universität wien

DIPLOMARBEIT

Titel der Diplomarbeit

Keine Angst! – Wir haben alles unter Kontrolle!

Eine Untersuchung zum Thema Überwachung und Datenschutz

Verfasserin

Dagmara Anna Zamojska

angestrebter akademischer Grad

Magistra der Sozial- und Wirtschaftswissenschaften (Mag. rer. soc. oec.)

Wien, 2012

Studienkennzahl lt. Studienblatt :	A121
Studienrichtung lt. Studienblatt:	Soziologie
Betreuerin:	Ao. Univ.-Prof. Dr. Hildegard Weiss

DANKSAGUNG

Eine universitäre Ausbildung erfordert viel harte Arbeit, starke Nerven und eine überdurchschnittliche Ausdauer. Ein Studium setzt demnach viel Selbstdisziplin, Durchhaltevermögen und Ehrgeiz voraus. Doch all diese Tugenden zusammen bringen den lang ersehnten Erfolg eines akademischen Abschlusses nicht, wenn es niemanden gibt, der hinter einem steht und an einen glaubt! Nur der Wille allein ist im Stande Berge zu versetzen.

An dieser Stelle möchte ich mich besonders bei meiner Familie für die großartige Unterstützung während des Studiums bedanken. Ihnen gebührt mein größter Dank und Respekt, nicht nur, weil sie mich finanziell durch das Studium begleitet haben, sondern vor allem auch, weil sie emotional mit Rat und Tat stets an meiner Seite waren und nie aufgehört haben an mich zu glauben. Ohne diese wundervolle Hilfe weiß ich nicht, ob ich jetzt jene Zeilen vor mir hätte schreiben können – Danke!!

Einen nicht zu unterschätzenden großen Beitrag zum Gelingen meines Studiums haben auch meine Freunde geleistet. Sie waren sowohl in guten, wie auch in schlechten Zeiten immer für mich da und haben weder an mir gezweifelt, noch mich jemals im Stich gelassen. Auch bei euch möchte ich mich von ganzem Herzen bedanken, besonders bei Kathrin Stecher und Susanne Dania.

Einen ebenso bedeutend großen Dank möchte ich mit aller Hochachtung meiner Betreuerin Frau Prof. Dr. Hildegard Weiss aussprechen. Ohne diese professionelle, aktive und hingebungsvolle Unterstützung, wäre die Realisierung dieser Diplomarbeit längst noch ein schlummernder Utopiegedanke. Ich danke Ihnen besonders für die anregungsvollen Ideen und aufmunternden Worte – Danke!!

Recht herzlich möchte ich mich auch beim Herrn Robert Strobl, für die wunderbare Unterstützung bei der statistischen Auswertung der empirischen Studie bedanken. Trotz des Stresses und Zeitdrucks, fanden Sie die nötige Zeit für mich und meine Fragen – Danke!!

Außerdem möchte ich Gerrit Prassl danken, wonach mir eine Vereinbarkeit von Beruf und universitärer Ausbildung ermöglicht wurde. Stets konnte ich auf deine Unterstützung und dein Verständnis hoffen – Danke!!

Ebenso möchte ich einem ganz besonderen Menschen in meinem Leben danken!! Im Sturm hast Du mein Herz erobert – für immer gehört es nur Dir! Was ich so lange gesucht habe, habe ich alles in Dir gefunden! Ich danke dir, dass Du moralisch mir immer zur Seite stehst, mein Schatz, Daniel Kern!

Abschließend möchte ich mich noch bei all jenen Personen für das Ausfüllen des Fragebogens und die tatkräftige Unterstützung bei der Durchführung meiner empirischen Erhebung zum Thema „Überwachung in Wien“ bedanken! Ohne eure Hilfe wäre es nie zu dieser Studie gekommen! Danke!!

EIDESSTATTLICHE ERKLÄRUNG

Ich erkläre hiermit an Eides Statt, dass ich die vorliegende Arbeit selbständig und ohne Benutzung anderer als der angegebenen Hilfsmittelangefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen

Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Wien, am 02. 04. 2012

_____

Dagmara Anna Zamojska

KURZFASSUNG

Das Thema der Überwachung einer Gesellschaft und seiner Individuen gewinnt immer mehr an Bedeutung und wird noch im Laufe der nächsten Jahrzehnte immer mehr Beachtung finden. Es stellt einen großen, nicht zu unterschätzenden Bestandteil soziologischer Analysen dar, da immer mehr Bereiche unseres Lebens überwacht und kontrolliert werden, bedingt durch die, sich von Tag zu Tag weiterentwickelnden, innovativen Informationstechnologien. Diese ständig wachsende Bandbreite an verschiedenen Techniken der Überwachung der BürgerInnen ermöglicht es, deren Verhalten, Verhaltensmuster und soziale Prozesse aufzuzeichnen, zu speichern und auszuwerten. Dadurch soll, so die prominenteste Annahme, nonkonformes Verhalten (vgl. Zurawski 2007: 7) erkannt, bestraft und im besten Fall gar verhindert werden, wie zum Beispiel durch den Versuch der Prävention von Straftaten, die Beseitigung organisierter Kriminalität, den Schutz vor Terrorismus und die Gewährleistung von Sicherheit. Aus einer kritischen Perspektive heraus, versucht diese Arbeit den gegenwärtigen Stand sozialer Überwachung im Überblick darzustellen. Die Ursachen und Hintergründen für die Herausbildung einer Überwachungsgesellschaft, sowie deren Entwicklung, sollen dabei aufgezeigt werden. Die Arbeit soll als Anregung und Beitrag für Diskussionen dienen und nicht nur im wissenschaftlichen, sondern auch im öffentlichen Raum für Interesse an diesem Thema sorgen. Anhand einer empirischen Erhebung wird die Meinung der Öffentlichkeit zu dieser Thematik erfasst, da ja letztendlich Individuen als Ganzes, sowie das Individuum als Einzelnes, den Kern sozialer Überwachung darstellen.

ABSTRACT

The surveillance of the society and its individuals becomes an increasingly important issue and will even attract more and more interest over the next few decades.

It represents a large, not to underestimated part of sociological analysis. In consequence of the day to day advancing, innovative information technologies more and more areas of our lives are kept under surveillance.

This ever-growing range of different techniques of surveillance of citizens makes it possible to record, store and evaluate their behaviour patterns and social processes.

Thereby the most famous assumption of surveillance, nonconformist behavior should get detected and punished, at best even prevented, such as the attempt of crime prevention, the elimination of organized crime, protection against terrorism and security guarantee.

From a critical perspective this work attempts to portray the current state of social control at a glance. The causes and backgrounds for the development of a surveillance society, as well as their growth should be pointed out.

This diploma thesis is intended to provide inspiration and to contribute to a discussion, not only in scientific but also in the public. Based on an empirical survey, the public opinion is recorded, because after all it’s individuals as a whole, as well as the single individual, that compose the root of social surveillance.

„Wer die Freiheit aufgibt,
um Sicherheit zu gewinnen,
wird am Ende beides verlieren“
(Benjamin Franklin[1])

Abbildung 1 Überwachungsstaatsadler[2]

[1] www.sevillana.de
[2] Das Foto wurde am 28. September 2005 in Linz aufgenommen und am 24. Oktober 2005 für jedweden Zweck im Internet zur Verfügung gestellt. Der/Die FotografIn gibt seinen/ihren Namen nicht bekannt (www.wikimedia.org).

INHALTSVERZECHNIS

1. Einleitung

1.1. Thema und Problemstellung

Wir wussten, es ist unmöglich –
darum haben wir es getan.
(Nelson Mandela[3])

Viele mögen denken, die Überwachungsgesellschaft sei eine Utopie. Doch was viele noch nicht ahnen, „d*er Überwachungsstaat, der jeden Lebensakt der Menschen registriert, ist längst abgeschlossen[4]*“, schreibt Dr. Hans Zeger[5], Lektor am Juridicum Wien, Mitglied des Datenschutzrates im Bundeskanzleramt und Geschäftsführer der e-commerce monitoring GmbH.

Lassen Sie mich diesbezüglich eine Geschichte erzählen, beginnend bei Ihrem Handy. Geräte mit eingebauten GPS-Modulen, wie beispielsweise Mobiltelefone oder Navigationsgeräte, PDAs, Notebooks, ermöglichen, solange diese eingeschalten sind, mit Hilfe von Satelliten, eine auf wenige Meter genau Peilung Ihres Standortes. Darüberhinaus wird am 1. April 2012 die Vorratsdatenspeicherung in Österreich in Kraft treten, womit sämtliche Verbindungsdaten des Telefonie- und Internetkonsums verdachtsunabhängig, dies bedeutet von allen BürgerInnen[6], für 6 Monate auf Vorrat gespeichert werden. Fast überall lassen sich Videokameras aufspüren. An öffentlichen Straßen und Plätzen, im Straßenverkehr, in Einkaufszentren, in den öffentlichen Verkehrsmitteln, auf Bahnhöfen, Flughäfen, vielleicht sogar auch in der Arbeitsstätte, je nachdem in welcher Branche man tätig ist, werden mit Hilfe dieser kleinen Helfer die Schritte und Tätigkeiten der BürgerInnen aufgezeichnet. Sobald Sie Ihren Einkauf mit Kreditkarte bezahlen, weiß die Bank wo Sie welche Summe ausgegeben haben. Besitzen und benutzen Sie womöglich noch spezifische Kundenkarten, so wundern Sie sich nicht, wenn Sie zu besonderen Anlässen, Prospekte mit ausgewählten Produkten (eine Strategie des gezielten Marketings) zu Vorteilspreisen ins Haus oder in die Wohnung zugeschickt bekommen, welche Sie mit Vorliebe konsumieren, oder auch nicht. Denn Dank der Kundenkarten werden nämlich sogenannte Kundenprofile erstellt, welche Ihr Konsumverhalten wiederspiegeln sollen. Falls auf einmal das Internet diverse Seiten vorschlägt, welche Sie möglicherweise interessieren könnten, hängt dies

