitergelaufen ist, nach absehbarer Zeit hat sich immer eine Gegenbewegung herausgebildet und die scheint mittlerweile angelaufen zu sein. Erkannt wird, dass Überwachungstechnik kein Allheilmittel ist, dass es eher auf fünf Ebenen darunter funktioniert als es funktionieren sollte. Auch bei der Gemeinde Wien, die zumindest schon zweimal den österreichischen *BigBrother*-Award erhalten hat, setzt ein Umdenken ein. Sie setzten früher mehrere Überwachungsmaßnahmen, Mistkübelüberwachung zum Beispiel oder bezüglich ihrer Kameras gab es bereits den obligaten Bilderskandal, wo es Filmvorführungen aus der Überwachungskamera gab, in denen die lustigsten Szenen a la *Youtube* gezeigt wurden. Die neuen Maßnahmen, die die

Gemeinde jetzt setzt, sind anders, sanfter. Mittels Putztrupps in öffentlichen Fahrzeugen will man den Vandalismus bekämpfen, auch der Hausmeister soll den verloren gegangenen Human Factor wiederbringen, der am besten von allen wirkt. Ein weiteres Beispiel dazu wäre die israelische Fluggesellschaft *El Al*, das Topziel aller TerroristInnen, in deren Flugzeuge noch nie etwas an Board geschmuggelt werden konnte, weil sie Security-Leute schulen, Fluggäste auf äußere Sensorik und Charakteristiken abzuchecken. Die Israelis haben die EuropäerInnen ausgelacht als sie hörten, dass diese Nacktscanner einführen wollen. Hingegen stellten die AmerikanerInnen laut GAO-Report tausende MitarbeiterInnen für die Gepäcksabfertigung, also am heikelsten Platz des Flughafens ein, ohne sie zu überprüfen, das heißt man wusste nichts über ihre Vergangenheit und fand schließlich Kriminelle darunter. (EM 22)

Ein wirksameres Vollzugssystem wird die Herausforderung der nächsten Zeit sein. Es ist unmöglich, hinter jede Datenanwendung einen eigene/n Datenschützer/in zu stellen und die Konformität irgendwie sicherzustellen. Die Rechtsschutzhürden sind in Österreich groß, neben der Datenschutzkommission hilft nur der Zivilrechtsweg mit AnwältInnenzwang bei potentiellen Datenschutzverletzungen durch öffentliche AuftraggeberInnen. Vor diesem Hintergrund ist es für den/die Einzelne/n oft nicht lohnenswert für seine/ihre Datenschutzrechte zu kämpfen, wo meist nur ideelle Rechte verletzt werden, die keine materiellen Folgen nach sich ziehen. Der Klagesweg wird meist erst bei finanziellen Einbußen oder Verlust des Arbeitsplatzes beschritten. Ein niedrigschwelliges Rechtssystem könnte Abhilfe leisten. Einen ersten Ansatz zeigt das Gütezeichenprojekt *Europrise*, von der EU koordiniert. AuftraggeberInnen von Datenanwendungen durchlaufen dabei selbst Audits, um sich Gütezeichen, Datenschutzsiegel anzueignen, die nur nach strenger Überprüfung vergeben werden. In Österreich gibt es nur eine Gütezeichenträgerin, die IT-Schmiede *Kiwi*, die Bilder von Videoüberwachungskameras automatisch verpixelt, nur bei Vorkommnissen wird ein Klarbild hergestellt.

Vor allem die technische Seite des Datenschutzes kann neben der juristischen noch verstärkt werden, um bereits bei der Herstellung Implementierungen zu setzen, die eine minimale Missbrauchsgefahr zulassen.

Ein weiterer Fortschritt Richtung Datenschutz wäre, ähnlich wie die kostenpflichtigen KFZ-Überprüfungen, eine Art Lizenzierung für Datenschutzkonformität, um die sich die DatenbankbetreiberInnen, -anwenderInnen, -auftraggeberInnen in regelmäßigen Abständen selbst kümmern müssen. (DZ 8, 9)

4.6.2.1 Zwischenfazit

In diesem Fazit gehe ich auf angesprochene Aspekte der ExpertInnen hisichtlich der Themenfelder Überwachung und Datensammlungen ein, die nicht zur Beantwortung der Forschungsfragen dienen, sondern in den Interviews ergänzend Erwähnung fanden und vergleiche sie mit der Literatur. Um mich nicht zu wiederholen, behalte ich mir Antworten zu den Forschungsfragen für das nächste Kapitel vor.

Laut den ExpertInnen lässt sich eher von einem technischer Rüstungskampf im Internet sprechen, wobei es schwieriger ist etwas zu verschleiern als etwas herauszufinden. Gegenüber Strafverfolgungsbehörden sind Verschleierungsdienste beispielsweise wirkungslos. Außerdem machen sich, wie auch Rötzer schreibt, wiederum genau diejenigen verdächtig, die einer Identifikation entgehen wollen.

Die zwei dazu befragten Experten bezweifeln eine Vervielfachung von Sicherheitseffekten durch staatliche Überwachungsmittel, weil Kriminalität und Terrorismus damit nach wie vor nicht zu zügeln sind. Ein Beispiel von Hempel dafür ist London, das trotz immenser Videoüberwachung die höchste Kriminalitätsrate Europas aufweist. EM meint, Überwachungstechnik sei teuer und bringe wenig, was auch die Verantwortlichen langsam einsehen würden, sieht hingegen die Freiheit scheibchenweise und schnell wie eine Salami verschwinden. Außerdem würde es einer rechtlichen Angemessenheit und Ausgewogenheit widersprechen, wenn die Vorratsdatenspeicherung als eine Art Generalüberwachung eingeführt würde. TerroristInnen und SchwerverbrecherInnen könnten diese leicht umgehen.

Die vier Experten, die die Vorratsdatenspeicherung ansprechen, übereinstimmen darin, dass die Funktion der Vorratsdatenspeicherung sein solle, Daten präventiv bereitzustellen. Sie wäre aber ein Eingriff in Privatsphäre und Freiheit des Menschen, so GR. Auch Albrecht sieht Persönlichkeitsrechte beschnitten und das Fernmeldegeheimnis verletzt.

Dass sich die Toleranzgrenze heiklen Veröffentlichungen gegenüber erhöhen könnte, verneinen die beiden dazu befragten Experten. Dafür hänge es zu sehr von dem/r Einzelnen, beispielsweise von dem/r Chef/in ab, wie er/sie solches Verhalten bewertet.

Die Überwachungswelle scheint wieder etwas abzuflachen, Datenschutz bekommt wieder mehr Aufschwung, es wird erkannt, dass Überwachungstechnik kein Allheilmittel sei. Trotzdem würden BürgerInnen selten für ihre bloß ideellen Datenschutzrechte kämpfen. Darum bedürfe es eines wirksameren, niedrigschwelligeren, modernisierten Vollzugssystems, so DZ, das kaum Rechtsschutzhürden in den Weg räumt. Auf der anderen Seite ließe sich die technische Seite des Datenschutzes verstärken und gelungene Projekte ließen sich mit Datenschutzsiegeln als eine Art Gütezeichen würdigen. Auch Schaar will Datensparsamkeit und –vermeidung bereits in die Planung und das Design der technischen Geräte und Technologien eingepflanzt wissen. Den UserInnen soll ein Höchstmaß an Anonymität zugestanden werden, so auch Rötzer. EM sieht den Human Factor als zielführender denn irgendwelche Videoüberwachungsmaßnahmen oder andere technische Maßnahmen. Ein/e Aufpasser/in verleiht mehr Sicherheit als eine Kamera.

4.7 Beantwortung der Forschungsfragen hinsichtlich Überwachungsmöglichkeiten freiwillig veröffentlichter Daten

In diesem Kapitel werden die Forschungsfragen hinsichtlich des Erkenntnisinteresses der vorliegenden Arbeit beantwortet. Die Ergebnisse der qualitativen Untersuchung werden dabei mit den Ergebnissen der Literaturanalyse kombiniert. Die speziellen Forschungsfragen werden einzeln abgehandelt, um die Facetten einer möglichen Überwachung besser aufzeigen zu können.

FF 1: Tragen freiwillig veröffentlichte, sensible Daten zu einem digitalen Fußabdruck bei?

Wir hinterlassen auf unseren Wegen durch das Netz Spuren, herrscht Einigkeit bei den ExpertInnen. Sie stimmen damit auch mit den Aussagen im theoretischen Teil überein. Über den Begriff ließe sich streiten, so benennt sie der eine als digitalen Klon, der andere als digitalen Fingerabdruck, die anderen als digitalen Fußabdruck. Ein Datenabgleich ist heutzutage für durchaus mehr Menschen möglich als früher, es lässt sich also eine Spur der passenden Person einfacher zuordnen. Der Name eines/r User/in ist im Web nicht schwierig zu eruieren, denn bei irgendeinem Dienst gibt man ihn bestimmt einmal ein. Da bei personenbezogenen Daten bzw. Daten, die auf eine bestimmte Person hinweisen aber das

Datenschutzgesetz greift, verzichten DatensammlerInnen gerne auf diesen und verwenden für die Identifikation einer Person an seiner Stelle Kennzeichnungen für gewisse Browser oder für bestimmtes NutzerInnenverhalten.
Ob damit die Identität einer Person bestimmbar wird bzw. tatsächlich bestimmt wird, ist wohl eine juristische Streitfrage. Im Grunde brauchen Unternehmen die Identität gar nicht, solange Daten einem Profil zugeordnet werden können, selbst wenn es namens- oder identitätslos geführt wird. Der Zweck der Datensammlung kann auch mit einer solchen Vorgehensweise erfüllt werden.
Die Veredelung des Fußabdrucks wurde mittlerweile kommerzialisiert. Wer peinliche Daten im Netz loswerden und einen gewissen, guten Ruf wieder herstellen lassen will, kann sich gegen Entgelt an ein Reputationsunternehmen wenden.

FF 2: Macht es einen Unterschied, ob wir Daten freiwillig hergeben oder gibt es ohnehin anderweitige Methoden der Datenerhebung?

Laut den ExpertInnen macht die Tatsache, dass Menschen freiwillig Daten veröffentlichen, sehr wohl einen Unterschied für diejenigen aus, die die Daten erheben und verwenden möchten. Da die Vorratsdatenspeicherung noch nicht eingeführt sei, so WZ, hätte der Staat nicht viel mehr als Sozialversicherungsdaten, die einer gesetzlichen Zweckbindung unterliegen und Überwachungsdaten über eine Person, für deren Erhebung Behörden einen richterlichen Bescheid brauchen, zur Verfügung. Daten aus dem AusländerInnenzentralregister kämen hier noch hinzu. Auch für Unternehmen stellen ungezwungen bereitgestellte Daten eine Bereicherung ihrer KundInnenprofile dar, denn sie bedürfen stets der persönlichen, jederzeit widerruflichen Zustimmung ihrer KundInnen als Rechtfertigungsgrund, um Daten andersweitig als zur Vertragserfüllung, beispielsweise für Marketingzwecke zu nutzen. Da einmal rechtmäßig veröffentlichte Daten (noch) keiner Zweckbindung unterliegen, sind sie gerade für wirtschaftlich orientierte Unternehmen, die außerdem versuchen, Breschen in Social Networks zu schlagen, ein gefundenes Fressen. Sie sind NutznießerInnen der Freigiebigkeit und der Möglichkeiten im Netz.
GR führt Bezeichnungen für die Methoden der Datengewinnung ein. Die bewusste Preisgabe von Daten, als willkürliche Transparenz einer Person beschreibbar, nennt er *Datenstriptease-Phänomen*, die unbewusst Transparenz, die durch Suchmaschinen und eher dubiose Dienste entsteht und von unbewusst und unbeabsichtigt hinterlassenen Daten genährt wird, nennt er *Google-Phänomen*. Zusammen führen sie zu einer Durchleuchtung

des Menschen. So meint auch EM, dass die zwanglos veröffentlichten Daten eine optimale Ergänzung sind zu anderen Methoden der Datenerhebung. Denn was nicht aktennotorisch ist, kann niemand erfahren, außer man erzählt es. Und Profile können mit solchen Daten prima erweitert werden.

FF 3: Wer nutzt beispielsweise Social Networks zu Überwachungszwecken?

Die ExpertInnen stimmen darin überein, dass wirtschaftliche Unternehmen von den Daten in Social Networks profitieren. Etwas unterschiedliche Auffassungen herrschen vor, ob und inwiefern der Staat solche Daten verwendet. Denkbar sei es jedenfalls, so der Grundtenor.

Laut DZ versuchen Unternehmen, Breschen als DrittanbieterInnen oder mittels Applikationen in die Networks zu schlagen. Auch gibt es FirmenvertreterInnen, die sich in eine Online-Gruppe schleusen und für bestimmte Produkte werben. Daten über Beziehungsgeflechte und Verbindungsstrukturen sagen manchmal mehr aus und helfen Firmen grundsätzlich mehr als sensible Daten, wie Auskünfte zur Religion oder über sexuelle Vorlieben, so WZ. Auch Weber bescheinigt der Verkehrsanalyse großes Potential, um ein komplettes Kontakt- und Kommunikationsnetzwerk aufzurollen. In Social Networks sind die Verbindungsstrukturen bereits integriert, eine Netzwerkanalyse damit bereitgestellt. GK meint, dass Unternehmen für Marketingzwecke genaue und echte Daten wollen, denn dann vervielfacht sich ihr Wert. Solche sind in Social Networks durchaus in umfangreichen Profilen zu finden. Das Durchpflügen der Networks ist keine rechtswidrige Handlung, auch Personensuchmaschinen sind von der Gewerbeordnung anerkannt.
Die Unternehmen versuchen durch Business Intelligence, Kauf- oder Verhaltenvorlieben der KundInnen zu definieren, das Marketing und den Verkauf zu optimieren und im Endeffekt Profit daraus zu schlagen.

Als etwas schwieriger erweist sich die Einschätzung in staatlicher Hinsicht. DZ nennt ein Beispiel, wo sich FinanzbeamtInnen in eine Forumsgruppe zum Thema Steuertricks und -tipps eingeschleust und diese Informationen für Steuerverfahren gewonnen hätten, hält die vom Staat ausgehende Missbrauchsgefahr solcher Daten aber geringer als die von Unternehmen ausgehende. GK erklärt, dass der Staat einen Rechtfertigungsgrund braucht, um auf solche Daten zuzugreifen. Das Recht regelt genau, was erlaubt ist und was nicht. „Also eine allgemeine Datenbank, wo man sozusagen alles zusammenfangen könnte von

jedem österreichischen Staatsbürger, wäre eben nicht zulässig.“ Wird aber ein bestimmter Sachverhalt überprüft, ziehen Strafverfolgungsbehörden eventuell schon Daten aus Social Networks heran, siehe die gerade erwähnten Beziehungsstrukturen. TerroristInnen und SchwerverbrecherInnen tummeln sich aber wahrscheinlich eher nicht in Social Networks. EM nennt Veranstaltungen der *NSA* in den letzten Jahren, die Anleitungen boten, wie Informationen aus Public Intelligence zu gewinnen seien. Auch für WZ ist anzunehmen, dass sich Geheimdienste öffentlicher Profile bedienen, doch wo staatliche Stellen eher an den Extremen interessiert sind, also an kriminellen oder einflussreichen Leuten, sind Firmen und Marketingabteilungen an allen Daten interessiert, weil sie überall eine potentielle Zielgruppe, einen potentiellen Markt, eine Kauflandschaft wittern. GR glaubt, dass *Google* mit westlichen Staaten kooperiert. In Diktaturen stehen Zensur und Überwachung sowieso an der Tagesordnung. Die USA können sich schließlich aufgrund des *Patriot Acts* die gesammelten Daten der dort ansässigen Unternehmen liefern lassen.

FF 4: Wird Überwachung im Web 2.0 eher personalisiert, das heißt für einzelne Privatpersonen ermöglicht?

Nach meiner sehr weitläufigen, breitgefächerten Definition von Überwachung lässt sich sagen, dass Überwachung für Einzelne ermöglicht und von Einzelnen auch praktiziert wird. GK würde aber nicht von Überwachung, sondern von einem Verlust an Privatsphäre seitens der UserInnen in diesem halböffentlichen Raum sprechen.

WZ meint, dass ein Datenabgleich in heutiger digitaler Zeit auch von Privatpersonen leicht durchgeführt werden kann. Der Informationsvorsprung für Geheimdienste schmilzt, sowie sich der technische Abstand zwischen Informationsdiensten und UserInnen verkleinert, so EM, der als investigativer Journalist die Networks oft selbst nach vielversprechenden Daten durchstöbert. Es lassen sich viele Informationen über Personen aus Social Network-Profilen lukrieren, so GR, der wie DZ das Beispiel erwähnt, dass ArbeitgeberInnen sehr wohl Social Networks auf BewerberInnen und ArbeitnehmerInnen hin durchsuchen, sie im Sinne der in dieser Arbeit verwendeten Definition überwachen, da sie Einfluss nehmen auf künftige Ereignisse, die diejenigen betreffen, deren Daten erhoben wurden.

FF 5: Welche Vorteile liegen in der Entwicklung hin zu mehr Überwachung?

Gesellschaftliche Vorteile in der Überwachung und in der steigenden Anzahl an Datensammlungen sehen die ExpertInnen kaum, wenngleich sie für die AuftraggeberInnen offenkundige Vorzüge bieten.

Die AuftraggeberInnen erhalten Mehrwert und Nutzen von den Daten, wenn sie oftmals auch mit den Geheimhaltungsinteressen der Betroffenen konkurrieren. Der Staat kann seinen Aufgaben leichter nachkommen und Unternehmen können KundInnen besser katalogisieren und die Effizienz steigern. Es hängt vom Kontext ab, welche Vorteile in der ständigen Datenerhebung liegen. Der Arzt kann ein umfassendes Paket an Gesundheitsdaten sehr wohl gutheißen, während solche Daten auch missbraucht werden könnten.

Die Gesellschaft war auch ohne Datensammlungen „überlebensfähig". Diese lassen uns eher in eine Überwachung rutschen und weg von einer liberalen, offeneren Gesellschaft, wogegen sich mittlerweile eine starke Opposition bildet. Einziger Lichtblick auf ExpertInnenseite in Form eines Beispiels von GR ist *Google Flu*, das aufgrund der Häufigkeit von dafür relevanten Suchanfragen den Eintritt einer Grippewelle vorherbestimmen kann, gegen die sich die Bevölkerung, Spitäler und ÄrztInnen dann hoffentlich zu rüsten wissen.

Im Sinne Foucaults hat Überwachung, eng gekoppelt an die Begriffe Macht und Disziplin, auch sehr wohl eine produktive Funktion. Ausgehend von einer Macht über den Körper war ein physiologisches, organisches Wissen über den Menschen erst möglich. Schließlich ziehen Überwachung und Kontrolle auch Leistungs- und Funktionssteigerung nach sich, immer Hand in Hand spazierend mit einem korrigierenden Normalisierungsfeldzug.

Auch Gottschalk-Mazouz kann einer Überwachung Vorteile abringen, sie bietet Zeit und Sicherheit für autonome Entscheidungen, Stabilität in unseren Erwartungen und über sie lässt sich Verantwortung abgeben und weiterreichen. Clarke erkennt ihre abschreckende Wirkung auf kriminelles Handeln als symbolischen Gewinn an.

FF 6: Welche Gefahren gehen von einer Überwachung aus?

Die Gefahren für Einzelpersonen liegen darin, dass ihnen durch die bereitwillige Preisgabe an Daten Nachteile widerfahren können, woran sie großteils selbst schuld sind. Oft strapazierte Beispiele, dass Arbeitsplätze verloren gingen bzw. nicht erhalten wurden, sind

eine Ausprägung der Kehrseite. Social Networks gefährden die Privatsphäre, meint GR. Das liegt laut GK eben daran, dass UserInnen zuviel preisgeben, ihre Privacy-Einstellungen zu wenig beachten und andererseits und das liegt nicht unbedingt im Einflussbereich der NutzerInnen, dass die Datensicherheitsmaßnahmen der Network-BetreiberInnen zu wünschen übrig lassen. Missbrauch entsteht, wo gegen den Willen der Betroffenen Daten erhoben werden, meint WZ. EM nennt das Beispiel *Facebook*, das NutzerInnen auffordert, Zugangsdaten zum Mail-Account und sein elektronisches Adressbuch herzugeben, wodurch auch Dritte gefährdet werden und was im Falle eines Firmen-Mail-Accounts arbeitsrechtlich relevant werden könnte.

Gesellschaftlich gesehen liegen die Gefahren einer Überwachung in der Verhaltensanpassung und -änderung, die sich bei den Betroffenen aufgrund der potentiellen Möglichkeit, überwacht zu werden, einschleicht. Dies zieht Freiheitseinschränkungen nach sich, die einer liberalen, demokratischen Gesellschaft widersprechen, es kommt zur Beweislastumkehr und zu einer Ironiefreiheit. Jedoch werden bereitstehende technische Möglichkeiten meist auch vollständig ausgenützt. Die Gefahren von Missbrauch, Datenabgleich und Zusammenführen von Datenbanken stehen ständig im Raum. So ist es auch die Regel, dass Daten verloren gehen, fehlerhaft sind, gestohlen werden, verschwinden, manipuliert, gehackt, veröffentlicht werden, obwohl sie nicht hätten dürfen. Leicht kann man dann Menschen, Firmen und Staaten erpressen, da die Daten oft geldlichen Wert besitzen oder Sprengkraft bergen. In Diktaturen erleichtert Überwachung die Zensur und das Bekämpfen der politischen Opposition.

Panoptische Überwachung, die bereits von den Individuen verinnerlicht wurde, trägt Verantwortung für einen gesellschaftlichen Druck, sich zu normalisieren, so Foucault, Verhalten wird nachvollziehbar, AusreißerInnen sind unerwünscht. Generell befindet Gaycken Überwachungstechnik als missbrauchstendenziöse Technologie.

4.8 Fazit - Bewertung der Hypothesen

Das Ziel der Arbeit war es, herauszufinden, komprimiert in der forschungsleitenden Fragestellung, ob Daten, die wir freiwillig im Internet hinterlassen, spezifischere Formen von Überwachung zulassen. Dazu möchte ich die aufgestellten Hypothesen knapp im Einzelnen bewerten.

Hypothese 1: Wir hinterlassen auf unseren Wegen durch das Web „digitale Fußabdrücke“.

Aufgrund der übereinstimmenden Aussagen sowohl in der Literatur als auch von den ExpertInnen getätigt, will ich diese Hypothese bestätigen. Spuren von uns bleiben im Netz auf jeden Fall erhalten.

Hypothese 2: Daten im Netz werden von unternehmerischer und staatlicher Seite gespeichert und die riesigen Datenmengen weiterverarbeitet.

Diese Hypothese ist so allgemein gehalten, dass es schwierig ist, sie zu bewerten. Der vorangehenden Diskussion nach lässt sich sagen, dass der Staat, dabei am ehesten Geheimdienste und vor allem wirtschaftliche Unternehmen für Marketingzwecke auf freiwillig veröffentlichte Daten zugreifen. Grundsätzlich lässt sich diese Hypothese also beglaubigen.

Hypothese 3: Diese Weiterverarbeitung geschieht zielgerichtet und ohne unser Wissen.

Diese Annahme lässt sich nicht ohne weiteres verifizieren. Dass eine solche Verarbeitung von Daten natürlich zielgerichtet geschieht, liegt auf der Hand und in der Sache selbst. Dass diese ohne unser Wissen passiert möchte ich aber verneinen. Mittlerweile sollten zumindest die meisten Menschen wissen, dass beispielsweise Daten in Social Networks ideal für Werbezwecke verwendet werden können oder *Google* die Suchanfragen zu Profilen verarbeitet.

Hypothese 4: Die freiwillige Preisgabe von Daten im Internet ist nur ein Tropfen auf dem heißen Stein in Bezug auf Überwachungsformen. Der Staat, Unternehmen und die Wissenschaften greifen auf andere Möglichkeiten der Datenerhebung zurück und generieren Daten selbst.

Diese Hypothese erscheint mir als falsch und wird deswegen verneint. Natürlich erhebt der Staat Daten auch anderweitig, beispielsweise aus der Sozialversicherung, um seinen Aufgaben effizient nachkommen zu können. Auch Web-Unternehmen speichern allerhand

Daten mittels Cookies usw. und die Wissenschaften nehmen für ihre Untersuchungen beispielsweise Daten aus Experimenten. Dennoch bieten freiwillig veröffentlichte Daten eine ideale Ergänzung zu diesen Methoden. Beziehungsstrukturen werden offenbart, Vorlieben, Interessen usw., die nicht aktennotorisch sind und deshalb nur von sich aus freiwillig erzählt werden können.

Hypothese 5: Überwachung wird personalisiert und dezentralisiert. Einzelne Personen, wie Firmenchefs/innen, LehrerInnen, DirektorInnen, usw. nutzen die freiwillige Preisgabe dieser Daten zu persönlichen Überwachungszwecken.

Überwachung wird für den/die Einzelne ermöglicht. Das oftmals angeführte Beispiel, dass ArbeitgeberInnen das Netz nach ihren BewerberInnen durchforsten und diese im Falle des Auffindens von unschicken Details nicht einstellen, belegt das. Auch die von den ExpertInnen ins Feld geführten Auffassungen, dass ein Datenabgleich leicht und für viele möglich ist und der Informationsvorsprung von Geheimdiensten schmilzt, sprechen für eine Personalisierung und Dezentralisierung. Nicht jede/r würde dies aber als Überwachung bezeichnen. Wenn die Ausforschung von Daten aber Konsequenzen für die DatenanbieterInnen nach sich zieht, nenne ich es Überwachung. Somit lässt sich die Hypothese bis auf Widerruf verifizieren.

Hypothese 6: Überwachung führt zu gesellschaftlich angepasstem Verhalten.

In der Literatur ist es ohnehin ein alter Hut, dass Überwachung aus Vorsicht zu Verhaltensanpassung führt. Foucault, Rössler und auch das Volkszählungsurteil des deutschen Bundesverfassungsgerichts bezeugen das. Daneben gibt es noch viele weitere Auswirkungen einer Überwachung. Die Hypothese ist zu bestätigen.

Wie schlimm ist die Überwachung nun wirklich? Eines steht einmal fest, die Gefahren, die von einer Überwachung ausgehen, von der Vernetzung von Datensammlungen, von einer Aufwertung der Daten an qualitativem Gehalt sind nicht zu unterschätzen. Dennoch scheinen mir Schriften, die das Ende der Anonymität oder das Ende der Privatsphäre voraussagen, etwas spekulativ und weit gegriffen zu sein. Auch generell erscheint mir der wissenschaftliche und mediale Diskurs auf Seiten der DatenschützerInnen etwas übertrieben

in Richtung des Bedrohlichkeitspotentials der Entwicklungen für unsere demokratischen Breitenkreise. Die Entwicklung trägt weitreichende „Konsequenzen für die Dynamik von Information und Wissen“ (Gottschalk-Mazouz 2008: 221) in sich, von einer Überwachungsgesellschaft lässt sich derzeit aber nicht sprechen, denke ich. Denn immerhin gibt es einige Institutionen, Organisationen und Gerichtshöfe, die die ÜberwacherInnen selbst überwachen und es gibt Gesetze, die das soziale Handeln regeln und somit eine ausgewogene Machtbalance gewähren. Trotzdem macht mir ein Diskurs in dieser Schärfe und Ausprägung durchaus Sinn. Erstens mussten die staatlichen Beschlüsse als Reaktion auf die Terroranschläge vom 11. September für BetrachterInnen unmittelbar auf eine extreme, unzeitgemäße Beschneidung der Menschen- und Persönlichkeitsrechte hinauslaufen. Andererseits ist eine zuspitzende Beschreibung der Umstände oftmals nötig, um ein Problem in das Bewusstsein der Öffentlichkeit zu rücken, es den Einzelnen klar zu machen. Und da stimme ich den ExpertInnen vollkommen zu, wenn sie nun eine Verflachung der Überwachungswelle spüren, einen Aufschwung des Datenschutzes sehen. Alleine die Vielzahl an kritischer Literatur in letzter Zeit zu diesem Thema, die ständige mediale Präsenz des Überwachungswahns, die Bewusstseinsbildung auf Seiten der Bevölkerung führt zu einer Gegenbewegung, die zugleich eine Opposition zu weiteren Maßnahmen wie der Vorratsdatenspeicherung oder Nacktscannern ausbildet und die eine Skepsis in Bezug auf die freiwillige Veröffentlichung von Daten zutage fördert. In diesem Sinne sollte sich weiterhin mit der Thematik der Überwachung auseinandergesetzt werden, sie sollte verstanden, erörtert und begriffen werden, um vonseiten der Verantwortlichen auch wirklich sinnvolle Maßnahmen zu setzen.

Literatur- und Quellenverzeichnis

27th International Conference of Data Protection and Privacy Commissioners o.A. (2005): Erklärung von Montreux. ‚Ein universelles Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt', URL: <http://www.bfdi.bund.de/cae/servlet/contentblob/416796/publicationFile/25216/IntDSK2005-MontreuxErklaerungDSInEinerGlobalisiertenWelt.pdf;jsessionid=28FC1A7999474728CF7C6CE2B2A5795C> [Abfrage: 15.03.2010].

Albrecht, Hans-Jörg (2008): Kosten und Nutzen technisierter Überwachung, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 129-147.

Barrera, Maria H./Okai, Jason M. (1999): Digital Correspondence: Recreating Privacy Paradigms, URL: < http://www.murdoch.edu.au/elaw/issues/v6n2/barrera62.html> [Abfrage: 11.02.2010].

Bentham, Jeremy (1995): The Works of Jeremy Bentham, Vol. IV, Repr. in 11 vol. of the 1843 ed., Thoemmes Press: London.

Bentham, Jeremy (1791): Panopticon; or, the Inspection-House: Containing the Idea of a New Principle of Construction applicable to any sort of Establishment, in which persons of any description are to be kept under inspection; and in particular to Penitantiary-Houses, Prisons, Houses of Industry, Work-Houses, Poor-Houses, Manufactories, Mad-Houses, Lazarettos, Hospitals, and Schools: with a Plan of Management adapted to the principle: in a series of Letters, written in the year 1787, from Crecheff in White Russia, to a friend in England. Dublin, printed: London, reprinted 1791, in: Bentham, Jeremy (1995): The Works of Jeremy Bentham, Vol. IV, Repr. in 11 vol. of the 1843 ed., Thoemmes Press: London.

Berdiajew, Nikolai A. (1971): Der Mensch und die Technik, Revidierte Fassung nach der ersten Übers., Verlag der Arche Zürich: Zürich.

BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) (2007): Fast jeder fünfte Mensch ist online, URL: <http://www.bitkom.org/de/presse/49919_46069.aspx> [23.5.2007] [Abfrage: 21.10.2009] Berlin.

Bodendorf, Freimut (2006): Daten- und Wissensmanagement, 2., aktualisierte und erweiterte Auflage, Springer: Berlin, Heidelberg, New York.

Bogner, Alexander/Littig, Beate/Menz, Wolfgang (Hg.) (2005): Das Experteninterview. Theorie, Methode, Anwendung, 2. Aufl., VS Verlag für Sozialwissenschaften: Wiesbaden.

Bogner, Alexander/Menz, Wolfgang (2005): Das theoriegenerierende Experteninterview. Erkenntnisinteresse, Wissensformen, Interaktion, in: Bogner, Alexander/Littig, Beate/Menz, Wolfgang (Hg.): Das Experteninterview. Theorie, Methode, Anwendung, 2. Aufl., VS Verlag für Sozialwissenschaften: Wiesbaden, S. 33-70.

Bredekamp, Horst/Bruhn, Matthias/Werner, Gabriele (Hg.) (2007): Bildwelten des Wissens. Systemische Räume (=Kunsthistorisches Jahrbuch für Bildkritik. Band 5,1), Akademie Verlag: Berlin.

Brin, David (1998): The Transparent Society. Will Technology Force Us to Choose Between Privacy and Freedom?, Perseus Books: Reading, Massachusetts.

Bull, Hans Peter (1984): Datenschutz oder Die Angst vor dem Computer, Piper: München.

Bush, George W. (2001): Auszüge der Rede von US-Präsident Bush im Wortlaut, 21.09.2001, in: Handelsblatt: URL: <http://www.handelsblatt.com/archiv/auszuege-der-rede-von-us-praesident-bush-im-wortlaut;461964> [Abfrage: 12.11.2009].

Cavalli, Alessandro/Krech, Volkhard (Hg.) (1993): Georg Simmel. Aufsätze und Abhandlungen 1901-1908, Bd. II, Suhrkamp: Frankfurt am Main.

Clarke, Roger (1987): Information Technology and Dataveillance, URL: <http://www.rogerclarke.com/DV/CACM88.html> [Abfrage: 23.02.2010].

Coy, Wolfgang (2008): Ich habe nichts zu verbergen. Technische Überwachung in Zeiten des Internet, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 47-52.

Datenschutzkommission/Bundesministerium für Unterricht, Kunst und Kultur/saferinternet.at (2010): DU bestimmst… Datenschutz - Fakten und Gefahren, Wien.

Dauk, Elke (1989): Denken als Ethos und Methode. Foucault lesen, (=Reihe historische Anthropologie, Bd. 5), Reimer: Berlin.

Dick, Philip K. (Hg.) (1993): Autofab. Sämtliche Erzählungen. Band 7, Haffmanns Verlag: Zürich.

Dick, Philip K. (1993a): Der Minderheiten-Bericht, in: Dick, Philip K. (Hg.): Autofab. Sämtliche Erzählungen. Band 7, Haffmanns Verlag: Zürich, S. 120-172.

Dix, Alexander (2008): Hat der Persönlichkeitsrechts- und Datenschutz bei Politikern (noch) eine Chance - Datenschutz als leichte Beute? Zum Problembewusstsein von Politikern, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 149-166.

Dreyfus, Hubert L./Rabinow, Paul (Hg.) (1987): Michel Foucault. Jenseits von Strukturalismus und Hermeneutik, (= Die weiße Reihe), Athenäum: Frankfurt am Main.

Dürr, Christian (2004): Jenseits der Disziplin. Eine Analyse der Machtordnung in nationalsozialistischen Konzentrationslagern, Passagen Verlag: Wien.

Engling, Dirk (2008): Vorratsdatenspeicherung, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 67-78.

Erling, Johnny (2010): Pekings Griff nach dem Internet, in: Der Standard, NetBusiness/Wissenschaft, 15.01.2010, S. 24.

Feyerabend, Erika (2002): Von der Vermessung des Schädels zur Analyse der DNA. Geschichte der biometrischen Erfassung, Essen, URL: < http://www.bioskop-forum.de/themen/kriminalpolitik/geschichte_der_biometrischen_erfassung.htm> [Abfrage: 18.02.2010].

Fink-Eitel, Hinrich (1989): Foucault zur Einführung, Junius Verlag: Hamburg.

Flick, Uwe/von Kardorff, Ernst/Steinke, Ines (2003) (Hg.): Qualitative Forschung. Ein Handbuch, 2. Aufl., Rowohlt Taschenbuch Verlag: Reinbek bei Hamburg.

Flick, Uwe/von Kardorff, Ernst/Steinke, Ines (2003a): Was ist qualitative Forschung? Einleitung und Überblick, in: Flick, Uwe/von Kardorff, Ernst/Steinke, Ines (Hg.): Qualitative Forschung. Ein Handbuch, 2. Aufl., Rowohlt Taschenbuch Verlag: Reinbek bei Hamburg, S. 13-29.

Foucault, Michel (1995): Überwachen und Strafen. Die Geburt des Gefängnisses, 9. Aufl., Frankfurt am Main.

Foucault, Michel (1987): Nachwort. Das Subjekt und die Macht, in: Dreyfus, Hubert L./Rabinow, Paul (Hg.): Michel Foucault. Jenseits von Strukturalismus und Hermeneutik, (= Die weiße Reihe), Athenäum: Frankfurt am Main, S. 241-261.

Foucault, Michel (Hg.) (1976): Mikrophysik der Macht. Michel Foucault über Strafjustiz, Psychiatrie und Medizin, Merve Verlag: Berlin.

Foucault, Michel (1976a): Macht und Körper. Ein Gespräch mit der Zeitschrift „Quel Corps?“, in: Foucault, Michel (Hg.): Mikrophysik der Macht. Michel Foucault über Strafjustiz, Psychiatrie und Medizin, Merve Verlag: Berlin, S. 105-113.

