Mathias Bliemeister
Website: http://www.lautesbuch.de
Kontakt: info@lautesbuch.de

# Die digitale Überwachung

# Inhaltsverzeichnis

# 1 Einleitung

Die moderne Gesellschaft errichtet zunehmend überwiegende Teile ihrer Strukturen auf den Säulen der Informations- und Kommunikationstechnik. Dadurch festigen sich unterschiedliche Elemente aus der Informations- und Kommunikationstechnik in private, soziale, wirtschaftliche, aber auch politische Bereiche. Der Computer als Schnittstelle zwischen dem Menschen und der Informations- und Kommunikationstechnik übernimmt hierbei eine besondere Rolle. Der einzelne Computer ist im Wesentlichen Übermittler und Empfänger von Informationen. Ist der Computer gar am Internet angeschlossen, so wird der Nutzer Teilnehmer eines virtuellen Raumes, in dem mittlerweile die Kommunikation von mehreren Millionen Menschen täglich stattfindet. Wesentliche Bereiche des Lebens werden durch die Nutzung des Computers und insbesondere durch die Nutzung des Internets teilweise leichter und angenehmer gemacht. Man kann an dieser Stelle zahlreiche Beispiele nennen, wodurch dieser Satz seine Rechtfertigung erfährt. Im Rahmen dieser Arbeit beschäftige ich mich jedoch mit einer anderen Sichtweise.

Die zunehmende Bedeutung des Computers, ja der Informations- und Kommunikationstechnik ermöglicht derjenigen Instanz, die Macht über diese Technik hat, die Nutzer und gar die Gesellschaft zu überwachen. Folgende technischen Werkzeuge bzw. Entwicklungen werden bereits in einem relativen Umfang für die Überwachung genutzt.

- Videoüberwachung
- Biometrie
- RFID-Chips
- Internet
- Gesundheitskarte
- Änderung des Bankgeheimnisses

Wer aber profitiert von der Überwachung einzelner Personen bzw. einer Gesellschaft? Ganz offensichtlich der Staat und große Konzerne. Der Staat, weil er somit seine Bevölkerung kontrollieren kann und zur Prävention von Deliktbegehung und zur Erleichterung von Deliktaufklärung. Die Konzerne, weil sie einen wirtschaftlichen Vorteil aus der Überwachung und der Transparenz gewinnen können. Dass dies an das Panoptikum Foucaults erinnert, ist nicht das Ergebnis paranoider Gedankengänge, sondern gegenwärtige Realität. Michel Foucault konstatiert:

„Wann immer man es mit einer Vielfalt von Individuen zu tun hat, denen eine Aufgabe oder ein Verhalten aufzuzwingen ist, kann das panoptische Schema Verwendung finden. Unter dem Vorbehalt notwendiger Anpassungen erstreckt sich eine Anwendbarkeit auf alle Anstalten, in denen innerhalb eines nicht allzu ausgedehnten Raumes eine bestimmte Anzahl von Personen unter Aufsicht zu halten ist. In jeder dieser Anwendungen ermöglicht es die Perfektionierung der Machtausübung: weil es die Möglichkeit schafft, daß von immer weniger Personen Macht über immer mehr ausgeübt wird; weil es Interventionen zu jedem Zeitpunkt erlaubt und weil der ständige Druck bereits vor der Begehung von Fehlern, Irrtümern, Verbrechen wirkt; ja weil unter diesen Umständen seine Stärke gerade darin besteht, niemals eingreifen zu müssen, sich automatisch und geräuschlos durchzusetzen, einen Mechanismus von miteinander verketteten Effekten zu bilden; weil es außer einer Architektur und einer Geometrie kein physisches Instrument braucht, um direkt auf die Individuen einzuwirken.“[1]

Datenschützer und Hackervereinigungen laufen bereits Sturm gegen derartige Entwicklungen, die den Datenschutz und die bürgerliche Freiheit beschränken. Im Rahmen dieser Arbeit möchte ich das Internet, die Biometriepässe und die Videoüberwachung im Kontext eines digitalen Panoptikums untersuchen. Darüber hinaus beschäftige ich mich mit der Subkultur der Hacker, da es sich hierbei ganz offensichtlich um eine Gruppe handelt, die dieser Entwicklung als Opposition gegenübersteht.

# 2 Entstehung einer Subkultur

In den 1950er Jahren gründeten befreundete Studenten am Massachusetts Institute of Technology (MIT) den „Tech Model Railroad Club“ (TMRC). Hier bastelten sie mit ausgedienten Telefonen und anderen elektrischen Resten und bauten damit umfangreiche und komplizierte Eisenbahnnetzwerke. Am MIT benutzten die Studenten das Wort „hack“ ursprünglich für studentische Scherzaktionen. Die Mitglieder des TMRC fanden in dem Wort Verwendung, wenn sie für ein besonders kompliziertes technisches Problem eine raffinierte Lösung entwickelten.[2]

Damals zählte das MIT zu einer der wenigen öffentlichen Einrichtungen, an denen Computer eingesetzt wurden. Hier bekamen die Hacker erste praktische Eindrücke von der Computer-

[1] Foucault, Michel. Überwachen und Strafen. Die Geburt des Gefängnisses. 1976. S. 264 f.
[2] Vgl. Gröndahl, Boris. Hacker. 2000. S. 40.

technik vermittelt. Kurze Zeit später wurde ein bis dahin völlig neues Computersystem eingerichtet: ein so genannter Minicomputer, entsprechend der Größe dreier Kühlschränke. Die Firma DEC entwickelte diesen Computer, mit dem es erstmals möglich war, mehrere Nutzer am System arbeiten zu lassen. Basierend auf dieser Technologie bot sich den Hackern erstmals die Möglichkeit Programmierarbeiten direkt am Computer zu verrichteten, was technisch betrachtet die Grundlage der programmierenden Arbeitsweise der Hacker wurde.[3] Die Hacker am MIT entwickelten die ersten Computerspiele und konzipierten grundlegende Voraussetzungen für die Entwicklung des Internets.