[3] www.sevillana.de
[4] www.vidc.org
[5] Studium der Philosophie, Mathematik & Sozialwissenschaften.
[6] Die vorliegende Arbeit wurde nach bestem Wissen und Gewissen in einer geschlechtsneutralen Sprache verfasst. Sollten sich dennoch Textpassagen finden lassen, welche eine geschlechtsneutrale Formulierung nicht aufweisen, so kann dies nur rein unbewusst geschehen sein und diese Teile sind dennoch als geschlechtsneutral zu verstehen.

damit zusammen, dass Google jede Suchanfrage mit der dazugehörigen IP-Adresse speichert. Haben Sie Google Street View nicht widersprochen, so ist Ihre Wohnung bzw. Ihr Haus in einer 360 Grad Ansicht im Internet zu begutachten. Sollten Sie demnächst in den wohlverdienten Urlaub fliegen, werden Sie am Flughafen von einem Nacktscanner in Empfang genommen. Die Reisepässe, mit einem RFID-Chip ausgestattet, enthalten bereits auch biometrische Daten, wie den genetischen Fingerabdruck. Über eine Iriserkennung wird bereits diskutiert. Bei einem konkreten Tatverdacht und einer vorliegenden richterlichen Anordnung darf ohne weiteres Ihr Telefon abgehört, ihr Computer von staatlichen Behörden durchsucht und in Ihrem Haus bzw. Ihrer Wohnung Wanzen installiert werden. Einer Verdachtsgewinnung bedarf es nicht. Ihr geliebtes Haustier wurde mit einem Chip ausgestattet, Ihre Elektrogeräte werden demnächst folgen (vgl. BECKER 2010 1-5; Schaar 2007: 11-15; Schulzki-Haddouti 2007: 25-32; Hornung 2007: 150-153).

> *„Überwachung rückt immer näher an die Bevölkerung heran, sie wird flächendeckend.*“ (Becker 2010: 3)

Dabei geht das Gefahrenpotenzial nicht unmittelbar von der Sammlung der Daten an sich aus, als vielmehr deren denkbare Vernetzung[7] aller gesammelten Informationen verschiedener staatlicher und privater Stellen. Zwar mögen wir an dieser Stelle noch von visionären Zukunftsszenarien sprechen, wenn wir als Beispiel anführen, dass es durchaus im Bereich des Möglichen liegt, dass Ihr/Ihre Bankbetreuer/Bankbetreuerin demnächst Zugriff auf die Gesundheitsdatenbanken der verschiedenen Krankenversicherungen haben wird, um im Bereich des Risikomanagements besser abwiegen zu können, wie profitabel es nun sei, Ihnen einen Kredit für die nächsten 5-10 Jahre zu gewähren (vgl. Schaar 2007: 179-183; 2007: 195-205).

> *„(...) I do see great dangers in some unintended consequences of surveillance, especially as far as it is connected with risk management classifications.“*(Lyon 2001: 136)

Durchaus denkbar ist auch eine Absage für eine begehrte, höchst angesehene Arbeitsstelle, weil aufgrund ihrer Billakundenkarte beispielsweise und dem monatlichen Verbrauch für diverse Genussmittel, mit Vorliebe Alkoholika, Sie bei Ihrem Arbeitsgeber den Eindruck erwecken, Sie leiden an einem Alkoholproblem. Wie bereits erwähnt stellen solche erdenklichen Zukunftsaussichten keine exakten, vorhersehbaren, planmäßigen Prognosen für künftige Entwicklungen dar, allerdings gut denkbare und zu erwartende Entwicklungsgänge. Es ist längst kein Geheimnis mehr, dass nichts von Dauerhaftigkeit

[7]Vgl. Kremer 2009; Biermann 2009: 1.

behaftet ist und sich die Gesellschaft, wie wir sie kennen, in einem ständigen Wandel befindet und immer befand. Doch dieser Wandel verläuft von Epoche zu Epoche immer schneller und zügiger. Die Entwicklungsverläufe der letzten 50 Jahre entsprechen in etwa jenen der letzten 300 Jahre. Vor gut 30 Jahren war es noch kaum denkbar gewesen, man könne eines Tages anhand eines tragbaren Mobiltelefons[8] ständig und überall verfügbar sein – heute ist ein Leben ohne Handy gar unvorstellbar. Ebenfalls heiß diskutiert wird der Einsatz des Fingerabdrucks als neues Zahlungsmittel – „Pay by touch" (vgl. Gspurnig). Was einst unmöglich klang, wird bald „gang und gäbe sein" und so ist es durchaus *möglich*, die Betonung liegt hier auf *möglich*, dass eines Tages die einst beschriebenen Horrorszenarien zum allgegenwärtigen Alltag gehören werden. Die Konsequenz dessen ist die allmähliche Auflösung der Privatsphäre und des Datenschutzes. Was einst geheim war, werde transparent. Daher ist es von äußerster Wichtigkeit aufzuzeigen, welche Daten, für wie lange, aus welchen Gründen, für welche Zwecke, wo und von wem erhoben, gespeichert und wie diese in weiterer Folge genutzt und verarbeitet werden. Denn auch hier liegt ein weiterer nennenswerter Kritikpunkt. Es ist anzunehmen, dass viele der Daten im Hintergrund ohne das Wissen der Beteiligten erhoben werden. Oft wissen die BürgerInnen erst gar nicht was für Daten, wann und für welche Zwecke gesammelt werden, bzw. was in weiterer Folge damit passiert, ganz zu schweigen davon, dass oft Zustimmungen bei der Bevölkerung nicht eingeholt werden, weder vorab noch im Nachhinein, wie beispielsweise bei der umstrittenen EU Richtline 2006/24/EG zur Vorratsdatenspeicherung (vgl. Unwatched 2007; Ball/ Wood 2006: 7).

Nichtsdestotrotz bedarf es, um das gesellschaftliche Zusammenleben normkonform gewährleisten zu können, auch deren Kontrolle mittels Überwachung. Sprich die Überprüfung eines ordnungsgemäßen Verhaltens, welches immer von den gegenwärtig vorherrschenden Wertvorstellungen abhängig ist (vgl. Nogala 2000; Peters 1995: 129ff; Scheerer 2000, zit. nach Singelnstein/ Stolle 2007: 47f).Wird delinquentes Verhalten nicht sanktioniert, wie beispielsweise eine Nichteinhaltung der zurzeit gültigen Gesetze, symbolisiert es dessen Akzeptanz und kann über längeren Zeitraum hinweg den Zerfall eines ganzen Systems zur Folge haben. Zwar mögen die hochgesteckten Ziele durch nonkonformes Verhalten schneller erreicht werden können, wie beispielsweise das Ziel der Kapitalmaximierung durch einen Bankraub, allerdings sind derartige Vorgehensweisen weder zielführend, noch tragen sie zum Bestehen eines Gesellschaftssystems bei. Somit sind Regeln für das Funktionieren einer Gemeinschaft und deren Mitglieder, welche ihre Handlungen danach ausrichten, unabdingbar um Chaos zu vermeiden. Regeln konstituieren unter anderem die Handlungsspielräume von Individuen, anhand derer sie sich orientieren

[8] Am 13. Juni 1983 ging das DynaTAC 8000X als erstes Handy der Welt in die Geschichte ein (Passenheim 2008).

können. Doch wie viel Überwachung und Kontrolle verträgt der Bürger, die Bürgerin? Wo ist hier die Grenze zu ziehen?

1.2. Forschungsgenstand und Aufbau der Arbeit

Ziel der vorliegenden Arbeit ist die empirische Untersuchung der allgemeinen Stellungnahme der Wiener und Wienerinnen zum Thema Überwachung in Wien. Im Zentrum dieser Auseinandersetzung steht die Erforschung der Gründe für die Akzeptanz vieler unterschiedlicher Möglichkeiten zur Überwachung und deren tiefen Eingriffe in die Privatsphäre. Besonders in der heutigen Zeit revolutionärer technischer Entwicklungen, wo die Produkte einer solchen Gesellschaft es ermöglichen allumfassende Informationen nicht nur zielgerecht zu generieren, sondern diese auch für unbestimmte Zeit, „*im Zuge der Digitalisierung und Computerisierung der Gesellschaft*“[9], zu speichern, sollte mit besonderer Vorsicht mit persönlichen Daten umgegangen werden. Die einem ständigen Wandel unterzogenen Weiterentwicklungen hervorgebrachter Errungenschaften der Menschheit auf dem Gebiet des Technologiesektors, zugunsten der Nutzen- und Leistungsmaximierung, schaffen immer mehr Möglichkeiten, verschiedene Aspekte menschlicher Lebensbereiche zu überwachen. Eine öffentliche Problembewusstseinswerdung bleibt dabei unter dem Aspekt der Nutzengewinnung aus (vgl. Gaycken/ Kurz 2008: 13f; Weber 2008: 284f). Infolgedessen dematerialisiert sich die kaum erkennbare Grenze zwischen Wirklichkeit und Utopie einer Überwachungsgesellschaft. Indem die gesellschaftliche Bevölkerung eine Gewissheit bezüglich der drohenden Gefahr, seitens totalitärer Überwachung, entwickelt, kann ein Rückgang rechtsstaatlicher Demokratien zu despotischen Regimen unterbrochen werden (vgl. Schaar 2007: 11f).

Was aber sind nun die Gründe für die Akzeptanz der vielfältig vorherrschenden Überwachungsmaßnahmen? Die folgende Abbildung (siehe Abb. 2) versucht die denkbaren Erklärungsversuche bildlich darzustellen (weder die Größe, noch die Nähe der einzelnen ovalförmigen Figuren spielt dabei eine Rolle).