Foucault, Michel (1976b): Räderwerke des Überwachens und Strafens. Ein Gespräch mit J.-J. Brochier, in: Foucault, Michel (Hg.): Mikrophysik der Macht. Michel Foucault über Strafjustiz, Psychiatrie und Medizin, Merve Verlag: Berlin, S. 31-47.

Foucault, Michel (1976c): Verbrechen und Strafen in der Sowjetunion und anderswo. Ein Gespräch mit K. S. Karol, in: Foucault, Michel (Hg.): Mikrophysik der Macht. Michel Foucault über Strafjustiz, Psychiatrie und Medizin, Merve Verlag: Berlin, S. 68-80.

Foucault, Michel (1976d): Von den Martern zu den Zellen. Ein Gespräch mit Roger-Pol Droit, in: Foucault, Michel (Hg.): Mikrophysik der Macht. Michel Foucault über Strafjustiz, Psychiatrie und Medizin, Merve Verlag: Berlin, S. 48-53.

Fraunhofer-Institut für Sichere Informationstechnologie (SIT) (2008): Privatsphärenschutz in Soziale-Netzwerke-Plattformen, Darmstadt, URL: <http://www.sit.fraunhofer.de/fhg/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf> [Abfrage: 08.03.2010].

Futurezone o.A. (2010): Facebook-User: Desinteresse am Datenschutz, URL: <http://futurezone.orf.at/stories/1638035/> [02.02.2010] [Abfrage: 11.02.2010].

Garfinkel, Simson (2001): Database Nation. The Death of Privacy in the 21st Century, O'Reilly Media: Beijing [u.a.].

Gaycken, Sandro (2008): Die Vergeistigung des Technotops. Neue Naturgefahren in einer neuen technischen Situation, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 25-44.

Gaycken, Sandro/Kurz, Constanze (Hg.) (2008): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld.

Geser, Hans (2006): Untergräbt das Handy die soziale Ordnung? Die Mobiltelefonie aus soziologischer Sicht, in: Glotz, Peter/Bertschi, Stefan/Locke, Chris (Hg.): Daumenkultur. Das Mobiltelefon in der Gesellschaft, transcript Verlag: Bielefeld, S. 25-39.

Gläser, Jochen/Laudel, Grit (2004): Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen, VS Verlag für Sozialwissenschaften: Wiesbaden.

Glotz, Peter/Bertschi, Stefan/Locke, Chris (Hg.) (2006): Daumenkultur. Das Mobiltelefon in der Gesellschaft, transcript Verlag: Bielefeld.

Gottschalk-Mazouz, Niels (2008): Die Spezifik technisierter Überwachung. Überlegungen zu Überwachung und Macht aus technikphilosophischer Sicht, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 209-230.

Groebner, Valentin (2004): Der Schein der Person. Steckbrief, Ausweis und Kontrolle im Europa des Mittelalters, Verlag C.H. Beck: München.

Harris Interactive Inc. (2008): Majority Uncomfortable with Websites Customizing Content Based Visitors Personal Profiles, The Harris Poll #40,
URL: <http://www.harrisinteractive.com/harris_poll/index.asp?PID=894> [10.04.2008] [Abfrage: 20.01.2010].

Heesen, Jessica (2008): Keine Freiheit ohne Privatsphäre. Wandel und Wahrung des Privaten in informationstechnisch bestimmten Lebenswelten, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 231-246.

Heidegger, Martin (1972): Sein und Zeit, 12., unveränd. Aufl., Max Niemeyer Verlag: Tübingen.

Hempel, Leon (2008): Die geschlossene Welt. Zur Politik der Überwachung am Beispiel von Videoüberwachung, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 79-100.

Hopf, Christel (2003): Qualitative Interviews - ein Überblick, in: Flick, Uwe/von Kardorff, Ernst/Steinke, Ines (Hg.): Qualitative Forschung. Ein Handbuch, 2. Aufl., Rowohlt Taschenbuch Verlag: Reinbek bei Hamburg, S. 349-360.

Hornung, Gerrit (2008): Datenschutz im Gefüge der Grundrechte und ihrem gesellschaftlichen Wandel, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 249-264.

Illetschko, Peter/Krichmayr, Karin (2009): Besser unauffällig verhalten, in: Der Standard, Forschung Spezial (Journal für Wissenschaft, Technologie und Entwicklung), 25.03.2009, S. 13.

Institut für Technikfolgen-Abschätzung (ITA) der Österreichischen Akademie der Wissenschaften (2009): Privatsphäre 2.0. Beeinträchtigung der Privatsphäre in Österreich. Neue Herausforderungen für den Datenschutz. Endbericht, (=Studie im Auftrag der Bundesarbeitskammer), Wien, URL: <http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a53.pdf> [Abfrage: 08.03.2010].

Krichmayr, Karin (2009): Die Kamera denkt mit, in: Der Standard, Forschung Spezial (Journal für Wissenschaft, Technologie und Entwicklung), 25.03.2009, S. 13.

Kurz, Constanze (2008): Biometrie nicht nur an den Grenzen. Erkennungsdienstliche Behandlung für jedermann, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 101-113.

Lamnek, Siegfried (2005): Qualitative Sozialforschung. Lehrbuch, 4., vollst. überarb. Aufl., Beltz Verlag: Weinheim, Basel.

Lemke, Martin (2008): Die Praxis polizeilicher Überwachung. Geschichten aus dem Alltag, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 167-178.

Lessig, Lawrence (2006): Code. Version 2.0, Basic Books: New York, URL: <http://pdf.codev2.cc/Lessig-Codev2.pdf> [Abfrage: 13.01.2010].

Luther, Martin (Übers.) (2001): Die Bibel, nach der Übersetzung Martin Luthers, mit Apokryphen und Wortkonkordanz, Deutsche Bibelgesellschaft: Suttgart.

Lyon, David (2002): Surveillance Society. Monitoring Everyday Life, Open Univ. Press: Buckingham, Philadelphia.

Mattern, Friedemann (Hg.) (2003): Total vernetzt. Szenarien einer informatisierten Welt (=7. Berliner Kolloquium der Gottlieb Daimler- und Karl Benz-Stiftung), Springer-Verlag: Berlin [u.a.].

Mattern, Friedemann (2003a): Vom Verschwinden des Computers - Die Vision des Ubiquitous Computing, in: Mattern, Friedemann (Hg.): Total vernetzt. Szenarien einer informatisierten Welt (=7. Berliner Kolloquium der Gottlieb Daimler- und Karl Benz-Stiftung), Springer-Verlag: Berlin [u.a.], S. 1-41.

Mayring, Philipp (2002): Einführung in die qualitative Sozialforschung. Eine Anleitung zu qualitativem Denken, 5. Aufl., Beltz Verlag: Weinheim und Basel.

Meuser, Michael/Nagel, Ulrike (2005): ExpertInneninterviews - vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion, in: Bogner, Alexander/Littig, Beate/Menz, Wolfgang (Hg.): Das Experteninterview. Theorie, Methode, Anwendung, 2. Aufl., VS Verlag für Sozialwissenschaften: Wiesbaden, S. 71-93.

Mill, John Stuart (1987): Über Freiheit, (=Die kleine weiße Reihe, Bd. 101), Athenäum: Frankfurt am Main.

Neue Zürcher Zeitung o. A. (22.2.2007): London gefährlichste Hauptstadt in der EU? Resultate einer europaweiten Umfrage mit einigen Fragezeichen, in: Neue Zürcher Zeitung (22.2.2007).

Nogala, Detlef (2001): Der Frosch im heißen Wasser, in: Schulzki-Haddouti, Christiane (Hg.): Vom Ende der Anonymität. Die Globalisierung der Überwachung, 2., aktualisierte Aufl., Verlag Heinz Heise: Hannover, S. 149-165.

O'Reilly, Tim (2005): What is Web 2.0. Design Patterns and Business Models for the Next Generation of Software, O'Reilly Media: Beijing [u.a.],
URL: <http://tim.oreilly.com/news/2005/09/30/what-is-web-20.html> [Abfrage 11.02.2010].

Orwell, George (1983): 1984, (Werkausgabe in 11 Bänden), Diogenes-Verlag: Zürich.

Phillips, David J. (2005): From Privacy to Visibility. Context, Identity, and Power in Ubiquitous Computing Environments, in: Social Text 83, Vol. 23, No. 2, S. 95-108, URL: <http://socialtext.dukejournals.org/cgi/pdf_extract/23/2_83/95> [Abfrage: 18.02.2010].

Purgathofer, Peter (2008): Eine kleine Geschichte der Überwachung, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 195-208.

Quéau, Philippe (1998): Eine ethische Vision der Informationsgesellschaft. Zur Notwendigkeit einer Informationsethik für eine globale Welt, in: Telepolis, URL: <http://www.heise.de/tp/r4/artikel/2/2539/1.html> [Abfrage: 15.03.2010].

Rammert, Werner (2007): Die Macht der Datenmacher in der fragmentierten Wissensgesellschaft, in: Bredekamp, Horst/Bruhn, Matthias/Werner, Gabriele (Hg.): Bildwelten des Wissens. Systemische Räume (=Kunsthistorisches Jahrbuch für Bildkritik. Band 5,1), Akademie Verlag: Berlin, S. 18-27.

Reding, Viviane (=Kommission der europäischen Gemeinschaften) (2009): Empfehlung der Kommission zur Medienkompetenz in der digitalen Welt als Voraussetzung für eine wettbewerbsfähigere audiovisuelle und Inhalte-Industrie und für eine integrative Wissensgesellschaft, Brüssel,
URL: <http://ec.europa.eu/avpolicy/media_literacy/docs/recom/c_2009_6464_de.pdf> [20.08.2009] [Abfrage: 20.01.2010].

Rieger, Frank (2008): Abhören und Lokalisieren von Telefonen. Der Stand der Dinge, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 53-66.

Ropohl, Günter (2008): Der heimliche Terror der Prophylaxe. Eine ethische Einrede gegen das ‚Prinzip Überwachung', in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 265-281.

Rössler, Beate (2001): Der Wert des Privaten, Suhrkamp Verlag: Frankfurt am Main.

Rötzer, Florian (2001): Vom Ende der Anonymität, in: Schulzki-Haddouti, Christiane (Hg.): Vom Ende der Anonymität. Die Globalisierung der Überwachung, 2., aktualisierte Aufl., Verlag Heinz Heise: Hannover, S. 167-179.

Schaar, Peter (2007): Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft, C. Bertelsmann Verlag: München.

Schneier, Bruce (2005): Terrorists Don't Do Movie Plots, URL: <http://www.schneier.com/essay-087.html> [08.09.2005] [Abfrage: 30.12.2009].

Schoeman, Ferdinand D. (Hg.) (1984): Philosophical Dimensions of Privacy. An Anthology, Cambridge University Press: New York [u.a.]

Schulzki-Haddouti, Christiane (2004): Im Netz der inneren Sicherheit. Die neuen Methoden der Überwachung, Europäische Verlagsanstalt: Hamburg.

Schulzki-Haddouti, Christiane (Hg.) (2001): Vom Ende der Anonymität. Die Globalisierung der Überwachung, 2., aktualisierte Aufl., Verlag Heinz Heise: Hannover.

Sennett, Richard (2001): Verfall und Ende des öffentlichen Lebens. Die Tyrannei der Intimität, 12. Aufl., Fischer Taschenbuch Verlag: Frankfurt am Main.

Simmel, Georg (1906): Psychologie der Diskretion, in: Cavalli, Alessandro/Krech, Volkhard (Hg.) (1993): Georg Simmel. Aufsätze und Abhandlungen 1901-1908, Bd. II, Suhrkamp: Frankfurt am Main, S. 108-115.

Stalder, Felix (2002): Opinion. Privacy Is Not the Antidote to Surveillance, in: Surveillance & Society 1 (1), S. 120-124, URL: <www.surveillance-and-society.org/articles1/opinion.pdf> [Abfrage 11.02.2010].

Trojanow, Ilija/Zeh, Juli (2009): Angriff auf die Freiheit. Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte, Hanser: München.

Van Dijk, Jan et al. (2005): The Burden of Crime in the EU. Research Report: A Comparative Analysis of the European Crime and Safety Survey (EU ICS) 2005, URL: <http://www.europeansafetyobservatory.eu/downloads/EUICS_The%20Burden%20of%20Crime%20in%20the%20EU.pdf> [Abfrage: 21.02.2010].

Warren, Samuel D./Brandeis, Lewis D. (1890): The Right to Privacy, in: Harvard Law Review, IV (5), Boston, S. 193-220, URL: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>, [Abfrage: 13.01.2010].

Wasserstrom, Richard A. (1984): Privacy. Some Arguments and Assumptions, in: Schoeman, Ferdinand D. (Hg.): Philosophical Dimensions of Privacy. An Anthology, Cambridge University Press: New York [u.a.], S. 317-332.

Weber, Karsten (2008): Informationsethik und technisierte Überwachung, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 283-302.

Weber, Max (1980): Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie, 5., rev. Aufl., Studienausg., J.C.B. Mohr: Tübingen.

Weiß, Ralph (2002): Vom gewandelten Sinn für das Private, in: Weiß, Ralph/Groebel, Jo (Hg.): Privatheit im öffentlichen Raum. Medienhandeln zwischen Individualisierung und

Entgrenzung, (=Schriftenreihe Medienforschung der LfR Nordrhein-Westfalen, Band 43), Leske + Budrich: Opladen, S. 27-87.

Weiß, Ralph/Groebel, Jo (Hg.) (2002): Privatheit im öffentlichen Raum. Medienhandeln zwischen Individualisierung und Entgrenzung, (=Schriftenreihe Medienforschung der LfR Nordrhein-Westfalen, Band 43), Leske + Budrich: Opladen.

Wendt, Rainer (2008): Der Nutzen der Überwachung, in: Gaycken, Sandro/Kurz, Constanze (Hg.): 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien, transcript Verlag: Bielefeld, S. 117-128.

Westin, Alan F. (1967): Privacy and Freedom, Atheneum: New York.

Whitaker, Reg (1999): Das Ende der Privatheit. Überwachung, Macht und soziale Kontrolle im Informationszeitalter, Kunstmann: München.

Zeger, Hans G. (2009): Paralleluniversum Web2.0. Wie Online-Netzwerke unsere Gesellschaft verändern, K&S: Wien.

Zeger, Hans G. (2008): Mensch. Nummer. Datensatz. Unsere Lust an totaler Kontrolle, Residenz Verlag: St. Pölten.

Abbildungsverzeichnis

Anhang

Interviewleitfaden

Allgemeine und organisatorische Fragen zu Person und Tätigkeit

- Geht das in Ordnung, wenn ich das Interview für eine bessere Transkription aufzeichne?
- Darf ich Ihren Namen erwähnen oder soll ich alles anonym behandeln?
- Bei der ersten Frage bitte ich Sie, dass Sie sich vorstellen und Ihr Forschungsgebiet bzw. Arbeitsgebiet kurz erklären?

Block Daten und Privatsphäre

- Welche Form von personenbezogenen Daten würden Sie als sensibel beschreiben?
- Wie werden diese Daten rechtlich geschützt?
- Einerseits schützen wir Daten, andererseits geben wir sie in Social Networks, *Youtube*, *Google* freiwillig her. Warum stellen wir solche Daten freiwillig ins Internet? Alternativ: Was bringt uns das, wenn wir Daten freiwillig hergeben?
- Vielleicht könnten sie ein paar extreme Beispiele geben, was wir in Social Networks preisgeben?
- Tragen solche Daten, die wir in Social Networks, auf *Youtube*, *Flickr* usw. hergeben, zu einem **digitalen Fußabdruck** bei?
- Wissen die Unternehmen namentlich wer das ist oder erstellen sie ein anonymes Profil?

- Vielleicht könnten Sie eine kurze Prognose geben, welche Daten noch kommen werden? Alternativ: Wie geht es zukünftig mit Social Networks weiter? Stellen wir unsere DNA bei *Xing* hinein, um zu zeigen, wie gute Gene wir haben?

- Wie wichtig ist Privatsphäre in der Form, dass wir bestimmen, wer welche Informationen über uns hat? Alternativ: Unterschätzen die UserInnen die Wichtigkeit der Privatsphäre?

- Kann man von einem Ende der Privatheit sprechen, einem Ende der Anonymität? Wie stehen Sie dazu?

Block Überwachung

- Macht es einen Unterschied, dass wir Daten freiwillig in Social Networks hergeben oder gibt es sowieso anderweitige Methoden der Datenerhebung? Alternativ: Fällt das überhaupt ins Gewicht, dass wir Daten in soziale Netzwerke stellen?

- Wer sind die Feinde der UserInnen von Social Networks zum Beispiel?

- Wer nutzt beispielsweise Social Networks zu Überwachungszwecken?

- Nutzt der **Staat** solche freiwillig hergegebenen Daten zu Überwachungszwecken? Mit Staat meine ich Sicherheitsbehörden, Verwaltungsbehörden, Finanzämter, Amt für Ausländer, usw.

- Was bringt dem Staat die Überwachung?

- Nutzt er Social Networks oder gibt es für den Staat andere Maßnahmen?

- Stichwort Vorratsdatenspeicherung: Wem nützt sie? Kommt sie?

- Nutzen **wirtschaftliche Unternehmen** solche freiwillig hergegebenen Daten zu Überwachungszwecken?

- Wer wertet die Unmengen an Daten aus? Programme oder Menschen?

- Wird Überwachung im Web 2.0 eher **personalisiert**, das heißt für einzelne Personen ermöglicht? Alternativ: Erleichtern sie eine Überprüfung/Überwachung für den alltäglichen Gebrauch, wie für Vorgesetzte, SchuldirektorInnen, FreundInnen, usw?

- Würden Sie noch vom Großen Bruder oder eher von den kleinen Geschwistern sprechen?

- Welche (gesellschaftlichen) **Vorteile** sehen Sie in dieser Entwicklung hin zu mehr Datenansammlungen, zu mehr Überwachung?

- Könnten sich vielleicht Gewöhnungseffekte beim Privatheitsverzicht, bei der Preisgabe von Daten und ihrer Überwachung einstellen? Alternativ: Könnte sich die Sensibilisierungsgrenze verschieben, das heißt die Toleranzgrenze in Bezug auf intime, bloßstellende Informationen erhöhen in der Form, dass wir Dummheiten im Netz verzeihen?

- Welche **Gefahren** gehen von einer Überwachung aus?

- Kommt es zu einer Beweislastumkehr? Muss ich beweisen, dass ich unschuldig bin?

- Verlieren wir eventuell Vertrauen in unsere Umgebung, wenn wir überall überwacht werden?

Spezifische Fragen für die ExpertInnen

- Wer kann mit unserem Surfverhalten etwas anfangen?

- Wie genau kann Werbung bereits geschaltet werden?

- Wissen Unternehmen über meinen Musikgeschmack vielleicht genauer Bescheid als ich selbst? Erklärungsbeispiel: Eine Lieblingsband, angegeben in *Facebook*, kann deshalb als solche gelten, weil sie vor Jahren *der* Begleiter in der Pubertät war. Mittlerweile hört die Person sie kaum noch. Unternehmen, die Musik anbieten und bei denen man sich registrieren muss, wissen aber ganz genau, welches Stück eine Person wann und wie oft hört.

- Wie weit werden die Auswertungsmöglichkeiten von Daten gehen?

- Kann man von einem technischen Rüstungskampf im Internet sprechen, Verschleierungsdienste zum Beispiel gegen ÜberwacherInnen und DatensammlerInnen?

- Können solche freiwillig hergegebenen Daten für die Wissenschaften dienlich sein?

- Was könnte eine Diktatur mit einem perfekten Überwachungssystem „erreichen“? Alternatives Gedankenexperiment: Wie wäre der Nationalsozialismus verlaufen, wenn man auf heutige Technikstandards und Datenbanken zurückgreifen hätte können? Hätte es enorme Überwachung gegeben?

- Kennen Sie das Werk Überwachen und Strafen von Michel Foucault?
- Wie könnte der Panoptismus auf das Internet übertragbar sein?
- Sollen wir im Internet diszipliniert werden?

Abschlussfragen und Raum für persönlich wichtige Aspekte

- (Nutzen Sie Social Networks wie z.B. *Facebook* und wie? Sind Sie auf *Youtube*-Videos und *Flickr* zu sehen? Wie gehen Sie persönlich damit um?)

- Wollen Sie aus Ihrer Sicht noch wichtige Aspekte benennen, die Ihrem Gefühl nach im Interview zu wenig berücksichtigt wurden?

Transkripte

(In chronologischer Reihenfolge)

Interview mit Wolfgang Zeglovits

Datum: 5. Februar 2010

Ort: leeres Besprechungszimmer

Dauer: gute 60 Minuten

1) Könnten Sie sich kurz vorstellen und Ihr Forschungsgebiet erklären?
Ja, mein Name ist Wolfgang Zeglovits, ich unterrichte auf der Publizistik und zwar dort Management neuer Medien, was eine Mischung ist eben aus meinen Forschungsinteressen auf der einen Seite und den beruflichen Erfahrungen als Geschäftsführer von Datenwerk, einer Webagentur, *Datenwerk Innovationsagentur*, auf der anderen Seite.
Meine Forschungsinteressen selbst sind vor allem die soziale Konstruktion von Technologie, und da von Software, von speziell Websoftware und da wiederum Spezialgebiet Weblogs, als Unterkategorie.
Meine Forschung selber ist angesiedelt im Bereich der Medienanthropologie, oder wie es in Frankfurt an dem Institut, an dem ich beheimatet bin, heißt, mediale Anthropologie, und beschäftige mich eben dort speziell mit der Entstehung von Software, als einen sozialen, kulturellen und ökonomischen Prozess.

Privatsphäre:
2) Welche Form von Daten würden Sie als sensibel beschreiben?
Daten würde ich jetzt noch nicht an sich als sensibel beschreiben, sondern eher das, was dann im Zusammenhang mit dem Informationsbegriff, den ich habe, es zu sensiblen Daten quasi macht.
Ich glaube, jedes Datum, die Einzahl von Daten, jedes einzelne Datum für sich genommen ist nicht sensibel, selbst wenn es sich um Daten handelt, die in einem Bereich, den man vielleicht sonst als gesellschaftlich nicht unbedingt weitergebbar sieht, abgibt, sonst würde zum Beispiel die ganze Markt- und Meinungsforschung nicht funktionieren. Schwierig wird es oder sensibel werden die Daten, wenn sie in Verbindung mit anderen Daten eben zu einem Informationsbild über eine Person, die rückführbar ist auf eine Person, werden.

3) Wenn sie personenbezogen sind?
Wenn Daten personenbezogen gesammelt werden können oder zusammengeführt werden und dadurch ein Bild von einer Person ergeben, die über das, was als Auskunft an die jeweiligen davon getrennten Stellen gegeben wurde, zusammengefügt werden. Und dann sind da schon Bereiche betroffen, die man benennen kann. Also da gibt es auf der einen Seite sensible Daten, die die Person an und für sich betreffen, zum Beispiel, was den Gesundheitsaspekt betrifft. Wenn das Auswirkungen hat auf Berufsaussichten, auf Versicherungszeiten, Auswirkungen auch auf Gesundheitsvorsorge oder Gesundheitsbehandlung selbst, dann sind das Daten, die potentiell missbrauchsmöglich sind oder auch systematisch zu einer Benachteiligung führen und daher sensibel sind. Auch Daten, die in bestimmten Fällen zu einer wie auch immer gearteten Verfolgung führen können, inhaltlicher Art, ob das jetzt religiöse Daten sind, also Daten über religiöse Motive und auch, und deswegen sind die auch sehr genau geschützt über Straffälligkeiten und dergleichen. Also alles, was das Bild, das man gerne nach außen präsentieren würde als Person, so weit untergräbt, dass damit die Person eigentlich Schaden erleidet, egal ob man das jetzt als positiv oder negativ sieht, dass das passiert oder nicht.

4) Wie werden diese Daten rechtlich geschützt?
Naja, ich meine, Sie haben das Datenschutzgesetz, als das für alle bindende Gesetz, die mit Daten umgehen oder die Daten sammeln und Sie haben dann in speziellen Bereichen dann noch mal, vor allem, wenn es sich um Institutionen handelt oder um staatliche Institutionen noch mehr, noch mal spezielle Schutzmechanismen. Also, Sie können zum Beispiel nicht Ihren Strafregisterauszug ohne eine persönliche Vorsprache beim jeweiligen Bezirksinspektorrat in Wien abholen, Sie können ihn sich nicht einfach zuschicken lassen. Und selbst dann, wenn Sie ihn sich abholen, bekommen Sie dann einen, wenn Sie keine strafregisterrelevanten

Einträge haben, aber Sie bekommen keinen, wenn Sie strafregisterrelevante Einträge haben. Das ist eine Möglichkeit des quasi verstärkten Schutzes.
In anderen Bereichen gibt es so etwas wie eine freiwillige Selbstkontrolle, also grad bei der Markt- und Meinungsforschung, in der ich auch stark tätig bin, ist es so, dass es die sogenannten *ESOMAR*-Richtlinien gibt [*European Society for Opinion and Marketing Research*, Anmerkung D.R.], also von dem Zusammenschluss europäischer Markt- und Meinungsforschungsinstituten, die bestimmte Regeln einfach definieren, unter denen Daten erhoben werden können, verarbeitet werden können und auch weitergegeben werden sollen. Da ist es zum Beispiel nicht opportun oder quasi geregelt, dass Sie nicht Daten von Aufzeichnungen, entweder Audio oder audiovisueller Art weitergeben an den Kunden, der Sie beauftragt hat mit der Marktforschung oder mit der Meinungsforschung. Das heißt, diese Daten sehr wohl zeigen können, aber nicht in die Hand geben als Videotape oder als CD-Rom oder DVD, um hier einen Missbrauch oder eine Missbrauchschance von vornherein zu minimieren.

5) Sie haben ja vorher gesagt, gesundheitliche Daten wären zum Beispiel sensible Daten und sie sind auch vom Datenschutzrecht als besonders schützenswürdig angegeben, trotzdem geben wir in Social Networks preis, welche Krankheiten man hat oder auch sexuelle Präferenzen als Beispiel. Warum stellen wir solche Daten ins Internet?
Das eine ist sicher die Unerfahrenheit mit dem Medium Internet an sich, im Sinne von, dass trotz, wahrscheinlich sogar, dem Verständnis dafür, dass hier Daten nicht einfach nur einmal preisgegeben werden und dann so wie in unserem realen Leben oder nicht EDV-gestütztem Leben dann auch wieder in Vergessenheit geraten oder quasi auch dementierbar sind, dass in einem Computernetzwerk wie dem Internet diese Daten einfach nicht verschwinden oder zumindest nicht mehr bewusst gelöscht werden können. Und selbst, wenn man das weiß, verhält man sich nicht entsprechend danach, weil es einfach diese Erfahrung nicht gibt, übersetzt als Tacit Knowledge oder als Implizites Wissen einfach nicht gibt, diesen Erfahrungsschatz zu wissen, wenn ich im Internet etwas preisgebe, dann wird diese Information eigentlich recht lang, wenn nicht über mein Lebensende hinaus sogar gespeichert und abrufbar sein. Und das nicht nur, und da kommen wir zu diesem Schützenswerten, das Sie gemeint haben bei den Daten, und das nicht nur an der Stelle, wo ich es abgegeben habe, sondern verbunden mit anderen Daten, die eben zu einem Gesamtbild oder zu einem Bild, das sich jemand von mir zeichnen will, zusammengeführt werden.
Das heißt, ich glaube, dass wir viele Daten von uns preisgeben unter anderem, weil uns diese Verknüpfung auch kognitiv nicht nachvollziehbar ist, die hier möglich ist und die hier betrieben wird, weil uns einfach auch die Möglichkeit der Vorstellungskraft der gemeinsamen Rechenleistung, die das Internet einfach durch seine Infrastruktur erbringt, nicht, zumindest derzeit noch nicht emotional und teilweise auch kognitiv nicht nachvollziehbar scheint.

6) Kann man das „Digitaler Fußabdruck" nennen, was wir im Web hinterlassen?
Sagen wir einmal so, wenn Sie Fußabdruck oder Fingerabdruck etc., da gibt es ja auch eine Debatte quasi, warum müssen wir uns Fingerabdrücke abnehmen lassen, wenn man wo einreist, in Japan oder in den USA, aber so ein Fingerabdruck ist erst dann etwas wert, wenn ich die Abgleichsmöglichkeit habe, das heißt es bringt nichts, einen Fußabdruck einfach nur zu sehen von einer Person, ich muss auch wissen oder vergleichen können, ob dieser Fußabdruck dann zu dieser Person passt. Und das, was wir, glaube ich, unterschätzen, ist die Möglichkeit jeder einzelnen Person von uns, dass sie diesen Datenabgleich eines Fußabdrucks von einer anderen Person einfach jetzt machen kann. Das heißt, ja, Sie hinterlassen eine digitale Spur, das haben Sie aber auch immer schon gemacht, nicht unbedingt eine digitale Spur, aber Sie haben andere Spuren hinterlassen. Spätestens mit der Aufnahme von Taufbüchern, und später Geburtsurkundenbüchern sind sie eigentlich schon früher zumindest, nicht unbedingt präventiv, aber im Nachhinein recht gut rückverfolgbar gewesen, wo ihre Ursprungs- oder Erstaufzeichnung herkommt, in Europa und in den USA. Wenn Sie sich anschauen die Digitalisierungsprojekte der Immigrationsbehörden in den USA von den ersten Immigrationsfällen weg, können Sie, wenn Sie Verwandte in den USA haben, sehr genau sagen, wann die eingereist sind. Also, das ist nicht so, dass die Angabe von Daten und die Speicherung der Daten über das eigene Lebensende hinaus neu werden oder neu wären, es ist nur die Möglichkeit des Abgleichs plötzlich soviel leichter auf der einen Seite für die, die es schon immer gemacht haben und sogar soviel möglicher für die, die bisher gar nicht den Zugang dazu hatten, das zu tun.

7) Kann man also eine Spur im Internet auf eine Person namentlich zuordnen?
Ich würde Ihnen gern die Dezemberausgabe vom *Wired* empfehlen, von diesem amerikanischen Magazin, Computermagazin, oder Web-, Kulturtechnikmagazin [http://www.wired.com/, Anmerkung D.R.]. Da war die Titelgeschichte *Gone* und da hat sich einer der Redakteure im August letzten Jahres versucht vier Wochen zu verstecken und das besondere war jetzt nicht, dass er versucht hat, sich zu verstecken, sondern dass es quasi über die *Wired*-Seite, und das Magazin ist jetzt ein populärwissenschaftlich teilweise angehauchtes, teilweise auch nur populäres Magazin, dass es doch eine gewisse Öffentlichkeit hat. Und auf diese Person wurde, nicht eben von gesetzlicher Stelle, sondern vom Arbeitgeber, vom *Wired*, einfach eine Erfolgsprämie ausgesetzt, wer

dazu beiträgt, dass diese Person in diesen vier Wochen nicht verschwunden sein kann und es hat sich eine kleine Community gebildet, die jetzt nicht übertrieben groß war, die diesen Typen einfach aufgespürt hat, obwohl er nach vielen Methoden vorgegangen ist, die er dann in diesem Artikel eben genau beschreibt, wie er versucht hat, sich eine andere Identität zu geben, inklusive Veränderung von Haarfarbe und Wachsen von Bart, also über ein „Ich verwende jetzt halt meine alte Telefonnummer nicht mehr“ hinausgehend, wie weit er da eigentlich gut verfolgt werden konnte plus, was das mit der Person gemacht hat.

8) Wurde er im Internet verfolgt?
Gerade im Internet. Alle wichtigen Daten und alle wichtigen Informationen, die die Verfolger aufgenommen haben, und die ihm am Anfang auch wiederum einen Wissensvorsprung gebracht haben, weil sie sich auch wiederum öffentlich darüber unterhalten haben, welche Daten sie von ihm haben, waren alle angeblich sogar zum größten Teil legal aus dem Internet erworben, inklusive Verbindungsdaten zum Konto usw., also wirklich sensible Daten, Finanztransaktionsdaten wären zum Beispiel solche sensiblen Daten.

9) Vielleicht könnten Sie eine kurze Prognose geben, welche Daten noch kommen werden? Kann das noch irgendwie weiter gehen?
Nein, ich glaube eher, dass es die Verbindung, was Sie digitalen Fußabdruck genannt haben, würde ich als digitalen Klon bezeichnen. Und da gibt es einfach eine Perfektionierung. Ich meine, was wollen Sie denn noch ein Mehr an Daten haben, Sie haben alles. Sie haben früher schon vermessen den Menschen mit Körpergröße, also im Reisepass steht die Körpergröße drin, die Augenfarbe, also quasi eine Beschreibung. Damit haben sie für den Computer die Möglichkeit, überhaupt eine Semantik zu haben. Sie haben Bilder, inzwischen ist *Google* soweit und setzen es nur deswegen nicht ein, weil sie es datenrechtlich nicht wirklich als unbedenklich einstufen lassen können, Bildverfahren, die es ermöglichen, dass Gesichter erkannt werden und diese Bildverfahren sind nicht im Einsatz nur bei Überwachungskameras oder vom Sicherheitspersonal, sondern diese Bildverfahren sind eingesetzt von Softwarelösungen, die Sie auf Ihrem *PC* haben oder auf Ihrem *Mac*. Die *IPhoto-Suite* von *Apple* verwendet Gesichtserkennung für Ihre privaten Fotos. D.h. hier geht es nicht darum, dass sie neue Daten bekommen, meiner Meinung nach, sondern dass erstens die Erkennungsverfahren besser sind und wenn Sie wollen, die Ergebnisse daraus, ja, das sind Daten, die sie in alten Datenkategorien hätten abbilden können. Aber das was passiert ist kein digitaler Fußabdruck meiner Meinung nach, sondern ein digitaler Klon, der aus den quantitativen Daten zu Ihrer Person einfach zusammengesetzt werden kann und der über ihre quantitative, also quasi über Ihre Beschreibung der Person selber hinausgeht inklusive des sozialen Netzwerks und der Verortung, wo Sie sich aufhalten und in welchen Kanälen Sie sich befinden, sowohl online als auch offline.

10) Ich habe mir auch ein Beispiel aufgeschrieben. Könnte es möglich sein, dass wir unsere DNA bei *Xing* hineinstellen, um zu zeigen, wie gute Gene wir haben?
Also bei *Xing* glaube ich nicht, ich glaube, dass es eher bei *Parship* oder bei Partnerbörsen interessant wäre. Allerdings ist da beides interessant zu beobachten. Nämlich auf der einen Seite, dass wir andere Daten und Konzepte schon seit Jahrzehnten eigentlich schon haben, die wir bei *Xing* auch nicht angeben, die auch möglicherweise etwas über Qualität zumindest indizieren würden, wenn auch schon nicht beweisen. Also ich denke da an den IQ, also ein Testmesssystem, das höchst umstritten ist natürlich, aber es eigentlich nur eine kleine Gruppe gibt, nämlich die Personen, die nachweislich einen IQ über 150 haben, sich in einer Gemeinschaft, Mensa zusammenschließen und quasi diese Gemeinschaft als ein Prädikat, als persönliches Prädikat oder als Eigenschaft mit sich tragen. Aber ich würde jetzt nicht, ich gehöre auch nicht zur Mensa, habe auch sicher keinen IQ von 150 oder darüber, aber ich würde jetzt nicht meinen IQ, wenn ich einen IQ-Test machen würde und er überdurchschnittlich wäre auf *Xing* hineinstellen, um zu zeigen, dass ich persönlich intelligent bin und daher wahrscheinlich ein interessanter Gesprächspartner oder Geschäftspartner bin. Da gibt es schon Formen von Daten oder von Ergebnissen, die wir jetzt schon nicht hineinstellen, obwohl sie verfügbar wären. Umgekehrt, das ist das andere, genauso wie beim IQ, dass das eigentlich relativ ein ungenaues Messverfahren ist für das, was es vorgibt zu messen, nämlich Intelligenz, nur dass das Konstrukt etwas schwierig ist zu benennen, umgekehrt ist es bei der DNA auch nicht so, dass quasi, nur weil sie eine gute DNA haben, ihre Kinder zum Beispiel oder auch Ihr Phänotyp, also so wie sich dann entwickelt haben, bedeutet, dass Sie irgend etwas besser oder anders oder ja, dass Sie sich da etwas unterscheiden würde, das sich auf Ihren Phänotyp übertragen würde.