Im Gegensatz zu den Vorständen der beiden großen Computer-Firmen IBM und DEC forderten in den 1970er Jahren zahlreiche Hacker, wie Lee Felsenstein, Bob Albrecht und Ted Nelson, dass die Gesellschaft Zugang zu Computern haben sollte.[4] Damit legten die Hacker den ersten Grundstein für die Idee und die Verbreitung des Personal Computers (PC) und nicht die Computer-Industrie. Ein bekanntes Beispiel aus der Gründerzeit des Personal Computers ist die Firma „Apple Computers“. Sie wurde von Stephen Wozniak und Steven Jobs gegründet und zählt bis heute zu den einflussreichsten Computerfirmen der Welt. In ihrer Gründerzeit bauten sie in einer Garage die ersten Apple-Computer.

## 2.1 Die „Hackerethik“

1984 erschien das Buch „Hackers. Heroes of the Computer Revolution“ von dem Journalisten Steven Levy. Er beschrieb darin die Hackerszene und verfasste ein Regelwerk, welches er als „Hackerethik“ bezeichnete. Die darin aufgeführten Regeln entsprachen seinen Interpretationen aus Beobachtungen und Gesprächen mit Mitgliedern der Hackerszene der früheren Generationen. Die Hackerszene gab es zu diesem Zeitpunkt bereits schon seit 30 Jahren. Seit seinem Erscheinen ist die Hackerethik wesentlich diskutiert und modifiziert worden, so dass im Laufe der Zeit unterschiedliche Auslegungen entstanden sind.

Nachfolgend wird die Hackerethik nach Steven Levy, Wau Holland und dem CCC aufgeführt:

- „Zugang zu Computern – und allem, was einem zeigen kann, wie diese Welt funktioniert – muss unbegrenzt und vollständig sein
- Alle Informationen müssen frei sein
- Misstraue Autoritäten – fordere Dezentralisierung

[3] Vgl. Gröndahl, Boris. Hacker. 2000. S. 42.
[4] Vlg. Gröndahl, Boris. Hacker. 2000. S. 52.

- Beurteile einen Hacker nach dem, was er tut, und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse oder gesellschaftlicher Stellung
- Man kann mit einem Computer Kunst und Schönheit schaffen
- Computer können das Leben zum Besseren verändern
- Mülle nicht in den Daten anderer Leute
- Öffentliche Daten nützen, private Daten schützen“.[5]

## 2.2 Entwicklung der Hacker-Subkultur in Deutschland

Als Anfang der 1980er Jahre in Deutschland ein Absatzmarkt für Homecomputer entstand, waren es nicht mehr nur Informatiker, die sich mit der Informations- und Kommunikations-technik auseinander setzten, sondern auch Personen, die ihren subjektiven Nutzen im Gebrauch eines Computers sahen.

Im Zuge der stärkeren Nachfrage nach Informationstechnik entstanden unter anderem privat genutzte Mailboxen, mit denen die Nutzer Informationen auf elektronischem Weg veröffentlichen konnten. Dazu war ein Modem[6] nötig, mit dem man sich an das Telefonnetz anschloss und eine Verbindung zu einer Mailbox herstellte. Als Mailboxen bezeichnet man in diesem Kontext Server, über die Daten übertragen und Nachrichten ausgetauscht werden. Das Monopol der Bundespost verhinderte jedoch den öffentlichen Verkauf von Modems und somit eine entsprechend hohe Verbreitung. Das hinderte jedoch einige Computernutzer nicht daran, die Datennetze dennoch zu nutzen. Der CCC beispielsweise unterstützte die Zugänglichkeit freier Informationsräume unter anderem mit dem Verkauf von Bausätzen und der Verbreitung von Bauanleitungen für Modems.

Mit den Forderungen bezüglich der uneingeschränkten Zugänglichkeit von Informationen und zahlreichen Aktionen in dieser Hinsicht erreichten die Hacker ein erhöhtes Medieninteresse. Dies geschah insbesondere in einer Zeit, in der die „Angst vor Überwachung und der Übermacht der Computer (…)“[7] einsetzte.

Einigen kriminell veranlagten Computerfreaks war es dann aber zu verdanken, dass das Ansehen der Hackerkultur in den Medien und in der Öffentlichkeit einen erheblichen

[5] http://de.wikipedia.org/wiki/Hackerethik. Download am 22.10.2005.
[6] Das Modem wandelt digitale Computerdaten in analoge Signale und umgekehrt. Das Wort Modem ist eine Zusammensetzung aus den Wörtern **Mo**dulator/**Dem**odulator.
[7] Barth, Thomas. Soziale Kontrolle in der Informationsgesellschaft: Systemtheorie, Foucault und die Computerfreaks als Gegenmacht zum Panoptismus der Computer- und Multimedia-Kultur. 1997. S. 177.

Imageverlust erlitt. Im medialen Interesse lag hierbei der „KGB-Hack“, an dem vier Computerfreaks beteiligt waren und für den KGB Wirtschaftsspionage betrieben.
Thomas Barth berichtet indes über Aktionen seitens Mitglieder des CCC, deren Gegenstand es war Sicherheitslücken aufzudecken (z.B. HASPA-Hack).[8] Die Bundesrepublik sah diesen Entwicklungen jedoch mit Besorgnis entgegen, da sie im Konflikt zu den Sicherheitsinteressen der Wirtschaft und der Regierung standen. Folglich leitete man drastische Maßnahmen ein, die es ermöglichen sollten massiv gegen Computerkriminalität vorzugehen. Daraufhin verabschiedete die Deutsche Regierung im Jahre 1986 das „Zweite Gesetz zur Bekämpfung von Wirtschaftskriminalität“. Dieses Gesetz stellt seitdem das „Ausspähen und die Veränderung von Daten“ unter Strafe.

## 2.3 Der Chaos Computer Club

Die wohl bekannteste Vereinigung von Hackern in Deutschland ist der Chaos Computer Club, kurz CCC. Boris Gröndahl definiert diese Vereinigung folgendermaßen: „In Deutschland sind Hacker seit Anfang der 80er Jahre praktisch synonym mit dem Chaos Computer Club. Der CCC und sein Übervater Wau Holland haben dem Hacken in Deutschland eine sehr medienwirksame und vergleichsweise politische Note verliehen“.[9]

Der CCC versteht sich als ein Forum, in dem sich seine Mitglieder mit der Technologie auseinander setzen. Es geht hierbei um die Auswirkungen der Technologie auf die Gesellschaft und auf das Individuum.