[9] Gaycken/ Kurz 2008: 13

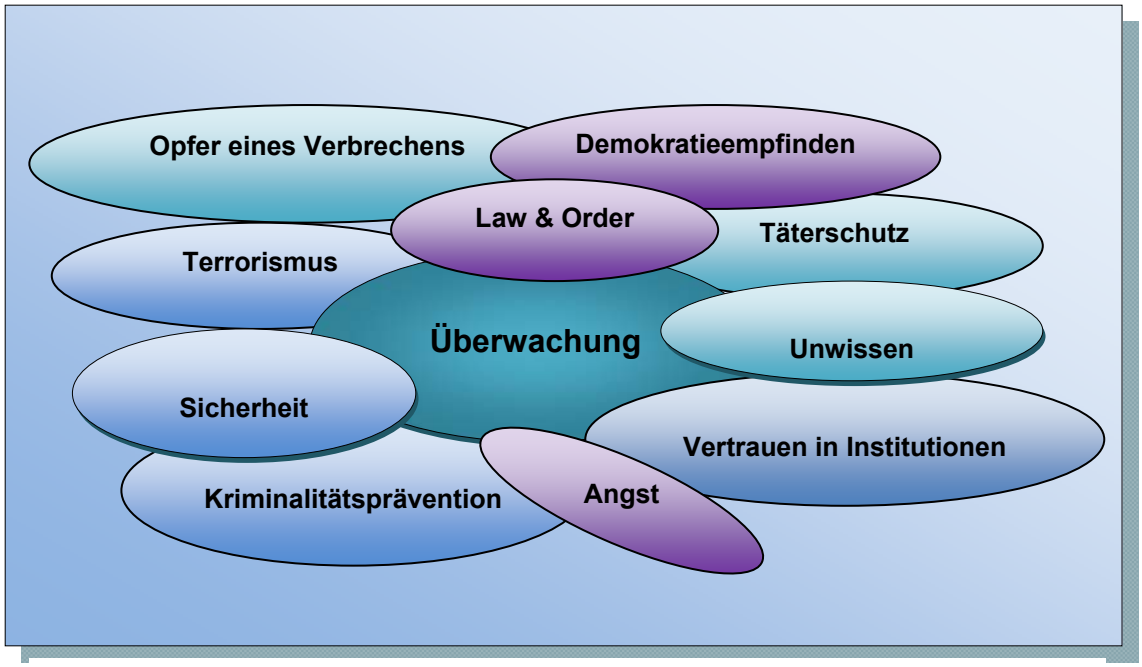


Abbildung 2 Denkbare Gründe für die Akzeptanz von Überwachungsmaßnahmen

Die Arbeit gliedert sich in zwei Teile. Einerseits in einen literarischen Teil und andererseits in einen empirischen Teil.

Kapitel 1 bietet einen kurzen prägnanten Einblick in vorliegende Arbeit und die verschiedenen Kapitel, was den Leser / die Leserin zu erwarten hat. Es wird kurz das Thema und der Problemaufriss vorgestellt.

Kapitel 2 beschäftigt sich mit den verschiedenen Erscheinungsformen überwachungstechnischer Maßnahmen und versucht kurz und doch prägnant in das Konzept der Überwachung einzuführen. Bedingt durch die enge Verflechtung der Überwachung mit dem wachsenden technologischen Fortschritt, bedarf es hier einer ständigen Aktualisierung, da sich im Zuge der technischen Innovationen, auch die Überwachungsmöglichkeiten permanent wandeln. Hier werden aphoristisch die unterschiedlichen Methoden der Überwachung beschrieben. Es soll vor allem, neben den Risiken, auch auf die positiven Aspekte vieler Überwachungsmaßnahmen aufmerksam gemacht werden. Die Arbeit hat den Sinn einer kritischen Auseinandersetzung mit dieser Thematik und nicht den Drang nach einer Feststellung, ob Überwachung an sich als gut oder böse deklariert werden kann.

Kapitel 3 beschäftigt sich mit dem theoretischen Rahmen der Überwachung und den soziologischen Theorien diesbezüglich. Hier werden soziologische Erklärungsversuche und Thesen herausgearbeitet

Kapitel 4 ist ganz und gar der Privatsphäre verschrieben. Hier wird erläutert was unter Privatsphäre verstanden werden kann. Wo diese verankert ist und welche Rechte damit verbunden sind.

Ein ebenso von großer Bedeutung behaftetes Thema, in Zusammenhang mit Überwachung, ist der Bereich des Datenschutzes, welcher sich in **Kapitel 5** wiederfindet. Hier wird darauf eingegangen was Datenschutz ist und warum dieser von so enormer Wichtigkeit ist.

Das **Kapitel 6** widmet sich der Empirie und der quantitativ erhobenen Studie zum Thema Überwachung in Wien. Hier werden der Forschungsstand kurz dargestellt, die Forschungsfragen erläutert, die Forschungshypothesen aufgestellt, das Untersuchungsdesign vorgestellt und die Methode samt den Erhebungsinstrumenten transparent und nachvollziehbar gemacht.

Kapitel 7 hat zur Aufgabe die aus der quantitativen Studie gewonnenen Erkenntnisse anschaulich zu präsentieren, die Ergebnisse zu diskutieren, sowie die in Kapitel 4 aufgestellten Hypothesen auf ihre Richtigkeit zu prüfen und allenfalls zu verwerfen.

Die Arbeit schließt mit einem Resümee in **Kapitel 8**.

2. Überwachung

Niemand ist hoffnungsloser versklavt als der,
der fälschlich glaubt, frei zu sein.
(Johann Wolfgang von Goethe[10])

An dieser Stelle muss geklärt werden, was es unter Überwachung zu verstehen gilt, da sich darunter unterschiedliche Aspekte vereinen lassen. Nach Lyon (2001: 2) beinhaltet Überwachung *"(…) any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered."* Indem Informationen, mit dem Ziel der Verwaltung und Steuerung bürgerlicher Tätigkeiten, gesammelt und verarbeitet werden, kann von Überwachung gesprochen werden. Ball und Wood dehnen ihren Definitionsversuch demgegenüber ein wenig aus, wonach „*Überwachung (...) die absichtliche, systematische, konzentrierte Routinebeobachtung von Personendaten zu Kontroll-, Anspruchs-, Management-, Beeinflussungs- oder Schutzzwecken [ist; DZ].*" (ebd.: 2006: 4). Christoph Dandeker[11] differenziert die Anwendung von Überwachung in drei Bereiche:

> *„The exercise of surveillance involves one or more of the following activities: (1) the collection and storage of information (presumed to be useful) about people or objects; (2) the supervision of the activities of people or objects through the issuing of instructions or the physical design of the natural and built environments. (…) (3) the application of information gathering activities to the business of monitoring the behaviour of those under supervision, and, in the case of subject persons, their compliance with instructions."* (Dandeker 1990: 37, zit. nach Whitaker 1999: 32*)*

Überwachung ist zu einem gängigen Begleiter aller einkommensstarken Industrieländer geworden. Somit stellt die Überwachungsgesellschaft längst keine fiktive Phantasiewelt mehr dar, sondern materialisiert sich allmählich zu einem sozialen Sachverhalt (vgl. Ball/ Wood 2006: 2; Becker 2010: 3). *„All societies that are dependent on communication and information technologies for administrative and control processes are surveillance societies"* (Lyon 2001: 1)*,* argumentiert ebenfalls Lyon, Professor der Soziologie an der Queens Universität in Kingston, Ontario. Organisiert und strukturiert sich eine Gesellschaft mithilfe überwachungstechnischer Instrumente, so kann von einer Überwachungsgesellschaft gesprochen werden. In einer solchen Institution werden die „*Bewegungs- und Handlungsdaten*" (vgl. Ball/Wood 2006: 3) der in ihr lebenden Individuen gesammelt und

[10] www.sevillana.de
[11] Dandeker, Christopher, B.Sc. (Soc.) Ph. D. Professor für „Military Sociology" - Department of War Studies, King's College London, England.

gespeichert. In weiterer Folge werden diese systematisch geordnet und als Nährboden für Entscheidungen, welche das

> *„Recht auf bzw. [den; DZ] Zugang zu Sozialleistungen, Arbeit, Waren und Dienstleistungen sowie Strafrechtspflege, Gesundheit und Wohlfahrt und unsere Bewegungsfreiheit im öffentlichen und privaten Raumbetreffen, herangezogen werden.*“ (Ball/Wood 2006: 3f)

Dabei ist es jedoch von äußerster Wichtigkeit zu betonen, dass die Herausbildung einer Überwachungsgesellschaft nicht auf kapitalistischer Konspiration, Ausbeute oder plutokratischem Drang aufbaut. Die Gründe ihrer Entstehung finden sich in der Komplexität politischer, sowie wirtschaftlicher Handlungssysteme moderner Gesellschaften, welche die Voraussetzungen derzeitiger Effizienz und des zeitgenössischem Komforts bilden (vgl. Lyon 2001: 2; 1994). Dabei wird Überwachung wiederkehrend mit dem Staat in Verbindung gebracht, welcher nicht notgedrungenerweise als der Hauptakteur verstanden werden kann oder muss (vgl. Zurawski 2007: 10). Denn nicht nur komplexe Systeme wenden Praktiken der Überwachung auf der Makroebene an, sondern diese werden sowohl vermehrt von privaten Stellen, wie zum Beispiel von Unternehmen oder Industrien, als auch von den Individuen auf der Mikroebene selbst angewendet. Sei es in der Partnerschaft zur Treuetestung, als Instrument eines Arztes zur Kontrolle des Gesundheitszustandes eines Patienten, oder in der Familie, um Kinder vor Gefahren zu schützen, so lange es diese noch nicht selbst tun können (vgl. Lyon 2001: 3; Ball/ Wood 2006: 9; Becker 2010: 129-133).