11) Wie wichtig schätzen Sie die Privatsphäre, also vor allem die informationelle, dass wir selber bestimmten, wer welche Informationen über uns bekommt?
Ich fürchte, dass die Privatsphäre ein soziales Konstrukt ist, weil mir persönlich, also wenn Sie mich persönlich fragen, dann sage ich, für mich ist Privatsphäre wichtig, wenn ich mir allerdings außerhalb und da reicht schon der europäische Kulturkreis, wenn man das Wort Kulturkreis überhaupt sagen darf, was auch ein etwas zynischer, anachronistischer Begriff ist, aber wenn man sich, sagen wir noch immer bestehende europäische Nationalkulturen ansieht und deren Umgang mit Privatsphäre, dann sind da schon extreme

Unterschiede feststellbar. Konkret wenn Sie in Holland durch eine Straße gehen in der Nacht, dann sind dort keine Vorhänge und Sie haben die Tendenz in Wien auch oder quasi merke ich auch, dass es auch hier zunehmend nicht mehr so ist, dass jeder sein Vorhänge schließt, wenn er in der Nacht das Licht aufdreht, also einen ganz anderen Eingriff oder quasi eine ganz andere Einblicksmöglichkeit gibt potentiell in die eigenen vier Wände. Umgekehrt, wenn Sie in Osteuropa unterwegs sind, dann haben Sie teilweise Autos, die ihre Windschutzscheiben, nicht nach vorne und nicht die direkt auf der Seite mit Vorhängen zuziehen bzw. getönte Windschutzscheiben sehen Sie auch auf unseren Straßen ab und an. Wenn Sie sich anschauen was jetzt, also das waren jetzt sehr konkrete Beispiele der Umgebung. Wenn Sie sich aber anschauen wie zum Beispiel in Schweden Gehaltsdaten und Steuerdaten gehandhabt werden und wie sie in Österreich gehandhabt werden, dann werden Sie einen eklatanten Unterschied sehen, weil Sie in Schweden mit einer einfachen Internetdatenbankabfrage herausfinden können, wie viel eine Person laut Finanzamt verdient und wie viele Steuern diese Person abgegeben hat in einem Jahr oder quasi über einen längeren Zeitraum. Das können Sie in Österreich nicht tun. In Österreich verstehen Sie es fast als einen Eingriff in Ihre Privatsphäre, wenn Sie sagen müssen oder wenn ich Sie fragen würde, was Sie im Monat verdienen oder was Sie an Barvermögen haben oder wie viele Schulden Sie haben. Also das würden Sie oder ich auch als einen Eingriff in Ihre Privatsphäre verstehen, wenn ich Sie das jetzt direkt fragen würde.
Also von da her glaube ich oder fürchte ich, dass das Thema Privatsphäre an sich ein Konstrukt ist. Auf der anderen Seite ist es doch etwas, was sehr stark uns ausmacht, einen Rückzugsbereich zu haben, der aber kulturell bedingt geformt ist oder politisch geformt ist oder gesellschaftlich geformt ist, dass es uns aber, wenn sich dieser Kontext oder wenn sich dieser Konsens, was in einer Gesellschaft als Privatsphäre definiert ist, ändert, zu großer Unsicherheit führt, weil es ganz tief einfach an unserer Person zu Veränderungen führt.

Überwachung:

12) Macht es einen Unterschied, dass wir die Daten freiwillig in Social Networks hergeben oder gibt es sowieso anderweitige Methoden der Datenerhebung? Fällt es überhaupt ins Gewicht, wenn wir Daten in Soziale Netzwerke stellen?

Es fällt insofern ins Gewicht, als dass Geheimdienste sich nicht mehr so schwer tun, Gesamtprofile über Personen anzulegen. Wenn sie sie eh freiwillig hergeben, ist die Notwendigkeit der Verknüpfung von verschiedenen Quellen zu einem gemeinsamen Profil nicht mehr so schwierig.

13) Wer sind eigentlich salopp formuliert die Feinde der UserInnen in Social Networks, also wer könnte das überwachen, wer könnte die Daten brauchen und verwenden?

Geheimdienste auf jeden Fall. Marketingfirmen auch auf jeden Fall. Also verwenden heißt aber noch lange nicht, meiner Meinung nach, dass Sie Feinde dieser Dinge sind oder User und Userinnen, sondern es ist meiner Meinung nach eben in der Verantwortung der einzelnen Person zu sagen, mache ich da mit und wie viel gebe ich davon preis. Feind oder quasi wirklich Missbrauch entsteht dort, jetzt schon und permanent, wo sie über eine Einladung in *Facebook* zum Beispiel an eine Person, die daran nicht teilnehmen will, damit etwas über diese Person preisgeben, weil es möglich ist, daraus quasi wiederum Profildaten von Personen zu erstellen, die gar nicht an diesem Spiel, wenn Sie so wollen, *Facebook* teilnehmen. Anders gesagt oder konkreter Fall, wenn Sie eine Person einladen, eine gute Freundin von Ihnen, die aber nicht bei *Facebook* dabei sein will, dann können Sie durch Ihre Nachricht an ihr eigenes Profil, also ihre Statusänderung, das sogar bekannt geben, dass Sie diese Person eingeladen haben, mit Namen und es können sofort alle Personen, die Sie kennen diese Person auch quasi bestärken, dass sie in *Facebook* kommt und als potentielle Freundin schon einmal vormerken, dass sie, wenn sie, sobald sie sich einloggt zum ersten Mal oder registriert eben, dass sie dann eine Freundschaftsanfrage auch gleich bekommt von Ihnen. Daraus lassen sich natürlich sogar über diese Person extrem viele Profildaten generieren, ohne dass sie bei *Facebook* überhaupt dabei ist. Businessmodell wird daraus gemacht bei *123people*, einem Suchservice, das in Österreich unter anderem entwickelt wurde, woher Sie dann auch sehen bei den Daten, wenn Sie Suchprofile in Österreich haben, dass die eigentlich relativ genau sind, wo einfach alle verfügbaren Quellen des Internets abgegriffen werden nach einem Personennamen. Haben Sie jetzt einen Personennamen Hubert Mayer oder Herbert Mayer, dann ist die Verwechslungsgefahr mit anderen natürlich sehr groß. Heißen Sie Rudlstorfer oder Wolfgang Zeglovits, dann gibt es da nicht mehr so viele, die einen ähnlichen Namen haben. Das heißt das Profil ist relativ schnell relativ genau. Feinde sind das aber eben nicht, sondern das sind einfach Nutznießer dieser Freigiebigkeit unserer Daten im Netz bzw. der Möglichkeiten, die sich aus dem Internet heraus ergeben. Feinde wären für mich Leute, die es versuchen würden zu zerstören. Aber die gibt es natürlich auch. Also Leute, die Datenschutz fordern gegen den Willen der Personen, weil die ja offensichtlich diese Daten eingeben. Aber selbst da merkt man auch Meldungen der *ARGE Daten* zum Beispiel, dass auch dort es eigentlich durch diese Freigiebigkeit der Personen oder der Menschen es auch der *ARGE Daten* schwer fällt zu sagen, was davon ist eigentlich schützenswert und was nicht. Also da hat man sogar dort das Gefühl, dass sich zwar ungewollt, aber doch ein Paradigma zerstört, nämlich, dass es hier irgendwas wie Privatsphäre gibt und man unbedingt darauf schauen muss, dass die geachtet wird und hält.

Und auch wenn man sich anschaut die *BigBrother*-Awards zum Beispiel sind das wirklich inzwischen, also das geht immer stärker in Richtung der Konsequenzen aus dem Datenmissbrauch oder der Datensammlung und nicht mehr so sehr in der Datensammlung an sich. Es geht nicht nur darum, dass Sie den *BigBrother*-Award bekommen, weil Sie Daten sammeln, sondern es geht eher darum, dass Sie schon damit etwas machen, was als verwerflich gilt.

14) Sie haben vorher gesagt, dass der Staat, also Sicherheitsbehörden oder Nachrichtendienste, es leichter haben Profile zu erstellen. Nutzt der Staat solche freiwillig hergegebenen Daten überhaupt oder sammelt er sie selbst anders?
Wie soll er sie anders sammeln?
Vor allem Nachrichtendienste, durch Vorratsdatenspeicherung zum Beispiel, sie wissen wer wen anruft, usw.?
Ja aber ich glaube, also wenn Sie sich die Menge, auch jetzt bei der Vorratsdatenspeicherung, die Menge der Daten ansehen, die dann semantisch irgendwie ausgewertet werden müssen, um überhaupt einen Informationswert zu haben, ist die Veränderung, die wir haben, nicht mehr so sehr das Suchen der Nadel im Heuhaufen, sondern eher das definieren, was ist die Nadel. Also, wenn Sie jetzt oder heute ein Profil anlegen wollen, tun Sie sich mit allein öffentlichen zugänglichen Internetdatenbankabfragen jeglicher Art leichter, ein Profil zu erstellen von einer Person, die Sie suchen, während Sie früher schwierigere Rahmenbedingungen vorgefunden haben. Aber trotzdem meiner Meinung nach die Arbeit, also quasi, ich meine, es heißt ja nicht umsonst Informationsdienste auch die Geheimdienste oder Intelligence, dass diese Intelligence ja zum größten Teil sehr wohl von öffentlich verfügbaren Daten kommt und in Spezialfällen und vor allem in Hollywoodfilmen dann halt quasi irgendwelche Satellitenaufnahmen von Gefangenenlager etc. sind, ja. Und wenn Sie sich anschauen, dass wir de facto mit *Google Maps* auch als Privatuser inzwischen über diese Daten verfügen, können Sie jetzt gar nicht mehr davon ausgehen, dass sie jetzt viel größere andere Zugangsmöglichkeiten haben als öffentlich zugängliche Daten. Was haben Sie dann noch viel. Also, Sie haben die Sozialversicherungsdaten, die vor allem Versicherungszeiten sind zum Beispiel in Österreich, ob das jetzt soviel hergibt, ist die Frage. Sie haben, ja Vorratsspeicherung gibt es noch nicht und sie haben, was sie schon haben, was andere nicht haben, ist Zugang zu Überwachungsdaten. Aber da müssen Sie erst die Nadel definiert haben, da müssen Sie erst die Person definiert haben, die sie eigentlich suchen wollen. Das was mit der Vorratsspeicherung passiert, ist ja eigentlich eher, dass man sagt, wir können inzwischen Nadeln im Heuhaufen finden, deswegen ist es besser, wir sammeln sehr viele Heuhaufen an und werfen sie nicht gleich weg, damit wir dann überhaupt erst suchen können. Das heißt, die Veränderung der Institutionen ist, sie können leichter ein Profil erstellen, aber sie haben keinen Vorsprung mehr zur Bevölkerung, was jetzt die generelle Überwachung betrifft. Aber sobald sie jemanden speziell suchen, dann brauchen sie neue Mittel wie zum Beispiel Vorratsdatenspeicherung und eben Abhörmöglichkeiten, damit Sie Zugriff zu einem Informationsvorsprung haben.

15) Was wird dem Staat das bringen, wenn er seine Bürger überwacht?
Ja offensichtlich nicht viel, weil sonst hätte es in den USA nicht diesen fast-Anschlag gegeben, im Dezember letzten Jahres mit diesem Flug nach Detroit.

16) Gäbe es sonst mehr Anschläge?
Ja, aber ich glaube, das ist eher eine Sache, die nicht zu sehr elektronisch, also wo die Daten eigentlich das Fundament geben, wo es wirklich um Informationsarbeit geht. Ich bin, und das kann ich nicht nachweisen und das ist auch quasi, ich will da jetzt auch nicht in Verschwörungstheorien hineinkippen oder so, aber ich bin der festen Überzeugung, dass zum Beispiel der britische Geheimdienst um einiges effizienter arbeitet als der US-amerikanische oder viele andere Geheimdienste. Weil dafür dass Großbritannien eigentlich ein ideales Terrorziel ist, von den Beteiligungen an den Kriegen mit den USA etc. und mit einem Ballungszentrum wie London, passiert dort eigentlich recht wenig. Und man hat doch oft den Eindruck, dass in London Terroranschläge bewusst, so dass man es mitbekommt, verhindert werden oder Menschen, die dann sogar nachweislich in Verschwörungsaktivitäten tätig waren, aufgegriffen werden. Umgekehrt haben Sie gerade in London, um beim britischen Beispiel zu bleiben aber auch in anderen Ballungszentren in Großbritannien eine extreme Form von Jugendkriminalität, die auch mit einer Überwachung nicht in den Griff zu kriegen ist.

17) Zur Wirtschaft. Wie kann die Wirtschaft, also wirtschaftliche Unternehmen solche freiwillig hergegebenen Daten nutzen?
Will ich gleich dazukommen, aber ich wollte nur, quasi weil Sie mich gefragt haben, was zu der staatlichen Kontrolle noch. Ich meine diesen Film vom Spielberg mit Tom Cruise in der Hauptrolle, wo es darum geht, Verbrechen vorher schon zu erkennen. [Gemeint ist *Minority Report*, Anmerkung D.R.] Das ist natürlich meiner Meinung nach die Vision, die jemand hat, der von einer Verbrecherbekämpfung und Sicherheitsmaxime ausgeht. Also quasi, ich mag einen absolut sicheren Staat haben oder eine absolut sichere

Gesellschaft, aber das widerspricht sich eben mit einer Generalüberwachung und einem Generalverdacht der Bevölkerung.

18) Aber vielleicht, also wenn man die Profile irgendwie so verarbeiten kann, dass irgendwie Tendenzen zu sehen sind, wer sich wie entwickeln könnte?
Ja, aber nur was hilft Ihnen das. Das würde nur bedeuten, dass wir unser Rechtssystem radikal umstellen und dass wir auf Verdacht jemanden einsperren oder quasi beschränken in seiner Freiheit. Das heißt eigentlich hat in einem demokratischen System, wie wir es jetzt noch kennen, jeder das Recht, nicht die Pflicht, aber das Recht, ein Verbrechen zu begehen. Und wenn Sie eine Totalüberwachung haben, mit der Möglichkeit quasi eines Vorwarnsystems, dann nehmen Sie, nicht dass das an sich verwerflich wäre eben das Recht eine Straftat zu begehen, aber Sie nehmen der Person das Recht zur willentlichen Entscheidung, die höchstwahrscheinliche Straftat doch nicht zu begehen.

19) Okay. Zur wirtschaftlichen Überwachung eben. Wie können Unternehmen die Daten nutzen, die wir freiwillig in Social Networks hineinstellen?
Ja, vor allem zu einer genaueren Definierung der Bedürfnisse der Zielgruppen, also eine Steuerung der Zielgruppen, ein Kennenlernen der Zielgruppen, und dann entsprechend zur Marketing-, also zur Verkaufsförderung des Produkts oder Bekanntmachung. Und da ist quasi, da sind die genauso interessiert an Daten, aber eben über viele Zielgruppen hinweg noch interessierter an Daten als glaube ich Geheimdienste über die eigene Bevölkerung herausfinden wollen. Also, ich glaube, dass staatliche Stellen eher an den Extremen interessiert sind, also quasi Leute, die eben, wie Sie vorher gesagt haben, möglicherweise eine hohe Wahrscheinlichkeit einer Kriminalität, also dass sie kriminell werden, dass man die quasi zu beobachten versucht, oder die in irgendeiner Form das Staatsgefüge politisch verändern könnten oder beeinflussen könnten, also sowohl rechts als auch links bzw. glaube ich, dass über Personen des öffentlichen Lebens, also vor allem Politiker und Politikerinnen sicher irgendwelche Akten auch in staatlichen Geheimdiensten gesammelt werden. Einfach um eine Einschätzung dieser dann doch einflussreichen Personen machen zu können. Marketing, also Firmen interessieren alle Daten von allen Personen, weil sie quasi potentiell überall ihren Markt haben, und weil sie quasi je nachdem welche Zielgruppen sie haben, dann natürlich entsprechend speziell, aber weil sie da natürlich eine extrem gute, vorbereitende Kauflandschaft vorfinden.
Aber da gibt es, also da sind hier auch Möglichkeiten zusätzlich zustande gekommen, die noch nicht zum Beispiel für alle möglich oder zugänglich sind, sondern die einen bestimmten Kapitaleinsatz bedürfen. Sie können zum Beispiel von allen Mobilfunkbetreibern die Verbindungsdaten kaufen, die die eingeschalteten Handys mit ihren jeweiligen Sendemasten eingehen. Die kriegen sie anonymisiert, das heißt, sie wissen nicht, welche Telefonnummer da jetzt herumspaziert, aber sie können relativ genau Profile machen von Punkten, wie Personen sich im öffentlichen Raum bewegen aufgrund ihrer Datenspur, die sie mit dem Mobilfunktelefon hinterlassen. Und da können sie dann Geschäftsmodelle generieren, sowohl auf der einen Seite von dem Anbieter, der diese Daten zusammensammelt bis hin zu dem, der quasi davon profitieren kann. Das konkreteste Beispiel ist, dass es in US-amerikanischen Shoppingmalls inzwischen üblich ist, dass sie nicht mehr Zählungen machen, also die Daten wurden nämlich früher auch erhoben, nur anders und schwächer, dass sie nicht nur Zählungen machen, wer geht wo an welchem Schaufenster vorbei und welche Wege werden verwendet in einem Shoppingmall, sondern sie lassen das 24 Stunden, also halt während der Öffnungszeiten einfach über die Mobilfunkmonitoren und können dann sogar entsprechend des Durchflusses an Personen, die bei ihnen vorbeigehen entsprechend die Mieten erhöhen oder quasi sagen, soundso viel an deinem Revenue würden wir gerne mitverdienen, weil du musst aufgrund der Laufkundschaft, die du hattest, dementsprechend Einnahmen gemacht haben.

20) Wie genau kann man Werbung bereits schalten?
Legen Sie sich einen *Gmail*-Account an und Sie werden begeistert sein, was Sie für tolle Werbevorschläge bekommen haben.

21) Treffen die auch zu?
In einem überraschenden Ausmaß ja. Also ich habe einen *Gmail*-Account und bin immer wieder überrascht wie genau die Anzeigen sind, die hier geschalten werden. Also es ist schon immer wieder auch Blödsinn dabei, aber es ist auch immer wieder überraschend wie genau das den Bedürfnissen, die sich aus diesem E-Mail heraus ableiten lassen würden, passt. Wobei das natürlich auch, muss man auch sagen, ein Henne-Ei-Problem ist. Also wenn sie keine Kunden haben, also wenn *Google* keine Kunden hat, die auch zu meinen Bedürfnissen passen, dann kann ich auch nur falsche Anzeigen bekommen. Wenn aber die Firmen in dem Werbeumfeld tätig sind, die mich sowieso interessieren, dann werde ich auch entsprechend passende Werbung finden, ja. Aber sie können, ja, der Punkt ist auch, dass für viele Dinge gar nicht die Menge der Daten entscheidet, sondern die Verbindung einzelner Parameter entscheidend ist. Also in manchen Bereichen ist es wichtig zu wissen, wie die Gruppe soziodemographisch aussieht, in anderen Bereichen ist es wichtig, wo die Personen zuhause sind, und in dritten Bereichen ist es gar nicht wichtig, wer die Person selbst ist, sondern es ist nur

wichtig, mit wem sie in Verbindung ist und zwar nicht aufgrund ihrer persönlichen Präferenzen, sondern aufgrund des Netzwerks an sich, das heißt, netzwerktheoretisch zum Beispiel ist es völlig unerheblich, wer Sie als Person sind, das heißt, sie braucht Sie gar nicht beschreiben. Wichtig ist im Zusammenhang mit allen anderen Personen, welche Kontakte Sie haben. Und wenn ich eine Beziehung habe, also eine so genannte Dreiecksbeziehung habe, mit starken Verbindungen zwischen zwei Polen, dann kann ich quasi relativ einfach Schlüsse auf die nächsten Verbindungen machen. Das heißt, oft ist es nur das Gefühl, dass wir quasi viele Daten brauchen, um zu einem Ergebnis zu kommen, aber dem netzwerktheoretischen und daraus ergebenden mathematischen Modelle reichen aus, mit viel weniger Information auf die gleichen Ergebnisse zu kommen.

22) Da sind ja zum Beispiel Social Networks ideal?
Da sind sie super, ja. Da haben sie natürlich auch den Namen und mehr noch an Information. Aber es ist jetzt bei *Facebook* zum Beispiel nicht notwendig, dass der Algorithmus, der dahinter läuft, um Ihnen Freunde anzuzeigen, die sie vielleicht haben, aber noch nicht als Freunde in *Facebook*, dazu braucht er nicht wissen, dass sie quasi vom Profil zusammenpassen, also ähnliche Interessen haben oder in ähnlichen Gruppen frequentieren oder ähnliche Seiten sich anschauen, sondern es reicht über Ihre Verbindungen, die Sie haben und die Verbindungen Ihres Freundes, den Sie schon haben, daraus abzuleiten, dass es eine dritte Person gibt, die zu Ihnen passt. Und das ist eben wirklich völlig unerheblich, ob sie dann quasi sonst Angaben ähnlich haben oder nicht. Sie sagen durch Ihr Beziehungsgeflecht in *Facebook* viel mehr aus, als über die Angaben, die Sie machen zu Ihrer sexuellen Orientierung oder ob Sie dort jetzt zum Flirten sind oder um Geschäfte zu betreiben.

23) Wer wertet die Unmengen an Daten eigentlich aus? Geschieht das alles schon vollautomatisch oder sind da noch Menschen dahinter?
Ja, wenn Sie eine Bedeutungsauswertung brauchen, dann brauchen Sie Menschen dahinter. Also, wenn Sie jetzt sagen wollen, quasi wie viele Postings positiv und wie viele Postings negativ zu einem Thema sind, dann brauchen Sie jemanden, der sich die Postings durchliest. Da reicht eine Keyword-Analyse nicht. Für alles, wo es um die Quantifizierung geht oder wo Sie eine genaue Hypothese haben, ist es Statistik, also kann alles automatisch ausgewertet werden.

24) Wissen sie zum Beispiel über meinen Musikgeschmack schon fast genauer Bescheid als ich, also durch Digital Rights Management kann man ja genau herausfinden, wer wann was wo horcht. Also, sie wissen ja eigentlich im Grunde besser Bescheid dann, was ich genau horche als ich, weil ich schreibe ja nicht mit?
Ja, ja. Haben Sie schon einmal *Last.fm* probiert zum Beispiel?
Genau das wäre ein Beispiel. Nein.
Also bei *Last.fm*, wenn Sie sich die Mühe machen, auch dann noch zu sagen, gefällt mir, gefällt mir nicht, dann kriegen Sie ein super Programm zusammen, das keine Wiederholungen hat, das immer was Neues findet und das genau zu Ihrem Musikgeschmack passt, mit dem Nachteil, dass Sie halt quasi nichts Neues entdecken außerhalb dieser Bahnen, in denen Sie sich dann bewegen. Das ist aber auch eine Algorithmus-Frage. Das Bedrohliche ist eher, dass wir es schlecht programmieren. Und zwar sowohl, dass es keinen Ausschaltknopf gibt und keine Alternative zu etwas, was einem ständig vorgeschlagen wird und dass es quasi eine Richtung vorgibt, in die man eigentlich nicht will oder die dann dazu führt, dass man sich denkt, eigentlich ist es schon langweilig und wieder aussteigt. Weil was man nicht vergessen darf bei allen Algorithmen und bei allen Daten, die gesammelt werden etc., es ist letztlich immer der Mensch, der den Algorithmus schreibt. Und es gibt zwar inzwischen auch Programme, die **KPXN** (???) ist zum Beispiel so ein Tool, das aus einer Riesenmenge an Daten, die unstrukturiert sind, also wirkliche Daten, nicht Information, sondern wirklich Daten, Trends vorschlägt. Nur letztendlich muss der Mensch beurteilen, ob diese Trends dann auch sinnvoll sind oder nicht.

25) Und funktioniert das?
Das funktioniert relativ gut, ja. Und sie können auch, das sind Dinge, die in Bezug auf, also die zum Beispiel ein *AMS* schwerer tun würde, also das *Arbeitsmarktservice* schwerer tun würde einzusetzen als das *Monster* zum Beispiel als Privatanbieter schon macht. Sie können eigentlich aufgrund von einigen persönlichen Daten im Vergleich zu anderen Fällen einen recht guten Index ausrechnen, wie hoch Ihre Employability ist zum Beispiel. Und auch da brauche ich nicht wissen, wie Ihre sexuelle Präferenz ist oder so, sondern auch da reichen mir bestimmte Kernaussagen oder Kernwerte, auf deren Basis ich dann ein Modell Ihrer Berufslaufbahn vernehmen kann.

26) Gibt es im Internet einen Kampf zwischen ÜberwacherInnen und Verschleierungsdiensten zum Beispiel. Kann man da von einem technischen Rüstungskampf sprechen?
Ja, das kann man definitiv. Also Sie haben einiges an Möglichkeiten, Dinge zu verschleiern, aber es ist schwieriger, etwas zu verschleiern oder zu verheimlichen als es derzeit leichter ist, etwas herauszufinden. Auch da noch mal dieser nicht jetzt wissenschaftliche, aber auch von der Herangehensweise spannende Artikel

in dem *Wired*, wo Sie lesen können, wie sogar das *TOR*-Network, also ein Verschleierungs-IP-Netzwerksystem, das auf Peer-to-Peer Basis funktioniert, wie das umgangen worden ist, um herauszufinden, wo diese Person sich einloggt mit seinem Computer. Das heißt, wenn Sie einen Fehler machen, hat man Sie. Umgekehrt, wenn ich eine Chance nicht wahrnehme, Ihre Daten zu sammeln, macht es nichts, ich kriege noch tausend andere Chancen. Sehr empfehlenswert, jetzt auch im letzten, nein 10.1. Entschuldigung *Spiegel*, glaube ich, war ein Artikel über *Google*, bei dem unter anderem auch diese Bilderkennungssoftware genannt worden ist, und ein etwas extremer Fall vorgestellt worden ist, von einer Frau, die sich für, sie haben es recht euphemistisch beschrieben, aber anscheinend für pornographische Aufnahmen zur Verfügung gestellt hat früher und der das natürlich dann entsprechend peinlich war, die sogar soweit gegangen ist, dass sie ihren Namen geändert hat und weggezogen ist, laut Beschreibung des Magazins, und für die wäre natürlich so eine Bilderkennungssoftware der Horror, weil quasi die ganze Deckung und dieses ganze Procedere des Veränderns des Lebensumfelds damit hinfällig ist.

27) Kann man sagen, dass durch die Social Networks Überwachung im Web 2.0 personalisiert wird? Sie haben schon angesprochen, dass der Staat im Grunde nicht mehr viele Vorteile hat. Beispielsweise können Freunde, LehrerInnen, Vorgesetzte dort nachschauen?
Es geht inzwischen, also wir sind alle zu Halböffentlichkeitspersonen geworden. Also es geht ja auch einher mit dem, was die Medien machen. Da gibt es auf der einen Seite die Geschichten, eben Web 2.0 und wie viel gebe ich von meiner Persönlichkeit preis, die ja nicht nur jetzt wissenschaftlich, sondern auch als Medienthema immer wieder herumgeistert, also diese Aufgabe der Privatsphäre und auf der anderen Seite haben Sie aber genau von den gleichen Medien in anderen Sendeformaten eine Vielzahl an Personen, an der die Öffentlichkeit früher kein Interesse gehabt hätte, also die ganzen B-, C-, D- und wie weit auch Sie immer dann die Kategorisierung vornehmen wollen, Promis sind völlig uninteressant für das, was sie geleistet haben oder getan haben, sondern es reicht diese Öffentlichkeit, die sie schaffen können oder diese Teilöffentlichkeit und letztendlich können Sie das auch und es geht eher nur darum, wie steuern Sie das oder versuchen Sie es zu steuern, wie versuchen Sie sich selbst darzustellen. Und dann gibt es natürlich tausend Möglichkeiten, Sie genauso wie in diesem Öffentlichkeitsbereich der Medien auch im Öffentlichkeitsbereich des Internets schlechter darstellen zu lassen.

28) Welche Vorteile sehen Sie in der Entwicklung hin zu mehr Überwachung?
Gar keine ehrlich gesagt. Also ich wüsste nicht, was ein Mehr an Überwachung hilft. Es ist eher durch die Rechenleistung der Computer und durch die Vernetzung dieser Rechenleistung ein konsequentes Ausnützen dieser Möglichkeiten, weswegen wir in eine Überwachung hineinrutschen. Aber, das heißt man kann sich jetzt gesellschaftlich zwar dagegen stellen, aber es wird einem nicht viel helfen. Aber positiv sehe ich daran gar nichts. Also, zu einer freieren oder offeneren Gesellschaft wird es nicht führen.

29) Vielleicht dazu, dass Bedürfnisse besser befriedigt werden können?
Naja, als Psychologe von der Grundausbildung her habe ich ein bisschen ein anderes Bedürfnisdefinitionsverständnis als das Marketing, als das Marketingfirmen haben, weil Marketingfirmen gehen davon aus, dass man Bedürfnisse schaffen kann. In der Psychologie gibt es einfach nicht nur den Maslow mit seinen Grundbedürfnissen, aber trotzdem eine Vorstellung, dass es einfach ein eingeschränktes Feld an Bedürfnissen gibt, die Sie haben, die nicht in einer Pyramide unbedingt dargestellt sind, aber, die mit sehr grundlegenden Dingen einfach abgedeckt sind und befriedigt sind, und das, was hier als Bedürfnisse normalerweise im Raum steht, eher interessensgeleitete Lüste oder Sehnsüchte sind als tatsächlich Bedürfnisse, die Sie haben. Das heißt, ja zur Sehnsuchtsgenerierung und vor allem dann zur Sehnsuchtsbefriedigung hilft es, aber die Frage ist, ob quasi, ob das notwendig ist oder nicht und ob das quasi die Idee eines nach Erkenntnis strebenden Menschen rechtfertigt oder ob wir uns von diesem Ideal sowieso schon verabschiedet haben.

30) Gegenfrage. Welche Gefahren gehen von einer Überwachung aus?
Ja, auf der einen Seite eben, dass Sie die Möglichkeit verlieren, sich frei in einer Gesellschaft zu entfalten und letztlich eigentlich auch persönliche Freiheiten, die die Moderne sich hart erkämpft hat oder die sich die Menschheit hart erkämpft hat in bestimmten Gesellschaften, dass wir diese wieder auch verlieren.
Es gab jetzt schon ein paar Datensupergaus meiner Meinung nach, also wie verlorene Daten von eben auch den vorher eigentlich so gelobten britischen Geheimdiensten, wie Zugriffs-, oder bzw. Kreditkartenbetrugsfirmen, also Kreditkartenbetrüger, die die Kreditkartenfirmen ausgenommen haben letztendlich oder vorher eigentlich die Konsumenten. Also insofern glaube ich, dass die Überwachung, also dass da genug Gefahren bestehen.
Und letztendlich auch diese Ironiefreiheit, die dadurch entsteht. Also wenn Sie jetzt etwas Ironisches ins Netz stellen, kann es Ihnen aus dem Kontext heraus in zwei, drei, fünf, zehn Jahren als Vorwurf gemacht werden. Gleichzeitig wird es aber auch nicht mehr, das ist die andere Entwicklung, die ich so erkenne, wird auch nichts mehr ernst genommen unter Anführungszeichen. Also, wenn Sie und das ist keine Internetentwicklung, sondern eher eine Medienentwicklung, wenn Sie sich anschauen, wie sich diese Gesetze der Soap, also von

fiktionalen Charakteren in fiktionalen Umgebungen inzwischen übertragen lassen auf andere Bereiche wie Gesellschaft, Wirtschaft oder Politik, dann ist es eigentlich auch völlig unerheblich, was sie zu welchem Zeitpunkt tun, weil Sie können mit jeder Aktivität, die sie danach setzen, das Davor nicht wegbringen, das definitiv nicht, aber zumindest aus der Aufmerksamkeit herausnehmen. Also ich denke da an, in der Politik an Aussagen oder Vorgänge wie Verbindungen, also quasi Generierung oder Entstehung von neuen Parteien oder auch Aussagen aller Couleurs, also da geht es jetzt nicht nur um die Veränderungen der BZÖ und der FPÖ, aber eigentlich ist es völlig egal, was diese Parteien oder Personen tun zu dem bestimmten Zeitpunkt, weil wenn sie quasi eine Aktion setzen beim nächsten Zeitpunkt ist das aus der Aufmerksamkeitsspanne einfach weg, obwohl es durchaus nachvollziehbar gewesen wäre, was passiert ist, es hat nur keine Auswirkungen oder Konsequenzen.

Haben Sie noch kurz Zeit?
Wie spät ist es denn?
Dreiviertel fünf.
Ja, ein bisschen.

31) Könnte es sein, dass man sich daran gewöhnt eben, dass solche Daten an die Öffentlichkeit kommen und, dass sich die Toleranzgrenze etwas verschiebt, insofern dass so Dummheiten toleriert werden?
Ja, aber da ist die Frage, was Sie unter tolerieren verstehen und es kommt eben darauf an, was Sie als Konsequenzen daraus ziehen.
Zum Beispiel, wenn ich Partyfotos im Netz habe von einer Person und der Arbeitgeber sieht die…
Ja, aber es wird nicht mehr, also das ist, glaube ich, dann sehr individualisiert. Also wenn Sie einen Arbeitgeber haben oder die Person, die das dann letztendlich entscheidet, die das außerhalb seiner oder ihrer Toleranzgrenzen sieht, werden sie einfach schlichtweg ein Pech haben und Sie werden der Person nicht vorwerfen können, dass sie die Partyfotos gesehen hat. Gesamtgesellschaftlich ist das wieder etwas anderes. Wenn man vom HC Strache Fotos aus seiner Jugend sieht, wo er angeblich nur Paintball spielen war, obwohl man andere Symbole sieht, die eindeutig auf eine rechtsradikale Wehrsportübung Rückschlüsse ziehen lassen, kommt er damit gesellschaftlich offensichtlich durch. Aber am Einzelfall kann man es, glaube ich, nicht festmachen, also an dieser Eins-zu-Eins-Geschichte.

32) Ja, eigentlich auch schon die Abschlussfrage, ob Ihnen noch irgendein wichtiger Aspekt fehlt, der vielleicht im Interview zu wenig angesprochen wurde?
Nur zum Schluss noch, Sie haben mich darauf aufmerksam gemacht, auf die Disziplinargesellschaft von Foucault.
Genau, stimmt, aber das ist sehr schwierig in eine Frage zu fassen.
Nein, weil da wollte ich Sie nur darauf hinweisen, da gibt es von Deleuze einen Antworttext, später entstanden, der heißt Kontrollgesellschaft oder Übergang zur Kontrollgesellschaft. Der, also ich bin jetzt kein Anhänger der Postmoderne und auch nicht des Deleuze im Speziellen, aber der doch recht schön herausarbeitet, dass die Disziplinarinstitutionen, wie sie da Foucault beschreibt, ihre Entstehung und ihre Veränderung, abgelöst werden oder zumindest ergänzt werden um eine Kontrollgesellschaft und ich habe schon den Eindruck, dass wir uns in diese Richtung bewegen. Also quasi es ist nicht nur notwendig, dass Sie Institutionen haben, die auf Sie aufpassen oder die Sie in einem Rahmen halten, sondern wir kontrollieren uns schon gegenseitig und das macht, glaube ich schon, einen Veränderungsprozess mit uns, und was wir bereit sind weiterzugeben oder zu sagen oder zu tun, aus.
Aber das sagt eh Foucault schon so ähnlich oder, dass wir uns selber disziplinieren und selber überwachen, ein Anpassen an die Norm irgendwie?
Ja.