Als weitere Kernpunkte ihrer Arbeit stehen die Informationsfreiheit sowie der Schutz der Privatsphäre und die Aufrechterhaltung des Datenschutzes.[10] Der CCC betreibt verschiedene Projekte und unterhält öffentliche Kampagnen, die sich mit aktuellen Themen aus diesen Bereichen beschäftigen. Dabei werden politische und wirtschaftliche Entscheidungen objektiv auf die Kernpunkte des CCC untersucht.

[8] Barth, Thomas. Soziale Kontrolle in der Informationsgesellschaft: Systemtheorie, Foucault und die Computerfreaks als Gegenmacht zum Panoptismus der Computer- und Multimedia-Kultur. 1997. S. 180.
[9] Gröndahl, Boris. Hacker. 2000. S. 64.
[10] Vgl. http://www.ccc.de. Download vom 07.11.2005.

# 3 Machtverlust durch Informationsverlust

Wie bereits eingangs erwähnt, ist es aus Sicht eines Staates besonders wichtig, dass innerhalb der Informations- und Kommunikationstechnik Sicherheits- und Kontrollmechanismen geschaffen werden, die einen Zusammenbruch der Netzwerke verhindern. Der ehemalige Bundesminister für Wirtschaft und Technologie, Dr. Werner Müller, schreibt schließlich nicht ohne Grund: „Von den modernen Informations- und Kommunikationstechnologien gehen nachhaltige gesellschaftliche, gesamtwirtschaftliche und beschäftigungspolitische Impulse aus. Die weltweite, ortsunabhängige und unmittelbare Verfügbarkeit von Inhalten hat ebenso wie die Fähigkeit zum raschen Austausch von Informationen und zur Erneuerung von Wissen existenzielle Bedeutung für Beschäftigung und Wachstum erhalten. Wir erleben die Entwicklung einer neuen Ökonomie – der Internet-Wirtschaft“.[11] Um diversen möglichen Formen der Bedrohung, wie beispielsweise die Ausspähung, die Manipulation oder auch die Löschung von Datenbeständen entgegenzutreten, investiert die Bundesregierung viel Geld in die Entwicklung von Sicherheitskonzepten und in die Errichtung von Organisationen, die sich mit der Aufgabe beschäftigen die Sicherheit zu gewährleisten.

Bevor ich die Entwicklung derjenigen Organisationen beschreibe, die in Deutschland für die Sicherheit der Informations- und Kommunikationstechnik zuständig sind, möchte ich folgend einen kurzen Überblick darüber verschaffen, welche Bedrohungen es im Bereich der Computertechnologie überhaupt gibt. Dieser Überblick ist keineswegs vollständig, da es zahlreiche unterschiedliche Möglichkeiten gibt, die aus der Beschäftigung mit der Umgehung von Sicherheitsbarrieren entstanden sind.

## 3.1 Malware

Malware ist die Bezeichnung für Computerprogramme, deren Ziel es ist Schaden anzurichten. Sie besitzen je nach Programmierung die Fähigkeit Dateien zu manipulieren oder gar zu löschen. Besonders raffiniert programmierte Viren sind in der Lage, ihren eigenen Programmcode zu verändern um nicht von Anti-Viren-Programmen erkannt zu werden (polymorphe Viren). Sie sind sogar dazu befähigt auf die Aktionen eines solchen Programms zu reagieren, indem sie sich selbst in einen anderen Bereich verschieben, der nicht vom Virenscanner untersucht wird, um sich dann nach der Untersuchung in den gerade als „sauber“ gekennzeichneten Bereich zurückzuschreiben.

[11] Dr. Müller, Werner. E-Privacy. Datenschutz im Internet. 2000. S. 5.

Zu der Gruppe von Malware gehören folgende Typen:

- **Computerviren**. Ihre Verbreitung findet durch die Vervielfältigung von sich selbst in Programme, Dokumente oder auch Datenträgern statt.
- **Computerwürmer** verbreiten sich über das Internet und befallen auf diesem Wege andere im Internet angeschlossene Computer.
- **Trojanische Pferde**. Einer Sicherheitslücke im Betriebssystem UNIX verdankte das erste Trojanische Pferd in den 1980er Jahren den Zugriff auf eine Reihe von Rechnern der NASA und des US-Militärs. Dabei handelt es sich um ein Programm, welches eingegebene Passwörter abfängt und damit unberechtigten Personen Zugang zu fremden Rechnern gewährt. Dabei gibt ein berechtigter Nutzer sein Passwort ein, daraufhin erhält er eine Fehlermeldung und versucht es erneut. Beim zweiten Versuch erfolgt das korrekte Login, gleichzeitig wird das vermeintlich falsch eingegebene Passwort an den Besitzer des Trojanischen Pferdes gemeldet.
- **Backdoors** sind Programme, die per E-Mail-Anhang oder mittels Computer-Spielen versteckt übertragen werden. So genannte Hintertüren ermöglichen dann die Fernsteuerung fremder Rechner durch unautorisierte Personen.
- **Sypware** ist die Bezeichnung für Programme, die sich häufig über Trojaner verbreiten. Sie verfolgen den Sinn, Informationen über den Benutzer zu sammeln um diese dann an ihren Autor weiterzuleiten.

Die Autoren derartiger Software bewegen sich ganz offensichtlich in einem illegalen Bereich der Gesellschaft. Kurioserweise werden durch einen Virenangriff aber Sicherheitslücken aufgedeckt, die den Softwareunternehmen und den Sicherheitsfirmen die Gelegenheit geben, diese zu beheben. Folglich verhelfen die in erster Linie als illegal bezeichneten Aktionen den Softwareunternehmen dazu ihre Produkte hinsichtlich Sicherheit und Qualität zu optimieren.