Allerdings erreicht der Mensch ab einem gewissen Alter eine gute Selbsteinschätzung für Gefahren und verlässt das gut behütete Nest, um sich selbst der Herausforderung „Leben“ zu stellen. Anders als im familiären Bereich wie zum Beispiel durch Auszug aus dem Elternhaus, Partnerwechsel, etc.), sind Individuen nicht im Stande dem gesellschaftlichen Bereich der Überwachung zu entrinnen. Selbst ein Widerstand im Sinne einer Nichtinanspruchnahme technologischer Gebrauchsgegenstände, was eine Exklusion aus der Gesellschaft zur Folge haben kann, verhindert einen Entzug aus der „*omnipräsenten Überwachung*“ nicht. Denn gänzlich ohne technische Hilfsmittel, kann mittlerweile anhand körperlicher Merkmale, auf die Identität einer Person geschlossen werden, so beispielsweise durch die ausdehnende Videoüberwachung staatlicher, wie auch privater Stellen. Zumal ist ein Entrinnen aus staatlichen Überwachungstechniken mit hohem Aufwand verbunden, wenn beispielsweise gewisse Praktiken durch Gesetze BürgerInnen zur Kooperation binden, wie die Einführung der biometrischen Reisepässe. Darüberhinaus stehen die Kosten des Verzichts und des Ausschlusses in keiner Relation zu den angebotenen Offerten, wodurch eine Akzeptanz widersprüchlicher Eingriffe in Privatsphäre und Datenschutz zugunsten der

Angebote mehr oder minder manipulativ erwirkt wird, besonders wenn jene dafür getätigten Einschnitte nicht transparent dargelegt werden, sondern lediglich deren nutzenbringender Gewinn (vgl. Schulzki-Haddouti 2007: 30f).

Desweiteren kann Überwachung einerseits offen, sprich sichtbar, wie auch verdeckt, also unsichtbar, erfolgen. Kammerer (2008: 168, zit. nach Becker 2010: 111f) unterscheidet an dieser Stelle bei polizeilichen Überwachungsmaßnahmen zwischen präventiven und repressiven Schritten. Gut sichtbare Überwachungsmethoden stellen präventive Maßnahmen dar. Charakteristika offener Überwachungsmaßnahmen sind einerseits die sofortige auffallende Erkennbarkeit für Individuen und andererseits die direkte Assoziation mit Überwachung, so wie beispielsweise auffällig installierte Videokameras in öffentlichen Verkehrsmitteln oder der präsente Einsatz von Polizeibeamten auf öffentlichen Plätzen. Sie verfolgen den Zweck der Abschreckung, sowie der Prävention gewalttätiger Betätigungen, Unruhen und Randale. Repressive Praxen der Überwachung werden hingegen heimlich durchgeführt. Mit ihrer Hilfe soll retrospektiv das kriminelle Handeln nachgestellt, Zeugen ausfindig und Täter überführt werden. Mit unsichtbaren Überwachungsmethoden sind all jene Praktiken und Techniken gemeint, mit denen Individuen unscheinbar überwacht werden können.

> *„Um Kriminalität und Terrorismus zu bekämpfen, erhalten Polizei und Nachrichtendienste immer weiter gehende Befugnisse.“* (Becker 2010: 2)

Folglich zählt zu den Besonderheiten verdeckter Überwachungsmöglichkeiten, dass diese auf den ersten Blick nicht den Eindruck des Wunsches nach Observation bei der Bevölkerung erwecken, wie beispielsweise bei den Kundenkarten. Doch in diesem Falle werden anhand dieser Karten „Kundenprofile“ erstellt, welche das Verhalten, speziell das Kauf- und Konsumverhalten observieren (vgl. Kapitel 2.2.8.). Die so entstandenen Profile liefern in den meisten Fällen jedoch ein verfälschtes Abbild unserer wirklichen Persönlichkeit und nur selten eine getreue Abbildung, da nicht alle Faktoren in die Analyse mit einbezogen werden und oft Hintergrundinformationen bei der Auswertung der Daten fehlen, da diese nicht zugänglich sind oder aus sonstigen Gründen in die Bearbeitung der Daten mit einfließen können. Unsichtbare Methoden zur Überwachung der BürgerInnen sind hingegen auch zahlreicher vertreten. Angefangen von Mobiltelefonen, welche als Peilsender fungieren können, über das Internet und dem Hinterlassen unlöschbarer digitaler Spuren, bis hin zu Reisepässen mit genetischen Fingerabdrücken. Unter dem Konzept einer erhöhten Sicherheit (vgl. Simon/ Simon 2008; Gaycken/ Kurz (Hg.) 2008; Zurawski (Hrsg.) 2007; Schaar 2007; Becker 2010; Ball/ Wood 2006), werden jene Maßnahmen in erster Linie nicht

mit Überwachung in Verbindung gebracht. Dass aber so beispielsweise zusammen mit den Reisepässen eine vollständige Auflistung genetischer Daten aller Gesellschaftsmitglieder eines Staates parallel mit entsteht, bleibt oft im Unterbewusstsein. Es erweckt den Eindruck, dass selbst fragwürdige, sowie höchst umstrittene Maßnahmen solange als legitim erachtet und gebilligt werden, solange diese dem Wohle der Gesellschaft und ihrer Sicherheit dienen oder zumindest im Zuge dessen als solche Akte gerechtfertigt werden können, selbst wenn dies Einbußen für die Individuen bedeutet.

2.1. Geschichtlicher Hintergrund & Entstehung

In vorindustriellen Gesellschaften beschränkte sich die Dokumentation persönlicher Sachverhalte auf ein Minimum, da ein Bedürfnis nach einer Erfassung dieser Daten nicht bestand. Allerdings führten seit dem Spätmittelalter italienische Stadtrepubliken gewissenhaft Buch darüber, wer zu welchem Zeitpunkt und aus welchen Gründen in ihren Grenzen verweilte. Verbannte und Verurteilte wurden ebenfalls namentlich notiert. Zunächst wurden Geschäfte per Handschlag abgeschlossen, da diese im überschaubaren Blickfeld stattfanden. Doch durch die Zunahme unberechenbarer Beziehungen ließ das Vertrauen nach (vgl. Schaar 2007: 32f).

> *„Die mannigfaltige Erhebung von Daten war insofern auch eine Folge der abnehmenden Bedeutung personaler Bindungen und stellte eine logische Reaktion auf den hiermit verbundenen Vertrauensverlust dar.“* (Schaar 2007: 33)

Auch die industrielle Produktionsweise trug zur Dokumentation und Buchführung bei, da sonst ein reibungsloses Funktionieren nicht hätte stattfinden können. Als früher das Wissen noch mündlich von Generation zu Generation überliefert und anvertraut wurde, bedurfte es nun der Aufzeichnung als Planungs-, Steuerungs-, und Bewirtschaftungsinstrument (vgl. ebd.: 33f).

> *„Surveillance is the means whereby knowledge is produced for administering population in relation to risk.”* (Lyon 2001: 6)

Ein erwähnenswertes Merkmal der Moderne stellt die Überwachung dar, welche zur verwaltungsmäßigen Ausdehnung des Nationalstaates beitrug. Als wesentlicher Bestandteil des Staates wurde diese zur Herrschafts- und Machtsicherung eingesetzt (vgl. Giddens 1985, zit. nach Zurawski 2007: 8).Eine maschinelle Massendatenverarbeitung setzte dann knapp 100 Jahre später in den USA 1890/91 mit der Volkszählung unter Verwendung von Lochkarten ein. Diese automatisierte Bearbeitung von Massendaten machte sich knapp ein

halbes Jahrhundert später auch das NS-Regime zur Erfassung der rassischen Zughörigkeit in Folge des Euthanasieprogramms zu Nutze. Es folgte der Einsatz des Computers zur Bearbeitung größerer Datenmenge. Dieser kam vorerst in der Buchhaltung zum Einsatz, sowie in der Meteorologie und Kryptologie[12]. Letztendlich verbreitete sich seine Anwendung auf alle möglichen Bereiche (vgl. Schaar 2007: 34ff).

> *„Spätestens als deutlich wurde, dass es eben keine wirtschaftliche oder gesellschaftliche ››Sättigungsgrenzen‹‹ für ihren Einsatz gab, wurden erste Forderungen erhoben, die Menschen vor den negativen Folgen zu schützen und dabei insbesondere Vorkehrungen zum Schutz der Privatsphäre zu treffen.*" (Schaar 2007: 36)

Die Speicherung, Auswertung und Verarbeitung größerer Datenmengen stellte infolge des revolutionären technologischen Fortschritts einen massiven Anreiz dar, diesen auch zu nutzen, unabhängig von den damit verbundenen Risiken für Datenschutz und Privatsphäre (vgl. ebd.: 36f).

> *„Speichermedien in der Größe eines Fingernagels haben heutzutage bisweilen eine größere Kapazität als vor zwanzig Jahren eine kühlschrankgroße Speichereinheit.*" (Schaar 2007: 37)

Der Computer stellt heute ein universell einsatzfähiges und unentbehrliches Instrument moderner Gesellschafen dar, dessen Informationsinfrastruktur ein unüberschaubares Angebot an Informationen bietet (vgl. Schaar 2007: 32-39).

> *„Es ist zu befürchten, dass (...) bald entsprechende Vorhaben zur Dauerbeobachtung lanciert werden.*" (Schaar 2007: 65)

In den permanent wachsenden technischen Weiterentwicklungen liegt die Ursache des Zuwachses bürgerlicher Überwachung (vgl. Coy 2008: 50; Gaycken/Kurz 2008: 13). Auch Ball und Wood (2006: 6) verweisen darauf, die Grundvoraussetzung gegenwärtiger Überwachungsmöglichkeiten in der Technologie zu suchen, warnen jedoch gleichzeitig davor, darin die universale Triebfeder der Entstehungsgeschichte zu sehen. Darüberhinaus wandelt sich nicht nur die Technik, sondern es findet auch eine Konversion der Überwachung statt, indem sich diese immer mehr und mehr auf die Zukunft, statt auf die Gegenwart, im Sinne der Vollbringung einer Präventionsleistung, bezieht. Sobald das technisch Machbare geschaffen ist, ist der Anreiz seines Einsatzes gegeben. Hier

[12] Militärisch genutzte Datenverschlüsselung

transformiert sich der Rechtsstaat zu einem „*Präventionsstaat*“, welcher primär dem Versuch einer Verhinderung nicht verwirklichter Straftaten nachgeht, während es sich im Rechtsstaat vorwiegend um die retrospektive Ahnung krimineller Vergehen handelt. Der Preis dafür ist die Privatsphäre der BürgerInnen jenes Staates. Als im Rechtsstaat noch die Unschuldsvermutung galt, bedingt Überwachung eine neue Dimension, in welcher jeder und jede als potentielle(r) Verdächtige(r) gilt (vgl. Simon/ Simon 2008: 258ff; Ball/Wood 2006: 8).