33) Könnte man das noch irgendwie auf das Internet umlegen?
Auf Internet, naja, ich meine. Also ich glaube, dass wir noch nicht den Umgang gefunden haben oder wir wissen noch nicht, was die Norm ist mit dem Umgang mit dem Thema Internet und das ist aber auch die größte Gefahr, weil jede bisher eingesetzte, neue Techologie und letztlich ist das Internet eine Technologie hat auch quasi seine Schattenseiten, die auch in der einen oder anderen Form zu bisher, und da wird das Internet nicht zu einer globalen Katastrophe werden, weil das hat der Joi Ito bewiesen, dass es manchmal auch nur die Angst vor dem Problem ist, die das Problem ist. Aber egal, welche Hochtechnologie sie hatten in den letzten hundert Jahren und das ist der Zeitraum, wo die meisten Hochtechnologien entstanden sind, gab es auch immer eine entsprechende Katastrophe, also von Tschernobyl über kleinere Störfälle in der Atomtechnologie bis zu jetzt schon, eh schon vorhandenen Datenfehlern oder quasi wo Daten eben verloren gegangen sind oder wo Daten an die Öffentlichkeit gegangen sind, die nicht hätten sein sollen bis zu Manipulationsversuchen oder Hacks auf ganze Staaten, also quasi ich glaube, Estland war das oder Lettland, die da angegriffen worden sind als Gesamtes. Also da tut sich Einiges, das wir einfach noch nicht abschätzen können oder wo wir noch nicht die Grenzen kennen, sowohl positiv als auch negativ. Und das ist aber in jeder Technologie so. Von dem

lebensbedrohenden Aspekt habe ich da eigentlich eher mehr Angst vor den ganzen Biotechnologien, die da noch auf uns zukommen als vor dem Internet.
Gentechnik usw.?
Ja aber auch also die ganze Nanotechnologie und eigentlich dieser ganze Biotech-Bereich, der meiner Meinung nach noch weniger durchschaubar ist und noch weniger transparent ist als das Internet, weil das eigentlich dafür wiederum sehr viel Transparenz gibt.

Vielen herzlichen Dank!
Bitte sehr.

Interview mit Gregor König

Datum: 9. Februar 2010

Ort: sein Büro bei der Datenschutzkommission

Dauer: ca. 45 Minuten

1) Das wäre jetzt eh gleich auch die erste einleitende Frage, dass Sie sich kurz vorstellen und ihr Forschungsgebiet oder Arbeitsgebiet, ein bisschen beschreiben könnten?
Ja, wie gesagt, meine Funktion habe ich gerade beschrieben. Die Datenschutzkommission selbst ist die nationale Kontrollstelle im Datenschutzbereich. Das Datenschutzgesetz 2000, das den österreichischen Datenschutz eben, mehr oder weniger darstellt, ist eine Umsetzung der Datenschutzrichtlinie von 1995 und in der Richtlinie wird eben vorgeschrieben, dass die Mitgliedstaaten eine unabhängige Kontrollstelle einrichten müssen und diese unabhängige Kontrollstelle ist in Österreich eben die Datenschutzkommission. Wir sind zwar, sie merken das auch hier anhand des Gebäudes, rein dienstlich in das Bundeskanzleramt eingebunden, sind eine Abteilung des Bundeskanzleramtes, sind aber inhaltlich vollkommen unabhängig und der Entscheidung der Datenschutzkommission pfuscht sozusagen niemand hinein, also inhaltliche Unabhängigkeit. Unsere Aufgaben sind einerseits wirklich förmliche Beschwerdeverfahren, wo jemand eine durchsetzbare Entscheidung, einen Bescheid bekommt bei Rechtsverletzung durch Auftraggeber des öffentlichen Bereichs, also Behörden, also die Trennung streng öffentlichen Bereichs, also Verletzungen durch behördliche Auftraggeber und dann der private Bereich also sprich Privatleute, Firmen usw. Das ist eigentlich, wenn es um die recht- um die förmliche Entscheidung geht, eine gerichtliche Zuständigkeit. Hier gibt es aber bei der Datenschutzkommission ein so genanntes Ombudsmannverfahren. Die Leute können sich an uns wenden und können sagen: „Ich habe ein Problem“, zum Beispiel in Bezug auf Social Networks oder was auch immer, auch im privaten Bereich eben, und wir versuchen hier in diesem Verfahren, das ist der Sinn des Verfahrens, den rechtsmäßigen Zustand herzustellen. Also wenn es darum geht, dass jemand das Problem hat, dass seine Daten nicht gelöscht werden, obwohl die gelöscht werden müssten, dann versuchen wir das herzustellen. Wir können in solchen Verfahren aber nur so genannte Empfehlungen aussprechen, wir können also keine rechtsförmliche Entscheidung, die irgendwie exekutierbar wäre, aussprechen. Das wäre eben die gerichtliche Zuständigkeit. Und diese Empfehlungen, die haben eben, wie der Name schon sagt, keinen rechtsverbindlichen Charakter, sondern Empfehlungen sind halt eben etwas, doch mit einem gewissen starken Druck, auch im Hinblick natürlich auf gewissen öffentlichen Druck, den man immer erzeugen kann, aber etwas was grundsätzlich nur ganz bestimmte Rechtsfolgen nach sich zieht, wo dann die Datenschutzkommission zwar auch ein Klagerecht hat, aber in erster Linie ist es dann natürlich schon die Aufgabe der Betroffenen, das mehr oder weniger selbst in die Hand zu nehmen, dass sie eben zu Gericht gehen müssen.
Das Problem ist bei Gericht habe ich natürlich die Kosten, die ich tragen muss oder das Kostenrisiko, das ich halt habe, wenn ich unter Umständen den Prozess verliere. Das habe ich bei der Datenschutzkommission nicht, unsere Verfahren sind alle kostenlos. Es gibt zwar gewisse Eingabegebühren, sind aber nicht jetzt für diese Verfahren, aber für andere Verfahren, sind aber ein paar Euro, also das ist nicht wirklich etwas, was sehr viel ist.
Dritte Sache ist: Wir sind das so genannte Datenverarbeitungsregister, das ist bei uns beheimatet, das hängt zusammen, dass in Österreich alle Datenanwendungen, das ist ein Begriff aus dem Datenschutzrecht, grundsätzlich gemeldet werden müssen. Es gibt zwar bis Ausnahme von der Meldung, so genannte Standardanwendungen zum Beispiel, ja, aber grundsätzlich gilt, jede Datenanwendung ist zu melden und dann gibt es noch andere Verfahren wie zum Beispiel Verfahren betreffend des internationalen Datenverkehrs bei uns und natürlich die internationale Arbeit. Wir sind auch vertreten in verschiedenen Gremien auf EU-Ebene, weil eben Datenschutz grundsätzlich ein von der EU ausgehendes Rechtsgebiet ist, was ja auch sehr viel Sinn

macht. Daten machen nicht vor den Grenzen Halt, sondern es ist ja halt ein zunehmendes internationales Kapitel und da haben wir natürlich auch einen gewissen Anteil an internationaler Arbeit. Das sind sozusagen unsere Arbeitsgebiete mal kurz beschrieben.

2) Vielen Dank. Der erste Block wäre eben Privatsphäre und Daten. Da will ich fragen, welche personenbezogenen Daten sind sensibel und welche würden Sie als sensibel beschreiben?
Also, aus unserer Arbeit wissen wir, dass Personen, zum Beispiel wenn sie an uns herantreten, oftmals irgendwelche Daten als sensibel bezeichnen, weil sie aus ihrer eigenen subjektiven Sicht sehr sensibel sind, Bankdaten, und so weiter und so fort. Das Datenschutzgesetz definiert aber diese sensiblen Daten ganz genau. Es gibt eine Definition im §4 Ziffer 2, da sind die sensiblen Daten definiert, die werden genau aufgezählt und alles, das was dort steht, ist sensibel und was nicht dort steht, ist nicht sensibel. Also zu den sensiblen zählen zum Beispiel eben nicht, gegen landläufiger Meinung eben, die Bankdaten oder die Kontodaten zum Beispiel, aber eben dazu zählen die Gesundheitsdaten, die Daten über die ethnische und rassische Herkunft, wie es so schön heißt, lustigerweise über die Gewerkschaftszugehörigkeit, über die Religion, ja, über die Sexualität. Das sind Daten, die zu den sensiblen Daten zählen. Sie finden übrigens das Datenschutzgesetz, wenn ich irgendwelche Paragraphen erwähne und Sie wollen das nachlesen, finden Sie das auf unserer Webseite hier auch abrufbar.
Also das heißt, sensible Daten sind genau vom Gesetz definiert , ist nicht etwas was sozusagen im subjektiven Betrachten des jeweils Einzelnen steht, wobei natürlich, na klar, auch versteht oft, dass die Leute halt einfach auch bei bestimmten Daten, etwas ja sozusagen ein erhöhtes Aufmerksamkeit oder erhöhtes Augenmerk darauf haben, das ist ganz klar, ja.

3) Ist das jetzt nur im Datenschutzgesetz geschützt oder gibt es noch etwas darüber hinausgehend?
Na ja, sozusagen das Grundrecht auf Datenschutz, das ja im §1 Datenschutzgesetz geregelt ist, das eben ein im Verfassungsrang stehendes Recht ist, ist natürlich die eine Sache. Daneben können auch noch andere Rechte hinein spielen, man hat natürlich, also gerade was zum Beispiel Bankdaten betrifft, ja, also unter Grundrecht auf Datenschutz stehen ja sowohl die normalen Daten als auch die sensiblen Daten, also beide Datenkategorien stehen da darunter. Das heißt jetzt nicht, dass normale Daten nicht geschützt sind, aber die sensiblen Daten stehen unter einem besonders hohen Schutzniveau, nochmals über dem normalen Schutzniveau.
Und eben neben dem Datenschutzrecht kann es natürlich noch Rechtsansprüche aus anderen Gesetzen geben, zum Beispiel das Bankgeheimnis oder die ärztliche Schweigepflicht, also das heißt, diese Rechte bestehen noch immer parallel. Das Datenschutzrecht sticht da nicht irgendein anderes Gesetz oder ein anderes Rechtsgebiet aus. Das ist parallel zu sehen.

4) Also die Daten, sensible Daten sind ja besonders schutzwürdig. Meine Frage: Warum geben wir sie dann freiwillig her? In Social Networks zum Beispiel findet man oft Angaben über sexuelle Präferenzen usw.
Na ja, das ist, glaub ich genau auch der Grund, warum wir die Initiative mit der Broschüre gestartet haben [Herr König meint die Broschüre *Datenschutzkommission/Bundesministerium für Unterricht, Kunst und Kultur/saferinternet.at (2010): DU bestimmst… Datenschutz - Fakten und Gefahren, Wien.*, die er mir zuvor ausgehändigt hatte, Anmerkung D. R.], weil Personen ganz allgemein, aber insbesondere Jugendlichen einfach die Tragweite der Handlung nicht bewusst ist und die geben das gerne her. Ja, auch in dem Gedanken jetzt sozusagen, ich teile es ja nur meinem Freund mit oder meinem Freundeskreis oder ich mach halt dieses und was jetzt da ganz modern ist, sind irgendwelche Nacktvideos, die ich reinstelle und zeige das aber nur meinen drei Freundinnen oder wie auch immer und sonst niemandem, aber eben dass ich dann unter Umständen das Video ganz woanders finde, das ist den Leuten dann ja nicht bewusst. Was uns ein Anliegen ist mit der Broschüre, ist einfach hier, diese Bewusstseinsmachung. Ich glaube, wenn man wirklich aufklärt, was mit den Daten alles passieren kann, dann würden die Leute sie auch weniger hergeben. Also ich glaube das ist wirklich in erster Linie darauf zurückzuführen, dass man einfach nicht weiß, was man damit sozusagen anrichtet und dass man eben vergisst, dass das Internet unter Anführungszeichen eben nie etwas vergisst, sondern dass die Daten halt, wenn sie einmal irgendwo veröffentlicht sind, im Internet auch irgendwo auffindbar sind.
Das Problem ist, und das ist wieder ein rechtlicher Punkt dazu, ist, nach dem österreichischen Datenschutzgesetz ist es so, dass so genannte allgemeine verfügbare Daten, ja, zum Beispiel veröffentlichte Daten, sofern sie rechtsmäßig veröffentlicht worden sind, nicht mehr unter dem Schutz des Grundrechts stehen. Das heißt ich kann dann mit diesen Daten weiter etwas tun. Typischerweise, Beispiel, ist halt einfach, Daten, die im Telefonbuch veröffentlicht sind, also im elektronischen Telefonbuch, könnten zum Beispiel für Marketingzwecke verwendet werden, obwohl das eigentlich gar nicht der ursprüngliche Zweck war. Hier gibt es aber auch schon Gedanken in Richtung einer Reformierung. Es gibt jetzt seit kurzem die DSG-Novelle 2010. Da war auch der Gedanke schon drin, dass man diese veröffentlichten Daten einfach ein bisschen mehr schützt und nicht sagt: „Einmal veröffentlicht rechtsmäßig, dann passt das schon“, sondern dass man das auch an den ursprünglichen Veröffentlichungszweck knüpft und sagt: „Okay, für diesen Zweck dürfen die Daten noch weiter verwendet werden, aber nicht für andere Zwecke.“ Das wäre vielleicht auch einmal ein Punkt, aber

das ist in der derzeitigen gesetzlichen Regelung nicht so, das ist leider in den Entwürfen zwar drinnen gewesen, ist aber dann im Endeffekt im Gesetz nicht enthalten.

5) Das heißt aber dann, es ist schon erlaubt, zum Beispiel, dass Adresshändler zehntausende Internetadressen von irgendeiner anderen Firma kaufen?
Ja, prinzipiell schon. Eben der Adressverlag, also, oft kommen auch Leute zu uns und sagen: „Gottes Willen, was passiert denn da, das ist ja was ganz Dubioses." Man muss aber auch dazu sagen, sowohl der Adressverlag, also die, der mit Adressen handelt, als auch das Direktmarketingunternehmen, das also Leute anschreibt mit dieser persönlich adressierten Werbepost, also nicht Postwurfsendung, sondern wirklich persönlich adressierte Werbepost, das sind zwei in der Gewerbeordnung definierte Gewerbe, ja, das heißt, es ist nichts Dubioses an sich. Dass es in dieser Branche natürlich schwarze Schafe gibt, ist ganz klar. Dass in dieser Branche unter Umständen prozentuell mehr vertreten sind, ja, liegt auch daran, dass natürlich da eben nicht jetzt unbedingt mit Gütern gehandelt wird, sondern mit Daten und da kann man natürlich manchmal auch entsprechend mehr Schindluder treiben, ja. Aber grundsätzlich sind das so Gewerbe, die auch rechtlich anerkannt sind, ja.

6) Würden Sie sagen, dass die Daten, die wir im Internet hinterlassen, also einen digitalen Fußabdruck bilden?
Na ja, das ist eine interessante, glaube ich, gesellschaftspolitische Frage, weil die Frage ist natürlich, in welcher Gesellschaft leben wir heute und welche technischen Möglichkeit gibt es, um eben Daten zusammenzuführen. Das ist halt heute schon etwas ganz anderes als es vielleicht war 1995, als die Datenschutzrichtlinie von der EU erlassen wurde, die dann eben mit dem Datenschutzgesetz 2000 umgesetzt worden ist. Die damalige Landschaft ist eben von so einzelnen Datenbanken und so weiter ausgegangen und die hat man dann halt gemeldet und da hat man dann jede einzelne Datenbank überprüfen können, ja.
Die heutige Landschaft, ja, ist eine totale Vernetzung. Daten schwirren um die Welt herum. Man weiß nicht, wo werden die Daten tatsächlich verarbeitet. Man weiß nicht, was passiert mit den Daten oder man weiß nicht, es ist zum Teil schwer durchschaubar. Die technischen Möglichkeiten, sagen wir mal so, gingen in die Richtung, dass sich halt in Zukunft natürlich, ja, über Personen Profile, oder man einen wirklichen Fußabdruck eben machen kann. Das sind die Gefahren. Ich meine, man sieht das heute an Suchmaschinen. Sie kennen vielleicht *123people*, wo das ja, wo ja auch eigentlich nichts Anderes, zumindest einmal, an sich nichts Rechtswidriges gemacht wird, sondern es werden die veröffentlichen Daten, die rechtmäßiger Weise veröffentlicht sind, zum Teil von der Person selbst, zum Teil einfach, weil man im Telefonbuch drin steht, durch eine Echtzeitsuche zusammengefasst und aber halt eben, und das ist der Unterschied zu bisherigen Suchmaschinen, irgendwie strukturiert dargestellt wird, also man bekommt also gleich irgendwie so ein Bild von der Person oder zumindest von mehreren Personen des gleichen Namens, ja, weil im Endeffekt wird ein Namenspaar abgefragt und nicht eine Person. Das heißt, es geht in die Richtung. Das sind die großen Gefahren, und wir sehen das, das sind die Herausforderungen auch, in erster Linie durch einen Gesetzgeber, in zweiter Linie auch durch uns als Behörde natürlich hier entsprechende Vorkehrungen zu schaffen, dass das nicht so weit kommt. In erster Linie, wie gesagt, ist eine Aufgabe des Gesetzgebers hier Schranken vorzubringen, das heißt, einerseits was den Datenzugriff betrifft, also Datensicherheitsmaßnahmen und andererseits natürlich auch was eben diese Zweckbindung angeht, dass die Datenschutzrechte auch immer dieser Zweckbindungsgrundsatz, wir haben auch vorher schon darüber gesprochen. Das ist eben ein sehr wichtiger Grundsatz, einfach auch.

7) Können Unternehmen das namentlich zuordnen, die Datenspuren, die wir hinterlassen, also *Google*-Einträge zum Beispiel, Sucheinträge oder…?
Na ja, also, es wird nur dann datenrechtschutzrechtlich interessant, wenn das möglich ist, ja, weil sofern sie nur reine statistische Daten haben, ist es datenschutzrechtlich unproblematisch, weil das Datenschutzrecht knüpft an den Begriff der personenbezogenen Daten an, ja, und dazu muss eine Person zumindest bestimmbar sein. Es heißt jetzt nicht, dass der Name vorliegen muss, weil wir ja zum Beispiel auch nach ganz einhelliger Judikatur, und dann noch jetzt abgebildet durch die neuen Regelungen zur Videoüberwachung, Bilddaten als personenbezogene Daten ansehen. Da steht ja typischerweise kein Name dabei, aber die Person ist bestimmbar. Sofern eben diese Datensätze für Unternehmen auf eine bestimmte Person hinweisen, ohne auch dass der Name genannt ist, sind es personenbezogene Daten. Dann wird es datenschutzrechtlich interessant, dann kommt das DSG zur Anwendung.
Telefon beginnt zu läuten
Also zum Beispiel bei Mitarbeitern wird das typischerweise öfter der Fall sein, ja, weil die kenne ich halt als Unternehmer, als zum Beispiel bei Kunden oder bei ganz fremden Personen, also wenn man das beim Bilddaten- oder Videoüberwachungsbeispiel hernimmt.

Kurze Telefonunterbrechung

8) Vielleicht könnten Sie eine kurze Prognose geben, welche Daten vielleicht noch kommen werden. Werden wir unsere Gene hineinstellen um zu zeigen, dass wir gute Gene haben?
Prognose ist ein bisschen schwierig, aber was sozusagen jetzt wirklich im Kommen ist, sagen wir so, es läuft ja meistens so, dass irgendwie Technologie sich verbessert, und dass wir mit diesen technologischen Verbesserungen zweifelsfrei Vorteile haben in irgendeine Richtung, aber dass dadurch eben, aus datenschutzrechtlicher Sicht auch immer mehr Daten generiert werden. Was jetzt zum Beispiel interessante Themen sind, sind natürlich die biometrischen Daten. Das ist ganz klar. Das ist so eine Richtung, in die es geht, wo man, natürlich klar, gewisse, gerade aus Sicherheitsaspekten, Vorteile sieht, wo man aber immer aufpassen muss halt, inwieweit man diese Daten denn verwenden kann. Da sind wir natürlich im Bereich der sensiblen Daten drin und da sind natürlich besonders hohe Verwendungsbeschränkungen gegeben oder bzw. auch nur ganz bestimmte Gründe, warum oder wann ich diese Daten überhaupt verarbeiten oder verwenden darf, ja. Also die biometrischen Daten sind ein wichtiger Punkt, ja.
Dann etwas, was natürlich auch schon in den letzten Jahren sehr stark hervorgekommen sind, sind die Daten über die Bonität eines Menschen. Bonitätsprüfungen, die mittlerweile sehr üblich sind, wann immer ich irgendetwas auf Rate kaufe, ja. Das beginnt beim Fernseher, den ich irgendwo kaufe auf Rate, oder beim Auto. Da gibt es natürlich, das ist natürlich auch die Aufgabe der Behörde in der Verhältnismäßigkeitsprüfung, immer abzuwägen, die legitimen Interessen eines Gläubigers, der natürlich wissen möchte, ob ein Schuldner seine Schulden, die er hier eingeht, zurückzahlen kann, ist ganz klar, aber auf der anderen Seite noch immer das Geheimhaltsinteresse des Schuldners an seinen Daten. Diese Interessensabwägung ist halt oft eine schwierige, ja. Da würden wir uns als Behörde natürlich immer wünschen, dass der Gesetzgeber einfach eine klare Regelung trifft, ja. Sonst muss man das halt natürlich etwa in der Verhältnismäßigkeitsprüfung, die man ja im Rahmen des Grundrechts bei privaten Auftraggebern machen kann, muss man da eben werten, welche Interessen sind da überwiegend. Das ist aber eigentlich, streng genommen, eine Einzelfallprüfung, ja. Nur kann man das nicht für jeden einzigen Fall eine Bonitätsprüfung machen, nicht. Das ist halt immer das Problematische dahinter. Aber auch hier, ganz klar, diese Bonitätsprüfungen, so genannte Kreditauskunfteien, ist auch wiederum ein von der Gewerbeordnung anerkanntes Gewerbe.
Das sind so Dinge, aber was sozusagen dann in weiterer Zukunft noch kommen kann, wage ich jetzt gar nicht irgendwie... Da müssten Sie mal so richtig Techniker, die so, wirklich up to date sind, die können wirklich sagen, welche Daten generiert werden können.

9) Ja, zum Beispiel bei *Google*, da gibt es ein Service *23andme*, da kann man irgendwie Gen-Prüfungen machen und veröffentlichen. Ist das legal, oder..?
Na ja, bei Google ist es halt so, dass die sozusagen außerhalb unseres Zuständigkeitsbereichs liegen, aber wäre es zum Beispiel jemand in Österreich, der so was anbieten würde, na ja, legal ist es solange ich, das ist ja auch wiederum ein wichtiger Grundsatz im Datenschutzrecht eben, die, in Deutschland nennt man es so, beschreibt es aber ganz gut, das *Informationelle Selbstbestimmungsrecht*, das heißt, solange ich die Zustimmung gebe, was mit meinen Daten passiert ist und diese Zustimmung eine ordentliche ist, sprich ich bin genau aufgeklärt, was passiert mit den Daten, ja, ist es aus datenschutzrechtlicher Sicht nicht problematisch. Genauso auch hier, wenn ich die Zustimmung gebe, die Gen-Daten dürfen in irgendeiner Form erhoben werden, verarbeitet werden, das Ergebnis wird mir zurückgeliefert, dann ist es okay. Problematisch sind dabei zwei Dinge, nämlich oftmals sind die Zustimmungserklärungen nicht wirklich sauber ausgeführt und manchmal werden sie vielleicht auch überschritten, dann bin ich natürlich in einem rechtswidrigen Bereich. Und das Zweite ist, im Datenschutzrecht ist diese Zustimmung auch, anders als zum Beispiel jetzt im Vertragsrecht, wo wenn ich eine Zustimmung gebe, also einen Vertrag eingehe, ich nicht einfach dann fünf Minuten später sagen kann, ich mache diesen Vertrag einfach nicht mehr. Im Datenschutzrecht ist die Zustimmung jederzeit widerruflich, das heißt, wenn dann jemand eine Zustimmung zum Beispiel zur Verwendung von Daten für Marketingzwecke: Ich möchte wirklich, ich stimme zu, dass ich auch vom folgenden Unternehmen Werbung bekomme. Wenn ich das widerrufe, ist ab diesem Zeitpunk natürlich die Verwendung der Daten für diesen Zweck nicht mehr erlaubt. Das ist immer auch das Problem dabei, nicht.
Solange wie gesagt solche Phänomene sich auf die Zustimmung des Kunden stützen, ja, ist es datenschutzrechtlich nicht so problematisch. Schwierig wird es dann, wenn hier sozusagen die Unternehmen auf diese Daten zugreifen, ohne in irgendeiner Form die Kunden darüber informiert zu haben bzw. die Zustimmung eingeholt zu haben. Solange es dazu nicht irgendwelche gesetzlichen Regelungen gibt, was es für diese Gentests wahrscheinlich nie geben wird, aber für andere Dinge ist es natürlich schon denkbar.

10) Gibt es im österreichischen Recht ein entsprechendes Gesetz für die informationelle Selbstbestimmung?
Das ist eben, das ist sozusagen, es ist ein Begriff aus dem deutschen Recht, aber er stimmt auch eins zu eins für das österreichische Recht, ja, weil eben durch das Grundrecht auf Datenschutz wird es ja ausgedrückt und es ist ja auch im Wesentlichen, wenn Sie sich im Datenschutzgesetz einerseits den §1, wo das Grundrecht geregelt ist, aber andererseits auch die §§ 8 und 9 ansehen, ja, dann werden Sie sehen, dass dort die Zustimmung als Rechtfertigungsgrund immer vorkommt, ja, und damit ist einfach das ausgedrückt, das heißt

eben nur bei uns nicht so in der Judikatur und in der Literatur, aber in Deutschland heißt das so. Das ist im Wesentlichen eh das Datenschutzgesetz.

11) Als nächster Block würde ich zur Überwachung gerne fragen: Denken Sie, dass es einen Unterschied macht, dass wir Daten freiwillig hergeben und ins Internet stellen oder gibt es sowieso anderweitige Methoden der Datenerhebung von staatlicher Seite, unternehmerischer Seite?
Ich glaube, dass im Wesentlichen Unternehmen, aber auch der..., also Unternehmen sind sicherlich auf die Freiwilligkeit der Kunden angewiesen, ja. Unternehmen erheben ja Daten für verschiedenste Zwecke. Grundsätzlich zum Beispiel werden ja Daten zunächst erhoben, wenn ich einen Vertrag mit einem Unternehmen eingehe, brauche ich gewisse Daten, Geschäftsanschrift usw. oder Handschrift und Kontodaten, um den Vertrag zu erfüllen. Für diesen Zweck, Vertragserfüllung, dürfen die Daten auch verwendet werden. Gibt es auch eine eigene Rechtfertigung sozusagen im DSG.
Wenn ich Daten aber für einen anderen Zweck verwende, ich möchte jetzt zum Beispiel das auch irgendwie generieren für Marketingzwecke und schauen: „Aha, den Kunden könnte das Buch auch noch interessieren", und dann schreibe ich ihn an, dafür brauche ich wiederum eine eigene Rechtfertigung im Datenschutzgesetz und das bietet mir im Wesentlichen dann nur die Zustimmung und die ist wie gesagt wieder jederzeit widerruflich. Das heißt ich muss dann immer auch schauen, für welchen Zweck sind die Daten hier drinnen und gerade für so Marketingzwecke sind das natürlich alles Daten, die sozusagen freiwillig von Kunden preisgegeben werden in irgendeiner Form. Bei einem Unternehmen einmal, wo ich vielleicht bei irgendeinem Gewinnspiel mitgemacht habe, aber dann diese Zustimmungserklärung noch zusätzlich unterzeichnet habe und da ist aber dann drinnen gestanden auch, dass diese Daten an ein Direktmarketingunternehmen weitergeleitet werden, dann bekomme ich plötzlich Post von einem Direktunternehmen und weiß jetzt gar nicht woher das kommt. Es kann aber nur rechtmäßiger Weise auf solchen Zustimmungen beruhen.
Von staatlicher Seite ist es ähnlich, nur halt hat der Staat natürlich aufgrund gesetzlicher Vorschriften gewisse Befugnisse, Daten zu erheben, aber auch wiederum für einen bestimmten Zweck, der in diesen Fällen natürlich gesetzlich vorgeschrieben sein muss. Die Daten, die sozusagen im Melderegister stehen zum Beispiel, die sind ja für einen bestimmten Zweck dort drin und die Daten, die im Firmenbuch oder im Grundbuch stehen, sind für einen bestimmten Zweck. Außerhalb dieser Zwecke, darf ich diese Daten nicht verwenden. Ich meine Firmen- und Grundbuch sind schlechte Beispiele. Das sind ja natürlich öffentliche Datenbanken, ja, aber denkt man zum Beispiel an die Daten bei den Sozialversicherungen. Die sind zu für einen ganz bestimmten Zweck dort oder auch die Sozialversicherungsnummer selbst dient ja nicht irgendwelchen Zwecken, sondern ganz bestimmten Zwecken. Und wenn ich diese Nummer dann für andere Zwecke verwende, dann brauche ich dafür irgendeine Rechtfertigung, die hat aber der Gesetzgeber genau so wenig. Also ich glaube, die Gefahr droht dann eher von Unternehmen, die Daten zum Beispiel jetzt für Marketingzwecke eben heranziehen, wo es keine Zustimmung gibt. Das sind dann die schwarzen Schafe. Überall dort, wo ich eine Zustimmung vorweisen kann, dann war halt der Konsument unvorsichtig zum Teil, ja, oder war es ihm nicht bewusst oder hat er vielleicht wirklich keine Zustimmungserklärung abgegeben und ist halt durchgerutscht unter Anführungszeichen. Das sind jetzt sozusagen die Gefahren der unternehmerischen Seite, ja.

12) Wer kann solche Daten, die wir in Social Networks freiwillig hinterlassen, irgendwie überwachen oder zweckentfremden und für eigene Motive nützen?
Na ja, das kommt auch einerseits auch darauf an, welche Datensicherheitsmaßnahmen die Social Network-Betreiber machen. Aber grundsätzlich muss man sich halt bewusst sein, es gibt ja bei den meisten Social Networks gewisse Privacy-Einstellungen, ja, und ich kann dort zum Beispiel auch, und das ist gerade ein wichtiger Tipp, ich kann dort ja auch einstellen, dass diese Social Network-Profile von Suchmaschinen nicht durchsuchbar sind. Typischerweise muss man ja beim Social Network in irgendeiner Form einmal zunächst Mitglied werden und überhaupt auf die Daten zugreifen zu können. Wenn ich aber das Profil schon so veröffentliche, dass ich sage, mir ist das wurst, ob das von *Google*, *123people*, wer auch immer, durchsuchbar ist, ja, dann habe ich ja plötzlich die Daten wirklich im Netz, ja, und dann ist es natürlich ein Einfaches, auf diese Daten zuzugreifen. Das heißt, einerseits die Datensicherheitsmaßnahmen des Unternehmens, des Betreibers des Social Networks sind wichtig, andererseits aber auch, dass ich auf meine eigenen Privacy-Einstellungen achte, ja, weil dann, kanalisiere ich natürlich die Daten auf den Kanal, der mich interessiert, nämlich meine Freunde oder Bekannte oder wie auch immer, die ich da in diesem Social Network habe.

13) Ein *Futurezone*-Artikel erwähnt so eine Studie, dass nur ein Drittel der Mitglieder ihr Profil nur für Freunde eingrenzt.
Ja, ja, das kann ich mir gut vorstellen. Das liegt wahrscheinlich an zwei Faktoren. Einerseits, dass das die Leute das zum Teil nicht wissen oder nicht richtig sozusagen aufgeklärt wurden. Sei das jetzt, weil sie einfach nicht genau genug schauen auf der Seite selber oder sei das einfach, weil es vielleicht wirklich versteckt ist auf der Seite. Und andererseits natürlich, haben wir den zweiten Faktor, dass es ihnen wurst ist, dass sie halt einfach meinen: „Das ist mir egal. Das kann ruhig jeder sehen, ja." Das muss ja einem auch nicht wirklich unbedingt jetzt etwas Schlechtes bedeuten, nur wenn ich dann halt irgendwelche Partybilder habe, wo ich

sturzbetrunken irgendwo herumhänge und zehn Jahre später bewerbe ich mich für einen Job und der Arbeitgeber sucht halt über *Google*, ja, und findet dann das Foto, ob das jetzt für die Bewerbung hilfreich ist, das ist halt dann die Frage, nicht. Das sind ja die Gefahren, dass man einfach nicht abschätzt, dass eben hier das Internet ein sehr langes Gedächtnis hat.

14) Sind Sie mit vielen solchen ähnlichen Fällen konfrontiert, also dass der Arbeitgeber...?
Nein, also das muss ich ganz ehrlich sagen, das sind also wirklich diese Social Network-Fälle, also sind, beschränken sich auf Anfragen. Wir haben eigentlich selten Probleme, ja, wo wirklich jemand ein gröberes Problem dadurch hatte. Das liegt einerseits daran, dass wie gesagt das eigentlich eine gerichtliche Zuständigkeit wäre, das liegt andererseits daran, dass die meisten Social Network-Betreiber ja nicht in Österreich angesiedelt sind und damit eigentlich die jeweilige Datenschutzbehörde in dem Land sozusagen zuständig wäre und es liegt drittens natürlich auch daran, dass zum Teil die Jugendlichen, die ja hauptsächlich in den Social Networks drin sind, wobei betrifft eigentlich natürlich auch alle, es gibt ja mittlerweile auch sehr viele Erwachsene in Social Networks, dass die zum Teil über die rechtlichen Möglichkeiten auch nicht gut genug aufgeklärt sind. Da ist eben für Jugendliche diese Broschüre gedacht und grundsätzlich, ja. Sonst sind natürlich diese ganzen Verfahrensarten usw., auf unserer Website auch beschrieben, ja, also das kommt sicher noch dazu, ja.

15) Zum Staat nochmals: Kann der solche freiwillig hergegebenen Daten verwenden zu Überwachungszwecken, zum Beispiel Nachrichtendienste, Sicherheitsbehörden?
Also, grundsätzlich kann er, also die reine Möglichkeit hat er natürlich, weil die Daten ja verfügbar sind, nur die Zulässigkeit einer solchen Maßnahme ist sicher nicht gegeben, weil gerade und das ist ja der Unterschied zum Privaten. Beim Privaten kann ich eben eine Verhältnismäßigkeitsprüfung machen, ob die Datenverwendung im Einzelfall gerechtfertigt ist, eben zum Beispiel vorher das mit den Gläubigerinteressen versus Schuldnerinteressen. Der Staat, ja, braucht für jeweilige Datenverwendungen, ja, eine rechtliche Grundlage. Diese rechtliche Grundlage, damit sie eine ordnungsgemäße Grundlage ist, die ja sozusagen ein Eingriff in das Grundrecht bedeutet, ja, muss genau der Zweck auch definiert sein und gerade in dem Bereich, wo wir dann hier sind, also im sicherheitspolizeilichen Bereich oder im strafbehördlichen Bereich, ja, also im Bereich des Sicherheitspolizeigesetzes und der Strafprozessordnung ist das noch viel immanenter, weil es um strafrechtlich relevante Daten geht und grundsätzlich im Sicherheitspolizeigesetz ganz genau definiert, was dürfen die Sicherheitsbehörden machen und welche Datenanwendung dürfen die Sicherheitsbehörden betreiben. Also eine allgemeine Datenbank, wo man sozusagen alles zusammenfangen könnte von jedem österreichischen Staatsbürger, wäre eben nicht zulässig.
Ob das einmal in Zukunft irgendwann einmal, ich meine, das Problem ist ja, dass sich die Gesellschaft so ein bisschen oder die, wie soll ich sagen, also der Datenschutzansatz ein bisschen wandelt von diesem „Ich ermittle Daten von einem Verdächtigen“, ja, zu hin „Grundsätzlich sind einmal alle potenziell Verdächtige und daher speichere ich einmal alle Daten, ich könnte sie ja einmal brauchen.“ Stichwort Vorratsdatenspeicherung und die Vorratsdatenspeicherung ist eben genau das zweitere Konzept und das ist eigentlich natürlich das, was aus datenschutzrechtlicher Sicht ja sehr skeptisch gesehen wird, ja, und da werden ja wirklich sozusagen Daten auf Vorrat gespeichert. Das geht ein bisschen in diese Richtung, aber dann muss man eben vorsichtig sein, dass es eben nicht zu weit in diese Richtung geht. Die Umsetzung wird jetzt gerade in Österreich diskutiert, aber meines Wissens wird eben auch jetzt überhaupt auch auf europäischer Ebene nochmals diskutiert, ob man nicht diese Richtlinie zurücknehmen will, aufgrund derer, die Staaten verpflichtet sind, dies umzusetzen.