## 3.2 Entwicklung der IT-Behörden in der Bundesrepublik

Der nachfolgende Abschnitt dokumentiert chronologisch die Entstehung der IT-Behörden in Deutschland:

- 1986 Übertragung des Aufgabenbereiches Computersicherheit an die Zentralstelle für das Chiffrierwesen (ZfCH)

- 1987 Bildung „Interministrieller Ausschuß für die Sicherheit in der IT“ unter Administration des Bundesinnenministers
- 1989 Umbenennung der ZfCH, aufgrund erweiterter Aufgabenstellungen, zu „Zentralstelle für Sicherheit in der Informationstechnik“ (ZSI)
- 1991 Ernennung zum Bundesamt für Sicherheit in der IT (BSI) mit Hauptsitz in Bonn und Aufnahme seiner Tätigkeit
- August 2001 Der Bundesinnenminister beschließt neue organisatorische, personelle und fachliche Rahmenbedingungen für das BSI. Dadurch entwickelt sich das BSI zum zentralen IT-Sicherheitsdienstleister des Bundes

Zu den Aufgaben des BSI gehört die Prüfung von IT-Sicherheitsrisiken, das Ausstellen von Sicherheitszertifikaten, die Entwicklung und Konzeption von IT-Sicherheitsanwendungen und entsprechenden Produkten, die Unterstützung der Behörden des Bundes sowie der Länder und der Industrie bei IT-Sicherheitsrelevanten Fragen. Zusätzlich informiert das BSI auf seiner Website[12] über Bedrohungen aus dem Internet und publiziert entsprechende Maßnahmen-kataloge zur Lösung entstandener Sicherheitsprobleme.

# 4 Der Staat und die Überwachung

Dass ein Staat besonderes Interesse an der Überwachung seiner Bevölkerung hat, ist kein Phänomen aus totalitären Regimes, sondern ein Bedürfnis demokratischer Volks-gemeinschaften. Der Unterschied liegt allerdings darin, dass die Bevölkerung demokratischer Staaten nicht jede Entwicklung in dieser Hinsicht hinnehmen braucht. Als beispielsweise im Jahre 1983 die damalige Bundesregierung eine Volkszählung[13] in Deutschland plante, opponierten verschiedene soziale und politische Gruppen. „Kritisiert wurde insbesondere, dass die Ausführlichkeit der Fragen in den Volkszählungsbögen bei ihrer Beantwortung Rückschlüsse auf die Identität der Befragten zulasse und somit den Datenschutz und das Recht auf informationelle Selbstbestimmung unterlaufe, damit folglich gegen das Grundgesetz

[12] http://www.bsi.de. Download am 22.10.05.

[13] Volkszählung bedeutet nicht, dass sich das Volk einer Zählung unterziehen muss. Vielmehr werden mit einer Volkszählung diverse persönliche Daten pro Einwohner mit Hilfe eines Fragebogens erhoben. Das offizielle Ziel einer Volkszählung ist die Anpassung der sozialen Versorgung sowie der Infrastruktur an die jeweilige Situation der Bevölkerung. 1987 fand die bisher letzte Volkszählung in der Bundesrepublik statt.

verstoße. Im Hintergrund stand die Befürchtung des "*gläsernen Bürgers*". Teilweise wurde die Volkszählung gar als Schritt in Richtung eines Überwachungsstaates gesehen.“[14]

Die Terroranschläge der vergangenen Zeit, regelmäßige Warnungen vor weiteren Terroranschlägen und diverse Berichterstattungen über weltweit operierende Terrorvereinigungen, die ihre Kommunikation über das Internet planen und realisieren, verunsichern die Bevölkerung zusehends. Die allgemeine Verbreitung mehr oder weniger gefährlicher Computerviren trägt ebenso nicht minder dazu bei, dass der Staat wachsende Befugnisse erhält Überwachungsmaßnahmen problemlos durchzusetzen und Einschnitte in den Datenschutz zu rechtfertigen. Jörg Splett stellt hierbei fest: „Mitunter hört man, das sei kein Problem für jemanden, der sich nichts vorzuwerfen habe. Aber Menschen haben – wiederum: allem möglichen Missbrauch voraus – bereits darum ein Recht auf Wahrung und Schutz ihrer Privatsphäre, weil es ihnen freigestellt bleiben muss, wen sie daran und in welchem Grade teilhaben lassen wollen“.[15]

Befürworter der zunehmenden staatlichen Überwachung festigen ihre Argumentation damit, dass es hierbei um die Prävention von Straftaten und um die effektivere Strafverfolgung von Kriminellen geht. Mit der Überwachung im Internet, der Einführung der Biometriepässe und mit der steigenden Anzahl von Überwachungskameras inmitten ausgewählter öffentlicher Plätze bestehen dafür ideale Voraussetzungen. Unter dieser Prämisse ist das Foucaultsche Panoptikum ein Werkzeug, das offenbar optimal auf die Kommunikations- und Informationstechnologie anwendbar ist. „Das panoptische Schema ist ein Verstärker für jeden beliebigen Machtapparat: es gewährleistet seine Ökonomie (den rationalen Einsatz von Material, Personal, Zeit); es sichert seine Präventivwirkung, sein stetiges Funktionieren und seine automatischen Mechanismen“.[16]

Obwohl Überwachungsmaßnahmen in einem demokratischen Rechtsstaat nur unter der Wahrung strenger Auflagen Gültigkeit finden und teilweise zeitlich begrenzt sind, ist diese Entwicklung bedenklich. Florian Rötzer gelangt zu der Überlegung, eine derartige Infrastruktur im Sinne der Überwachung sei höchstwahrscheinlich nicht mehr rückgängig zu machen. Käme überdies in ferner Zukunft ein Regime an die Macht, welches die

[14] http://de.wikipedia.org/wiki/Volksz%C3%A4hlung_in_der_Bundesrepublik_Deutschland_%281987%29. Download am 22.10.05.
[15] Splett, Jörg. Biometrik Human? Zu ethischen Fragen im Zusammenhang mit biometrischen Identifikationsverfahren. 2001. S. 74.
[16] Foucault, Michel. Überwachen und Strafen. Die Geburt des Gefängnisses. 1976. S. 264 f.

entsprechenden Gesetze ignoriert, so hätte die Gesellschaft in einer katastrophalen Situation zu leiden.[17]

## 4.1 Das Internet

Um verstehen zu können, weshalb das Internet im Sinne der Überwachung ein hohes Potenzial besitzt, möchte ich eingangs die technischen Aspekte der Adressierung im Internet etwas expliziter erörtern.