2.2. Methoden der Überwachung

Folglich wird das Arsenal der Überwachungsmöglichkeiten kurz vorgestellt. Im Zuge des technischen Fortschritts weitet sich dieses entsprechend aus. Was gestern unmöglich erschien, ist heute alltäglicher Gebrauch. Die Begründung in der Überwachung der BürgerInnen liegt in erster Linie in der besseren Verfolgung, Aufklärung und Prävention von Straftaten (vgl. Becker 2010: 105-112). Neben Rasterfahndungen, Lauschangriffen, Videoüberwachungen, bestehen noch Möglichkeiten der Telekommunikations- und Online-Überwachung, Erstellung von Bewegungsprofilen, oder Sammlung biometrischer Daten. Die Möglichkeiten auf diesem Terrain sind unerschöpflich. Unlängst plant die EU neben der Vorratsdatenspeicherung dieses System nach selbigem Prinzip auf eine flächendeckende Videoüberwachung und die Ausstattung aller Konsumartikel mit RFID-Chips im gesamten europäischen Raum auszuweiten[13]. Befürworter sehen den Nutzen im Kampf gegen Kriminalität und Terrorismus, Gegner betonen die Einschnitte in den Grundrechten der BürgerInnen. Die Mittel und Ziele der Überwachung können weder als rein negativ noch als durchaus positiv gesehen werden. Das Sortiment an Überwachungsmöglichkeiten ist allerdings vielfältig und die Auswahl ist dementsprechend groß, weshalb jene Methoden nur mit besonderer Sorgfalt eingesetzt werden sollten.

2.2.1. Rasterfahndung

Bei der Rasterfahndung werden aus Datenbeständen jene Personen herausgefiltert, welche einem vorab erstellten Täterprofil anhand bestimmter Merkmale gleichen. Durch elektronische Abgleiche werden diese ausgesondert und in weiterer Folge genauer untersucht, mit dem Ziel der Einschränkung der zu überprüfenden Personen. Jene Fahndungsmaßnahme wurde in Österreich am 01.10.1997 als befristetes Gesetz auf vier Jahre erlassen und in nach Ablauf in ein unbefristetes Gesetz umgewandelt. Zur Durchführung eine Rasterfahndung bedarf es einer richterlichen Anordnung und dem Vorliegen schwerer und/oder organisierter Kriminalität. Die Kritik richtet sich einerseits gegen den unsachgemäßen Gebrauch erhobener, personenbezogener Daten nicht polizeilicher

[13] Vgl. http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=11563vpp, 19.02.2012.

Stellen, sowie andererseits gegen eine Diskriminierung Unschuldiger aufgrund des Aufweisens ähnlicher Eigenschaften wie der/die TäterIn (vgl. Cometo Eduhi: 2). Es kommt zu einer Verknüpfung polizeilicher Daten mit unterschiedlichen Dateninventaren nicht polizeilicher Erhebungsherkunft. Der Suchansatz setzt nicht, wie im Falle einer konventionellen Fahndung, bei einer kundbaren Zielperson an, sondern umfasst

> *„Daten von Menschen (...), für die keinerlei Verdachtsmomente vorliegen“* (Schaar 2007: 128)

Jene Personen, welche aufgrund einer Übereinstimmung mit den gesuchten Prüfermerkmalen übereinstimmen, unterliegen fortan einer sorgfältigen Überwachung behördlicher Stellen (vgl. Schaar 2007: 128f). Nach 9/11

> *„(...) erhoben die Länderpolizeien personenbezogene Daten von Universitäten, Einwohnermeldeämtern und aus dem Ausländerzentralregister und glichen diese Datenbestände anschließend anhand festgelegter Rasterkriterien gegeneinander ab.“* (Schaar 2007: 129)

Vom Berliner Datenschutzbeauftragten wurde ermittelt, dass an die Polizei in diesem Falle 58.063 Datensätze ginge, aus jenen nach einer vorher gesetzten Prioritätenliste gerastet wurde (so beispielsweise nach Hautfarbe, Herkunft, Wohnsitz, etc. (vgl. Cometo Eduhi: 2). Schließlich wurden bei 114 Personen eine Übereinstimmung jener Suchbegriffe festgestellt. Über jene „Gezogenen“ wurden Ermittlungsakte angelegt und einer weiteren tiefgehenden Überprüfung unterzogen. Die Kontrolltätigkeiten verliefen allerdings ergebnislos und konnten zu keiner Entlarvung jener gesuchten Täter führen (vgl. Schaar 2007: 129f).

2.2.2. Lauschangriff

Eine heimlich durchgeführte, akustische Ermittlungsmethode ist auch unter dem Namen Lauschangriff bekannt (vgl. Cometo Edhui: 2). Unterschieden wird zwischen dem kleinen, zum Abhören öffentlicher im Freien gelegener Orte, und dem großen Lauschangriff, dem Mithören privater Geschehnisse in den eigenen vier Wänden (vgl. Simon/ Simon 2008: 174). Ziel dessen ist die Erfassung und Überwachung sowohl verbaler als auch nonverbaler Äußerungen verdächtigter Individuen für die Zwecke einer Strafverfolgung, welche in Form von Bild- und/ oder Tonaufzeichnungen überliefert werden. Auch die Anbringung sogenannter „Wanzen“ in Wohnräumlichkeiten tatverdächtigter Personen ist gestattet (vgl. Schaar 2007: 106-110). Handover-Interfaces bzw. auch LI[14]-Schnittstellen sind jene Stellen,

[14] Lawful Interception (vgl. Rieger 2008: 53f)

anhand derer ein unbemerktes Abhören ermöglicht wird und von jedem Telefonanbieter in den Schaltzentralen bereit gestellt werden müssen. Da das Errichten jener Abhörbereiche nicht vom Staat finanziert wird, tragen die Kosten dafür letztendlich die Kunden selbst und zwar in zweierlei Hinsicht. Einerseits werden vom Provider für die Erzeugung besagter Schnittstellen Gebühren an die Kunden verrechnet, so das paradoxerweise die Kunde selbst für die Gelegenheit bezahlen, abgehört zu werden und andererseits stehen den Anbietern keinerlei Möglichkeiten zur Verfügung einen Überblick darüber zu gewährleisten, wann ein Zugriff auf die Daten erfolgt oder nicht. Diese können auch rückwirkend nicht nachgewiesen werden (vgl. Simon/ Simon 2008: 175). Hauptgrund dieser Vorgehensweise ist die Gewinnung stichhaltiger Beweise zur Überführung Krimineller vor Gericht. Dabei ist der Gebrauch zur Verdachtsgewinnung unzulässig. Bei der Inanspruchnahme dieser Fahndungsmethode bedarf es ebenfalls einer richterlichen Anordnung. 1998 fand jene Methode Verankerung im österreichischen Gesetz, welche 2002 durch die Schwarz-Blaue Regierungskoalition ins Dauerrecht übernommen wurde (vgl. Cometo Eduhi: 2). Eine durch die EU im Jahr 2000 beschlossene Richtlinie COPEN 32 regelt zum Einen den Austausch erhobener Informationen auf internationaler Ebene und zum Anderen gestattet diese ein grenzübergreifendes Abhören (vgl. Simon/ Simon 2008: 176).

> *„Artikel 18 besagt, dass die Behörden ohne richterliche Genehmigung eine Zielperson im Ausland bis zu zwölf Tage lang abhören dürfen.*“ (Simon/ Simon 2008: 176)

Kritik an jenem Vorgehen richtet sich in erster Linie gegen die Unübersichtlichkeit und mangelnde Qualität der erhobenen Daten, welche eine weitere Auswertung erschweren. Zudem fallen laut ARGE DATEN bei einem Lauschangriff[15] pro Straffällige(r) bis zu hundert Unschuldige ins Abhörraster (vgl. Cometo Eduhi: 2).

2.2.3. Videoüberwachung

Die ARGE DATEN, Österreichische Gesellschaft für Datenschutz, definiert Videoüberwachung wie folgt:

> *„Als Videoüberwachung sind alle optisch-elektrischen Einrichtungen zu verstehen, die geeignet sind Bildaufzeichnungen von überwachten Räumen und Personen durchzuführen (Video-Installationen).“* (ARGE DATEN 2002)

[15] Der letzte in Österreich bekannt gewordene Lauschangriff erübrigte sich im Sommer 2011. Dazu wurden laut FORMAT Nr. 35/2011 zusätzlich zur Observation, der gesamte Festnetz-, Mobiltelefon-, E-Mail-, SMS- und MMS-Verkehr dreier Lobbyisten von 1. Juni bis 1. Juli 2011, unter dem Vorwand mutmaßlicher Geldwäsche und dem Verdacht der Bestechung von Politikern und anderen Amtsträgern, von der Polizei überwacht (vgl. News).

Laut ARGE Daten gibt es keine Statistiken bezüglich dessen wie weit verbreitet die Videoüberwachung in Österreich ist. 3 000 Kameras werden von der ASFINAG[16] betrieben, bei bestimmten Branchen (wie Banken oder Tankstellen) liegen die Schätzungen bei etwa einer Million[17] Kameras an etwa 50-100 000 Standorten[18] (vgl. ARGE DATEN 2010). Im aktuellsten Datenschutzbericht von 2009 wurde veröffentlich, dass ca. 2600[19] gemeldete Videoüberwachungsanlagen[20] im Datenverarbeitungsregister vorliegen (vgl. Datenschutzbericht 2009: 72). Laut einer E-Mailanfrage an die Datenschutzkommission vom 01.03.2012 liegen jener, nur gemeldete Datenanwendungen von Auftraggebern vor. Die Meldung einer Videoüberwachungsanlage kann eine bis mehrere hundert Kameras umfassen. Nach § 50c Abs. 1 DSG 2000 unterliegen Videoüberwachungen der Meldepflicht gemäß den §§ 17 ff DSG 2000. Eine Videoüberwachung ist von der Meldepflicht ausgenommen, wenn eine Echtzeitüberwachung oder einer Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium erfolgt. Darüberhinaus sind nach § 17 Abs. 2 Z 6 DSG 2000 Datenanwendungen, die einer Standardanwendung entsprechen, nicht meldepflichtig. Diese Standardanwendungen werden in der Standard- und Muster-Verordnung 2004 (StMV 2004), BGBL.[21] II Nr. 312/2004 festgelegt. Die SA032 „Videoüberwachung“ sieht Ausnahmen der Meldepflicht für folgende Bereiche vor: A) Bank, B) Juwelier, Handel mit Antiquitäten und Kunstgegenständen, Gold- und Silberschmied, C) Trafik, D) Tankstellen, E) Bebautes Privatgrundstück (samt Hauseingang und Garage), F) Botschaften und Vertretungen internationaler Organisationen[22].