16) Also, das heißt der Staat greift nicht oder wenig auf die Profile zurück, die wir selber erstellen?
Kann ich mir nicht vorstellen. Im Wesentlichen wird auf solche Daten dann zurückgegriffen, wenn ich als Strafverfolgungsbehörde, ja, keine Ahnung, dann werde ich natürlich, also als Strafverfolgungsbehörde einen bestimmten Sachverhalt prüfe, ja, eine bestimmte, ein bestimmtes strafrechtliches Vergehen oder mögliches strafrechtliches Vergehen und dann schau ich natürlich schon, dann werden wahrscheinlich Ermittler das schon so machen, dass sie auch auf so veröffentlichte Daten zugreifen. Nur die, die das, wie soll man sagen, die so typischerweise strafverdächtig sind, sind wahrscheinlich weniger in Social Network-Profilen unterwegs, ja, also aber grundsätzlich kann man sagen: Nein. Der Staat macht das nicht, nein.

17) Und wirtschaftliche Unternehmen, warum verwenden die so oder was können die mit den Daten anfangen?
Na ja, die wirtschaftlichen Unternehmen, wenn sie eben so veröffentlichte Daten haben, oder die Zustimmung haben, ja, für die Verwendung. Dann geht es natürlich meistens um Marketing, das ist natürlich, weil dafür haben die Daten dann tatsächlich einen Wert, ja, und das merkt man auch daran, dass Datensätze auch gehandelt werden. Also dann müssen sie auch natürlich einen pekuniären Wert haben im Wirtschaftsleben, ja, und je genauer, ja, die Daten sind und je echter und richtiger die Daten sind, nicht nur reine Spekulation. Es gibt ja auch vielfach immer so Berechnungen, das heißt, ganz interessant, also zum Teil, also wirklich Wahrscheinlichkeiten gibt, dass aufgrund des Vornamens einer Person man einschätzen kann, welcher

Alterskategorie sie zuzuordnen sind. Also, solche Berechnungsmethoden gibt es zum Teil, ja. Dass jemand, der zum Beispiel Aloisia heißt, nicht 1990 geboren ist, sondern sehr wahrscheinlich eben 1920, ja, und damit in dieses Alter, zwischen 1920 und 1930 geboren, fällt. Das wären sozusagen Daten, die zwar schon ganz gut sind für solche Marketingzwecke, aber natürlich ist es den Unternehmen lieber, sie haben sozusagen ein möglichst vollständiges Bild, weil umso mehr ist dieser Datensatz natürlich wert. Das ist sozusagen das, was die Unternehmen damit anfangen. Man braucht auch nicht glauben, wann überall man irgendwo freiwillig mitmacht oder vielleicht irgendwie was bekommt, ja, und dafür seine Daten preisgibt, dass das eben nie ohne Gegenleistung basiert, sondern die Gegenleistung sind halt die Daten, weil die Daten eben für die Unternehmen auch einen Wert haben.

18) Wer wertet dann diese Unmengen an Daten aus, stehen da Menschen dahinter oder geschieht das schon alles automatisch?
Also, ich glaube mittlerweile können das Menschen nicht mehr auswerten, ja. Also wir haben, gerade bei solchen Dingen, glaube ich das auch nicht, dass das irgendwie Menschen sinnvoller Weise machen können. Wo wir es noch, wo wir es noch, sozusagen händische Auswertungen haben, sind nämlich jetzt nicht jetzt an der Spitze der technologischen Entwicklung sondern wirklich im Breitenfeld, sind Videoüberwachungsanlagen. Da muss wirklich noch ein Mensch rein schauen, weil eben die Software noch nicht so weit ist, dass man eben bestimmte Personen oder ein abweichendes Verhalten schon automatisch erkennen kann, ja. Das wird aber wahrscheinlich in Zukunft auch irgendwann einmal so sein, dass man dann nur noch den Menschen einschaltet, der dann nur noch die Bildsequenzen bekommt, wo ein abweichendes Verhalten zum Normalverhalten gegeben ist, ja. Das ist zum Beispiel etwas, was sicherlich sozusagen in der technischen Entwicklung schon leicht möglich ist, ja. Aber grundsätzlich gerade solche reinen Felder, Datenbankfelder das wird sicherlich alles nur noch elektronisch ausgewertet. Das ist ja auch eine Menge und sonst nicht machbar, also ich wüsste nicht, dass das Unternehmen anders machen.

19) Gibt es schon Kameras eigentlich, die Personen erkennen können?
Also, sozusagen, für die breite Masse noch nicht, aber wir kennen schon sozusagen Kameras, die erkennen können zumindest einmal, dass hier eine Person ist und was diese Person macht, also ob sie dahinschaut oder dort hinschaut usw. Es gibt auch natürlich grundsätzlich Entwicklungen, die in die Richtung gehen, dass natürlich das bewegte Kamerabild einer Person, ja, mit einem Foto einer Person in irgendeiner Datenbank abgeglichen wird, ja. Das ist zum Beispiel aber etwas, was vom Datenschutzgesetz verboten ist, also der Bildabgleich ist zum Beispiel explizit verboten worden in der DSG-Novelle, ja, aber jetzt mal grundsätzlich von der Technologie dahinter, ist es schon sehr weit. Das Problem, das man hat natürlich ist, man braucht immer auf dem Video dann irgendwo eine Frontalansicht von der Person, ja, also soweit dass die Technik, wie man es in manchen Hollywoodfilmen sieht, dass man irgendwo nur so ein Profilbild sieht und dass dann mit hundertprozentiger Wahrscheinlichkeit einer Person, wo man ein Frontalfoto hat, zuordnen kann, das spielt es nicht. Also das hätte ich noch nicht gesehen, muss ehrlich gesagt sagen, aber das ist sicherlich etwas, was in die Richtung geht, dass man natürlich das auch so weit wie möglich automatisieren möchte.

20) Denken Sie, dass Überwachung im Web 2.0 also personalisiert wird, weil eben jeder Zugriff hat auf so Profile und...?
Ja, ich würde das nicht als Überwachung bezeichnen, nicht, aber es gibt dort einfach die Möglichkeit, dass man seine Privatheit ein bisschen verliert, einfach, nicht, wenn man sehr viele Daten preisgibt und das einfach, was man früher nicht gemacht hat, auch mangels Möglichkeit, dass man das jetzt einfach macht und natürlich einen größeren Freundes- oder Bekanntenkreis oder vielleicht auch Freunde von Freunden, nicht, das irgendwie zugänglich macht.
Ich würde es aber nicht als Überwachung bezeichnen, weil da müsste irgendein bestimmter Wille dahinter stehen, das irgendwie wirklich fortlaufend systematisch zu machen. Das glaube ich aber ist nicht jetzt der typische Social Network-User, aber es ist natürlich so, dass man damit etwas öffentlicher wird für seine Freunde, oder für Freunde von Freunden oder wer auch immer dann Zugriff hat. Das ist ja meistens ein recht unbestimmter Kreis.

21) Wird die Privatheit den Leuten weniger wichtig?
Ja, das ist eine interessante Frage. Ich glaube, sie verändert sich einfach, ja, also... Mit Dingen, die man vor 20, 30 Jahren nicht ausgeplaudert hat, hat man heute einfach kein Problem mehr, ja. Das ist bis zu einem gewissen Grad gesellschaftlich bedingt und muss jetzt gar nicht auch negativ sein, aber bis zu einem gewissen Grad kann das natürlich auch dazu führen, dass man einfach jegliche Vorsicht fallen lässt und dass man sozusagen mit seinen Daten verfährt, wie wenn es ihnen überhaupt nicht mehr wichtig wäre. Also es ist, glaube ich, eine gesellschaftliche Veränderung, dass die Privatheit sich verändert und... weniger Wert, glaube ich, wenn Sie jetzt eine Umfrage machen würden und 100 Leute auf der Straße fragen würden, würden glaube ich nicht mehr als 20 sagen: „Es ist mir eigentlich wurst“, sondern ich glaube, dass die meisten sagen würden: „Meine Privatheit ist mir wichtig.“

Ich glaube einfach, dass den Leuten zum Teil, eben wie gesagt, die Bedeutung auch ein bisschen abgeht mit den elektronischen Medien, weil ich halt hier nicht unmittelbar irgendeine Wirkung auf das, was ich, auf die Ursache, die ich setze sozusagen, sehe, ja, sondern die Daten sind halt im Netz und man glaubt halt, sie sind nur dort, wo ich sie hintransportiert habe und nirgends woanders.

22) In der Literatur habe ich jetzt öfter gelesen, es wird eine Überwachungsgesellschaft geben. Würden Sie dem zustimmen?
Also Überwachungsgesellschaft, nein würde ich nicht sagen. Ich würde sagen, wir sind eine Informationsgesellschaft und das ist natürlich auch etwas, worin sich die Gesellschaft in den letzten zehn, zwanzig Jahren stark verändert hat, wo auf der einen Seite legen wir sehr viel Wert über Informationen auf der anderen Seite ist eben auch jetzt mein Glaube, ist es, dass wir natürlich auf die Privatheit auch noch Wert legen. Also wir leben in einer Informationsgesellschaft, in einer Überwachungsgesellschaft leben wir nicht. Man muss aber vorsichtig sein in diese Richtung, weil es natürlich Tendenzen gibt, ja, in Richtung Überwachungsgesellschaft, also zum Beispiel in Großbritannien, in London werden wirklich tausende Kameras auf der Straße betrieben, ja, vom Staat, ja, und das geht schon in eine Richtung Überwachungsgesellschaft. Das ist Gott sei dank in Österreich nie ein Thema gewesen, ist es auch in den nächsten Jahren nicht und wird es hoffentlich auch nie sein, ja, solche Tendenzen zu haben, ja, aber ich glaube in einer reinen Überwachungsgesellschaft leben wir nicht, ja. Wie gesagt, die Vorsicht ist halt gegeben, Vorratsdatenspeicherungsrichtlinien, Fluggastdaten und so weiter und so fort. Das sind Tendenzen, die zum Teil auch von den USA auf uns rüberschwappen, ja.
Aber ich glaube, dass jetzt irgendwie wieder so eine bisschen so eine Zeit gekommen ist, wo man das ein bisschen zurücknimmt auch. Ich meine, das ist alles natürlich auch Folge der Terroranschläge 2001, ja, und der weiteren Terroranschläge, die es dann gegeben hat und da hat man ja immer wieder sozusagen anlassbezogen versucht dem ganzen Herr zu werden, indem man sozusagen jetzt gerade in den USA, eben Tendenzen entwickelt hat, mehr und mehr Daten eigentlich zu speichern und in irgendeiner Form bereit zu halten. Das ist ja, glaube ich, der eigentliche Hintergrund der Überwachungsgesellschaft, dass ich die Daten vorrätig habe, ja, und von dem geht man jetzt schon ein bisschen tendenziell wieder ab, zumindest in Europa, ja. In den USA, kann ich schwer einschätzen, wie da die Überlegungen in Zukunft sind, aber in Europa ist es schon, glaube ich eher so, dass der Datenschutz jetzt doch wieder ein bisschen mehr Aufschwung bekommt.

23) Sehen Sie da Vorteile in der ständigen Datenerhebung?
Na ja, so allgemein kann man das nicht sagen. Das kommt immer auf den bestimmten Kontext an, ja. Also in bestimmten Bereichen ist eine, also sagen wir einmal so, es hat jedes immer zwei Seiten einer Medaille. Wenn ich einen Gesundheitsakt habe, einen chronischen, über den ja auch schon jahrelang in Österreich diskutiert wird, dann hat das sicher sein Gutes, weil sozusagen ich meine gesamten Gesundheitsdaten mehr oder weniger auf einer Karte habe, ja, und der Arzt, zu dem ich hingehe, dem ich das in die Hand drücke, der hat sofort ein Bild von mir, sozusagen. Auf der anderen Seite, wenn diese Daten irgendwo gespeichert sind, besteht immer die Gefahr von Missbrauch. Man kann keine Daten hundertprozentig schützen und das ist halt immer die Kehrseite der Medaille, ja, und ob man dann, für gewisse Dinge das haben möchte oder nicht, ist zunächst einmal eine gesellschaftspolitische Diskussion und in weiterer Folge dann auch eine Aufgabe des Gesetzgebers, das so zu gestalten, dass eben der Missbrauch minimiert wird, ja. Aber so ganz allgemein, grundsätzlich zu sagen, an der Datenerhebung gäbe es irgendetwas Positives, glaube ich eher nicht. Die Gesellschaft war auch vor den Möglichkeiten, die moderne Datenverarbeitung bietet, lebensfähig unter Anführungszeichen, also, es ist nicht unbedingt so, dass man für alles eben eine Datenerhebung braucht oder dass da irgendwie grundsätzlich positive Dinge dahinter wären, aber ich meine, es gibt natürlich immer von allen Dingen, wo Daten erhoben werden, auch Vorteile. Das ist ganz klar.

24) Welche, also was würden die größten Gefahren sein, die davon ausgehen?
Die größten Gefahren sind, dass Daten abgeglichen werden, glaube ich, ja. Also wenn ich sozusagen eine Datenerhebung für einen bestimmten Zweck habe und ich habe dann eine Datenbank, die qualitativ gute Daten für diesen Zweck erhoben hat, ja, auf dem einen Punkt und ich habe eine andere Datenbank, die andere Daten für einen anderen Zweck erhoben hat, ja, dann ist das für sich genommen natürlich auch eine gewisse Gefahr, ja, aber wenn ich dann irgendwo die Möglichkeit habe, diese Daten zusammenzuführen, ja, und dann daraus wiederum neue Daten zu generieren, das sind dann eigentlich die Gefahren, die dann davon ausgehen... Das sind die Dinge, wo man immer frühzeitig beginnen muss, weil Datenabgleich, ja, das sind ja auch Dinge, die jetzt schon passieren, weil genau das ist ja das, was mit den Fluggastdaten passiert. Oder das ist ja das, was mit den Bankdaten passiert oder Stichwort *SWIFT* oder was mit den Vorratsdaten passieren soll, dass eben Daten abgeglichen werden gegen andere Daten, die ich halt erhoben habe. Das ist für sich genommen, ja, ist es jetzt an sich noch nicht so gefährlich, sondern das Problem ist eben dieser Zugriff und wenn die Daten vorhanden sind sozusagen, ist ja auch immer die Missbrauchsmöglichkeit gegeben. Solange ich gar keine Daten erhebe, ist die Missbrauchsmöglichkeit eben nicht gegeben.

25) Als Schlussfrage noch, ob es vielleicht noch irgendwelche Aspekte gibt, die zu wenig angesprochen worden sind?
Nein, ich glaube wir haben alles so im Wesentlichen ganz gut durchgenommen, ja.
Ich würde Ihnen empfehlen, vielleicht auch nochmals, sich sozusagen das Datenschutzgesetz durchzulesen, jetzt nicht das Ganze, aber so die Paragraphen 1 bis 9, da sehen Sie dann im Wesentlichen mal zunächst das Grundrecht und dann sozusagen den grundsätzlichen Hintergedanken, wie prüfe ich die Zulässigkeit einer bestimmten Datenanwendung. Da werden Sie sehen: „Aha bei Gesetzgeber ist eben eine gesetzliche Grundlage erforderlich und für den privaten Auftraggeber gibt es halt noch andere Möglichkeiten, eben diese Verhältnismäßigkeitsprüfung, ja, und das, ja, kann ich noch mitgeben, sonst unsere Website, die kennen Sie wahrscheinlich eh und wie gesagt, wenn sie da irgendwie gerade auch in ihre Arbeit einbauen wollen, irgendwelche Hard-Facts aus der Praxis zu Social Networks, ja, da hilft Ihnen sicher *Saferinternet* weiter, da können Sie den Herrn Magister Jungwirth, heißt der, mit th am Schluss, den können Sie da gerne anschreiben und können Sie auch dem sagen, Sie kommen von mir, ja, der hilft Ihnen sicher gerne weiter, wenn Sie da irgendwelche Daten brauchen. Die haben wie gesagt, jetzt gerade unlängst eine Studie gemacht und haben vielleicht auch noch anderes Material dazu.

Vielen herzlichen Dank
Bitte schön, ja.

Interview mit Gerald Reischl

Datum: 9. Februar 2010

Ort: Büro im Kurier; ein zweiter Journalist arbeitet am Schreibtisch daneben, er hat Kopfhörer auf, achtet nicht auf uns

Dauer: ca. 42 Minuten

1) Bei der ersten Frage würde ich Sie bitten, dass Sie sich kurz vorstellen und Ihren Forschungs- oder Arbeitsbereich erklären?
Gut, ich bin Magister Gerald Reischl, ich bin Ressortleiter *Kurier* des Ressorts Digital, zuständig für alles Technische, was berichtet wird im *Kurier* von USB-Mikros bis Internet, bis Web 2.0, bis Hardware, Flat-TV, Handy und so weiter und so fort, nicht nur für die Tageszeitung *Kurier*, sondern auch für den *Online-Kurier* und auch für *TV-Woche* mit *Techno* und Beilagen und, ja daneben bin ich auch Buchautor dreizehnfacher, und befasse mich halt mit den Themen Privatsphäre, Überwachung seit 1998 , seit meinem ersten Buch *Im Visier der Datenjäger*.

Kurze Telefonunterbrechung

2) Welche Daten würden Sie als sensible beschreiben?
Sensible Daten sind personenbezogene Daten und personenbezogene Daten sind meines Erachtens Religionsbekenntnis, Alter, natürlich auch der Name in manchen Bereichen und alles, was im Prinzip über, ja, das sind sensible Daten. Sensible Daten sind aber auch Gesundheitsdaten, Gesundheitsinformationen über mich selber. Sensible Daten sind private Daten, was die Familie anlangt, was habe ich für ein Kind, wie heißt das Kind, wie alt ist das Kind usw. Es ist eine Definitionssache, für jeden sind sensible Daten anders sensibel. Ich bin ein bisschen sensibler auf dieses Thema, anderen ist es wahrscheinlich immer wurst, ja, und sagt: „Okay, mir ist es egal, sollen die Leute wissen von mir, ich habe ja eh nichts zu verbergen“, und das ist aber die große Problematik in der ganzen Geschichte, dass viele sagen: „Alle können nun alles wissen über mich, da ich ein braver Bürger bin und ich nichts zu vergeben habe, kann mir sowieso nichts geschehen“, und das ist aber im Prinzip der falsche Ansatz.

3) Wie würden Sie sich das erklären, dass sensible Daten eigentlich rechtlich besonders geschützt sind und wir sie freiwillig hergeben in Social Networks zum Beispiel?
Na, ganz einfach, ich habe eine Philosophie, die ich immer in meinen Vorträgen sage, ist die: In der heutigen Zeit, in der IT-Ära, in einer Zeit , in der halt Internet eine Rolle spielt, in der wir mit Handys und Display umgeben sind und die Jugendlichen, die junge Generation, die genau in diese Ära hineingewachsen und hineingeboren wurde, denen ist es…, die setzen die Freiheit über die Privatsphäre. Die Freiheit, das über sich

veröffentlichen zu dürfen, was sie wollen, ist ihnen wichtiger als die Privatsphäre. Sie sind ganz einfach stolz darauf, dass sie auf *Facebook* oder auf irgendeinem anderen sozialen Netzwerk, dass sie über sich Fotos online stellen können, dass sie private Informationen online stellen können. Sie sind stolz darauf, ja, und sagen ganz einfach: „Okay, das ist Teil der Gesellschaft, das ist Teil des Spieles der Gegenwart, darum mache ich das." Ja, und ich glaube, dass das für die Meisten in einigen Jahren dann ein böses Erwachen gibt, weil wie alle wissen: Die sozialen Netzwerke sind eine Fundgrube für viele, die halt wirklich Informationen finden wollen über eine gewisse Person.

4) Ist den Jugendlichen die Privatsphäre nicht mehr so wichtig?
Nein, ich glaube nicht, ich glaube, dass die Jugendlichen auch gar nicht wissen, was Privatsphäre zum Teil bedeutet. Ich bin überzeugt, dass viele Jugendliche einfach sagen: „Okay, dadurch dass ein Jeder eh alles über sich preisgibt, verliert im Prinzip die Privatsphäre an Bedeutung." Das ist ganz anders als bei der älteren Generation, bei meiner Generation, bei meiner Elterngeneration und Großelterngeneration. Für die ist Privatsphäre was anderes, die sind ja auch in einem zweiten Weltkrieg groß geworden oder haben den überlebt. Die wissen sehr wohl was Spionage bedeutet, und und und. Der heutigen Jugend ist es nicht so bewusst, weil ihnen offensichtlich noch nichts passiert ist, ja. Es gilt etwas solange als ungefährlich, solange man nicht selbst Opfer dieser nicht sichtbaren Gefahr geworden ist. Ich war kürzlich bei einem Vortrag in Deutschland. Moment, das suche ich jetzt gleich heraus, was dieser Hirnforscher gesagt hat und angemerkt hat, das habe ich mir nämlich aufgeschrieben…
Unser Gehirn funktioniert so, dass das, was ich nicht wahrnehme, für mich nicht existiert. Und das ist die Problematik bei der ganzen Geschichte. Für die Leute existiert keine Gefahr, dass die Privatsphäre untermauert wird, dass mit den Daten Schindluder betrieben wird und solange das nicht passiert, existiert auch diese Gefahr nicht in einem Gehirn.

5) Wüssten Sie ein paar extreme Beispiele, was man so in Social Networks findet?
Moment einmal, da muss ich mich umdrehen, weil da bleibe ich gleich ein bisschen in der Präsentation, die ich gehalten habe. Ich habe viele bekannte Fälle. Bei meinen Vorträgen, sage ich immer. Den ganzen Vortrag, also den kann ich Ihnen theoretisch auch als PDF schicken, aber den dürfen Sie nicht, nirgends weiterverbreiten, bitte.
Ich bin ja auch auf *Facebook*, aber ich bin auf *Facebook* aus einem ganz bestimmten Grund, damit ich genau nachkontrollieren kann bzw. sehe, wie die heutige Gesellschaft funktioniert, wie sie tickt, was sie alles preisgibt an Daten. Ich kann Ihnen sagen, Radiomoderatorin, sehr bekannt, hat auf *Facebook* gesagt: „Mensch, habe ich gestern viel getrunken, ich werde langsam zum Bsuff!" Das ist im Prinzip etwas, wo die vielleicht darauf stolz ist, dass das drinnen steht. Ihr künftiger Arbeitgeber oder was auch immer, würde sagen: „Okay, die trinkt ein bisschen zuviel offensichtlich." Regelmäßig lese ich bei meinen *Facebook*-Freunden, oder die zumindest meine Freunde sind auf *Facebook*: „Mir ist langweilig im Büro" , ja, oder „Heute ist Montag, ich habe überhaupt keine Energie" oder „Wann ist endlich Wochenende, mir ist schon so fad im Büro an einem Freitag", ja, das sind einfach Meldungen, die lustig klingen, aber die mir als Arbeitgeber im Prinzip genau signalisieren: Dem ist offensichtlich wirklich, der hat ein kleines Motivationsproblem. Also wenn ich weiß, ich muss in der heutigen Zeit und wir leben in einer wirtschaftlich schwierigen Situation, ich muss Geld und Leute einsparen, würde ich sofort wahrscheinlich so einen mir schnappen und sagen: „Okay, du schreibst sowieso auf *Facebook*, dass dir fad ist, also jetzt kann dir länger fad sein, weil du bist gekündigt!"
Aktueller Fall, Österreich, Schauspielerin hat auf der Wall in *Facebook* geschrieben: „Ich lasse mich scheiden!" und hat mehr oder weniger Journalisten auf diesen Umstand aufmerksam gemacht und das Arge ist, ich kenne diese Schauspielerin, ich kenne auch ihren Mann, und der Mann hat von mir erfahren, dass seine Frau die Scheidung auf *Facebook* praktisch öffentlich gemacht hat, ja, ist in Österreich ein konkreter Fall.
Im August 2009, aber da brauchen Sie nur recherchieren in *Google* oder *Bing*, oder wo auch immer: „Auf *Facebook* Chef beschimpft, Frau verliert Job!" lautete der Titel. Hat einfach gesagt: „Mein Chef ist ein Wappler" oder was auch immer. Ich glaube, sie hat ein bisschen ein etwas saftigeres Wort verwendet, ja, hat natürlich nicht bedacht, dass der Chef auch ein Teil einer ihrer Freunde war, der hat sie natürlich gekündigt. Und ein bekannter Fall ist auch: „Schweizerin verliert Job, weil sie im Krankenstand war!" Sie ist heimgegangen wegen einer Migräne, und hat aber genau in diesen Tagen im Krankenstand *Facebook*-Nachrichten abgesetzt, wurde gekündigt, weil man gesagt hat: „Okay, jemand der Migräne hat, muss in einem dunkleren Raum sich befinden. Jemand, der in einem dunkleren Raum ist, hat natürlich keinen, will nicht vor einem hellen Bildschirm sitzen oder vorm Computer, also hat sie offensichtlich gelogen und war eigentlich gar nicht krank." Sie hat dann vor Gericht argumentiert, ja, sie hat mit dem Handy die *Facebook*-Nachrichten abgefragt, ja, und hat mehr oder weniger die Postings gemacht, hat aber nicht gegolten, sie ist gekündigt geblieben. Solche Fälle gibt es zuhauf da drinnen im Internet oder schauen Sie sich an in *Facebook*, ich habe erst vergangene Woche einmal geschaut. Zur Zeit ist es gerade in oder hip in Wien, dass stillende oder junge Mütter, ein Profilfoto von sich hinein geben, das sie zeigt, wie sie gerade das Kind stillen mit halbnackter Brust, ja. Ja, mag mancher Manns Geschmack sein, meiner ist es nicht, ja, nicht weil ich irgendwie verklemmt bin, wirklich nicht, ja, aber das geht meines Erachtens ein bisschen zu viel. Auf der anderen Seite weiß ich

einen Fall von einem Freund von mir, der ist Fotograf, der ist Erotikfotograf, hat auch erotische Bilder hineingestellt ins Internet, hat praktisch die Brustwarzen, alles abgeklebt, ja, auf dem Foto mit dem Photoshop, damit er ja nicht anzüglich ist und der wird hinausgehaut und dem hat man seinen ganzen Account gelöscht. Solche Geschichten gibt es.
Also, ich kann Ihnen zuhauf solche Geschichten erzählen. Sie werden wahrscheinlich in Ihrer Arbeit ja eh auch auf die Studie vom *Frauenhofer-Institut* für sichere Informationstechnologie gestoßen sein, oder? Die neueste *AK*-Studie ist ja genau, geht ja genau in die gleiche Richtung. Soziale Netzwerke gefährden die Privatsphäre.

6) Kann man sagen, dass ein digitaler Fußabdruck im Netz bleibt?
Alles was im Netz geschrieben wird oder ins Netz geschrieben wird, das bleibt drinnen wie auf einer Anschlagtafel, aber der Unterschied zu einer Schultafel ist der, dass nichts gelöscht werden kann. Jede Zeile, jedes Foto, jedes Video, was einmal im Netz ist, das bleibt drinnen, ja, da hab ich keine oder fast keine Chance es herauszubekommen. Ich glaube, es gibt in meiner ganzen journalistischen Karriere, habe ich es erst ein Video gesehen, das ich nicht mehr gefunden habe im Netz. Das war, wie ein Notebook von einem, ich glaube ein japanischer Hersteller, bei einer Präsentation ist das Notebook in Flammen aufgegangen, ja. Dieses Video hat der Hersteller offensichtlich echt geschafft, dass er es aus dem Netz herauskriegt, ja. Das habe ich nie wieder gefunden. Zum Thema *gespeichert*...Was fällt mir noch für eine Geschichte ein? Ja, ein deutscher Privatsender hat vergangenes Jahr einen interessanten Versuch gemacht. Und zwar haben sie ein Gewaltvideo gedreht und zwar wurde in einem Parkhaus hinter einem Auto offensichtlich eine Frau verprügelt. Sie haben natürlich nur so getan und dieses Video auf *Youtube* gestellt und haben gewartet was passiert, weil normalerweise müsste *Youtube* ein Gewaltvideo sofort herausnehmen, ja. Die Filter haben dort versagt. Der Effekt war, dass das Video nach zwei Tagen noch immer drinnen war und es wurde schon fleißig kommentiert, vor allem echt arg kommentiert, wo „Recht geschieht ihr!“ und und und, also wirklich auf tiefste Kommentare. Dann hat man *Youtube* informiert, also *Google* informiert, dass sie das Video wieder offline stellen sollen. Das haben sie dann gemacht. Plötzlich ist aber das Video auf einer anderen Videoplattform wieder weiter verbreitet worden. Sprich, wenn einmal etwas im Netz ist, irgendeiner kopiert das herunter, mit der rechten Maustaste oder was auch immer und das ist schon verbreitet.

7) Da gibt es aber auch Reputationsunternehmen…?
Ja, natürlich, aber diese Reputationsunternehmen. Komm, ich schicke Ihnen diese Präsentation, die ich gemacht habe.
Es gibt ja auch den *Reputation-Defender*. Da zahlen Sie zum Beispiel 9 Euro 95 im Monat , damit Sie im Prinzip schauen können, dass Sie immer eine weiße Weste kriegen, ja, oder es gibt den *Datenwachschutz.de*, wo Sie im Prinzip den Auftrag geben, was steht über Sie drinnen im Netz, der schickt Ihnen dann eine Linkliste, was er alles gefunden hat, und dann sagt er, dann können Sie sagen: „Okay, ich möchte, dass der Link Nummer 117733 und 840 gelöscht wird, sprich, diese Information möchte mehr oder weniger nicht mehr im Netz sehen“, und die probieren dann das herunter zu löschen, was natürlich nicht immer leicht ist und der österreichische Aspekt ist ja auch zum Beispiel die Suchmaschine *123people*. Die Personensuchmaschine ist ja im Prinzip nicht nur darum gemacht, dass man Informationen findet über jemanden, sondern die sind ja gekoppelt an diese *Reputation Defender* und da gibt es zum Beispiel eine interessante Kooperation, dass eben im August 2008, seit August 2008 kooperiert *123people*, die Personensuchmaschine, mit dem Online-Schutzdienst *Reputation-Defender*, ja. Das heißt ganz einfach: Du suchst zuerst auf *123people*, was über dich gefunden steht, ist da irgendwas drinnen, was dir nicht passt, kannst du gleich beim *Reputation-Defender* dein Monatsabo oder Jahresabo abschließen. Das ist im Prinzip der ganze Hintergrund in dieser Geschichte. Das ist ein Business-Modell, ja, nämlich: „Finde etwas über dich, was dir nicht gefällt! Wir bringen dir mit einem anderen Service, schauen wir, dass wir wieder deine weiße Weste herstellen.“

8) Ist das alles namentlich, also die digitale Spur, die wir hinterlassen?
Zum Teil sicher, ja. Das Problem ist natürlich immer, dass man irgendwann einmal im Laufe des digitalen, des Internetsurfens gibt man einmal seinen Namen ein, ja, und dann kann es halt leicht passieren, dass diese Daten verknüpft werden und wenn die Daten verknüpft sind, und der Name ist dabei, entsteht ein schönes Konvolut an Daten. Beste Beispiel ist aber, da bin ich aber ein bisschen nicht ganz objektiv oder schon objektiv. Ich bin ja einer der größten *Google*-Kritiker, die es gibt. *Google* ist ja das Paradebeispiel für ein Unternehmen, das genau das macht, ja, sammelt. *Google* hat mehr, wie wir seit heute wissen mehr als 150 verschiedene Dienste, die Leute wissen das gar nicht. Für die meisten ist *Google* eine Suchmaschine, aber es gibt 150 Dienste, Services und Geschäftsfelder, wo die tätig sind und in jedem, bei jedem dieser Dienste generieren die Daten. Natürlich, da bin ich überzeugt, wenn bei irgendeinem Dienst, irgendwann einmal ein Name fällt, dass der einfach in das Profil, vom Data-Mining-System von *Google* aufgesogen wird und damit wird das Profil ergänzt.

9) Und was bringt das *Google*, wenn das immer genauer wird und wenn das immer mehr Daten werden?
Ganz einfach, was bringt das zum Beispiel *Google*.... Wart, machen Sie Pause?

Kurze Telefonunterbrechung

Ganz einfach, *Google*, das große Geschäftsmodell *Googles* besteht darin, dass sie Werbung verkauft, ja, die *Google*, was gratis ist, das ist zwar alles recht nett, aber das große „Gerstel" machen die mit *AdWords*, mit den Werbeanzeigen, mit den vierzeiligen und wenn ich da jetzt darauf klicke auf so eine Anzeige, muss der, der diese Werbeanzeige schaltet, Geld an *Google* zahlen. Wie groß ist die Wahrscheinlichkeit, dass ich darauf klicke auf etwas, was mich nicht interessiert, sehr gering. Wenn die mich aber sehr wohl kennen, wenn die mein Suchverhalten kennen, wenn die relativ viele Informationen über mich wissen, gesammelt haben, wenn die meine Interessen kennen, wofür ich mich interessiert habe in der Vergangenheit und und und, dann ist die Wahrscheinlichkeit, dass ich auf eine Werbung, die genau platziert ist, eher darauf klicke, als wenn das nur zufällig auf meinen Suchbegriff hin gemünzt ist. Wissen Sie, was ich meine? Die Geschichte, die Suche der Zukunft soll ja so funktionieren, wenn ich jetzt zum Beispiel eingebe: *Nikon D 300*, das ist ein Wert der digitalen Spiegelreflexkamera, möchte *Google* künftig genau wissen, ob ich eine besitze, ob ich mich dafür interessiere, ob ich ein Problem habe mit dieser Kamera, ja. Das soll im Prinzip die Suchmaschine sofort die Antwort darauf geben, weil sie verschiedene Informationen aus den verschiedenen Diensten mehr oder weniger zusammen lukriert. Das heißt, zum Beispiel habe ich in einem sozialen Netzwerk, jetzt will ja *Google* mit *Google Wave*, ah *Google Mail* ja auch *Twitter*, ein *Twitter*-ähnliches Tool integrieren, wird heute gelauncht. Jetzt natürlich, wenn ich jetzt in Ihren *Twitter*-Account Ihnen schreibe: „Meine depperte *D 300* funktioniert nicht, die hat irgendwie ein Problem mit dem Auto-Focus", oder was auch immer, ja, weiß das *Google* automatisch, kombiniert diese Information mit meinen anderen Informationen und sobald ich jetzt eingebe: *Nikon D 300*, klicken mir die sofort hin Servicestellen von *Nikon D 300*, zum Beispiel, und das ist im Prinzip das ganze Geschäftsmodell.

10) Wie genau geht das schon?
Wie genau geht das? Da muss man *Google* fragen. Ich glaube, dass es sehr genau geht. Mehr will ich aber derweil nicht sagen darüber, ja. Das Andere wäre Mutmaßung, ja. Also ich glaube, dass es sehr genau heruntergebrochen werden kann, aber da man *Google* nicht in die Karten schauen kann, weil *Google* ja keinen Zugriff in die Datensysteme erlaubt, kann man nur mutmaßen.

11) Wer wertet das dann irgendwie aus? Sind da Menschen dahinter, oder...?
Ich glaube, dass viel automatisiert ist. Ich sag immer wieder, das Lustige ist ja, wir machen uns immer Gedanken, das ist ja so ein Datenwulst, der kann doch nicht analysiert werden. Ich sage immer: „*Google* ist der größte Data-Mining-Experte, den es gibt auf dem Globus." Die schaffen es in 0,1235 Sekunden mir irgendeine Trefferliste mit weiß ich nicht, mit wie vielen Treffern hinzuknallen, wenn ich einen Suchbegriff eintippe. Also die werden ja wohl selbst fähig sein, die eigene Datenbank nach gewissen Suchkriterien zu durchforsten und sortieren zu können.

12) Noch zu den Daten, die wir freiwillig ins Netz stellen: Wie weit, denken Sie, wird das noch gehen? Ich habe mir als Beispiel aufgeschrieben: Stellen wir unsere DNA bei *Xing* hinein, um zu zeigen, dass wir gute Gene haben?
Na sicher, ja, ist ja schon so weit. *23andme* ist ein *Google* Service. Da habe ich mich selbst akkreditiert, ah selber angemeldet. Da kriegt man so ein Plastikröhrchen zugeschickt und da spuckt man rein und dann wird die DNA analysiert und drei Wochen später kann ich auf einer Plattform genau nachschauen, welche Gene, welche genetischen Voraussetzungen habe ich, ja, und heute zufällig habe ich gekriegt vom *23andme*-Team, Moment einmal, wo ist er, wo ist im Prinzip das Mail, heute, heute, heute, das war relativ in der Frühe, was ich gesehen habe, *23andme*-Team: „Dear Gerald. Have you ever wondered whether you are related to anyone in the *23andme*-database. Now you can connect with them and begin exploring how you are related with a new free tool from *23andme* called relative-finder." Sprich, ich kann mit meiner DNA, meine DNA kann ich vergleichen mit den anderen DNAs in dieser Datenbank und kann schauen, zu wie viel Prozent bin ich verwandt mit dem und dem und dem und dem und gibt es vielleicht sogar Verwandte, von denen ich gar nichts weiß auf dieser Welt, aber die zufällig auf dieser DNA-Datenbank gespeichert sind. Und die zweite Geschichte ist ja, dass im Prinzip einer von den Telekom, also von den *23andme*-Vorständen gesagt hat, sein Ziel wäre es, oder ideal wäre es , wenn man eine DNA-Komponente in einem sozialen Netzwerk integriert und im Prinzip die Leute sich kennen lernen aufgrund der DNA. Wenn es eine Übereinstimmung gibt und die passen zusammen, dann sollen sie sich doch kennen lernen.