Das Aufrufen bestimmter Internetseiten, oder neudeutsch das Surfen im Internet, entspricht dem Anfordern von Daten, die sich auf einem bestimmten Webserver befinden. Damit der Computer eine Antwort auf seine Anforderung erhält, benötigt er eine so genannte IP-Adresse, welche während der Anforderung an den Empfänger weitergeleitet wird. Es handelt sich hierbei um eine weltweit eindeutige Zahlenkennung, die von dem jeweiligen Provider bezogen wird und dem Computer eine eigene Adresse verschafft, unter der er identifizierbar und erreichbar ist. Verfügt der Nutzer über keine zusätzlichen Sicherheitseinstellungen bzw. über Software, die eine zusätzliche Anonymisierung unterstützt, werden außerdem noch weitere Informationen unfreiwillig über das Internet hinausgetragen, mit denen Rückschlüsse auf das Surfverhalten bzw. die Klickwege des Nutzers zu verzeichnen sind. „Um aus dem Verhalten des Nutzers noch mehr Informationen über diesen gewinnen zu können, besteht eine beliebte Taktik darin, diesen so zu markieren, dass er jederzeit wieder identifiziert werden kann“.[18] Hierfür gibt es eine Reihe von technischen Möglichkeiten, wie etwa Cookies oder Session-IDs.[19] Mit einem Globally Unique Identifier (kurz GUID) ist es überdies möglich Daten zu einem Rechner weltweit zuzuordnen.[20] Die GUID ist eine eindeutige Kennung, die in Hardware oder Software integriert ist.

Bestimmte Institutionen sind in der Lage, jede noch so triviale Bewegung, die der Nutzer im Internet tätigt, mit Hilfe der eben aufgezählten Techniken aufzuzeichnen. Der E-Mail-Versand, der Kauf einer CD im Internet, der Aufruf einer bestimmten Internetseite, all diese alltäglichen Aktivitäten lassen sich mit dem Einsatz der oben genannten Techniken ohne großen Aufwand problemlos aufzeichnen und speichern. Es sei allerdings hierbei angemerkt, dass der einzelne Kauf einer CD noch kein Problem im Sinne der Überwachung erzeugt.

[17] Rötzer, Florian. Das Recht auf Anonymität. 2000. S. 30.
[18] Wiese, Markus. Unfreiwillige Spuren im Netz. 2000. S. 13.
[19] Ebd.
[20] Vgl. Wiese, Markus. Unfreiwillige Spuren im Netz. 2000. S. 17.

Werden diese Informationen allerdings mit vielen weiteren Informationen kombiniert und ausgewertet, so entsteht ein individuelles Persönlichkeitsprofil eines möglichen Kunden. Davon profitieren Firmen, die für den einzelnen User individuelle Werbemaßnahmen konzipieren wollen. Christiane Schulzki-Haddout schreibt: „Ziel ist das so genannte Eins-zu-eins-Marketing, die direkte Kundenansprache. In der Regel informieren die Firmen die Nutzer jedoch nicht über ihre Praktiken.“[21]

Bei vielen Nutzern stellt sich aber einfach nicht die Frage, welche Konsequenzen sich aufgrund der Aufhebung ihrer Privatsphäre ergeben. Florian Rötzer bemerkt in seinem Beitrag, dass Anonymität im Internet lediglich durch die Nutzung und Zuhilfenahme von bestimmter Soft- und Hardware möglich ist, da dies aber gewissermaßen umständlich und mit Anstrengung verbunden ist, wird davon in der Regel abgesehen.[22] Doch genau hier liegt die Möglichkeit aus dem digitalen Panoptikum zu entfliehen. Was offenbar bei Benthams Panoptikum auszuschließen war, lässt sich insbesondere im Internet realisieren. Hacker unterstützen mit ihrer Arbeit und mit ihrem Wirken den Datenschutz und die Anonymität im Internet. Neben der Entwicklung von Computerprogrammen, auf die ich später noch eingehen werde, veröffentlichen die Hacker Empfehlungen, die den Nutzer im Internet unsichtbar machen.

Derartige Informationen sind unter anderem auf der Webseite des CCC zu finden. Dort wird beispielsweise für das Abrufen und Übertragen von Internetseiten empfohlen, das als sicher geltende Protokoll HTTPS zu verwenden. HTTPS (Hypertext Transfer Protocol Secure) garantiert eine verschlüsselte Verbindung zwischen dem Webbrowser und dem Webserver. Bietet ein Webserver das Protokoll HTTPS an, so braucht der Nutzer dieses lediglich an den Anfang der URL im Webbrowser zu setzen. Auf der URL des Chaos Computer Clubs heißt es dazu: „Warum sollte das Abrufen von Webseiten verschlüsselt passieren, die Inhalte sind doch öffentlich? HTTPS bietet nicht nur die Verschlüsselung, sondern auch die Authentizität und Integrität der abgerufenen Daten. Ein vierter Punkt ist die Anonymität der Kommunikation. Neben den Inhalten der abgerufenen Seiten gibt es "die näheren Umstände der Kommunikation". Die Information, dass Person X die Webseiten Y abgerufen hat, bezeichnet man als Verbindungs- bzw. Verkehrsdaten. Wenn genügend Verbindungsdaten zusammen-

[21] Schulzki-Haddouti, Christiane. Unsichtbar und raffiniert – die verdeckten Ermittlungen der kleinen Schwestern. 2000. S. 20.
[22] Vgl. Rötzer, Florian. Das Recht auf Anonymität. 2000. S. 27.

gefasst werden, lässt sich ein Bewegungsprofil einer Person erstellen. Dieses Bewegungsprofil kann dann mit anderen Datenbeständen abgeglichen werden (= Rasterfahndung). Am Ende steht die totale Überwachung jedes einzelnen und der Verlust jeglicher Privatsphäre“.[23]