Der Anwendungsgrund beruft sich auf die Angst vor der Überwachung, wonach divergierendes Verhalten durch die Anwesenheit von Videokameras zum Unterlassen einer abweichenden Tat animieren soll (vgl. Becker 2010: 112). Diese sollen zur Sicherheit beitragen und werden im Allgemeinen begrüßt.

> *„(...) Kameras sollen Kriminalität verhindern (Prävention), zur Aufklärung von Straftaten beitragen (Repression) und das Sicherheitsgefühl der Bevölkerung stärken.“* (Kreutzträger/ Osterholz 2007: 89)

[16] Autobahn- und Schnellstraßen- Finanzierungs- Aktiengesellschaft.
[17] Es kann angenommen werden dass die Anzahl der registrierten Videokameras erst die Spitze des Eisbergs darstellen, wohl gemerkt, dass diese auch nur auf Schätzungen beruhen und das fehlende Informationen im Hinblick auf nicht registrierte Videokameras bestehen. *„Nur „Datenanwendungen“ müssen dem Datenverarbeitungsregister gemeldet werden (vgl. §§ 16 ff DSG 2000). Eine „Datenanwendung“ liegt vor, wenn die zur Erreichung des Zwecks der Datenanwendung vorgenommenen Verarbeitungsschritte „zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen“ (§ 4 Z 7 DSG 2000).“ (Datenschutzbericht 2009: 65)*
[18] Eine Anfrage per E-Mail an die ARGE DATEN vom 19.02.2012, ob sie denn verwertbare Informationen bezüglich der Anzahl registrierter Überwachungskameras (bzw. Videokameras) in Österreich, sowie in Wien hätten, blieb unbeantwortet. STATISTIK AUSTRIA antwortete auf selbiges E-Mail am 24.02.2012, dass sie diesbezüglich keine Statistiken o.ä. hätten.
[19] Stichtag der Videoüberwachungsstatistik 31.12.2009.
[20] Können von einer bis zu mehreren hundert Kameras umfassen.
[21] Bundesgesetzblatt
[22] E-Mailkorrespondenz vom 01.03.2012 mit der Datenschutzkommission Österreich.

Doch die Kriminalität schwindet durch Überwachung nicht. Sie wird lediglich verlagert und auf andere Orte verdrängt, welche (noch) nicht überwacht werden (vgl. Kube 2003: 123; ARGE DATEN 2009). Die im Auftrag der Europäischen Union durchgeführte Studie „European Crime and Safety Survey", veröffentlicht durch das Gallup Institut in Zusammenarbeit mit dem Max-Planck-Institut, liefert Ergebnisse, wonach in keinen anderen europäischen Ländern die Kriminalität derart hoch sei, wie in Großbritannien und Nordirland. Dabei gilt London als ein Paradebeispiel für eine am lückenloseste videoüberwachte Großstadt Europas (vgl. Biermann 2009: 2; Schaar 2007: 26f). Weltweit hat Großbritannien die meisten Überwachungskameras. Die Schätzungen belaufen sich ab einer Million aufwärts. In London wurden 10.524[23] Überwachungskameras in 32 Stadtteilen gezählt (vgl. Klaß 2007). Laut den Statistiken eines Berichts des Londoner Evening Standards, bringen mehr Kameras nicht unbedingt auch mehr Sicherheit mit sich (vgl. Klaß 2007). Es konnte nachgewissen werden,

> *„(…) dass die Anzahl der öffentlichen Überwachungskameras keinen nennenswerten Einfluss auf die Verbrechensbekämpfung hat."* (Klaß 2007)

Ein weiterer springender Punkt ist die Lückenlosigkeit der Videoüberwachung. Kaum noch bleibt etwas unerkannt.

> *„Es ist ein sonniger Tag auf dem Obersalzberg.*
> *»Wie ich verstehe, hat dir unser Film gestern Nacht nicht gefallen«,*
> *meint Adolf Hitler in Bezug auf die Filmvorführung vom Vortag.*
> *»Ich weiß was du magst. Du magst ›Vom Winde verweht‹ nochmals sehen.«"*
> (Simon/Simon 2008: 32)

Zu jenen Hitlers gesprochenen Sätze existieren weder Tonbandaufzeichnungen, noch schriftliche Protokolle und dennoch ist es möglich, 64 Jahre danach zu rekonstruieren, was der damalige Diktator zu jener Zeit auf der Terrasse des Berghofs äußerte. Die Antwort auf die Frage wie dies möglich sei, liegt in den modernen Überwachungstechniken. Anhand der gegenwärtigen Methoden ist es nicht nur möglich den momentanen Augenblick[24] zu überwachen, sondern ebenfalls auch die Vergangenheit, so wie die Zukunft (vgl. Simon/ Simon 2008: 32)

[23] Stand 21.09.2007
[24] 2007 wurde in Großbritannien der Versuch gestartet, Minidrohnen mit Videokameras auszustatten, um so öffentliche Plätze lautlos überwachen und einzelne Personen observieren zu können (vgl. Schaar 2007: 64).

Desweiteren ist zu befürchten, dass der kombinierte Einsatz von Videoüberwachung mit biometrischen Daten zu einer Identifizierung aller gefilmten Personen führen wird (vgl. Schaar 2007: 63).

2.2.3.1. Typen von Videoüberwachungen in Österreich

1. Firmensitze/Betriebsgelände
2. Kaufhäuser/Geschäfte
3. Trafiken
4. Juweliergeschäfte
5. Banken
6. Geldausgabeautomaten
7. Lokale
8. Schnellimbiss-Restaurants
9. Konferenz-/Messezentren
10. Hotels
11. Munitionsfabrik
12. Energieversorgungseinrichtungen
13. Casinos
14. Wettcafés
15. Mehrparteienhäuser
16. Einfamilienhäuser
17. Tankstellen
18. Fahrgastbereich in Taxis
19. Parkgaragen/Parkplätze
20. Autobahnrastplätze
21. Spitäler
22. Museen
23. Theater
24. Fußballstadien/Sportplätze
1. Abfallsammelstellen
26. Schulgelände (Außenbereiche)
27. Öffentliche[25] Gebäude (Ministerien, Parlament, Amtsgebäude)
28. Öffentliche Plätze (durch die Sicherheitsbehörden aufgrund des SPG)
29. Öffentliche Verkehrsmittel – Fahrzeuge
30. Öffentliche Verkehrsmittel – Stationen

(Datenschutzbericht 2009: 73)

2.2.4. Vorratsdatenspeicherung

> *„Vorratsdatenspeicherung im Allgemeinen bezeichnet das anlassunabhängige und nicht zweckbezogene Sammeln von personenbezogenen Daten zur späteren Verwendung.“* (Gaycken/ Kurz 2008: 67)

[25] *„ „Öffentlicher Raum“ ist jener Bereich, in dem sich jedermann grundsätzlich unbeschränkt aufhalten darf und eine Zutrittskontrolle rechtlich nicht – oder nur aus besonderem Anlass – zulässig ist. Dies betrifft etwa Straßen, Plätze, die freie Natur etc.“ (Datenschutzbericht 2009: 67f)*

Am 15. März 2006 wurde von der Europäischen Union eine Richtline 2006/24/EG zur verdachtsunabhängigen Überwachung und Speicherung der gesamten Telekommunikationsdaten aller EU-BürgerInnen für mindestens 6 Monate und maximal 2 Jahre beschlossen. Diese ist auch unter dem Namen „Vorratsdatenspeicherung" bekannt. Heftige Kritikpunkte an dieser Maßnahme, neben den tiefen Eingriffen in die Privatsphäre der BürgerInnen, sind Unklarheit, hoher Erklärungsbedarf und viel Raum für interpretative Auslegungen.

> *„Gespeichert sollen alle Verbindungs- und Standortdaten, welche beim Telefonieren, SMS, E-Mailen, VoIP[26], Faxen und Surfen im Internet entstehen, etwa die Benutzerkennung, Name und Anschrift des Teilnehmers, die IP-Adresse, Kennung oder Rufnummer, als auch die erfolglosen Verbindungsversuche."* (ARGE DATEN 2006)

Verdachtsunabhängig bedeutet dabei, dass die Telekommunikationsdaten *aller* Bürger und Bürgerinnen auf Vorrat gespeichert werden. Dabei wurde die Zustimmung der BürgerInnen zur Speicherung ihrer Daten vorab und auch im Nachhinein nicht eingeholt. In Österreich tritt diese Richtline im April 2012 in Kraft. Als Begründung führt die EU die Ermittlung, Feststellung und Verfolgung schwerer Straftaten[27], die Bekämpfung der organisierten Kriminalität sowie die Ausforschung von Terrorverdächtigten an.