13) Ist das nur für Sie einsehbar oder für alle?
Mein Profil ist nur für mich einsehbar, aber da es eine *Google*-Company ist, würde ich einmal behaupten, weil ich auch der Hauptfinancier bin dieses Services, dass ich natürlich auch Einblick habe in diese Daten.

14) Würden Sie meinen, dass es ein Unterschied ist, dass wir die Daten freiwillig hergeben in Social Networks oder so oder gibt es sowieso anderweitige Methoden der Datenerhebung?
Schauen Sie, ich habe, da muss ich Ihnen die Präsentation, glaube ich schicken. Ich habe in den vergangenen zwei Wochen am Datenschutztag in Südostbayern einen Vortrag gehalten, der hat geheißen: „*Google*, Online-Schnüffler und Datenschutz im Web 2.0-Zeitalter“ und da gibt es im Prinzip bei mir zwei Folien, die interessant sind. Es gibt die unwillkürliche Transparenz im Internet, die entsteht durch Suchmaschinen, diverse dubiose Dienste. Das nenne ich *Google-Phänomen*, d.h., da werde ich transparent, ohne dass ich es will, ohne dass ich es merke und die zweite ist die willkürliche, das sind die Social Networks und das nenne ich *Datenstriptease-Phänomen*, ja. Das eine unbewusst, das andere bewusst, und die zwei gemeinsam ergeben meines Erachtens den gläsernen Menschen, wobei das ein Begriff ist, weil der eh schon so einen langen Bart hat, aber die zwei Sachen kombiniert, ist im Prinzip etwas, was ich als eines der größten Probleme der Gegenwart sehe.

15) Wer, denken Sie, sind die größten Feinde der UserInnen in Social Networks, also wer kann etwas mit den Daten anfangen, Zweck entfremden, usw.?
Ganz einfach, da will ich Ihnen auch gleich…, Zweck entfremden. Das Problem ist, dass im Prinzip jeder Zweck entfremden kann, weil ja aufgrund der Suchmaschinen viele Daten gefunden werden, weil ja viele User unfähig sind, die Privacy-Einstellungen zu beherrschen und *Facebook* hat ja erst vor einigen Wochen die Privacy-Einstellungen geändert und das Arge war, die Grundstellung war, alle dürfen alles sehen, ja, und erst danach musste ich die Hakerln überall deaktivieren, damit ich wirklich auf meine Privatsphäre Wert legen konnte und dass ich meine Privatsphäre schützen konnte und wer ist interessiert an den Daten? Zwei von drei Personalchefs lassen ihre Bewerber googeln, ja. Wenn Sie sich jetzt vorstellen, würde ich wahrscheinlich auch zuerst in *Google* nachschauen und das machen aber zwei von drei Personalchefs. 36 Prozent der Personalchefs versuchen, also jeder Dritte, über ein soziales Netzwerk mehr über den Bewerber herauszufinden. Großkonzerne lassen mehr recherchieren als kleine Firmen und fast jeder zweite Personalchef findet lustige Urlaubs- und Partyfotos, was ziemlich hip ist in der *Facebook*-Gemeinde, in der Social Network-Gemeinde, finden solche Partyfotos überhaupt nicht amüsant, ja, und ein Kommentar über den eigenen Arbeitsplatz finden drei von vier Personalchefs nicht klasse, auch im Prinzip logisch. Und es gibt einige Berufsgruppen, die zum Beispiel ein absolutes *Facebook*- und Social Network-Verbot haben. Kein Anwalt ist in einem Social Network vertreten. Vielleicht auf *Xing* von mir aus, aber nicht auf *Facebook*. Wenn Sie einen Anwalt finden, verliert der irrsinnig viel an Reputation. Ich habe kürzlich einen Vortrag auch gehalten, da war ein anderer Anwalt dabei, der nach mir den Vortrag gehalten hat und der hat zu mir gesagt, also hat dort vorgetragen, dass, wenn sie einen Bewerber haben für Ihre Kanzlei, das ist eine riesige Kanzlei gewesen, lassen sie, schauen sie auch nach, finden sie was über den im Internet. Sobald sie etwas finden, ja, wo er zum Beispiel abgebildet ist, der Herr Anwalt Dr. Müller mit einem Gläschen Wein bei irgendeiner Vernissage, oder was auch immer, hat der schon verloren und kriegt den Job nicht, ja. Ein Anwalt mit Alkohol in Kombination, darf so ein Foto, darf im Prinzip nicht im Internet sein.

16) Gibt es da keine Gewöhnung daran oder Toleranzbereitschaft?
Nein, das glaube ich nicht, weil ich glaube ganz einfach, dass in gewissen Schichten solche Sachen nach wie vor als nicht state-of-the-art gesehen wird, als nicht geziemend, zum Beruf passend.

17) Wer könnte sonst noch Social Networks zu Überwachungszwecken nutzen?
Na ja, im Prinzip jeder, weil im Prinzip kann jede Behörde, ja ist ein Innenministerium, ein Geheimdienst, aber da sind wir ein bisschen in der Verschwörungstheorie drinnen, könnte mit diesen Daten, die dort publik sind, natürlich viel anstellen, ja. Die weiß genau, wer, wie, was tickt usw. Und man erinnert sich an die Chat-Seiten zurück. Wann man hin und wieder manchen Chattern zugehört oder wenn man da mitgelesen hat, hat man also wirklich gedacht, da sitzt irgendwie ein Psychopath am Computer und so ähnlich ist es natürlich auch bei sozialen Netzwerken. Da kann ich natürlich über, je mehr jemand über sich preisgibt, umso mehr weiß ich auch über den, ja, also umso besser kann ich ihn einschätzen, ja. Wenn Sie mir Zugriff geben würden zu ihrem Computer und ich schaue mir einmal Ihre Linkliste an und Ihre Lesezeichen oder Verlaufsliste, weiß ich auch, wofür Sie sich interessieren und so weiter und so fort. Wenn Sie jetzt, sag ich einmal, wenn ich jetzt Zugang habe oder Freund bin auf *Facebook* und ich schaue mir an, welche Fotos haben Sie publik, welche Infos haben Sie online gestellt, welche, welcher Freund welcher Gruppe sind Sie oder bei welchen Gruppen sind Sie dabei, weiß ich genau, sind Sie Raucher, sind Sie Nichtraucher, sind Sie rechts, links, Mitte politisch, welches Religionsbekenntnis haben Sie, und, und, und,... und darum geht es eben. Manche stellen da freizügigst Informationen hinein und sind sich eigentlich der Bedeutung nicht bewusst, was im Prinzip, was eine Auswertung dieser Daten bedeuten könnte.

18) Greift auch der Staat zurück auf solche Profile?
Das weiß ich nicht, also ich bin überzeugt, dass einmal der Staat sicherlich mit *Google* kooperiert, ja, weil *Google* hat ein eigenes Lobbying-Büro in Berlin und diese Lobbyisten, die sind regelmäßig in den westlichen

Staaten unterwegs und sprechen mit den Behörden und da werden sicherlich auch Spezialwünsche erfüllt und in Amerika ist es sowieso, dass aufgrund des *US-Patriot-Acts*, wo es um die Terrorismusbekämpfung geht, ja ohnehin jedes Unternehmen verpflichtet ist, Daten im Kampf gegen den Terrorismus bekannt zu geben und zu mir hat einer der führenden IT-Experten der Gegenwart gesagt: „Jeder muss naiv sein, der glaubt, dass Geheimdienste nicht einen Online-Zugang zu *Google* haben."

19) Geht die Vorratsdatenspeicherung auch in die Richtung?
Natürlich ist Vorratsdatenspeicherung die gleiche Problematik, ja. Ich speichere Daten für den Fall, für einen Fall, der noch nicht passiert ist. Es könnte ja sein, dass..., ja. Es könnte sein, dass Sie irgendwann einmal kriminell sind, ja, oder kriminell werden oder irgendeine Straftat begehen und für diesen Fall, tue ich gleich die Daten reservieren, dass ich im Nachhinein nachschauen kann, was da passiert ist. Also ich finde, das ist ein Eingriff in die Privatsphäre und in die Freiheit des Menschen.

20) Also wirtschaftlich haben wir schon ein bisschen gesprochen. Es gibt ja auch das *Last.fm* zum Beispiel. Wissen die schon genauer wie ich selber, was mein Musikgeschmack ist?
Ja, aber ja das ist im Prinzip etwas, was im Prinzip ja eigentlich etwas Normales ist, gehört natürlich auch dazu zu dieser Geschichte. Musikgeschmack, was weiß ich, manche schreiben ihren Musikgeschmack per *Facebook* hinein. Aber *Last.fm*, natürlich wissen die genau, was mein Musikgeschmack ist. Es weiß aber im Prinzip auch *Amazon*, was mein Lesegeschmack ist, ja, wofür ich mich interessiere, ja. Ob ich jetzt, weiß ich nicht, *Hitler: Mein Kampf* bestelle, kann ich natürlich entweder rechtsradikal sein oder ein interessierter Mensch, der einfach wissen will, was hat der Hitler wirklich hineingeschrieben in diesem *Mein Kampf*. Kabelbetreiber, die Kabelbetreiber wissen doch ganz genau aufgrund ihrer digitalen Systeme, welcher Haushalt sich was anschaut im Fernsehen, ja. Die wissen ganz genau, wer die Blue Movies sich anschaut, 100prozentig. Und ich bin überzeugt, dass gerade aufgrund dieser Tatsache, dass man genau weiß, wer interessiert sich für was, zielgerichtete Werbung schalten kann, ja. Wann ich genau weiß, okay da schaut jetzt gerade der, weiß ich nicht, der Mayer, nennen wir ihn Mayer oder Müller, oder was auch immer, schaut sich gerade einen Blue Movie, einen Film an, dann knalle ich rein die Werbung mit Kondomen oder Whiskey, oder was auch immer, ja, immer dazu passend zur Zielgruppe. Wenn ich weiß, die schauen sich gerade einen Kinderfilm an, kommt die Schokolade, die Zuckerlwerbung, oder was auch immer, die Kindermilchschnitte, ja. Das kann ich ja alles erahnen und da wird auch die Zukunft hingehen.

21) Denken Sie, kann man von einem technischen Rüstungskampf im Internet sprechen? Also die Überwacher, Datensammler auf der einen Seite und auf der anderen die Verschleierungsdienste zum Beispiel?
Das glaube ich nicht. Ich glaube nämlich, dass die Verschleierung nicht so wirklich funktioniert. Weil ja die Verschleierungsdienste sich auch an Gesetze halten müssen. Ich kann natürlich mittels Verschleierungsdienste gewissen Dingen ein Schnippchen schlagen, indem ich sage: „Okay, ich verwende jetzt *Notraxx*, ein Anonymisierungsdienst und verschleiere mir meine IP-Adresse, damit *Google* nicht weiß, wer ich bin oder damit irgendein anderer Dienst nicht weiß, wer ich bin", oder ein Journalist verwendet in seiner Recherche einen verschleiernden Anonymisierungsdienst, damit man nicht weiß, dass jetzt gerade die *Mediaprint* oder der *Kurier* die und die Geschichte recherchiert, ja. Das, okay funktioniert. Nur, auch diese Verschleierungsdienste sind verpflichtet, im Falle einer Straftat die Daten preiszugeben, ja, also vor den Behörden schützt so etwas nicht. Vor den Behörden kann ich mich nicht wirklich schützen, ja, wenn ich eine Straftat vorhabe, vor Privatunternehmen kann ich mich wahrscheinlich eher schützen. Aber nehmen wir jetzt nicht das Schlechteste an. Natürlich sind Anonymisierungsdienste, ich verwende sie auch hin und wieder und ich empfehle sie auch für jemanden, der wirklich irgendwie eine *Google*-Neurose hat oder was auch immer.

22) Denken Sie, dass Überwachung im Web 2.0 eher personalisiert wird, also für einzelne Personen ermöglicht?
Was meinen Sie da konkret jetzt?
Dass jetzt der Einzelne eben bei *Facebook* schauen kann, eben wie Sie schon gemeint haben, mit Vorgesetzten oder so und Freunde, dass die jetzt genauer noch sehen können, wer was macht usw.?
Das kann ich ja sowieso schon machen, ja. Sobald ich Freund bin von jemanden, sehe ich genau, was der andere macht ja, also eigentlich ist es ja... Persönlich kann ich auf meinem *Facebook*-Account genau sehen, was meine Freunde machen, aber das hängt natürlich davon ab, wie freizügig der mit seinen Daten umgeht, ja und das ist der springende Punkt. Ich schreibe relativ wenig hinein. Mein *Xing*-Profil ist zu fünfzig Prozent komplett und mein *Facebook*-Profil ist auch zu fünfzig Prozent komplett. Mehr gebe ich nicht hinein. Es muss im Prinzip jeder entscheiden, wie weit will er was von sich preisgeben, ja. Bei mir hört es bei fünfzig Prozent auf, bei anderen hört es bei neunzig oder fünfundneunzig Prozent auf und der Dritte ist stolz, dass hundert Prozent dort steht.

23) Sehen Sie auch Vorteile in der Entwicklung hin zu mehr Datensammlungen?

Was meinen Sie mit Vorteil? Dass das Datensammeln ein Vorteil sein kann?
Ja, also dass sich gesellschaftliche Vorteile ergeben dadurch?
Naja, ich weiß nicht, ob Datensammeln so ein gesellschaftlicher Vorteil ist. Natürlich ist es interessant, weil gewisse Dienste vielleicht gescheiter entwickelt werden können. Zum Beispiel, was wäre ein Vorteil des Datensammelns? Ich kann natürlich alles pro und contra verwenden. Natürlich ist es interessant, wenn jetzt *Google* anbietet ein Service, *Google Flu*, wo im Prinzip aufgrund der Suchanfragen analysiert werden kann oder prognostiziert werden kann, dass eine Grippeepidemie im Anmarsch ist. Das haben Sie schon gehört, oder? Dass das geht? Wenn jetzt zum Beispiel *Google* feststellt, dass in die Suchmaske oft hineingetippt wird: Heiserkeit, Husten, Kopfweh, Halsschmerzen wissen die, aha, wenn das öfter auftritt, dass eine Grippeepidemie im Anmarsch ist. Die wissen das offensichtlich, oder behaupten sie, zehn bis fünfzehn Tage vorher. Das natürlich hat einen Sinn, wenn ich sage: „Okay, die Pharmaindustrie, die Spitäler, Ärzte können sich dafür rüsten, darauf vorbereiten und sich mit Medikamenten eindecken", hat natürlich aber in der *Google*-Sache natürlich einen anderen Aspekt, weil natürlich *Google* dann feststellen kann, oder die Preise für Click-Werbung hinaufsetzen kann. Wenn ich jetzt weiß, okay da kommt eine Grippewelle auf mich zu, dann tue ich recht schnell die *AdWords*-Werbung, die Clickpreise von zehn Cent pro Click auf 50 Cent pro Click hinaufsetzen für einen, weiß ich nicht, einen Pharmakonzern, der für sein Kopfwehmittel zum Beispiel wirbt, ja. Also, auf der anderen Seite ideal, aber auch kann konträr sein und so geht es in allen Bereichen. Wenn ich weiß, es interessieren sich Leute für einen gewissen Stadtteil in Wien, weiß ich nicht, Hausnummer im sechzehnten Bezirk gibt es ein Grätzel, das stadtentwickelt, also entwickelt werden soll, kann ich aufgrund der Suchanfragen eigentlich feststellen, interessiert das die Leute, ja oder nein. Wenn ich natürlich als Behörde die Daten habe, ja da gibt es Leute, die interessieren sich für so etwas, könnten die die Stadtentwicklung dort vorantreiben, ja. Auf der anderen Seite natürlich können die Immobilienmakler genau mit diesen Informationen die Preise hinauf treiben, ja, und das ist immer ein Für und ein Wider.

24) Und welche gesellschaftlichen Gefahren gehen von Überwachung aus?
Die gesellschaftlichen Gefahren von Überwachung, ist klar, dass wir in einer BigBrother-Gesellschaft leben. Dass im Prinzip alles, was wir tun, jeder Schritt, beobachtet wird. Und das habe ich in meinem ersten Buch schon geschrieben: Wir haben Handys, ein Handy ist im Prinzip ein Peilsender in der Hosentasche, ich gehe hinaus aus dem Büro und bin sofort von irgendeiner Webcam oder Überwachungskamera erfasst, gehe auf die Straße, bin schon wieder von einer Überwachungskamera erfasst, fahre auf der Autobahn, aufgrund der Handy-Position, weiß ich natürlich genau, wie ich bin, wo ich bin, wie schnell ich fahre, natürlich auch. Bin außerdem in der *ASFINAG*-Kamera drinnen. Du, vielleicht kriege ich noch ein E-Mail auch dazwischen oder tue ein Sms schicken oder telefoniere dazwischen, also im Prinzip, die IT öffnet Tür und Tor zur totalen Überwachungsgesellschaft, ja. Und wenn man so hört, es gibt ja auch Absichten, dass man alle Kameras, die es gibt, alle Überwachungskameras vernetzt.

25) Ich habe nämlich in der Literatur,... da hat wer von kleinen Geschwistern gesprochen statt vom großen Bruder. Denken Sie, dass das zutreffen würde?
Was meinen Sie, kleine Geschwister, großer Bruder?
Dass nicht jetzt ein Überwachungsstaat besteht, sondern jeder für sich schaut, dass er irgendwie Daten generiert.
Nein, ich glaube, dass es nicht einen großen Bruder gibt, sondern es gibt viele große Brüder und die liefern im Prinzip gemeinsam, die kooperieren gemeinsam und liefern sich gegenseitig die Daten zu und diese großen Brüder sind jetzt nicht nur auf die Privatwirtschaft beschränkt, wie etwa auf *Google* oder… ich bin überzeugt, dass *Facebook* mittlerweile ja fast genauso gefährlich ist, zum Teil gefährlicher ist als *Google*, ja, weil ja die Leute dort freiwillig die Daten bekannt geben. Wenn ich jetzt überlege, *Google* ist ein großer Bruder, *Facebook* ist ein großer Bruder, dann habe ich natürlich verschiedene Staaten, die natürlich auch Große Bruder-Staaten sind. Brauchen wir nur ein bisschen nach Asien schauen, angefangen von Nord-Vietnam bis China und sogar in Myanmar. Es gibt viele große Große Brüder, ja. Gefährlich wird es nur, wenn die alle zusammenarbeiten und sich gegenseitig die Informationen zuschieben. Ich glaube aber, dass der Größte Bruder, die Amerikaner sind, ja. Aus einem ganz banalen Grund, weil die meisten Dienste in der Privatwirtschaft sind US-Unternehmen und aufgrund des US-*Patriot-Acts*, den ich eh schon vorher erwähnt habe, muss ein jedes Unternehmen Daten an die Behörden liefern dort, an die Geheimdienste liefern, und darum glaube ich, dass Amerika den größten Zugriff zu den größten Datennetzen und Datenbanken hat.

26) Ist es in einer Demokratie so gefährlich, wenn jemand so viele Daten hat?
Naja, der einzige Nachteil ist, für den Datensammler oder für den Staat, dass sie vor lauter Daten nicht wissen, was sie machen sollen, ja, also, vor lauter Bäumen den Wald nicht sehen, oder wie sagt man da, vor lauter Wald den Baum nicht sehen, und das ist das Problem. Wenn ich das Handwerk nicht beherrsche, aus den Daten Information herauszufiltern, dann sind die Daten wertlos, ja, weil im Prinzip ist ja auch alles, was ich sehe, sind ja alles Daten. Information wird sie erst und Wissen wird sie erst in meinem Kopf, wenn ich mir die Bits und Bytes zusammenzähle ja, wenn die kombiniert werden im Hirn. Davor ist es im Prinzip nichts anderes

als Nullen und Einser und irgendetwas, was da geschrieben wird auf einem Display. Wissen Sie was ich ungefähr sagen möchte. Genauso ist es bei einer Datensammlung, wenn da keine Suchkriterien, nach bestimmten Kriterien abgefragt werden kann, dann hat der Staat nicht viel von dieser Datensammlung.

27) Eine Frage noch: Kommt es zu einer Beweislastumkehr vielleicht, dadurch dass ständig Daten über uns erhoben werden und wir uns dann rechtfertigen müssen, das haben wir nur deswegen gemacht... eben wie zuvor dieses Hitler-Beispiel?
Na sicher ist es so. Das ist ja genau das Problem, dass ich mich rechtfertigen muss für etwas, was vielleicht ja gar nicht schlecht gemeint war, ja. Wenn ich mir jetzt *Hitler: Mein Kampf* bestelle, kann im Prinzip jemand sofort interpretieren, der ist rechtsradikal, offensichtlich ist er irgendwie ein Neo-Nazi oder was auch immer. Das muss aber nicht so sein. Das ist vielleicht, ich bin ein Journalist und mich interessiert das einfach, ja, und darum möchte ich es lesen. Natürlich ist ja genau das die Problematik, dass aufgrund der Datensammlerei, aufgrund der, wir sind immer und überall überwacht, jede Handlung im Web ist kontrolliert, dass wir uns da rechtfertigen müssen. Das ist ja auch ein Dilemma, ja. Viele sagen: „Okay, ist mir wurst, ich habe ja eh nichts zu verbergen und dann sage ich ihnen halt, ich habe das recherchiert für das oder das“, aber das kann im Prinzip, da sind wir wieder bei der Arbeitsplatzsuche, sollte ein potentieller Chef erfahren, dass ein Kandidat *Mein Kampf* gelesen hat, kann das im Prinzip schlechte Auswirkungen haben. Es kann aber auch schlechte Auswirkungen haben, wenn der Chef jetzt wissen will: „Hast du schon eine DNA-Analyse bei *23andme* gemacht? Hast du es nicht gemacht, da hast du zweihundert Dollar und lasse es machen, ich möchte wissen, wie es um deine Gene bestellt ist, ob du irgendwie krank wirst.“

28) Und was könnte eine Diktatur mit einem perfekten Überwachungssystem erreichen?
Na, ja. Da braucht man eh nur nach China schauen, oder? Da braucht man, glaube ich, gar nicht mehr viel dazu sagen,.... Eine Diktatur, aber... Im Iran ist es so, in China ist es so, da brauchen Sie sich im Prinzip nur die Geschichte... Wie hat unsere Geschichte geheißen, Benjamin? (*Fragt seinen Arbeitskollegen*) Die größten Feinde des Internets, zehn Länder haben wir, glaube ich, aufgelistet.
In der Form, dass eine Opposition nicht mehr geduldet wird?
Nein, das Problem ist, dass eine Opposition in einer Diktatur ja insofern nicht möglich ist, weil ich sofort als Diktator kontrollieren kann, wer schaut im Internet immer auf was, wer schickt sich welche Nachrichten zu. Ich kann das kontrollieren. Ich kann jedes Sms kontrollieren. Ich kann jedes E-Mail kontrollieren. Ich kann überall Wort-Scanner einbauen, und darum ist es schwierig eine Diktatur zu stürzen, weil die natürlich die Information früher haben als den Gegnern recht ist. Beste Beispiel: Die ganzen Aufstände in den Philippinen vor weiß nicht vor wie vielen Jahren, sind alle organisiert worden per Sms.
***Arbeitskollege Benjamin spricht**:* Aktuell ist es in Weißrussland. In Weißrussland sind 2010 Wahlen, und die haben jetzt schon den Internetzugang und die Internetkontrolle verschärft. Also die Opposition, die soundso nur im Netz agieren kann, weil sie öffentlich nicht auftreten darf, selbst sozusagen dort wo sich formieren könnte, nicht dazukommt.

29) Ja, ich wäre mit meinen Fragen am Ende und wollte zum Schluss noch fragen, ob vielleicht irgendwelche Aspekte für Sie noch wichtig sind, die zuwenig vorgekommen sind?
Nein, wissen Sie was, ich schicke Ihnen jetzt einmal meinen Vortrag.

Vielen Dank!
Bitte, bitte.

Interview mit Erich Möchel:

Datum: 18. Februar 2010

Ort: Bürozimmer in seinem Haus

Dauer: ca. 75 Minuten

1) Bei der ersten Frage würde ich Sie bitten, dass Sie sich kurz vorstellen und Ihren Arbeitsschwerpunkt erklären?
Hallo, ja die Vorstellung ist einfach. Mein Name ist Erich Möchel. Ich arbeite für *ORF.at*, für das Webportal des *ORF* und zwar für den Technikteil *FUTUREZONE.ORF.at*. Ich war dort in den Jahren 1999 bis 2006 leitender Redakteur, also so eine Art Ressortleiter und übe jetzt mehr die Funktion so des älteren

Kommentators und Analytikers aus. Und nebenbei mache ich natürlich weiter meine eher investigativ orientierten Netzpolitik-Themen, wie: alles was mit Überwachung, Zensur und Ähnlichem zu tun hat.

2) Zur Privatsphäre, das wäre der erste Block. Welche Form von personenbezogenen Daten würden Sie als sensibel beschreiben?
Das ist schwer, das so allgemein zu sagen. Es kommt darauf an, wem man sie gibt. Zum Beispiel sind Krankheitsdaten über meine körperliche Gesundheit, die gebe ich am besten alle meinem Arzt, auch wenn sie die sensibelsten sind, während ich in anderen Environments, in anderen Umgebungen natürlich wesentlich restriktiver mit meinen Daten umgehen muss. Das heißt, es ist irrsinnig schwer eine Grenze zu ziehen, weil auch die Sensibilität für jeden Menschen anders anzusetzen ist. Ich sage Ihnen ein Beispiel: Es gibt zum Beispiel Leute, ich will da jetzt auf niemanden im Einzelnen weisen, die bekamen einen Hoden amputiert. Es gibt Leute darüber, die das total schamhaft verschweigen und manche, denen ist das einfach Plunze und die machen rüde Witze über sich selbst und das ist ihre Art mit dem, damit fertig zu werden. Sie sehen es handelt sich in beiden Fällen um eine Art Sensibilität, nur wird die eine sozusagen öffentlich bezwungen und die andere sagt nein, hier Stopp, ich spreche gar nicht. Also ist es relativ schwierig das festzunageln, weil wir hier schon mitten in der Individualität des Menschen sind und da ist nun mal genau nicht jeder gleich, da sind alle verschieden. Und darum kann man das, muss man eigentlich die Sensibilitätsschwelle sehr, sehr niedrig ansetzen, dass auch die, die am empfindlichsten sind, geschützt sind.
Und ein weiteres Problem ist dabei noch, dass man es den Daten sehr oft nicht ansieht, dass sie sensibel sind, weil sie erst in der Verknüpfung gefährlich werden. Das heißt man gibt dort ein bisschen Daten ab, da ein bisschen Daten ab, da ein bisschen Daten ab, da ein bisschen Daten ab und die sind alle für sich sagen wir, naja eh wurst. Und dann kommt wer her und vernetzt all diese Daten zusammen und Patsch ist es überhaupt nicht mehr wurst, sondern eine Katastrophe.

3) Jetzt ist es ja einerseits so, dass vom Datenschutzrecht her, sensible Daten ja besonders schützenswürdig sind und auf der anderen Seite geben wir sie aber in Social Networks zum Beispiel, *Youtube*, *Google* freiwillig her?
Wir ist relativ.
Aber ein Großteil, sage ich jetzt einmal. Und warum stellen diese Leute solche Daten freiwillig ins Internet?
Weil sie, glaube ich, noch nicht im Internet angekommen sind. Die leben noch in einem anderen Medienzeitalter und zwar das, das vor dem Internet alles dominiert hat: Fernsehen und da spreche ich von den Privatkanälen in erster Linie. Schauen Sie sich bitte diese Zurschaustellungen dort an. Man weiß ganz genau, dass ganz Deutschland lachen wird, wenn man nicht singen kann und doch zu Dieter Bohlen geht und vorsingt, aber die Leute tun es trotzdem, sie machen sich zum Affen auf der Bühne. Aber sie tun es trotzdem, weil es offenbar so wichtig ist, dass man einmal da zu sehen war, weil sie das Gefühl haben, es gibt sie gar nicht, wenn sie im Fernsehen nicht vorkommen, weil jetzt schon alles im Fernsehen vorkommt. Da gibt es Familien, die in diesen, was Harald Schmidt Unterschichtfernsehen nennt, da sind die in diesen Nachmittagstalkshows, da gehen Leute mit ihren Familienstreitigkeiten vor die ganze Nation und machen sich zum Affen, dass es nicht mehr höher geht. Warum tun die das? Weil das dem Fernsehzeitalter entspricht. Die anderen, die in *Facebook* bedenkenlos alles über sich zur Schau stellen, die haben, glaube ich, alle noch nicht wirklich eine Ahnung, was ein solches Informationsnetz bedeutet. Fernsehen ist over, wenn die Sendung vorbei ist. Fernsehen gilt als flüchtiges Medium. Das hier ist nicht flüchtig. Der *Google*-Cash ist äußerst nachhaltig und gut gefüllt. Und das ist, glaube ich der Hauptgrund, warum die Leute so bedenkenlos mit ihren Daten umgehen.

4) Was bringt das den Selbstdarstellern?
Ich schätze mal das Streben nach sozialer Anerkennung, ganz einfach. Und schaut mich an, so viele Freunde habe ich, was bin ich nicht für ein beliebter Mensch. Das wäre natürlich. Ich meine, wenn ich unterrichte an der FH, dann gebe ich den Studenten meistens solche Ratschläge: Wenn dir bei einem Vorgang nicht klar ist, welche Motive dahinter stehen, dann liste die möglichen Motive in abfallender Reihenfolge einmal auf. In abfallender Reihenfolge heißt: Zuerst kommen die edleren Motive und dann kommen die nichtswürdigen, diese egoistischen, die ganz bösen Motive und dann nehmen Sie dieses Motiv, picken Sie dieses Motiv heraus, das wahrscheinlich ist und das, das am unteren, weiter am unteren Ende der Skala steht, ist immer das leider das stimmt, das richtige. Es ist fast immer das einfachste, nichtswürdigste und abzulehnendste aller Motive. Meistens geht es um Gier in irgendeiner Form. Und dass wir in einem Zeitalter der Gier leben, das ist ja wohl unbestreitbar.

5) Tragen solche Daten, die wir eben hinterlassen, zu einem digitalen Fußabdruck bei?
Wie ist das jetzt gemeint? Footprint? Meinst du jetzt Fingerprint? Fußabdruck verbindet man meistens mit Klima oder mit Satelliten.
Digitaler Fußabdruck, so dass wir eine Spur hinterlassen.

Nur Spuren. Schauen Sie sich bitte die österreichische Medienlandschaft an. Fast alle Printtageszeitungen haben *Google Analytics* integriert. Sie senden alle Clickstreams ihrer Benutzer an *Google*, sprich *Der Standard*, dann *oe24*, also dieses komische Fellner-Blättchen da, und jede Menge anderer Zeitungen schicken alle ihre Daten an *Google*. Was bedeutet das? *Google* weiß, welcher Österreicher in welcher Reihenfolge welche Nachrichten konsumiert an welchem Tag, wann er nicht liest. Das registrieren die Algorithmen von *Google*. Interessensprofile machen die. Wenn sie Interessensprofile machen können und die mit einer IP-Adresse verknüpfen bzw. die IP-Adresse durch eine viel eindeutigere Eigenerkennung des betreffenden Browsers, es geht ja alles über Cookies im Browser. *Google* sagt immer: Nein, wir speichern keine IP-Adressen. Eh klar, die brauchen sie auch gar nicht. Die brauchen sie genau nur einmal und immer nur ganz kurz, weil die Leute nur normal von verschiedenen Rechnern und von verschiedenen IP-Adressen daherkommen, dies aber die gleichen sind. Das sind nicht drei User, sondern das bin ich immer von wo anders. Einmal mobil mit meinem Laptop habe ich eine andere IP. Und wenn *Google* natürlich alle Daten kriegt von fast allen Medien. Der *ORF* hat übrigens nie welche weitergegeben und der *Kurier* hat *Google Analytics* herunter geschmissen, weil sie sagen: „Unsere Kundendaten: Wir betreuen, niemand anderer." Das ist meiner Meinung nach auch der vernünftigste Ansatz. Und dadurch entsteht das Bild, was ich dir zuvor geschildert habe. Jedes für sich ist harmlos, kriegt aber einer alle und das ist immer *Google*, die kriegen sie aus allen Ecken, die Daten. Und dann läuft eben am Nutzerverhalten gerechnet der Identifizierungsvorgang. Sie haben nicht deinen Namen. Den wollen, brauchen sie auch nicht wirklich. Das Geschäft geht ja auch ohne deinen Namen, weil du bist ja der, der, sagen wir, du sitzt am anderen Ende, du bist der Werbungsschauer. Das ist ja keine Suchmaschine, *Google*. Das ist nicht ihr Kerngeschäft, Suchmaschine. Ihr Kerngeschäft ist größter Vertreiber, Online-Distributor von Suche bezogener Werbung und einer der größten Distributor für Bannerwerbung. Das ist das Geschäft *Googles* und nicht Suchmaschine. Suchmaschine ist ein Mittel zum Zweck.

Wie würden Sie das nennen anstatt digitalem Fußabdruck? Spur vielleicht?

Ja, man kann, mir ist das klimametaphorisch durcheinander gekommen und es gibt dann noch den Ausdruck Footprint. Das sagt man für den Ausstrahlungsbereich eines Satelliten, also welchen Fußabdruck er und wo und sozusagen was er ausleuchtet. Das nennt man Fußabdruck. Ich würde eher sagen, wäre der Ausdruck Fingerabdruck schon angebrachter.

6) Was denken Sie, welche Daten da noch kommen werden, die wir freiwillig hineinstellen?

Sehr viele Daten können nicht mehr dazukommen, weil praktisch schon alles hineingestellt wird. Schauen Sie sich bitte das Geschäft an von *23andme*. Das ist eine Firma, die unter anderem, die einem, ich glaube der Gattin eines der beiden *Google*-Gründer, ich glaube einmal das ist die Frau Brin, wenn ich mich nicht täusche, die Frau von Sergej Brin. Sie hat diese Firma und da ist ein bisschen Risikokapital auch vom Gatten dabei und diese Firma fordert die Leute auf: „Schicken Sie uns Ihre DNA. Wir machen Ihnen eine Analyse." Kostenpunkt irgendwas 200 Dollar und danach können sie schauen, mit wem sie allen über fünf Ecken verwandt sind. Und die Leute machen das. Und die werten da die DNAs aus. In unserem Strafrecht dürfen DNA-Proben nur bei schweren Verbrechen genommen werden. Die Schwelle sinkt zwar auch schon jetzt, weil sie auch billiger geworden sind, diese DNA-Analysen, dadurch, dass sie so häufig stattfinden, wird ja alles günstiger. Und das wird, wie gesagt, von der Polizei als Identifikationsmittel vor allem bei schweren Verbrechen eingesetzt und die dort machen irgendwie ein Hobbygeschäft daraus. Da schicken sicher massenweise Leute ihre DNA-Daten hin. Dass man da natürlich auch die Neigung zu Krankheiten sieht drinnen, dass diese Firma *23andme* anders als *Google* sehr wohl über Namen, Wohnort und Bankverbindungen verfügt, weil man musste ja bezahlen dafür. Also, das ist Sprengstoff, was da drinnen, was die in ihrer Datenbank haben. Das sind extrem wertvolle Daten. Sie sehen ja, wie wertvoll Datensätze sein können an den Beispielen Liechtenstein und Schweiz. Da wird viel Geld hingelegt für Daten, weil die Daten mehr wert sind als dieses Geld für den Fiskus. Haben will er 2,5, lukrieren wird man, man lukriert schon jetzt, weil sich so viele selber anzeigen vor Angst. Lukrieren soll man, wird kolportiert, so um die 100. Na, das ist doch eine hübsche Rendite, oder?