Neben weiteren Empfehlungen gibt es außerdem zahlreiche Computerprogramme und Verfahren, mit denen das anonyme „Surfen“ im Internet ermöglicht werden kann. „Aufgrund einer Studie zur Internet-Kriminalität, die das BKA in Zusammenarbeit mit Providern, Banken und E-Commerce-Firmen erstellt hat, sei man zum Schluss gekommen, dass die Konstruktion des weltweiten Computernetzes einige Faktoren beinhalte, die Kriminalität begünstigen, beispielsweise frei zugängliche Hackerprogramme und die hohe Anonymität im Internet. Daher müsse die Verbreitung von Hackerprogrammen eingeschränkt und die Anonymität beim E-Commerce reduziert werden, außerdem sollten Zulassungskriterien für die Internet-Provider entwickelt werden.“[24] Dann müsste indessen auch die Benutzung von Internet-Cafés und Telefonzellen eingeschränkt oder gar verboten werden, da dort die Anonymität ohne Zuhilfenahme zusätzlicher Techniken erreichbar ist. Eine anders lautende Meinung wird von Boris Gröndahl vertreten: „Solche Techniken werden aber in vielen Fällen von denselben Sicherheitsbehörden bekämpft und von denselben Unternehmen ignoriert, die andererseits Panikmache vor Hackern betreiben. Man kann sogar die These vertreten, dass die Informations-Infrastruktur sicherer wäre, wenn man auf die Ratschläge der Hacker hören würde“.[25]

## 4.2 Die Biometrie

Im Zuge der Terrorismusgesetze der USA einigten sich die Mitgliedsstaaten der Europäischen Union auf die Einführung der Biometriepässe ab Mitte 2006. Als Vorreiter bei der Entwicklung von Lösungsansätzen in diesem Bereich traten die Bundesrepublik und insbesondere das BSI in den Vordergrund.

In Deutschland ist die Einführung biometrischer Reisepässe ab dem 01. November 2005 vorgesehen. Ab 2006 werden Personalausweise ebenfalls biometrische Daten aufweisen. Die herkömmlichen Pässe behalten allerdings nach wie vor ihre Gültigkeit. Die Speicherung der biometrischen Daten soll auf RFID-Chips erfolgen. Aus Sicht des Datenschutzes stellt dieser Lösungsansatz allerdings Probleme dar.

[23] http://www.ccc.de/https/?language=de. Download am 07.11.2005.
[24] Rötzer, Florian. Das Recht auf Anonymität. 2000. S. 31 f.
[25] Gröndahl, Boris. Hacker. 2000. S. 89.

Allgemein betrachtet geht es um die digitale Aufnahme biometrischer Daten im Passwesen. Mit der Einführung der neuen Pässe wird zunächst das Gesicht des Passinhabers gespeichert und im nächsten Schritt, das heißt im Jahre 2007, ist die Implementierung des Fingerabdrucks geplant.[26] Die Speicherung der biometrischen Daten erfolgt auf so genannten RFID-Chips. RFID (Radio Frequency Identification) ist eine Methode, um Daten berührungslos und prinzipiell ohne Sichtkontakt durch Radiowellen lesen und speichern zu können. Ursprünglich war es seitens der USA geplant, die in den Pässen gespeicherten Daten ohne optischen Zugriff seitens der Lesegeräte auszulesen. Dadurch bestand jedoch die Gefahr im Verlust der „informationellen Selbstbestimmung".[27] Aufgrund des leicht zu versteckenden Senders gäbe es somit keinen Einfluss mehr darauf, welche Informationen zu welcher Zeit offenbart würden. Datenschützer kritisierten dieses Konzept und erreichten dadurch eine Einlenkung seitens der USA. Daraufhin einigte man sich auf die Verfahren „Basic Access Control" und „Extendet Access Control". Mit dem Einsatz dieser Verfahren funktioniert das Auslesen der Daten nur dann, wenn das Lesegerät einen optischen Zugriff auf den Chip bzw. auf den Pass hat.[28]

Es bleibt anzumerken, dass die biometrischen Erkennungsverfahren durchaus sinnvolle Anwendung in diversen Bereichen finden. Im Bereich der Nutzerfreundlichkeit und der Datensicherheit wird sich die Biometrie ganz ohne Zweifel durchsetzen. Betrachtet man diese Art der Authentifizierung genauer, so bleibt jedoch durchaus ein fader Beigeschmack. Die Verifizierung der Person erfolgt bei dem biometrischen Verfahren aufgrund körpereigener Merkmale. Und genau hier liegt das Problem. Astrid Albrecht und Thomas Probst warnen davor, dass die Person selbst zum Erkennungsobjekt wird und dies Fragen der Menschenwürde und des Persönlichkeitsrechts betrifft.[29]

Die technisch realisierbare Symbiose zwischen biometrischer Gesichtserkennung und der Verwendung von Videoüberwachungskameras verschafft der Diskussion eine weitere Brisanz. „Durch moderne Verfahren, die eine automatisierte Erfassung biometrischer Daten von vielen Personen ermöglichen, erwächst ein ernstzunehmendes Überwachungspotential. So ist durch

[26] Vgl. http://www.bsi.de Download am 12.11.2005.
[27] https://berlin.ccc.de/index.php/Verlust_der_b%C3%BCrgerlichen_Freiheiten. Download am 12.11.2005.
[28] Vgl. ebd.
[29] Vgl. Albrecht, Astrid, Probst, Thomas. Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme. 2001. S. 29.

eine Kopplung von Videoüberwachungskameras mit Gesichtserkennungssystemen, wie sie ansatzweise im britischen Newham verwendet werden, die Erstellung von Bewegungsprofilen einzelner Personen möglich – sie können automatisiert von Kamera zu Kamera weitergereicht und so der Aufenthaltsort einer Person aufgezeichnet werden."[30]

Neben der eigentlichen biometrischen Authentifizierung einer Person besteht das Risiko noch weitere passive Informationen an die überwachende Instanz zu übergeben. Mit Hilfe von Videoaufnahmen des Gesichtes und insbesondere des Augenhintergrundes, lassen sich – wie Astrid Albrecht und Thomas Probst beschreiben – zusätzlich „Diagnosen von Krankheiten" erkennen. Darüber hinaus lassen sich „Geschlecht, ungefähres Alter und Hinweise auf die ethnische Herkunft gewinnen".[31]

## 4.3 Die Videoüberwachung

„Und je mehr wir uns aus der vertrauten materiellen Welt entfernen und in die digitale Welt eintauchen, desto kenntlicher werden wir, paradoxerweise eben auch in unseren privaten Räumen, in denen wir im vernetzten Zeitalter stärker an der Öffentlichkeit teilnehmen und in ihr sind, als wenn wir uns in die alten öffentlichen Räume begeben."[32] Doch sind die öffentlichen Räume mittlerweile nicht auch Räume entzogener Anonymität? Bahnhöfe, Einkaufzentren, Autobahnen oder auch Einkaufsstraßen bieten an manchen Orten bereits nahezu flächendeckende Videoüberwachung, die sämtliche Bewegungen aufzeichnet und protokollierbar macht.