> *„Im österreichischen Entwurf (…) findet sich derzeit bloß die Formulierung, die Daten seien „[...] für einen Zeitraum von sechs Monaten ab dem Zeitpunkt der Beendigung der Kommunikationsvorganges zum Zweck der Ermittlung, Feststellung und Verfolgung von mit beträchtlicher Strafe bedrohten Handlungen [...] zu speichern."* (www.unwachted.org)

Laut dem SPG[28] §17[29], sind dies in Österreich alle strafbaren Handlungen, welche mit mehr als einer einjährigen Freiheitstrafe bedroht sind. Inwiefern die Daten tatsächlich zur Bekämpfung dieser Verbrechen genutzt werden sollen, ist bis dato noch unklar. Denn für Mitglieder krimineller, sowie terroristischer Organisationen ergeben sind dennoch zahlreiche Möglichkeiten die Vorratsdatenspeicherung zu umgehen, wie beispielsweise durch die Nutzung anonymer Wertkarten-Handys[30]. So sind im Grunde genau jene Personen die Leidtragenden, welche gar nicht das Ziel dieser Überwachung bilden (vgl. die Presse). Die

[26] Voice over Internet Protocol = Telefonieren über Computernetzwerke
[27] Abhängig vom nationalen Recht eines jeden einzelnen Mitgliedsstaates.
[28] Sicherheitspolizeigesetz
[29] Mit beträchtlicher Strafe bedroht sind gerichtlich strafbare Handlungen, die mit mehr als einjähriger Freiheitsstrafe bedroht sind." (www.ris.bka.gv.at)
[30] Darüberhinaus besteht beispielsweise die Möglichkeit der Nutzung öffentlicher Telefonzellen, pseudonymer Mobiltelefone, im Ausland erworbener Prepaidkarten oder sogenannter Anonymisierungsservices im Internet wie Tor & Jap. Diese sind im Stande die Herkunft einer Verbindung gegenüber den Anbietern der Dienste zu verschleiern (vgl. Gaycken/Kurz 2008: 74-76; vgl. Simon/Simon 2007: 27f).

Sammlung und Speicherung dieser Telekommunikationsdaten ermöglicht die Erstellung konkreter Bewegungs- und Verhaltensprofile.

> *„Wer sein Mobiltelefon täglich angeschaltet mit sich führt und normale Gebrauchsmuster an den Tag legt, hat zu befürchten, automatisierten Bewegungsmustererkennungen aufzufallen.“* (Gaycken/ Kurz 2008: 76)

2.2.5. Online-Überwachung

Infolgedessen dass jeder getätigte Mausklick im Internet nachvollziehbar und rückverfolgbar ist, stellt das Erstellen sogenannter Onlineprofile eine Leichtigkeit dar (vgl. Schaar 2007:191). Vertreter von Sicherheitsbehörden, Polizeigewerkschaften und Politiker setzen sich darüberhinaus vermehrt für ein heimliches Zugriffsrecht der Polizei und Nachrichtendienste auf Computersysteme ein. Diese Online-Durchsuchungen sollen der Bekämpfung des Terrorismus und der Kriminalität dienen, indem relevanten Behörden der Zugang mittels Trojaner welche per Hacking auf private Rechner durch einen Internetanschluss der zu überwachenden Personen übertragen werden, Zutritt zu privaten Dateien gewähren. Befürworter dieser Maßnahme sehen in Online-Durchsuchungen eine Abwandlung der Hausdurchsuchung. Kritiker betonten jedoch die tiefen Eingriffe in die Privatsphäre, welche Rückschlüsse auf die Persönlichkeit zulassen, die kaum begrenzbare Reichweiter dieser Ermittlungsmethode und die fortlaufende heimliche Dauerbeobachtung der einzelnen BürgerInnen, im Gegensatz zu einer einmaligen Hausdurchsuchung in Anwesenheit von Zeugen. In den USA wurden beispielsweise infolge der Anschläge 9/11, Geheimdiensten und Polizeibehörden uneingeschränkte Befugnisse, ohne vorherige öffentliche Diskussion, zum Abhören von Telefonen, zum Mitlesen von E-Mails und zu heimlichen Zugriffen auf alle verfügbaren Datenansammlungen zugesprochen (vgl. Schaar 2007: 120-125).Laut Kurier[31] sind Online-Durchsuchungen in Österreich bis dato nicht erlaubt. Allerdings plane die SPÖ/ÖVP Regierung bereits eine Gesetzesänderung für eine mögliche legale Rechtsgrundlage, wie beispielsweise dies in Deutschland der Fall ist (vgl. Kurier 2011; Handelsblatt 2011).

2.2.5.1. Google

Der amerikanische Weltkonzern und die globale Suchmaschine „Google“ entsprang 1998 unter seinen Erfindern Larry Page und Sergey Brin. Der Grundgedanke ist die Bereitstellung von Wissen auf globaler Ebene durch Suchanfragen (vgl. Google). Seit 01. März 2012 gelten die neuen Datenschutzbestimmungen und Nutzungsprinzipien für all jene, welche künftig auch weiterhin die Services von Google in Anspruch nehmen möchten. Dabei hat Google

[31] Vgl. www.kurier.at. Artikel vom 13.10.2011, letztes Update am 05.12.2011.

seine 60 Datenschutzbestimmungen zu einer einzigen Richtlinie für alle seine Angebotezusammengeführt (vgl. Faz 2012). Hierbei findet sich nachstehende Erklärung seitens Google:

> *„Wir erheben Informationen, um all unseren Nutzern bessere Dienste zur Verfügung zu stellen – von der Feststellung grundlegender Aspekte wie zum Beispiel der Sprache, die Sie sprechen, bis hin zu komplexeren Angelegenheiten wie zum Beispiel der Werbung, die Sie besonders nützlich finden, oder der Personen, die Ihnen online am wichtigsten sind.“* (Google)

Jene Daten werden von Google auf zweierlei Arten generiert. Einerseits durch eigenständige Bereitstellung der Informationen (Erstellung eines Google-Kontos bzw. eines Google-Profils) und andererseits infolge der Nutzung der Google Dienste. Dabei wird erfasst welche Dienste genutzt werden, als auch die Art und Weise wie diese genutzt werden. Diese Sammlung beinhaltet:

- *Gerätebezogene Informationen*

  verwendetes Hardware-Modell, die Version des Betriebssystems, eindeutige Gerätekennungen, Informationen über mobile Netzwerke, einschließlich der Telefonnummer

- *Protokolldaten*

  - Einzelheiten bezüglich der Art und Weise, wie die Dienste genutzt wurden (z.B. Suchanfragen)
  - Telefonieprotokollinformationen wie Telefonnummer, Anrufernummer, Weiterleitungsnummern, Datum und Uhrzeit von Anrufen, Dauer von Anrufen, SMS-Routing-Informationen und Art der Anrufe
  - IP-Adresse
  - Geräteereignissen wie Abstürze, Systemaktivität, Hardware-Einstellungen, Browser-Typ, Browser-Sprache, Datum und Uhrzeit der Anfrage und Referral-URL
  - Cookies, über die ein Browser oder ein Google-Konto eindeutig identifiziert werden können

- *Standortbezogene Informationen*

  Erfassung des tatsächlichen Standorts, über die von einem Mobilfunkgerät gesendeten GPS-Signale. Darüber hinaus werden zur Standortbestimmung verschiedene Technologien verwendet, beispielsweise die Sensordaten eines Geräts,

welche Informationen über nahegelegene WLAN-Zugänge oder Sendemasten enthalten

- *Eindeutige Applikationsnummern*

  Bestimmte Dienste weisen eine eindeutige Anwendungsnummer auf. Diese Nummer und installationsspezifische Daten, wie die Art des Betriebssystems oder Anwendungsnummer der Version, werden bei der Installation oder Deinstallation an Google gesendet, ebenso wenn der Dienst aufgrund automatischer Updates Kontakt mit Googles Servern herstellt

- *Lokale Speicherung*

  Lokale Erhebung und Speicherung von Informationen (einschließlich personenbezogener Daten) auf dem Nutzungsgerät via Mechanismen wie dem Webspeicher des Browsers (einschließlich HTML 5) und Applikationsdaten-Caches

- *Cookies und anonyme Kennungen*

  Mithilfe verschiedener Technologien werden Informationen erhoben und gespeichert, sobald ein Aufruf eines Google Dienstes erfolgt, wobei ein oder mehrere Cookies bzw. anonyme Kennungen an das Nutzungsgerät versendet werden. Diese werden auch versendet, sobald eine Interaktion mit Diensten stattfindet, welche Google den eigenen Geschäftspartnern anbietet, zum Beispiel Werbedienste oder Google Funktionen, welche auf anderen Websites auffindbar sind.

(vgl. Google 2012)

In der Argumentation über die Nutzung jener gesammelten Daten, findet sich unter anderem auch der Ausdruck „*zum Schutz (...) unseren Nutzern*“. Inwiefern Nutzer des Dienstes Google schutzbedürftig wären, wird nicht erläutert. Darüberhinaus erfolgt in weiterer Folge eine Verknüpfung der gesamten erhobenen personenbezogenen Daten über alle Google Dienste hinweg. Aufgrund dessen, dass Google weltweit vertreten ist, erfolgt eine Verarbeitung generierter Daten nicht ausschließlich im Erhebungsland, sondern kann global in einem anderen Land verwertet werden (vgl. Google 2012).

Aufgrund dieser Erfassung durch Google entstehen Online Profile welche nicht nur das Nutzungsverhalten widerspiegeln, sonder auch tiefe Einblicke in die Persönlichkeit eines Einzelnen gewähren. Dies stellt gravierende Verstöße gegen Verbraucher- und Datenschutzrecht dar. Besonders kritisch ist der Verarbeitungsprozess gesammelter Daten, welcher weltweit in jenen Ländern, in welchen Google vertreten ist, erfolgen kann. Desweitern ermöglicht die Erhebung, Speicherung, Auswertung und Verknüpfung besagter

Daten ein zielgerichtetes Marketing, mithilfe dessen, höhere Profite für den Weltkonzerngeschlagen werden können (vgl. Faz 2012; Schaar 2007:191f).

Ein weiterer Dienst von Google ist seit Jänner 2010 „Google Street View“, dank dessen, Straßen in einer 360 Grad Ansicht im Internet zugänglich gemacht werden. In Österreich wurde 2011 dieser Dienst im Datenverarbeitungsregister eingetragen. Bei diesen digitalen Ortschaftsbesichtigungen handelt es sich um Moment- und keine Liveaufnahmen. Die Datenschutzkommission hat diesbezüglich am 21 April 2011 Empfehlungen an Google ausgesprochen, betreffend der Unkenntlichmachung der Gesichter und Autokennzeichen. Darüberhinaus steht den Betroffenen ein Widerspruchsrecht gemäß § 28 Abs. 2 DSG[32] 2000 zu, wonach mindestens 12 Wochen vor einer Veröffentlichung der Daten ein Widerspruch gegen jene Herausgabe von Gebäuden besteht (vgl. www.dsk.gv.at). Inwiefern diese Informationsbereitstellung in die Bevölkerung eingedrungen ist, ist allerdings fragwürdig.