7) Unterschätzen da die UserInnen die Wichtigkeit ihrer Privatsphäre?

Die unterschätzen völlig, wie wertvoll ihre Datensätze sind. Sie unterschätzen es völlig, dass mit diesen Daten ein Irrsinnshandel betrieben wird inzwischen. Schauen Sie sich es an, Sie gehen auf Ihren *Gmx*-Account und wollen jemandem mailen und plötzlich poppt Ihnen dessen *Facebook*-Seite entgegen, von selber. „Aha, so geht das." Die wissen das nicht. Ich meine, die Leute können mit den Kommunikationsmedien im Internet nur völlig rudimentär umgehen. Sie wissen halt grad, wie es ungefähr geht, dass man eine Kommunikation zusammenbringt. Unter welchen Umständen diese Kommunikation stattfindet und wer aller noch dabei sein könnte, den man nicht sieht und hört, über das machen sie sich keine Gedanken. Es ist irrsinnig oft vorgekommen, dass Leute, die ich gewarnt habe, wenn sie sich wirklich krass leichtsinnig verhalten haben, die haben zu mir gesagt: „Hör auf, sag mir das nicht, ich will das gar nicht wissen." Ich meine, wie blöd kann man denn sein? Sich auf ein durchaus gefährliches Territorium zu begeben, und das Internet ist ein gefährliches Terrain, wenn man ein Windows-User ist ganz besonders. Die lauern überall auf irgendetwas, was nicht

gepatched ist und die schnappen sich jede Maschine, die sie kriegen können erstmal und machen dann Blödsinn mit der Maschine und plötzlich ist die Kripo dann vor der Tür, weil auf deinem Rechner, das ist ein typisches Beispiel, weil auf deinem Rechner Kinderpornographie gehostet wird. Das passiert praktisch alles auf gekidnappten Rechnern. Das heißt, eine jede Internetsperre, da greift man sich auf den Kopf über soviel populistische Dummheit. Das sind infizierte Rechner. Die haben Schadsoftware drauf und werden von jemandem ferngesteuert bzw. bei der Kinderpornographie machen sie sich oft gar nicht die Mühe, sondern mieten einfach irgendeinen Webspace bei einem großen Provider, das kannst du ja über das Netz, zahlen mit einer falschen Kreditkarte, das machen sie immer, die auf wen ganz anderen ausgestellt ist und bis dass eben beeinsprucht wird, mieten sie da mit dieser gefakten Zahlung Speicherplatz auf irgendeinem Webhost bei einer Webhosting-Agentur, das kriegt man ja irrsinnig billig schon, und versuchen das dann in Kombination mit Spam, das zu bewerben. Häufiger tun sie es natürlich mit etwas anderem, mit Phising-Websites und sonst was. Also, das wird alles auf den Rechnern gemacht von nichts ahnenden Benutzern. Und da sagt mir einer: „Ich will ja das gar nicht wissen, was mich bedroht." Ich meine, macht der auch beim Autofahren auf der Autobahn die Augen zu, wenn es gefährlich wird? Man sieht haufenweise völlig irrationales Verhalten. Die, die schon ein bisschen eine Ahnung haben, dass das gar nicht alles so gerade aus und einfach und hübsch und schöne, neue Kommunikationswelt ist, da gibt es zwei Gruppen. Die einen interessieren sich dafür und die anderen versuchen das mit aller Macht zu verdrängen, weil sie unbedingt so weiter tun wollen wie bisher, weil das so leiwand war. Da kommt es zu den perversesten Reaktionen, wirklich zu den ärgsten Reaktionen. Dass sie eben sagen: „Nicht sagen." „Um Gottes willen, du kannst doch nicht die Datei so verschicken!" - „Ah." Oder wenn man ihnen erzählt, sie sollen keine Attachements schicken. Dann schauen sie alle wie die Autobusse. Dann muss man ihnen sagen: „Fucking E-Mail ist nicht für fucking binary data." E-Mail ist, da wird alles im ASCII-Code prozessiert am Mailserver. Damit kannst du keine einzige Schadsoftware dir einfangen durch eine normale E-Mail ohne Anhang. Geht nicht. Nein, aber sie müssen auch noch über Mailserver, auch wenn man eh Dateien anderswo austauschen kann mit FDP und das geht eh schon auf so vielen Websites. Nein, sie schicken es via E-Mail, da muss das gesamte Attachement im Mailserver umgecodet werden in ASCII-Code und dann am anderen Ende nach dem Prozessieren wieder hergestellt werden als Doc-File oder so etwas. Erstens ist es einmal riskant, dass da irgendein Bitfehler oder irgendetwas passiert und sich das Dokument dann nicht öffnen lässt. Und zweitens belastet man die Mailserver mit einem völlig unsinnigen Vorgang, für den sie nicht gebaut sind. Die sind dafür gebaut, schnell und verlässlich Text zu kommunizieren und das andere ist eine Krücke. Das soll man nicht tun. Die Leute verschicken die einfachsten Texte als Word-Doc. Das führt nur dazu, dass die Gegenseite länger braucht, um es zu öffnen und das ist genau im Fall der Aufmerksamkeitsgesellschaft tödlich, vor allem für PR-Leute. Du musst deine Message ganz vorne haben. Ich zähle das alles nur auf als Beispiel dafür, wie wenig generell mit sämtlichen Internettools umgegangen wird und wie selten richtiger und sicherer Umgang ist.

8) Der nächste Block ist Überwachung. Macht es einen Unterschied, dass wir Daten freiwillig hergeben oder gibt es sowieso anderweitige Methoden der Datenerhebung?
Ich würde einmal sagen, das ergänzt sich. Gewisse Sachen können wir nur selber von uns weitergeben, weil die sind eigentlich nirgendwo aktennotorisch. Also kann es auch niemand anderer so einfach wissen, außer ich erzähle es. Das ergänzt sich prima, um bestehende Profile abzugleichen und um Profilzüge zu ergänzen, die man aus den eigenen Datensätzen, wo gewisse Interessen sich in den eigenen Datensätzen nicht so widerspiegeln, ja. Ein Beispiel: Mein Netzbetreiber hier weiß zum Beispiel, dass dieses Telefon sehr selten unterwegs ist, weil ich das meiste von hier aus mache. Er kann natürlich aus seinen Daten ganz einfach Kundenprofile erstellen, wie viel telefoniere ich, wie oft ins Ausland, welche Nummern, so für Marketingzwecke zum Beispiel. „Wir bieten Ihnen jetzt ein neues Rundum-Sorglos-Paket an, das genau für Ihre Ansprüche passt, ja. Sie haben so und so viele Auslandstelefonate, das ist alles inkludiert und weil sie so ein Telefonverhalten haben, bieten wir Ihnen das und das an zum immer fixen Preis." Das ist zum Beispiel eine Form, wie es die Telekoms und wie die Telekoms diese Daten benützen, um ihr Geschäft zu optimieren und viele andere auch noch. Aber sie wissen nicht, sie können es zum Beispiel nicht in Zusammenhang bringen mit meiner Internetusage und meinen Internetinteressen, weil ich bei *Orange* kein Kunde bin internetmäßig. Wenn ich da unterwegs bin, benütze ich einen Netzzugang von *Drei*. Hier habe ich einen Zugang von *UPC Inode*. Ich habe meine Daten auf drei verschiedene Anbieter aufgeteilt, die Konkurrenten sind. So kann ich mir sicher sein, dass es bei dieser Aufteilung bleibt und keiner zuviel weiß. Niemals alles aus einer Hand nehmen. Wer das macht ist stupid, wirklich.

9) Was wären da dann die größte Gefahr, wenn einer zuviel weiß?
Der erpresst Sie. Entweder auf freundlich, indem er ein Produkt andrehen will oder, und das ist in letzter Zeit ja irrsinnig oft passiert, die Daten gehen verloren. Das ist der gefährlichere Fall. Die gehen ja einfach verloren, die kommen denen aus. Und wenn sie einmal kopiert sind, sind sie verloren, obwohl sie noch da sind. Weil sie haben sich dupliziert und damit sind sie in der Hand eines Unbefugten und die haben bis jetzt nur so Zeugs gemacht wie Erpressung. In Italien war es ein ganzer Erpresserring, der eine eigene Agentur gehabt hat. Da konntest du dir Telefonverkehrsdaten von beliebigen Anschlüssen bestellen. Sind, ich glaube, zwölf

Verhaftungen, nein 24, darunter die Hälfte ungefähr Techniker und die anderen zwölf Verhafteten waren lauter Carabinieri und der stellvertretende Militärgeheimdienstchef. Die haben alle mitgeschnitten. Also das war rein mafiamäßig. Und die haben auch die ETSI-Überwachungsschnittstellen, die ja für die Polizei sein sollte, um die Verbrecher zu überwachen, die haben sie, dort haben sie die Promis abgehört und die Interviews teuer den italienischen Zeitungen verkauft, die Telefonate. Fußballer, da gab es ja den Begriff *Laziogate*, das waren genau diese Typen. Die haben da die Fußballpräsidenten abgehört am Telefon und haben das Transkript am nächsten Tag in der Zeitung gedruckt. Also, das ist nicht irgendwie ein vielleicht einmal vorstellbarer Fall. Dieser Fall bei der *Telekom Italia* hat bitte mit dem Tod des Netzwerk-Security-Chefs geendet. Der ist in Neapel von einer Brücke gestürzt, Selbstmord ohne Abschiedsbrief. Und ein Jahr davor ist dasselbe in Griechenland passiert. Der Sicherheitschef von *Vodafone Greece* wurde erhängt aufgefunden, einen Tag nachdem aufgeflogen ist, dass die komplette Regierung rund um die Uhr abgehört worden ist von Unbekannten, die die ETSI-Schnittstellen gehackt hatten, in *Ericssons* Telefonnetz. Das ist die Regel, dass Daten verloren gehen. In den USA vergeht kein Tag ohne dass wieder 200.000 Datensätze im Nirwana verschwinden und danach tauchen sie bei den Spammern zum Beispiel auf. Das ist noch die harmloseste Variante und da steht halt: „Wir haben ein Verzeichnis aller Ärzte des Bundesstaates Kentucky. Vorname, Nachname, Sozialversicherungsnummer, alles. So und so viele Dollar, wenn du es haben willst für Marketingzwecke." Also, mit diesen Daten wird gedealt und bei dem jüngsten Datenskandal bei der *Deutschen Telekom*, da wird gerechnet, dass die Zahl der Datensätze, die da abgezogen wurden, die sind dann in Rotlichtkreisen wieder aufgetaucht. Datensätze von Kunden von der *Deutschen Telekom* und dass die Daten einen verwertbaren Wert von jährlich 50 Millionen Euro darstellen. Ja bitte, das ist doch nicht nichts. Einen Coup landen mit 50 Millionen Euro. Das ist nicht einmal in einem Postzug drinnen, ja. Nur damit man die Dimension sieht. Das heißt, durch diese ganzen Wahnsinnsdatenansammlungen, die dann schlecht geschützt sind, das ruft einfach die Einbrecher auf den Plan, wenn die Daten zu verwerten sind. Und als Daten kann man sie auch sogar relativ leicht anonym verwerten. Es sind ja nur Daten. Die kann man ja virtuell herum schieben, wo man will. Die kann man ja irgendwo deponieren und gegen ein Passwort zugänglich machen oder sonst was. Das geht irrsinnig einfach. Und da sehe ich die größte Gefahr und die allergrößte Gefahr geht natürlich von Mitarbeitern des Unternehmens selbst aus. Sieht man doch bitte. Man müsste Techniker in der Schweiz werden, IT-Techniker bei einer Schweizer Bank. Das ist ein Traumjob. Du kannst nach zwei Jahren, wenn du Glück hast, mit zweieinhalb Mille in Pension gehen und kriegst vom deutschen Bundesnachrichtendienst noch dazu eine neue ID. Ach wie nett, das ist doch schön, es gibt doch noch Chancen im Leben.

10) Wer nutzt Social Networks zu Überwachungszwecken?
Alle.
Von - bis?
Vom amerikanischen Geheimdienst NSA bis zum investigativen Journalisten Erich Möchel nutzt jeder Social Networks um Personen seines Interesses, Details über diese Personen zu erfahren und ihre Affiliationen. Ich sage dir ein Beispiel. Ich habe da jetzt einen Vortrag beim Chaos Computer Club gehalten des Inhalts: Die Schnittstellen, also die technischen Schnittstellen für die Vorratsdatenspeicherung, wie diese Daten übertragen werden und die Datenbankstruktur für die Vorratsdatenspeicherung, wie das technisch genau, wie die Felder anzuordnen sind und so weiter und so fort. Macht im *European Telecom Standards Institute* das britische *Government Communications Headquarters*. Das ist bitte das *NSA*-Gegenstück und ein militärischer Geheimdienst. Die stehen sogar dabei, die Namen. Die *NSA* hat wiederum in den letzten Jahren nur irgendwelche Veranstaltungen, die ganz im Fokus waren, so Veranstaltungen, wie man Intelligence gewinnt aus Public Intelligence, also öffentlich vorliegende Information. Damit meinen die natürlich Social Networks, weil da verraten die Leute ja Zeugs. Naja, ein Teil dieser Geschichte behandelte eine zweite Militärgeheimdienstlerin, die auch da drinnen sitzt und an den Standards mitarbeitet und diese Dame ist Oberstleutnant der *US-Airforce* und sie arbeitet für eine Firma namens *Tridea Works*. Die hat auf ihrer Website keine Geschäftsführung, keinen Firmensitz, nichts. Es steht dort nur in ganz, fünf dürren Kapitel, dass sie sich gut mit Telefonie-Netzen auskennen und gerne beraten. Und wenn du dann schaust, wo diese Firma ist und wer das ist, wir haben das dann ganz gut rausgekriegt. Wir hatten dann auch Fotos von der Dame gefunden, die sogar das *Department of Defence* veröffentlicht hat vor zehn Jahren, da sahen wir dann die Lady, ich schick dir dann die Links, kannst du dir anschauen, ist alles auf *Krypton* (???) öffentlich, was ich dir jetzt hier sage, auf Englisch, mit geschwärztem Gesicht und einem Notruffunkgerät bei der Koordination einer Militärübung. Die sitzt auch drinnen im Europäischen Standards Institute und hilft dabei, Standards für die Vorratsdatenspeicherung zu machen. Na, wie nett. Und bezahlen tut das durch diese Firma *Tridea* das *Space and Naval Warfare Center*. Das war auch leicht rauszukriegen. Und dann haben wir geschaut: Ja, wer könnten denn da die Mitarbeiter sein für diese Firma? Na, genau eine Minute habe ich gebraucht, dann hatte ich die komplette Firma abgebildet auf dem Social Network *Xing*, alle Angestellten schön aufgelistet. Auf der Website tun die irre geheimnisvoll, kein Name, kein Headquarters und dann findest du einen Namen raus und gehst in ein Social Network und ziehst mit einem Fischzug alle raus. Das meine ich, wie man das gebrauchen kann. Na, glaubst du, das was ich Würstel kann, das kann die NSA nicht? Die kann das automatisiert. Das könnte ich auch mit ein paar guten Technikern von der *Quintessenz* oder aus dem *Metalab*, selbst zusammenschustern,

weil so bei: So Anforderungen formulieren an ein System, das kann ich ziemlich gut, wenn ich es auch nicht selber bauen kann. Und dann noch ein bisschen Geld braucht man auch dafür. Das ist nichts mehr rocket science wie früher. Es arbeitet jeder nur mehr auf Over the Shelf, COTS-Equipment nennen das die Amis, Customized Over the Shelf, also Massenware. Die *NSA* arbeitet mit demselben Typ Hardwarerechnern wie wir. Sie tun es nur ein wenig anders konfigurieren. Also es ist alles in der Beziehung mit Überwachung anders geworden. Die Überwachung ist, früher hieß es, teure Spezialgeräte bei den Geheimdiensten, die sie alle selbst gemacht haben oder gegen Geheimauftrag irgendwo gegeben haben und dann da auf der anderen Seite das Ziel und was ist heute? Die Überwachung ist in den Netzwerken drinnen, sie ist integriert, sie ist ein Feature der Netzwerke und technisch auf der anderen Seite hat sich aber der technische Abstand zwischen den Geheimdiensten und Usern, die vielleicht was gegen die haben, sehr verringert. Also, der technische Fortschritt spielt nicht allein denen in die Hände, die den nur ausnützen, um weitere Überwachungsmethoden einzufordern. Bei jedem Ereignis wird stereotyp gesagt: „Wenn wir mehr Überwachung gehabt hätten, dann wäre das nicht passiert." Das sind lauter unbewiesene Behauptungen, lauter unbewiesene Behauptungen. Man hat im Gegenteil schon jetzt vielmehr den Eindruck, aber diese Nachrichten muss man sich von weit weg zusammentragen, aber es ergibt sich das Bild: Sie brauchen jetzt Softwares, vor allem die Briten, die das mit dem Überwachungskamerawahnsinn am weitesten getrieben haben. Jetzt brauchen sie Softwares unbedingt, die diese Kameras automatisch überwachen auf besondere Vorfälle, weil die Leute mit dem Schauen nicht mehr zusammenkommen und weil man draufkommt, dass das gar kein Traumjob ist, sondern dass das irre anstrengend ist, zwölf Bildschirme parallel im Auge behalten zu müssen, dass die Beamten ab einer kurzen Zeit völlig ineffizient sind und man sie eigentlich so wie die Fluglotsen im Stundenrhythmus tauschen müsste. Weißt du, was das dann kostet? Mörderkohle, das kostet weit mehr als es je einspielen kann. Die Überwachung hat die *Wiener Linien* ich weiß nicht wie viele Millionen gekostet, mit Kameras und wenn man es so aufrechnet gegen die Vandalismusfälle, gegen die Vandalismusschäden pro Jahr, haben sie gesagt, das sind 300.000 Euro. Dann würde das Kamerasystem, das sie jetzt überall eingebaut haben, 25 Jahre problemlos laufen müssen, um diese Kosten wieder hereinzuspielen. Das ist bescheuert, ganz einfach. Wenn die untertags öfters mal Leute durchschicken, die den Wagen kehren, dann geht der Vandalismus zurück. Weil dann sagen die Leute: „Okay, das kann ich jetzt auch nicht machen, den Sitz aufschlitzen, während die da zusammenkehren. Das wäre unfair, ja." Weißt so. Nur, wenn alle das Gefühl haben, es ist eh wurst, der haut eh auch die Zeitung hinunter, dann schaut es sofort aus in einer Bim. Da gibt es so gruppendynamische Effekte und mit Kameras hältst du da überhaupt nichts ab. Die Plätze, die am stärksten mit Kameras und am längsten mit Kameras gesichert sind, sind die Banken. Na, was ist mit der Zahl der Banküberfälle? Sind die signifikant zurückgegangen? No, die sind gestiegen trotz Kameras, obwohl überall jetzt schon eine ist, oder mehrere. Es gibt nichts mehr, was keine Überwachungskamera hat. No, kein einziger ist dadurch verhindert worden. Die ziehen sich einfach etwas über den Kopf und sagen: „Kohle."

11) Welche Motive stehen hinter der staatlichen Überwachung?
Man hat es einmal probiert. Dann hat man gesehen, die großen Fische gehen einem so sicher nicht ins Netz und dann sagt man: „Jetzt haben wir es schon, jetzt machen wir das und das damit." Das wird immer sofort downgescalt. Wenn neue Überwachungsmethoden kommen, wird groß herumtrompetet, Vorratsdatenspeicherung Musterbeispiel. Das geht stereotyp seit zehn Jahren so. Irgend etwas passiert, ein Bombenanschlag, ein Attentat, große Betroffenheit und danach großes Geschrei: „Mehr Überwachung hier, mehr Überwachung da, dann hätten wir und dann dings", und dann muss die EU handeln, Richtlinie, ja, die wird dann so eher breit formuliert, dass jeder nach seinem dings, also dass es nationale abweichende Implementierungen geben kann, und in dem Moment, wo das in nationales Recht umgesetzt wird, werden plötzlich, sind plötzlich die Filesharer mit dabei. Delikte, die gerade mit einem halben Jahr bedingt bestraft werden und auch nur in schwereren Fällen sind plötzlich unter Schwerstverbrechen und Terrorismus. Es wurde dezidiert nur für Schwerverbrechen und Terrorismus eingeführt und jetzt wird verhandelt, ob man sogar unter ein Jahr mit der Schwelle gehen sollte. Ja, sollen sie gleich sagen, sie wollen alles damit tun. Und genau auf dasselbe läuft es immer raus. Das geht so scheibchenweise. Die Salami verschwindet, die Freiheit verschwindet wie eine Salami scheibchenweise, aber schnell.

12) Dann zu wirtschaftlichen Unternehmen. Was fangen die mit den Daten an, die wir freiwillig hergeben?
Das nennt man Business Intelligence, die haben schon einen Begriff dafür. Die Unternehmen wollen natürlich möglichst viel über ihre Kunden wissen, weil je mehr man über den Kunden weiß, umso mehr kann man ihm verkaufen, ist klar. Da braucht man nicht lange nachdenken, was das für Gründe sind. Die anderen Unternehmen, also diese Web 2.0-Betreiber, na ja das ist ja denen ihr Geschäftsmodell: „Hier komm hierher, treibe alles Mögliche, was du sonst verstreut treibst in meinem Reich. Ich biete dir so und soviel Giga gratis. Du kriegst das, das, das und das und kannst das auch noch nutzen. Wir kriegen dafür dein Profil."

13) Das zielt vor allem darauf, dass Werbung geschaltet werden kann?

Ganz einfach Vermarktung, wenn die sagen: „Wir haben da jetzt, wir zeigen dies…“ Bei *Google* ist es ja so, wenn du ein großes Unternehmen bist, und einen großen Auftrag bei *Google* abgibst, dann schicken sie dir schon einen Verkaufsberater. Der sagt dann: „Okay, wir schalten Ihr Inserat immer nur dann, wenn ein User mit dem bestimmten Interessensprofil auf der Page ist, dem zeigen wir es. Und was wollen Sie gezielt für eine Zielgruppe, gezielt? Und dann schaust ganz einfach im Interessensprofil. Da gibt es so, was lesen die Personen gern in welchem Alter und in welcher Stellung, also wo du Rückschlüsse ziehen kannst, wonach er sucht, wer er ist. Und das kostet dann mehr, wenn wir es nur denen spielen und dann kannst du dir die Zielgruppen praktisch aussuchen, das heißt, du kannst sagen: ‚Okay, mit dieser Kampagne ziele ich auf die, aber nur auf die. Und den anderen zeige ich es lieber gar nicht, weil das würde vielleicht sogar einen gegenteiligen Effekt haben auf meine Kampagne. Ich mache drei verschiedene, aber das was im Fernsehen ist, was im Fernsehen läuft, dazu kommen noch zwei im Internet für eine andere Zielgruppe. Das wandeln wir so und so ab.’“ Das ist natürlich für jemanden, der einen Market hat, Traumland, für den ist das super, der kriegt es genau runtersegmentiert, so wie er es runtergebrochen hat in der Analyse. Er kriegt genau die Leute nach den Eigenschaften, die er selber in seinen Daten hat. Damit kann man es rückvergleichen, und und und, also es gibt da jede Menge Methoden. Du kannst den ganzen Verkauf optimieren mit so etwas, in einer Firma.

14) Wer wertet die Unmengen an Daten dann aus? Passiert das schon alles automatisch?
Algorithmen.
Oder sind da Menschen dahinter?
Ja, die stehen dann ganz am Ende der Datenkette. Die nehmen dann das, was er ausspuckt. Und darum können ja diese Datensammler irrsinnig oft behaupten: „Wir sammeln keine persönlichen Daten über Sie und auch nicht Ihre IP-Adressen“, so wie *Google* sagt, ja. Glaube ich ihnen auch, weil *Google* braucht die IP-Adressen nur einmal ganz am Anfang kurz. Und ansonsten interessiert sie die IP-Adresse relativ wenig, weil nämlich die Browserkonfiguration… Du glaubst es nicht, wie individuell sich die Leute in ihrer Browserkonfiguration unterscheiden. Und gerade die geübteren User haben ein charakteristisches Bild an PlugIns, was sie verwenden, welches Betriebssystem sie haben, wann sie wechseln, usw., ja, ob sie Java-Script aktiviert haben oder nicht.

15) Wie weit werden die Auswertungsmöglichkeiten noch gehen, also werden die laufend verbessert?
Unbegrenzt, das ist vollkommen unbegrenzt. Wenn du so genaue Datensätze hast, ja, kannst du alle möglichen Fragen an diese Datensätze stellen. Das kannst du zweitverwerten, drittverwerten, viertverwerten und jeweils für andere Produktlinien, für andere Firmen, andere Teile aus diesen Datensätzen. Das heißt der Vermarktbarkeit sind da überhaupt keine Grenzen gesetzt und das ist ein völliger Mythos: „Das sind eh so viele Daten, die können sie ja eh nie alle durchschauen und mich wird man schon nicht finden.“ Das ist so ein grandioser Irrtum. Das ist falsch, das stimmt schon seit zehn Jahren nicht mehr. Ganz einfach, das ist falsch, das ist Blödsinn. Wer das sagt, hat keine Ahnung und muss sich belehren lassen. Natürlich geht das. Das kann ja sogar ich. Es gibt zehn verschiedene Open Source Data-Mining-Tools für *Linux*. Das ist trivial. Das Schwierige dabei ist, die Fragen zu formulieren, was will ich eigentlich wissen. Du kannst nicht full-random da drüber gehen über die Datensätze, da werden die Ergebnisse auch full-random sein, Zufall.

16) Dass da vielleicht Prognosen schon erstellt werden können, über die Zukunft?
Das machen die jetzt schon, das machen die doch jetzt schon. Das ist doch Teil der Profile. Die wissen, was du heute tun wirst aller Wahrscheinlichkeit nach, weil du am Dienstag immer das tust. Und wenn du das einmal nicht tust, schlägt das System Alarm, wenn vom Verhaltensmuster abgewichen wird. So kannst du es auch einstellen. Also du kannst endlos Dinge machen mit diesen Daten und das geht sehr wohl in die Zukunft. Du kannst sagen: „Die letzten drei Jahre ist er im Juni immer in Griechenland gewesen. Aha, heuer fährt er gar nicht. Ist er krank?“ Ja, ist so, wenn ich die Daten habe, das ist ein Kinderspiel, das rauszukriegen. Da brauche ich nur schauen, wo das Mobilfunk, in welcher Funkzelle das eingeloggt war. „Aha, sieht man eh, Homing aus Griechenland.“ Kinderspiel.

17) Vielleicht gesellschaftliche Prognosen?
Wenn es so weiter geht, ist es finster, sind sie finster. Nur ich habe so das Gefühl, dass sich irgendwie das Momentum der Überwachungswelle etwas verflacht. Das hat nicht mehr die Dynamik wie in den letzten Jahren. Es gibt plötzlich Zeichen, dass da auch in der Politik angefangen wird, umzudenken, weil der ganze Schas in Wirklichkeit nichts bringt und nur teuer ist. Ich meine, wir leben im Zeitalter der Virtual Private Networks. Das ist eine *Linux*-Maschine, das ist eine *Linux*-Maschine, da hinten ist eine *Linux*-Maschine und wenn ich die drei irgendwo verteile auf der Welt und mit einer VPN-Verbindung, die bitte da im Betriebssystem integriert ist, diese drei Maschinen miteinander über das Internet vernetze, dann kann sich jede *NSA* brausen gehen, weil sie diese Verschlüsselung nicht in Echtzeit aufkriegen. Aus Pause. Das kriegen sie nicht auf. Das ist mit einem von ihnen selbst approbierten Algorithmus, dem *ARS* und der ist öffentlich und den haben sich alle namhaften Kryptographen weltweit angeschaut und bis jetzt ist keine Angriffsmöglichkeit bekannt, wo man sozusagen quer hineinkäme an die Daten, indem man gewisse völlig umständliche

Rückrausrechnungen eben nicht brute force macht, das heißt, es werden einfach alle Kombinationen durchprobiert, sondern dass man da seitlich reinkommt. Wie gesagt, das gilt einfach als sicher. Wenn ich diese drei Rechner mit dem zusammenhänge, dann können sie sich die Vorratsdatenspeicherung auf den Bauch hauen, dann können sie sich auch die Echtzeitüberwachung auf den Bauch hauen und überhaupt alles andere auch, weil die drei kommunizieren miteinander in einem geschlossenen Netzwerk und da bin ich drinnen und sonst keiner bzw...

18) Aber das ist eher eine Ausnahme?
Das hat doch jede Firma. Das hat jede Firma, das ist Standard bei jeder Firma, die Außenstandorte hat, weil sie ja sonst anfällig gegen Hacker ist, wenn du das nicht machst. Du kannst nicht ins Firmennetz, du kannst aus dem Firmennetz heraus nicht einfach eine ungesicherte Verbindung über ein fremdes Netz drüberjagen und dann Firmendaten, vertrauliche drüberleiten. Das geht über lauter fremde Router im Klartext drüber. Wenn da bloß einer deppert ist und ein Programmerl geschrieben hat, der sagt: „Alles, was an Switch-Ausgang *Switch 1* reinkommt, bitte auch auf Ausgang *Switch 2* kopieren." Das geht, das ist in den Geräten drinnen. Genauso wie ein Virtue Private Network da drinnen ist. Glaubst du nicht, dass jeder bessere Verbrecher das natürlich sofort benutzt und nicht mit dem Handy, sondern über Voice over IP telefoniert über ein VPN. Aber natürlich, und damit sind diese ganzen Maßnahmen schon wieder nur mehr gegen Eierdiebe gerichtet und gegen Filesharer. Das möchte die Musikindustrie gern, weil denen bringt das etwas, natürlich. Nur leider sieht der Gesetzgeber das nicht vor, weil das wurde ja im Kampf gegen den Terrorismus, wird das ja gebraucht, angeblich, ja, wo es genau nichts nutzt. Nein, ich meine, das musst du mir erzählen, welcher Terrorist ist nach all diesen Vorfällen so blöd und telefoniert mit einem Handy und tut ungesichert über E-Mail kommunizieren. Das tun die Deppen, die kleinen Leute, die kleinen Betrüger, genau solche fängt man damit. Die, die eh eine Woche drauf dann von selber über ihre eigenen Haxen fallen, weil Betrüger sind dumm. Die haut es immer, sie sind zwar irrsinnig gerissen auf der einen Seite, aber sie haut es immer mit ganz, ganz hoher Sicherheit irgendwann auf, ja. Einfach, das ist so sicher wie das Amen im Gebet. Na und dafür machen wir so eine Generalüberwachung der gesamten Bevölkerung. Ich meine, die Juristen reden immer von Angemessenheit und Ausgewogenheit. Ich meine, du kannst natürlich auch mit einer 8,8er-Flak auf einen Spatzen schießen, aber ob das einen Sinn macht.

19) Kann man da auch im Internet von einem technischen Rüstungskampf sprechen?
Ja sicher, sicher. Was die an Überwachung dazukriegen, das kriegen wir an Waffen in die Hände. Uns überwachen die nicht so einfach. Das möchte ich einmal sehen, ob mir da einer über die Firewall so einfach kommt. Ich kenne die besten zwei Forensiker in Wien, ja. Wenn ich irgendeinen Verdacht habe, gibt es eine kurze verschlüsselte E-Mail an den einen und sage: „Schau dir bitte meinen Router an, hier ist das Passwort. Da stimmt etwas nicht." Also da kommt keiner rein, so einfach.

20) Denken Sie, dass generell Überwachung im Web 2.0 personalisiert wird?
Vollständig, vollständig. Das basiert ja auf dem Ganzen. Ich meine, die Leute sind ja so wahnsinnig, dass sie… Also, da war ich, ehrlich gesagt, auch ich ein bisschen baff. Als ich mir so einen *Facebook*-Account zulegte, den ich für ganz andere Zwecke unter anderem Namen habe, poppte mir entgegen: „Um deine Freunde schneller kennen zu lernen, gib uns doch hier deinen Zugang zu deinem Web-Mail-Account." Was? Username und Passwort. Oder „Lade dein Adressbuch hier herauf." Ja, die Leute tun das alle, die Leute tun das alle. Und damit gefährdest du auch Dritte. Ich sage dir ein Beispiel: Als ich diesen Zombie losgeschickt habe, den Hakank Merzenogian, hatte der am Anfang überhaupt keine Kontakte. Ich wollte nur einmal schauen, wie das ist. Kommt da viel Spam drinnen, gibt es Betrüger und so was, weil über kurz oder lang klappern die ja alles ab, ja. Und auf einmal poppt mir da eine Message auf der Website entgegen und da steht: „Hey Erich." und ich: „Psst, ja, nichts Erich", und dann maile ich mit dem Typen. Das ist einer von der Richie Birker (???). Das ist einer von denen, die immer noch daran glauben wollen, dass es eh zu viele Daten sind, weil er sich halt so urgern präsentiert, ja und sagt: „Naja, wird nicht so schlimm sein. Weißt eh, ich halte ja von diesem ganzen Dings da nicht so viel wie du", und damit sagt er: „Bist ein Volldepp." Habe ich gesagt: „Wie kann das passieren, wie hast du denn das gefunden?" Hat er gesagt: „Ich weiß nicht, ist mir einfach entgegen gepoppt." Hakank Merzenogian ist ihm entgegengepoppt! Dann habe ich gesagt: „Du Trottel hast denen deinen E-Mail-Zugang gegeben." Sagt er: „Ja, ich glaube." Da hat er einen *Quintessenz*-Newsletter drinnen gehabt und da ist eben dieselbe Mail-Adresse *hakank@quintessenz.org* verwendet worden wie die, die ich dort zur Anmeldung genommen habe und *Facebook* hat die Daten über, hat uns zugeordnet, weil sie Mails von mir in seinem Postfach gefunden haben. Naja, die haben einen Vogel, die so was machen. Und sie wissen auch überhaupt nicht und deswegen bleibe ich dabei, dass die Leute mit diesen Tools nicht umgehen können. Etwas, was da *Facebook* und Co fordern, das ist auch arbeitsrechtlich relevant. Wenn ich zum Beispiel meinen ORF-Usernamen und mein Passwort weitergebe, ist das ein Grund für eine fristlose Kündigung. Also, das ist das Spiel, das diese Web 2.0-Betreiber betreiben. Sie fordern die Leute zu einer vollkommen gefährlichen Handlung auf in jeder Beziehung. Ich meine, du würdest doch nicht einem wildfremden Unternehmen da bei uns dein Adressbuch in die Hand drücken und sagen: „Kopiert es euch, wenn ihr es brauchen könnt." „Ja, da können wir Ihnen bessere Produkte liefern", sagt der Greißler, „Gib mir dein Adressbuch!" Das wäre ja absurd

die Vorstellung und da sagen die: „Ja, ist halt *Facebook*." Und denen ihr Geschäftsmodell ist mit diesen Daten ein Geschäft zu machen natürlich. Also die Leute wissen einfach nicht, was sie tun da in diesem Fall. Nur schön langsam setzt sich bei manchen schon die Erkenntnis durch, weil man es doch immer öfters hört, dass jemand einen Job verloren hat oder nicht gekriegt hat wegen seinem Profil, ja. Da setzt sich schon schön langsam, ich meine, es ist ein bisschen raus die Wucht, dass die Bürger gesagt haben: „Ja hurra, mehr Überwachung, ja ja, dann sind wir sicher." Hat man eh gesehen, dass es nicht mehr Sicherheit bringt. Was hat das Londoner Kamerasystem verhindert? Gar nichts. Alle Bomben sind in die Luft gegangen, sie haben nur nachher schneller gewusst, wer es war. Na super und dafür so eine Rieseninvestition. Das meine ich damit.