Die Frage sei berechtigt, ob Videoüberwachung den erforderlichen Nutzen auch wirklich erbringt. Kann man sich sicher fühlen, wenn beispielsweise in der U-Bahn Kameras installiert sind? Die Kameras zeichnen zwar das Geschehen auf. Doch kommt es zu einem Verbrechen, dann sind es meist die Passanten, die zur Hilfe eilen oder zumindest Hilfe rufen. Mittels der Kamera wird meistens lediglich der Tathergang im Nachhinein rekonstruiert. Obwohl die Kamera sichtbar ist, fehlt die Gewissheit, dass es jemanden gibt, der die Aufzeichnung analog zum Geschehen überwacht. Die Anwesenheit einer Videokamera ist oftmals aufgrund seiner Größe oder aufgrund seiner absichtlichen Verborgenheit optisch kaum wahrnehmbar. Der

[30] Albrecht, Astrid, Probst, Thomas. Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme. 2001. S. 32.
[31] Albrecht, Astrid, Probst, Michael. Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme. 2001. S. 33.
[32] Rötzer, Florian. Das Recht auf Anonymität. 2000. S. 27.

offensichtliche Nutzen, die Abschreckung von Straftaten, könnte demnach ebenfalls darunter leiden.

Hier gibt es ganz offensichtlich eine Diskrepanz zum architektonischen Panoptikum Benthams, welches Foucault folgendermaßen beschreibt: „Die Wirkung der Überwachung ist permanent, auch wenn ihre Durchführung sporadisch ist“.[33] Das heißt, dass es nicht erforderlich ist, die Überwachung tatsächlich permanent zu besetzen. Weiter schreibt Foucault: „Zu diesem Zweck hat Bentham das Prinzip aufgestellt, daß Macht sichtbar, aber uneinsehbar sein muß; sichtbar, indem der Häftling ständig die hohe Silhouette des Turms vor Augen hat [auf das digitale Zeitalter bezogen die Kamera], von dem aus er bespäht wird; uneinsehbar, sofern der Häftling niemals wissen darf, ob er gerade überwacht wird; aber er muß sicher sein, daß er jederzeit überwacht werden kann“.[34] Wodurch aber lässt sich die Illusion herbeiführen, dass ein Häftling dahingehend getäuscht wird, einer permanenten Überwachung unterworfen zu sein? Das Panoptikum existierte lediglich in der Vorstellung Benthams. Eine tatsächliche Realisierung seines Modells hatte Bentham nicht mehr miterlebt. Erst innerhalb des Viktorianischen Zeitalters entsprachen viele Gefängnisse seiner Idee.[35] Eines der besten Beispiele hierfür ist das Gefängnis Port Arthur, welches in der damaligen Zeit die größte Sträflingskolonie Australiens war.[36] Die Illusion der allgegenwärtigen Überwachung basiert vor allem auf der Architektur, auf die Wirkung des herausragenden Turms in der Mitte des ringförmigen Gebäudes. „Damit die Anwesenheit oder Abwesenheit des Aufsehers verborgen bleibt, damit die Häftlinge von ihrer Zelle aus auch nicht einen Schatten oder eine Silhouette wahrnehmen können, hat Bentham nicht nur feste Jalousien an den Fenstern des zentralen Überwachungssaales vorgesehen, sondern auch Zwischenwände, die den Saal im rechten Winkel unterteilen, und für den Durchgang von einem Abteil ins andere keine Türen: denn das geringste Schlagen, jeder Lichtschein durch eine angelehnte Tür hindurch könnten die Anwesenheit des Aufsehers verraten.“[37]

[33] Foucault, Michel. Überwachen und Strafen. Die Geburt des Gefängnisses. 1976. S. 258.
[34] Ebd. S. 258 f.
[35] Vgl. http://de.wikipedia.org/wiki/Panopticon. Download am 22.10.2005.
[36] Ebd.
[37] Foucault, Michel. Überwachen und Strafen. Die Geburt des Gefängnisses. 1976. S. 259.

# 5 Das digitale Überwachungspanoptikum

Am Beispiel der Verbannung der Lepra und der Bannung der Pest erläutert Foucault die Ziele des panoptischen Prinzips und die Intention einer politischen Macht über die Gesellschaft. Weiter notiert Foucault: „Einmal ist es der Traum von einer reinen Gemeinschaft, das andere Mal der Traum von einer disziplinierten Gesellschaft. Es handelt sich um zwei Methoden, Macht über die Menschen auszuüben, ihre Beziehungen zu kontrollieren und ihre gefährlichen Vermischungen zu entflechten.“[38]

Mit der zunehmenden Digitalisierung von Informationen und insbesondere von personenbezogenen Informationen wird der Weg in eine Richtung beschritten, welche dem panoptischen Prinzip näher kommt. Digitale Informationen lassen sich komfortabel speichern, und bearbeiten. Florian Rötzer schreibt: „Und mit den wachsenden Möglichkeiten immer mehr Daten aller Art speichern, aufbereiten und durchsuchen zu können wachsen auch die Begehrlichkeiten, sie weitest gehend auszunutzen und sich die Daten anzueignen, egal ob es dabei um wissenschaftliche Forschung, Verbrechensbekämpfung, Authentifizierung, Wirtschaftspionage, Überwachung der Bürger und Angestellten, Verkehrsmanagement, medizinische Versorgung, Risikoplanung, Werbung und Marketing oder was auch immer geht“.

Fest steht, dass Computernetze und Datenbanken sowie unterschiedliche technologische Entwicklungen (z.B. RFID-Chips) die elementaren Bausteine für das moderne Panoptikum sind und gerade auch zukünftig sein werden. Thomas Barth formuliert in diesem Zusammenhang die Frage: „was wir mit dem kommenden Cyberspace machen wollen (oder was wir wollen, dass er mit uns macht) als politische, aber auch als soziale Problematik“.[39] Die physischen Mauern des Benthamschen Panoptikums wurden aufgelöst. Es wird neu aufgebaut, doch statt aus Steinen besteht es nun primär aus Bits und Bytes, aus Nullen und Einsen. Foucault bemerkt: „Aber das Panopticon ist nicht als Traumgebäude zu verstehen: es ist das Diagramm eines auf seine ideale Form reduzierten Machtmechanismus; sein Funktionieren, das von jedem Hemmnis, von jedem Widerstand und jeder Reibung abstrahiert, kann zwar als ein rein architektonisches und optisches System vorgestellt werden: tatsächlich ist es eine Gestalt politischer Technologie, die man von ihrer spezifischen Verwendung

[38] Foucault, Michel. Überwachen und Strafen. Die Geburt des Gefängnisses. 1976. S. 255.
[39] Barth, Thomas. Cyberspace, Neoliberalismus und inverser Panoptismus. 1997 http://swiki.hfbk-hamburg.de:8888/technoterroristen/3. Download am 22.10.05.

ablösen kann und muß“.[40] Was übrig bleibt, ist die Möglichkeit der Machtausübung ausgehend von wenigen Menschen, übertragend auf viele. Die Gesellschaft befindet sich nunmehr in einem virtuellen Gebäude, in dem jeder gesehen wird, doch niemand seine Überwacher sehen kann. „Das Panopticon ist eine Maschine zur Scheidung des Paares Sehen/Gesehenwerden: im Außenring wird man vollständig gesehen, ohne jemals zu sehen; im Zentralturm sieht man alles, ohne je gesehen zu werden.“[41]

[40] Foucault, Michel. Überwachen und Strafen. Die Geburt des Gefängnisses. 1976. S. 264.
[41] Foucault, Michel. Überwachen und Strafen. Die Geburt des Gefängnisses. 1976. S. 259.

# 6 Fazit

Es stellt sich die Frage, welchen Preis die Bevölkerung für eine sichere und weitestgehend entkriminalisierte Gesellschaft zahlen will. Es ist unumstritten, dass die digitalen Datennetze sowohl für kriminelle Aktivitäten als auch für die Verbrechensbekämpfung ein geeigneter Nährböden sind. Ein Grund dafür ist die mögliche Anonymität, die durch die Zuhilfenahme von bestimmter Soft- und/oder Hardware realisiert werden kann. Wird das Recht auf Anonymität jedoch verwehrt, so führt dies unweigerlich zur Eindämmung jeglicher persönlicher Entfaltung. Das digitale Panoptikum scheint bereits in einigen Bereichen unserer gesellschaftlichen Ordnung Einzug zu halten. Es bleibt mit Spannung und vor allem mit Obacht abzuwarten, wohin seine Entwicklung geht.

Abschließen möchte ich meine Arbeit mit einem Zitat von Benjamin Franklin:
„Diejenigen, die grundlegende Freiheiten aufgeben würden, um vorübergehend ein wenig Sicherheit zu gewinnen, verdienen weder Freiheit noch Sicherheit“.[42]

[42] Benjamin Franklin.

# 7 Literaturverzeichnis

**Albrecht, Astrid, Probst, Thomas:** Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme.
In. Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven.
Hrsg. Behrens, Michael und Roth, Richard
Vieweg. 1. Auflage. 2001

**Barth, Thomas**: Soziale Kontrolle in der Informationsgesellschaft: Systemtheorie, Foucault und die Computerfreaks als Gegenmacht zum Panoptismus der Computer- und Multimedia-Kultur.
Pfaffenweiler. Centaurus-Verl.-Ges.1997

**Dr. Müller, Werner**: E-Privacy. Datenschutz im Internet.
Hrsg. Bäumler, Helmut
Vieweg. 1. Auflage. 2000

**Foucault, Michel**: Überwachen und Strafen. Die Geburt des Gefängnisses.
Suhrkamp, 1976

**Franklin, Benjamin**.

**Gröndahl, Boris**: Hacker.
Hrsg. Martin Hoffmann.
Rotbuch 3000. 2000

**Rötzer, Florian**: Das Recht auf Anonymität.
In E-Privacy. Datenschutz im Internet.
Hrsg. Bäumler, Helmut
Vieweg. 1. Auflage. 2000

**Schulzki-Haddouti, Christiane**: Unsichtbar und raffiniert – die verdeckten Ermittlungen der kleinen Schwestern.
In. E-Privacy. Datenschutz im Internet
Hrsg. Bäumler, Helmut
Vieweg. 1. Auflage. 2000

**Splett, Jörg**: Biometrik Human? Zu ethischen Fragen im Zusammenhang mit biometrischen Identifikationsverfahren.
In. Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven.
Hrsg. Behrens, Michael und Roth, Richard
Vieweg. 1. Auflage. 2001

**Wiese, Markus**: Unfreiwillige Spuren im Netz.
In. E-Privacy. Datenschutz im Internet.
Hrsg. Bäumler, Helmut
Vieweg. 1. Auflage 2000

**Barth, Thomas**: Cyberspace, Neoliberalismus und inverser Panoptismus. 1997.
http://swiki.hfbk-hamburg.de:8888/technoterroristen/3
Download am 22.10.05

**Biometrie**
https://berlin.ccc.de/index.php/Verlust_der_b%C3%BCrgerlichen_Freiheiten.
Download am 12.11.2005

**Bundesamt für Sicherheit in der Informationstechnik**
http://www.bsi.de
Download am 12.11.2005

**Chaos Computer Club**
http://www.ccc.de
Download vom 07.11.2005

**Hackerethik**
http://de.wikipedia.org/wiki/Hackerethik
Download am 22.10.2005

**HTTPS**
http://www.ccc.de/https/?language=de
Download am 07.11.2005

**Panoptikum**
http://de.wikipedia.org/wiki/Panopticon. Download am 22.10.2005
Download am 22.10.05

**Volkszählung**
http://de.wikipedia.org/wiki/Volksz%C3%A4hlung_in_der_Bundesrepublik_Deutschland_%281987%29.
Download am 22.10.05