21) Sehen Sie auch irgendwelche Vorteile in der Entwicklung hin zu mehr Überwachung?
Ja, weil die Opposition wächst dadurch schneller, und sie wächst tatsächlich schneller. Bitte in Deutschland haben 30.000 Leute Vollmachten zu einer Verfassungsklage unterzeichnet gegen die Vorratsdatenspeicherung. Bei einer Demonstration in Berlin waren knapp 100.000 Leute auf der Straße. Das wäre vor drei Jahren völlig undenkbar noch gewesen, dass es überhaupt Demos zu dem Thema gibt und jetzt passiert das. Hier in Österreich ist es die halbe Republik ist gegen diese Vorratsdatenspeicherung. Sämtliche Journalistenvereinigungen, die gesamte Privatangestelltengewerkschaft ist dagegen. Die Ärztekammer, die evangelische Kirche, die katholische Kirche verlangt eine Ausnahme für ihre Telefonseelsorge. Es ist die Wirtschaftskammer dagegen, es sind die Internetprovider, die Telekoms dagegen und es traut sich fast überhaupt keiner sagen, dass er dafür ist, weil inzwischen diese Argumente Pro ins Nichts zerronnen sind, weil diese ganzen populistischen Pseudoargumente, was man da in den letzten Jahren aus Deutschland an populistischem Blödsinn gehört hat, ja, das hat einen die Haare sträuben lassen. „Wir stellen jetzt Stopptafeln gegen Kinderpornos auf." Ich meine, eine geisteskränkere Idee habe ich noch nie im Leben gehört. Noch etwas Blöderes und Uneffizienteres kann man nicht tun eigentlich. Und das wurde da in der Öffentlichkeit ganz einfach abgehandelt als wichtige und wunderbare Möglichkeit von lauter Blinden, die von der Farbe geredet haben. Oder Leute, und das finde ich das eigentlich Schlimmste und die erbärmlichste Sorte von Politikern, das sind die, die wider besseres Wissen handeln, die intelligent genug sind zu erkennen, dass das ein politischer Blödsinn ist und ein technischer Unsinn ersten Grades, was sie da gerade vorschlagen, aber es passt, es ist nicht ein politischer Blödsinn, ich korrigiere das, es ist ein technischer, völliger Unsinn, aber sie brauchen dieses Argument jetzt gerade, um irgendein anderes Ziel zu erreichen oder sie benutzen das Argument nur, damit es ein anderer nicht aufbringen kann. Das ist auch schon vorgekommen. Sehr oft bei ÖVP-Politikern, wenn sie den rechten Rand, wenn sie sich nach rechts stark machen so wie nach dem Motto von Franz Josef Strauß in der CSU „Rechts von uns darf es niemanden geben, ja!" Also muss man selber so weit rechts sein.

22) Nochmals kurz, sie sind zwar eh schon angesprochen worden, aber was sind die größten Gefahren, die von einer Überwachung ausgehen?
Die größten Gefahren sind, dass sich die User nicht wehren oder zu wenig wehren, dass die andere Seite die Oberhand bekommt. Das ist meiner Meinung nach die größte Gefahr. Ich bin kein Schwarzseher, der sagt: „Jetzt sind wir schon, fast werden wir im BigBrother-Staat versinken, es wird ein Rollback geben." Es ist keine Welle in einer, sagen wir in einer Gesellschaft hat es niemals eine Welle von irgendetwas gegeben, die immer gleich ungebrochen weitergegangen ist. Es hat immer in absehbarer Zeit zu einer Gegenbewegung geführt und die scheint jetzt schön langsam einzusetzen, weil das Zeugs funktioniert genau gegen das… Wogegen es funktionieren soll, da funktioniert es nicht. Es funktioniert nur auf fünf Ebenen drunter, bei Leuten, die sich eben nicht verstecken oder die zu blöd sind, sich zu verstecken, ja. Und das setzt sich doch schön langsam fest, dass das kein Allheilmittel ist. An der Gemeinde Wien sieht man auch ein Umdenken zum Beispiel. Ich weiß nicht, wie oft die den österreichischen *BigBrother*-Award schon gekriegt haben in der Kategorie, einmal in der Kategorie *Business* und einmal in der Kategorie, was weiß ich, *Behörden und Verwaltung*. Es war eine Überwachungsmaßnahme nach der anderen in den letzten Jahren, von denen gesetzt. Was hat es gebracht, die ganzen Kameras? Nicht wirklich etwas. Es hat natürlich den obligaten Bilderskandal schon gegeben. Da gab es dann Filmvorführungen aus der Überwachungskamera, wo die lustigsten Szenen… Ich meine, das ist alles kurz vor *Youtube* gewesen. Und im letzten Jahr haben sie dann noch so eine Fragebogenbefragung gemacht und da haben sie dazugeschrieben: „Sie können ihn ja auch anonym ausfüllen", aber haben einen Barcode draufgegeben mit der Ordnungszahl des Gemeindebaumieters. Aber einen Barcode, einen 2D-Barcode, wo du es nicht gesehen hast, was drinnen ist, ja und drauf ist gestanden: „Sie können es anonymisiert abgeben und wie sind Sie mit Ihren Nachbarn zufrieden?", also heikle Fragen. „Wie ist das Wohnklima?" Sehr persönliche Fragen. Naja und plötzlich, auch heuer schaut es ein bisschen anders aus. Letztes Jahr noch Mistkübelüberwachung im Gemeindebau. Überall Mistkübelüberwachung, weil dann geht der Vandalismus zurück. Der geht einen Dreck zurück, das ist nur ein Hilfsmittel. Vandalismus bekämpft man so nicht, das sind nur Symptome. Man sieht doch, dass die neuen Maßnahmen, die sie jetzt setzen, sind etwas anders. Jetzt sagen sie: „Der Hausmeister soll wieder her, weil der kann zum Beispiel einen aufkommenden Streit, wenn er es merkt, schon vorab schlichten, kann zum Beispiel auffälligen Jugendlichen auf nett schon vorher sagen: ‚Burschen, nicht bei uns. Ich muss dann putzen.'" Weißt du, so der Human Factor, der völlig abhanden gekommen ist, der am besten von allen wirkt. Und diese Option heuer, dass sie anfangen, Putztrupps durch die

U-Bahnen zu schicken, das ist da der mächtigste Schlag gegen Vandalismus, den man führen kann. Mit solchen sanften Methoden macht man das. Aber doch nicht bitte mit Gefängnishofmethoden, jede Ecke ausleuchten. Das sollen sie bitte im Gefängnishof praktizieren, ja, wo gefährliche Leute sind, die einmal eine zeitlang von der Gesellschaft getrennt werden müssen, okay, aber doch nicht bitte alle. Ich sag nur ein Beispiel noch dazu: Das Topziel aller Terroristen seit 30 Jahren heißt *El Al*. *El Al*, das ist die israelische Fluggesellschaft. Das ist doch das Topziel, das ist doch logisch. Es ist in 30 Jahren kein einziges Mal gelungen, irgendetwas an Board einer *El Al*-Maschine zu bringen, kein einziges Mal. Und wie machen das die Israelis? Die machen das ganz klug. Und die haben gelacht, wie sie gehört haben, die Europäer verlangen jetzt Nacktscanner auf dem Flughafen, die haben gelacht drüber. Die haben eine weit bessere Methode. Die schulen ihre Leute auf äußerliche Sensorik, auf gewisse Dinge, die charakteristisch sind, die man nicht weiß, wenn man sie nicht gesagt kriegt. Ich bin mal so einem untergekommen am Flughafen Wien. Ich wartete darauf, dass der Schalter aufgeht, dass ich einchecken kann nach Griechenland. Und neben dran steht eine Riesenschlange *El Al* und daneben steht so einer, na ja kleiner Mann, der hat so ein weites Hemd angehabt, das ziemlich weit runter ging und ich sah, da hatte er etwas darunter, ja. Sogar mehr, also das war mindestens eine Krachen und ein Funkgerät, ja. Das Funkgerät habe ich dann gesehen, ja, die Krachen hat er auf der anderen Seite gehabt. Naja und ich stehe so da und ich sehe schon, dass mich der immer aus den Augenwinkeln anschaut. Weil ich bin ein sehr aufmerksamer Mensch, wenn ich irgendwo bin, ja, irrsinnig viele halten mich für einen Cop und zwar davon, wie ich schaue. Ja und der hat mich angeredet, wohin ich fliege. Sage ich: „Ich fliege nach Athen auf Urlaub, da schauen Sie habe ich eine Angel drinnen. Und Sie sind der Security-Mann für den *El Al*-Flug, gel und Sie machen jetzt Routinecheck?“ Hat er gesagt: „Ja, genau“, und ich sage: „Bei mir brauchen Sie nichts befürchten, ich fliege bloß in Urlaub und stehe nur zufällig da herum. Das ist mein Schalter, auf den warte ich, dass er aufsperrt.“ Dann hat er gesagt, nein, nein, das hätte er eh schon gemerkt und so, aber er muss es halt machen. Und die haben mit dieser Weise jeden und jede noch erwischt, jeden. Die in den USA sind bloß nicht geschult alle, das Personal ist nicht geschult. Ich lese immer die GAO-Reports vom Government Account, vom Rechnungshof. Das ist völlig absurd, ja. Am Anfang haben sie, irrsinnig schnell haben sie 10.000 Leute anheuern müssen und dann sind sie draufgekommen, dass von den Security Screeners, das heißt, die Typen, die in der Gepäcksabfertigung Dienst machen und das Gepäck durchsuchen sind 1200 selber nicht durchleuchtet gewesen vorher. Man wusste nichts über ihre Vergangenheit. Und dann haben sie Kriminelle gefunden. „Ja, wir mussten den Zeitplan so schnell erledigen“, so haben sie sich gerechtfertigt. 5000 haben sie dann gleich wieder hinausgehaut, weil sie nicht, sie haben sie in den heikelsten Platz des Flughafens hineingesetzt und nicht gescreent vorher. Ich meine, geht es noch blöder? Verstehst? Und solchen soll ich meinen Daten anvertrauen, ich bin doch nicht wahnsinnig.

Ich sage recht herzlichen Dank.
Gerne.
Und zum Schluss: Hätten Sie vielleicht noch einen wichtigen Aspekt, der Ihnen zu wenig angesprochen worden ist?
Nein, das war eh sehr umfangreich.

Interview mit Daniela Zimmer

Datum: 4. März 2010

Ort: leeres Besprechungszimmer

Dauer: ca. 22 Minuten, die Dame hatte leider nicht länger Zeit

1) Als erste Frage hätte ich Sie gebeten, dass Sie sich kurz vorstellen könnten?
Daniela Zimmer.

2) Es ist ja einerseits so, dass vom Datenschutzrecht personenbezogene, sensible Daten als besonders schutzwürdig gelten, andererseits stellen aber viele Menschen solche Daten freiwillig ins Internet, auf Social Networks-Plattformen zum Beispiel. Warum machen das Personen, warum stellen sie solche Daten ins Netz?
Wahrscheinlich tun Sie sich mit Ihrem Ausbildungshintergrund sogar leichter, das zu beantworten. Ich bin Juristin, ich kann da auch nur spekulieren bzw. sozusagen auf das bisschen an Motivforschung zurückgreifen, was halt publiziert ist. Ich meine, das ist ein Trend sozusagen zu starker Präsenz in Medien, gewisser Druck wahrscheinlich auch schon unter Jugendlichen, diese Präsenz zu haben, will man halt in seiner Peer Group

sozusagen dazuzählen. Ob das jetzt zwangsläufig und Zwang ist, sensible Daten von sich preiszugeben, jetzt in einem juristischen Sinn ja, weiß ich nicht. Also ich würde eher davon ausgehen, dass der Themenfokus doch etwas anderes ist als, was weiß ich, über seine politische Gesinnung in *Facebook* sozusagen sich auszutauschen, aber, also wenn Sie im weiteren Sinn meinen, heikle Daten, die doch ein gutes Personenprofil ermöglichen ja, pflichte ich Ihnen da sicher bei.

3) Würden Sie da jetzt auch von Ihrem Hintergrund an der AK sagen, dass diese Daten zu einem digitalen Fußabdruck beitragen?
Mit Sicherheit. Da ist eine wunderbare Studie der EU anlässlich dieses Datenschutztages 2010, die gezeigt hat, dass, glaube ich, 40 Prozent der Anbieter ihre Netzwerkseiten durch automatische Voreinstellung nur den Zugriff von Freunden das bereitgestellte Profil ermöglichen. Also im Umkehrschluss, 60 Prozent haben die Voreinstellungen so gewählt, dass halt jeder Netzwerknutzer oder überhaupt die ganze Internetgemeinde Zugriff hat und dass man davon ausgehen kann, dass der Durchschnittsnutzer sich mit diesen Sicherheitseinstellungen eher nicht beschäftigen wird oder sie in dieser Voreinstellung belassen wird. Weiß man, dass also all das, was angegeben wird, auch sozusagen einen unbeschränkten Kreis an Internetnutzern zur Verfügung gestellt wird.

4) Macht es einen Unterschied, dass wir diese Daten im Netz freiwillig hergeben oder gibt es von wirtschaftlicher und staatlicher Seite sowieso anderweitige Methoden der Datenerhebung?
Die Frage müssen Sie näher erläutern.
Seit Social Networks ist es so, dass wir alles freiwillig eigentlich hineinstellen und auf die Web 2.0-Plattformen. Greift die Wirtschaft zum Beispiel auf diese Daten zurück oder generieren sie Daten sowieso anders durch das Kaufverhalten, indem sie alles aufzeichnen?
Okay, also soweit es sozusagen um kommerzielle Nutzungen geht, muss man zwangsläufig davon ausgehen, dass die Wirtschaft zumindest versucht, Breschen zu schlagen in diese Netzwerke in unterschiedlichster Form. Entweder, indem sie halt selber Drittanbieter sind auf den Netzwerkseiten und über Applikationen direkten Zugang halt zu Nutzerdaten bekommen. Oder ja, wenn, wie es immer wieder sozusagen die Runde macht, auch gezielt versucht wird in Netzwerkgruppen einzelne Firmenvertreter einzuschleusen. Bei Netzwerkgruppen, die groß genug sind, ist das also zumindest denkmöglich. Beliebtes Beispiel ist da immer der Pharmavertreter, der in irgendeiner Selbsthilfegruppe sich plötzlich zu Wort meldet und halt irgendwie gute Stimmung macht für ein bestimmtes Arzneimittelprodukt.

5) Und von staatlicher Seite?
Das sprengt jetzt vorderhand meine Vorstellungskraft. Auf internationaler Ebene bei einer Konferenz wurde einmal behauptet, in Belgien hätten sich Finanzbeamte in eine große Gruppe gewissermaßen eingeschleust und in diesem Rahmen wurde recht offenherzig über Steuertricks und -tipps irgendwie kommuniziert und daraus dann Informationen für Steuerverfahren gewonnen. Ja, denkbar ist es, also im großen Stil, wie das nutzbar gemacht werden könnte und missbraucht werden könnte. Ja, das ist, glaube ich, sozusagen vorderhand die geringere Gefahr als dass Unternehmen das als Chance sehen, zielgruppenspezifisch zu werben oder umgekehrt Informationen über Kauf- oder Verhaltenvorlieben generieren wie es halt bei den derzeitigen Werbemedien halt in der Form nicht möglich ist, vor allem so kostengünstig, ja.

6) Würden Sie sagen, dass Social Networks zu Überwachungszwecken verwendet werden?
Das könnten Sie vielleicht auch noch ein bisschen näher beschreiben, woran Sie da denken oder was da Ihr Fokus wäre.
Wird Überwachung im Web 2.0 personalisiert. Das heißt, dass für Einzelne, also nicht mehr Institutionen oder der Staat auf die Daten zurückgreift, sondern eben der Arbeitgeber als Beispiel?
Ach so. Naja, also das ist ja auch irgendwie ein bereits oft beschriebenes Fallbeispiel, dass im Rahmen des Recruitings sehr wohl so weit eben öffentlich zugänglich, nicht, auf solche Daten zurückgegriffen wird. In Wahrheit ist es, sage ich einmal, ein Verantwortungsmix beider Seiten. Sicherlich mal des Nutzers, der grundsätzlich diese Sicherheitseinstellungen ja so wählen kann, dass der Arbeitgeber oder potentielle Arbeitgeber keinen Zugriff darauf hätte. Umgekehrt ist es aber sicher, auch gerade aus der Sicht einer Verbraucherschützerin, Aufgabe der Netzwerkbetreiber, die Sicherheitsanforderungen so zu definieren, dass ein Durchschnittsverbraucher sie versteht und auch einfach nutzt. Man kann auch durch Komplexität so eines Systems oder ein Überangebot an Informationen so desinformierend wirken, dass kein Verbraucher also diese an und für sich wichtigen Tools zum Schutz seiner Privatsphäre nutzt.

7) Sehen Sie vielleicht auch, also man hört jetzt immer von der Überwachungsgesellschaft, das ist zwar sehr negativ konnotiert, aber sehen Sie vielleicht auch Vorteile in der Entwicklung hin zu mehr Überwachung, mehr Datensammlungen?
Naja, also man kann das jetzt in mehrerer Hinsicht beantworten. In puncto Social Networks sind die Vorteile irgendwie auch auf der Hand liegend, also bei allen Gefahren wird keiner bestreiten, dass das auch bis zum

gewissen Grad eine Erfolgsgeschichte ist. Sozusagen unkompliziertes sich austauschen und im Netz rudeln oder lange sozusagen nicht gesehene Menschen wieder, mit denen in Kontakt treten zu können.
Allgemein jetzt von diesen Netzwerken abgesehen, wenn Sie Ihre Frage offenbar weiter spannen. Also man muss immer natürlich auch den Blickwinkel des Auftraggebers sich vor Augen führen. Für den hat das natürlich… schaffen Datenbanken, die leicht vernetzbar sind, die mit Datenmengen befüllbar sind, wie es vor einigen Jahrzehnten noch nicht vorstellbar war, unmittelbaren Mehrwert und Nutzen, ob das jetzt der Staat ist, der sozusagen seinen Aufgaben damit effizienter glaubt nachkommen zu können, teilweise sicher auch nachkommen kann. Ob es die Wirtschaft ist, die darüber halt sozusagen den Kunden auch besser katalogisieren und einordnen kann. Also der Nutzen und damit auch der berechtigte Zweck auf der Auftraggeberseite ist relativ leicht abgesteckt. Die schwierige Frage ist nur, gibt es überwiegende Geheimhaltungsinteressen, nicht. Also reicht das wirtschaftliche Interesse oder das Effizienz- oder Kostenspar-, Einsparungsinteresse auf Seiten der Auftraggeber aus, um solche, weiß nicht, beispielsweise Datenbankprojekte durchzuführen oder überwiegt im Einzelfall einfach das Geheimhaltungsinteresse des Betroffenen mehr. Und das sind wichtige gesellschaftliche Fragen, die einfach auch immer nur vor dem Werthintergrund einer Gesellschaft beantwortbar sind, selten nur ganz eindeutig sozusagen objektiv in die eine oder andere Richtung beantwortbar sind. Und man sieht auch im europäischen Kontext, obwohl wir eigentlich einen einheitlichen Datenschutzrahmen haben und Datenschutzrichtlinien, wie unterschiedlich die Interpretationen in den einzelnen Mitgliedstaaten ausfallen, je nachdem vor welcher datenschutzrechtlichen Tradition ein Land steht. Also Großbritannien wird in vieler Hinsicht sozusagen vor seinem liberalen Hintergrund und auch wenig schlimmen historischen Erfahrungen manches sozusagen salopper handhaben als beispielsweise Deutschland.

8) Und welche Gefahren würden Sie als die größten beschreiben, die von einer Überwachung ausgehen?
Also ich meine, die Folgen von zuviel Überwachung sind seit Jahrzehnten Aufgabe dieses klassischen Volkszählungsurteils des Deutschen Bundesgerichtshofs, wo recht schön schon in den 70er, 80er Jahren skizziert ist, dass es einfach zu einer Verhaltenskontrolle kommt, allein durch die Gefahr oder diese potentielle Sich einer Überwachung ausgesetzt fühlen und das muss im Einzelfall nicht einmal sozusagen ein tatsächlicher Überwachungsnachweis erbracht werden, dass der Einzelne gewissermaßen sich in seinem Verhalten ändert, sondern allein die potentielle Chance, dass man zu einem Überwachkreis zählt, wirkt verhaltensändernd. Und das hat der Gerichtshof ja schön ausgeführt, dass das für eine westliche, demokratische Gesellschaft, die sich sozusagen in Freiheit entwickeln möchte, kontraproduktiv ist und die Gefahr ist natürlich auch, dass also technische Möglichkeiten, die einfach vorhanden sind, ja, also es in der Natur der Sache liegt, dass man sie auch ausschöpfen möchte. Datenschutz hat eine wichtige sozusagen Begleitaufgabe, hier ausgleichend halt zu wirken, nicht. Dass alles, was technisch möglich ist, auch in der Form angewendet wird, zeichnet sich aber sozusagen ganz klar ab, dass also auch wenn die Regulierung in vielen Feldern sogar durchaus ambitioniert ist und gar nicht so übel, einfach Vollzugsdefizite auftreten, die klarmachen, dass, glaube ich, die Herausforderung der nächsten Zeit ist, wie kommt man zu einem wirksameren Vollzugssystem. Ich meine, also beispielsweise wie sehr hübsch ein deutscher Datenschützer letztes Jahr gesagt hat: „Es ist unmöglich, hinter jede Datenanwendung einen eigenen Datenschützer zu stellen und die Konformität irgendwie sicherzustellen." Die Rechtsschutzhürden, also gerade in Österreich sind derzeit noch enorm, nicht. Wir haben neben der Zuständigkeit der Datenschutzkommission für, also primär, nicht nur, aber primär für potentielle Datenschutzverletzungen durch öffentliche Auftraggeber halt den Zivilrechtsweg, da kriegt man auch noch Anwaltszwang. Also vor dem Hintergrund ist mit also so einem dichten Bemühen halt des Einzelnen nicht zu rechnen, für seine Datenschutzrechte zu kämpfen. Zumal oft, also nicht immer, aber oft es halt auch nur eine Verletzung ideeller Rechte ist und interessant wird es für viele erst, wenn es halt auch sozusagen materielle Folgen nach sich zieht. Erst dann wird oft sozusagen doch der Klagesweg beschritten, was weiß ich Arbeitplatzverlust oder wenn man irgendwelche finanziellen Einbußen dadurch hat. Also wichtig wäre es natürlich, dass man ein Rechtsschutzsystem findet, das niedrigschwelliger ist, damit auch Leute sagen: „Auch wenn ich einen ideellen Schaden habe, ist es mir wert, da diese Verletzung aufzuzeigen." Und, also viel spricht dafür, aber das ist, glaube ich, ein mühsamer Weg in der Rechtspolitik, wo noch viel Überzeugungsarbeit zu leisten ist, dass also Auftraggeber von Datenanwendungen selber Audits durchlaufen, sich halt irgendwelche Gütezeichen aneignen. Es gibt da auch durchaus, also in Form von *Europrise*, einem von der Europäischen Union koordinierten Gütezeichenprojekt, ein sehr ambitioniertes Vorhaben. Also die Kriterien sind sehr streng. Das ist nicht so, dass man da gleich irgendwie den Lebensmittelbereich assoziiert, wo also Gütezeichen auch durchaus inflationär vergeben werden. Also die Prüfvoraussetzungen sind da sehr streng angelegt. Das hat zur Folge im Übrigen, dass es derzeit nur einen Gütezeichenträger in Österreich gibt, in anderen europäischen Ländern aber bereits zahlreiche, also auch das wäre irgendwie ein wichtiges Projekt für die Zukunft.

9) Welches ist das in Österreich?
Das ist eine kleine IT-Schmiede. *Kiwi* glaube ich, heißen die. Die Verschlüsselungs- und so Verpixelungssoftware anbieten, vor allem für den Einsatz bei Videokameras. Man sagt: „Okay, Videoüberwachung hat einfach schon so eine Breitenwirksamkeit erreicht, dass man damit wird leben müssen, dass sie auch von Privaten zum Einsatz gebracht wird. Aber wenigstens soll man sicherstellen, dass die

technischen Systeme technischen Datenschutz gewährleisten. Und das am besten eben mit einer Verpixelung.“ Das heißt der Auftraggeber sieht das Klarbild eigentlich gar nicht und nur wenn im Einzelfall irgendein Vorkommnis ist, es gibt einen Übergriff, es gibt irgendwie ein Eigentumsdelikt, werden die verpixelten Bilder den Sicherheitsbehörden zur Verfügung gestellt und die können dann halt mit einem entsprechenden Schlüssel ein Klarbild erst wieder erhalten. Also das sind so kleine Maßnahmen technischen Datenschutzes, wo ich glaube, dem gehört die Zukunft, ja. Also gar nicht nur so sehr die juristische Seite, die da schon ihre Meriten verdient hat, aber im Grunde genommen geht es um Formen von technischem Datenschutz, dass bei jeder Datenanwendung das schon frühzeitig mitgedacht wird, was muss irgendwie implementiert werden, dass also eine möglichst geringe Missbrauchsgefahr besteht. Und was auch irgendwie langfristig hübsch wäre, wäre so eine Art von, ja, Lizenzierung, um das sich jeder Datenbankbetreiber selber kümmern muss. Also sozusagen unser beliebtes Beispiel ist immer, dass man auch als Lenker eines Wagens jährliche Überprüfungen auf eigene Kosten machen muss. Also wir glauben, dass ein Gutteil der Vollzugsdefizite vielleicht auch damit behoben werden könnte, dass Datenbankbetreiber, Anwender, Auftraggeber sich in regelmäßigen Abständen um so eine Art, ja, Bescheinigung bemühen müssen bei unabhängigen Instituten, dass ihre Datenbanken einfach datenschutzkonform betrieben werden.

Vielen Dank.
Ja gerne.

10) Ich wäre schon am Ende mit meinen Fragen. Am Schluss vielleicht noch, ob Ihnen irgendetwas am Herzen liegt, das zu wenig berücksichtigt wurde?
Ich kenne jetzt nicht den Fokus Ihrer Arbeit, was…
Es ist sehr allgemein. Es geht darum eben… Die freiwillige Hergabe von Daten, wie es in Social Networks passiert, ob die jetzt andere Formen von Überwachungsmöglichkeiten erlaubt?
Ja, also wahrscheinlich schon. Ich glaube halt bloß, aus diesem unstrukturierten Riesenhaufen an Daten ist es auch wieder ein besonderer Aufwand, daraus irgendwie so strukturierte Informationen zu ziehen, dass also vielmehr… ja, die Frage da zwischendurch, Staat oder Wirtschaft daraus also so einen hohen Mehrwert ziehen können. Ist doch ein gewisser Aufwand damit verbunden, aus der Flut, der Massen an Infos irgendwie das so strukturiert auszuwerten, dass es also wirklich sozusagen aussagekräftiges Material ist. Vor dem Hintergrund, glaube ich, dass es auch eine gewisse Barriere gibt, einfach nicht nur aufs Gutdünken hin irgendwelche Foren oder so zu durchpflügen. Auf der anderen Seite so ein Einzelbeispiel wie das skizzierte da über Pharmafirmen, die dann also gezielt versuchen, also Selbsthilfegruppen zu beeinflussen letztlich werblich ohne aber ihre Identität aufzudecken, dass sie eben nicht ein Betroffener sind in einer Selbsthilfegruppe, macht eher klar, dass es auch medienrechtliche Fragen sind. Also es ist gar nicht so sehr, wenn Sie Ihre Arbeit auf Social Networks erstrecken, nicht nur ein Datenschutzaspekt, sondern es bringt auch das Medienrecht an Grenzen oder zeigt neue Herausforderungen. Ab wann ist man bloßgestellt durch eine Äußerung? Das war bislang irgendwie anders, wenn man sagt: „Naja, man hat eine Zeitung und ein Journalist berichtet darüber was und die Zeitung hat eine Reichweite von zwei Millionen Lesern“, ist sozusagen der bloßstellende Charakter in der Öffentlichkeit natürlich leichter nachzuweisen als in einem so heterogenen System wie dem Internet, wo sie Kleinstgruppen haben, aber in denen sie Informationen öffentlich zugänglich machen, auch grundsätzlich das Potential, dass da Milliarden zugreifen, werden sie aber nicht tun. Also der Nachweis, welche Öffentlichkeit man damit erreicht hat, ist zum Beispiel so eine Detailfrage, die zwar medienrechtlich zu beantworten ist, aber gar nicht so leicht, wie sozusagen vorderseits des Internets. Also Medienrecht wäre etwas, was sozusagen auch noch so ein Anliegen wäre, weil es nicht in jeder Hinsicht internetfit ist.

Vielen Dank!
Ja gerne.

Abstract - Deutsch

„Die Preisgabe sensibler Daten im Internet. Möglichkeiten einer Überwachung und ihrer Gefahren“ (Rudlstorfer Daniel 2010)

Im Zuge dieser Magisterarbeit sollte der Frage nachgegangen werden, ob diejenigen Daten, die wir freiwillig im Internet hinterlassen bzw. veröffentlichen, spezifischere Formen von Überwachung zulassen.

Dies wird mittels zweierlei Methoden bewerkstelligt. Auf der einen Seite soll eine umfassende Literaturrecherche und -analyse theoretische und rechtliche Grundlagen liefern, auf der anderen Seite soll eine empirische Erhebung in Form von qualitativen ExpertInneninterviews helfen, die konkretisierten Forschungsfragen zu beantworten, praxisorientierte Ansätze einzubeziehen, speziellere Aspekte zu beleuchten und das Material zu ergänzen.

Nach der Einleitung in das Thema rücken zunächst grundlegende Begriffe in den Mittelpunkt. Die Dimensionen der Daten und der Privatsphäre werden charakterisiert und historisch sowie philosophisch erörtert, um danach die Preisgabe von Daten und dahinterliegende Motive zu deuten und mit Fallbeispielen zu versehen. Ein kommunikationswissenschaftlicher Kontext wird hergestellt, wenn die partizipativen Elemente des Mediums Internet und ihre Auswirkungen auf private Rückzugsgebiete erläutert werden. Rechtliche Aspekte fließen immer wieder ein, um die Normen im Umgang mit Datenschutz und Privatsphäre zu verstehen.
Im Folgenden wird die Dimension der Überwachung aus verschiedenen Perspektiven unter die Lupe genommen. Ist erst eine sinnvolle Definition gefunden, können Theorien zur Überwachungsgesellschaft und dem selbstdisziplinierenden, leistungssteigernden Panoptismus eingebracht werden. Eng verbunden mit einer Technologie werden auch die technischen, medialen Artefakte der Überwachung einbezogen. Um später den eventuellen Zugriff seitens des Staats und wirtschaftlicher Unternehmen auf freiwillig veröffentlichte Daten zu überprüfen, rücken staatliche und wirtschaftliche Überwachung in den Fokus. Erst dann werden die Vorteile, Gefahren und etwaige Auswege aus Problemsituationen beschrieben.

Die qualitativen ExpertInneninterviews werden in Form von problemzentrierten Leitfadeninterviews durchgeführt.

Die Ergebnisse der empirischen Untersuchung besagen in Bezug auf die Hauptforschungsfrage, dass freiwillig preisgegebene Daten eine optimale Ergänzung zu anderen Formen der Datenerhebung darstellen. Da für die Verwendung bereitwillig veröffentlichte Daten keine Zustimmung erforderlich ist und sie derzeit auch keiner Zweckbindung unterliegen, stellen diese echten und genauen Daten gerade für Unternehmen einen profitablen Nutzen dar, um Marketingzwecken nachgehen zu können und Profile der KundInnen zu schärfen. Auf staatlicher Seite sieht das Unterfangen etwas problematischer aus, da die Behörden einen Rechtfertigungsgrund brauchen, um auf solche Daten zugreifen zu können. Um einen bestimmten Sachverhalt zu prüfen, ziehen aber vor allem Sicherheitsbehörden und Geheimdienste Informationen aus der „Public Intelligence“ heran. Gerade Netzwerkstrukturen lassen sich durch die Social Networks besonders gut skizzieren. Die größten Gefahren auf individueller Ebene sind, dass die Privatsphäre der Personen unbemerkt oder auch bewusst eingeschränkt wird, und diesen Nachteile widerfahren können, wenn Informationen in falsche Hände geraten. Gesellschaftlich gesehen liegen Gefahren einer Überwachung darin, dass sie in eine Verhaltensanpassung und -änderung mündet, die sich bei den Betroffenen aufgrund der potentiellen Möglichkeit, überwacht zu werden, einschleicht. Dies zieht Freiheitseinschränkungen nach sich, die einer liberalen, demokratischen Gesellschaft widersprechen. Zusätzlich kommt es zur Beweislastumkehr und zu einer gewissen Ironiefreiheit. Viele Beispiele belegen auch, dass Daten oft verloren gehen und missbraucht werden. In Diktaturen erschwert Überwachung Versuche, gegen die Machthabenden anzukämpfen.

Abstract - English

“The exposure of sensitive data on the internet. Possibilities of surveillance and their dangers.” (Rudlstorfer Daniel 2010)

In this final thesis for M.A. degree it should be investigated whether the data we expose voluntarily on the internet, allows more specifically forms of surveillance.

This will be shown by two different methods. On the one hand, the theoretical and legal foundations are provided by an extensive research and analysis of literature, on the other hand an empirical survey of qualitative interviews of experts should help to answer the substantiate research questions and to include practice orientated approaches. Furthermore it should be used to examine more specific aspects and to complete the material.

The introduction into the topic is followed by the description of basic terms. The dimension of data and privacy will be characterized and argued historically and philosophically in order to indicate the motives behind the exposure of data. This will be underlined by case studies. The participative elements of the medium internet and the impact on private shelters reveal the context of communication studies. In the course of this work, legal aspects are consistently a vital necessity to understand the norms in association with data protection and privacy. Furthermore the dimension of surveillance will be examined from different perspectives. Firstly, there has to be found a useful definition. Then theories of our monitoring society and of self-disciplined, performance enhancing panopticism can be introduced. In addition, the technical, medial artefacts of surveillance are included closely linked to a technology. In order to validate the possible access of the state and economic enterprises to voluntarily published data, the focus will be on state-run and economic surveillance. The advantages, dangers and some resorts out of problem-situations can then be described.
The qualitative interviews of the experts are implemented in the form of problem-centered guided interviews.

In relation to the main research question the results of the empirical investigation indicate that voluntarily exposed data are an ideal amendment to other forms of data collection. Due to the fact that there is no affirmation needed for willingly published data and that it is not

underlying any appropriation, this real and exact data is particularly for enterprises a profitable benefit in order to use it for marketing purposes and to sharpen the profiles of customers. Regarding the state, the access to such data is somewhat limited as the authorities need a warrant reason. As a matter of fact security agencies and the secret service often use information from “Public Intelligence” in order to examine a certain issue. Social networks are especially useful to outline network structures. For individuals the major dangers are that their privacy is restricted unnoticed or even deliberately and disadvantages may occur when their data is falling into false hands. Dangers of surveillance for society in general are adaption and change of behaviour which is caused by the potential opportunity to be monitored. Consequently, this results in a restriction of freedom which contradicts to a liberal, democratic society. Furthermore it generates a shifting of the burden of proof and a certain freedom of irony. Numerous examples allocate that data is often lost or abused. In dictatorships, surveillance complicates attempts to fight against the ruler.

Lebenslauf

Daniel Rudlstorfer Bakk. Phil.

Persönliche Daten:

Geboren am 31.01.1983 in Linz, Oberösterreich

Ausbildung:

Februar 2007	Beginn des Magisterstudiums PKW
	Abschluss des Bakkalaureatstudiums PKW
Oktober 2003	Beginn des Publizistik und Kommunikationswissenschafts-Studiums an der Universität Wien
Oktober 2002	Beginn des Philosophiestudiums an der Universität Wien
Juni 2001	Matura mit Auszeichnung
1993-2001	Sportrealgymnasium Linz Peuerbachstraße
1990-1993	Volksschule Ottensheim, Oberösterreich
1989-1990	Volksschule Linz-Dornach

Bisherige Tätigkeiten:

Herbst 2009	Schauspielertätigkeit bei *Bühne Ottensheim*
Frühjahr 2009	Mitarbeit an einem philosophischen Forschungsexperiment, einer wissenschaftlichen Studie zu Retro-Priming unter der Leitung von Dr. Alexander Batthyany

1999-2009	Diverse Ferialarbeiten *VOEST*, Baufirmen, Gastronomie, Bürotätigkeiten
Seit Oktober 2008	Mitbegründer und Macher der Sendung *KommPass* auf *Radio Orange*
Sommer 2008	Praktikum bei *Life Radio*
Frühjahr 2008	Schauspielertätigkeit für Hauptrolle in 30-minütigem Film
2004-2008	Gitarrist der Band *blowhappad*
1990-2008	Fußballer des *TSV Ottensheim* Landesliga Ost in Oberösterreich
Februar bis Juli 2003	Reise durch Indien
Jänner bis August 2002	Bundesheer in Hörsching *Betr.RV. Kompanie*
1993	Schachstaatsmeister U10