2.2.6. Bewegungsprofile

Werden beispielsweise ortsgebundene Daten gespeichert, wie im Falle von GPS-Ortungen oder dem Einsatz sogenannter RFID-Chips, so dienen diese in weiterer Folge als Datenbasis für die Erstellung sogenannter Bewegungsprofile (vgl. Simon/ Simon 2008: 21f).

> *„(...) allein die Möglichkeit, dass Bewegungsdaten aufgezeichnet, gespeichert und ausgewertet werden können, [stellt; DZ] eine sehr schwerwiegende Veränderung im Überwachungspotential einzelner Menschen dar“ (Čas/Peissl 2000: 20).*

2.2.6.1. GPS

GPS, ein globales Positionierungssystem (global positioning system), ermöglicht über jene im Weltall die Erde umkreisenden Satellitensysteme, eine Positionierung eines, signalaussendenden Gegenstandes, beispielsweise Mobiletelefone oder Navigationsgeräte (vgl. Simon/ Simon 2008: 191). Wählt in Deutschland eine Person den dort ansässigen Notruf, so muss vom Netzbetreiber der Standort übermittelt werden. Zum Ausforschen vermisster Personen, sowie als Überwachungsmethode, bedient sich dieser Technik auch die Polizei. Allerdings stellt diese Herangehensweise im Falle einer Entführung beispielsweise ein kaum verlässliches Instrument dar, da, nur so lange das Gerät eingeschalten ist, ein Signal empfängt bzw. versendet. Die rechtliche Grundlage für den Gebrauch dieser Maßnahme in Österreich findet sich im neuen Sicherheitspolizeigesetz (SPG), welches 2007 beschlossen wurde und besagt, dass bei „*››Gefahr in Verzug‹‹*“ es

[32]Datenschutzgesetz

keiner richterlichen Anordnung mehr bedarf, gesuchte Personen zu orten. Im SPG findet sich diesbezüglich folgender Paragraf:

> *„§ 24. (1) Den Sicherheitsbehörden obliegt die Ermittlung des Aufenthaltsortes eines Menschen, nach dem gesucht wird (Personenfahndung),*
>
> *1. weil eine Anordnung zur Festnahme nach Art. 4 Abs. 1, 2 oder 4 des Bundesverfassungsgesetzes über den Schutz der persönlichen Freiheit, BGBl. Nr. 684/1988, besteht;*
>
> *2. befürchtet wird, ein Abgängiger habe Selbstmord begangen oder sei Opfer einer Gewalttat oder eines Unfalles geworden;*
>
> *3. der Mensch auf Grund einer psychischen Behinderung hilflos ist oder Leben oder Gesundheit anderer ernstlich und erheblich gefährdet;*
>
> *4. ein Ersuchen gemäß § 146b ABGB vorliegt, an der Ermittlung des Aufenthaltes eines Minderjährigen mitzuwirken.*
>
> *(2) Den Sicherheitsbehörden obliegt das Aufsuchen von Gegenständen, die einem Menschen durch einen gefährlichen Angriff gegen das Vermögen entzogen worden sind oder die für die Klärung eines gefährlichen Angriffes (§ 22 Abs. 3) benötigt werden (Sachenfahndung).“ (www.internet4jurists.at)*

Die Telekommunikationsanbieter sind verpflichtet der Polizei die Identität, Anschrift, Standort und Verbindungsdaten des Gesuchten unverzüglich mitzuteilen. In Deutschland darf aufgrund richterlicher Anordnung und bei Verdacht des Begehens eines schweren Verbrechens das digitale Kommunikationsverhalten des/der Verdächtigten ohne sein/ihr Wissen überwacht und aufgezeichnet werden (vgl. Simon/ Simon 2008: 20, Schaar 2007: 57ff).

2.2.6.2. RFID-Chips

RFID Chips, Kurzform für Radio-Frequenz-Identifikation[33] Chips, sind digitale Funketiketten mit einer weltweit unikalen, nicht löschbare Nummer, dem Electronic Product Code (EPC), versehen mit einem 96-Bit-Schlüssel.Diese Transponder können auf Gegenstände geklebt oder in Produkte eingesetzt werden. In jedem Transponder findet sich ein Mikroprozessor. Das Prinzip eines RFID Chips funktioniert aufgrund elektromagnetischer Wellen, welche ein Lesegerät aussendet. Durch den dadurch erzeugten Strom in der Antenne des Transponders, reagiert der Mikrochip und sendet so Identifikationsnummer und je nach Prinzip weitere Daten zurück. Unter anderem sind die neuen Reisepässe[34] mit RFID Chips ausgestattet. Derartige Chips könnten sich in naher Zukunft in fast allen Produkten

[33] Identifizierung mithilfe von elektromagnetischen Wellen

[34] „Die als Maßnahme gegen Terroristen eingeführten Reisepässe mit biometrischen Daten sind unsicherer als gedacht. Ein Sicherheitsexperte konnte die RFID-Chips, auf denen Passbild und künftig auch Fingerabdrücke gespeichert sind, problemlos klonen.“ (www.spiegel.de)

wiederfinden, wie im untenstehenden Beispiel, in Bekleidungen (vgl. Simon/Simon 2008: 85-94, Schaar 2007: 50-56).

> *„Johannes K. kauft ab und zu im Omni-Center ein, besitzt aber keine Kundenkarte. Als er sich dem Verkaufsschalter der Herrenabteilung nähert, registriert das System, dass ein Unterhemd in den Empfangsbereich geraten ist, das vor 18 Monaten hier gekauft worden ist und in drei weitere Einkäufe involviert war. Die Verkäuferin liest diskret von ihrem Display ab, dass dieser Kunde eine Vorliebe für Billigsocken und preisreduzierte Jacketts besitzt, und lässt ihn vorerst allein herumirren, während sie mit ihrem charmantesten Lächeln Herrn Müller-Lüdenscheid namentlich begrüßt, den das System aufgrund seiner Kundenkarte und der vergangenen Umsätze als finanzstarken Premiumkunden ankündigt.*“ (Simon/Simon 2008: 92)

2.2.7. Biometrische Daten

> *„Unter biometrischen Verfahren sind alle technischen Methoden zu verstehen, die geeignet sein können, aufgrund biologischer Merkmale Personen zu identifizieren oder die Identifikation erheblich zu erleichtern (Biometrie). Insbesondere sind Fingerabdrucke, DNA-Spuren, Iris-Muster, sonstige Gesichtsmerkmale, Zusammensetzung der Stimme darunter zu verstehen.“* (ARGE DATEN 2002)

Seit Erfindung der Fotographie stehen biometrische Verfahren im Einsatz. Sie dienen dem Zwecke der Personenerkennung (vgl. Schaar 2007: 81).Constanze Kurz (2008: 101f) spricht in diesem Zusammenhang von „*››Sicherheitstechnologien‹‹*“. Biometrische Verfahren sollen zur Bekämpfung des internationalen Terrorismus eingesetzt werden. Doch auch hier ist Vorsicht geboten, denn eine vollkommene Sicherheit kann nicht garantiert werden. Das technische Prinzip der biometrischen Verfahren vergleicht momentan aufgenommene Daten mit bereits hinterlegten Informationen, sogenannten Referenzdaten. Im Falle einer Gesichtserkennung wird beispielsweise eine digitale Aufnahme mit einem gespeicherten Passfoto verglichen. Dabei handelt es sich um eine Feststellung von Ähnlichkeiten und Übereinstimmungen, welche aufgrund von Messfehlern, sowie körperlichen Veränderung, variieren und so die Leistung dieser Methode beeinträchtigen können (vgl. Schaar 2007: 76-77). Ein wesentlicher Kritikpunkt an der Verwendung biometrischer Verfahren liegt in der automationsgestützten Auswertung der Daten, welche zusätzliche Überwachungsmöglichkeiten bieten. So können beispielsweise jene Verfahren in Kombination mit videoüberwachungstechnischem Material zur Personenidentifikation dienen. Des Weiteren können biometrische Daten höchst sensible Informationen enthalten, wie den

Gesundheitszustand, Verhaltensgewohnheiten, die Stimmungslage oder weitere psychologische Faktoren, welche sich aufgrund der Beschaffenheit der Iris, der Stimmlage oder den Bewegungen schlussfolgern lassen. Besonders problematisch wird es, wenn diese Daten in „*automatisch erschließbaren Datenbanksystemen gespeichert werden*“ (vgl. Schaar 2007: 80-82). Im Falle des biometrischen Reisepasses werden über die Grenzen hinaus über den darin enthaltenen Chip die drauf gespeicherten Daten von ausländischen Behörden gelesen. So gesehen können außerhalb des Schengen-Raumen biometrische Datenbanken angelegt werden, wo auch hier wieder eine Verknüpfung mit Fahndungsdatenbanken erfolgen kann. Darüberhinaus unterscheiden sich die datenschutzrechtlichen Bedingungen, zum Schutz vor missbräuchlichem Gebrauch und Zweckentfremdungen, von Land zu Land, so dass Reisende die Kontrolle über ihre biometrischen Daten verlieren. In Bezug auf die Unverwechselbarkeit der biometrischen Daten existiert nur ein Merkmal zur eindeutigen Identifizierung einer Person, nämlich deren DNA. Es ist gut denkbar, dass dies eine Zukunftsperspektive in den modernen Überwachungstechnologien darstellt, wohlgemerkt dass in der DNA das Erbgut eines jeden einzelnen Menschen gespeichert ist (vgl. Kurz 2008: 108ff). Die Geburt eines „›‹*gläsernen*›‹“[35] Menschen wäre somit vorprogrammiert.

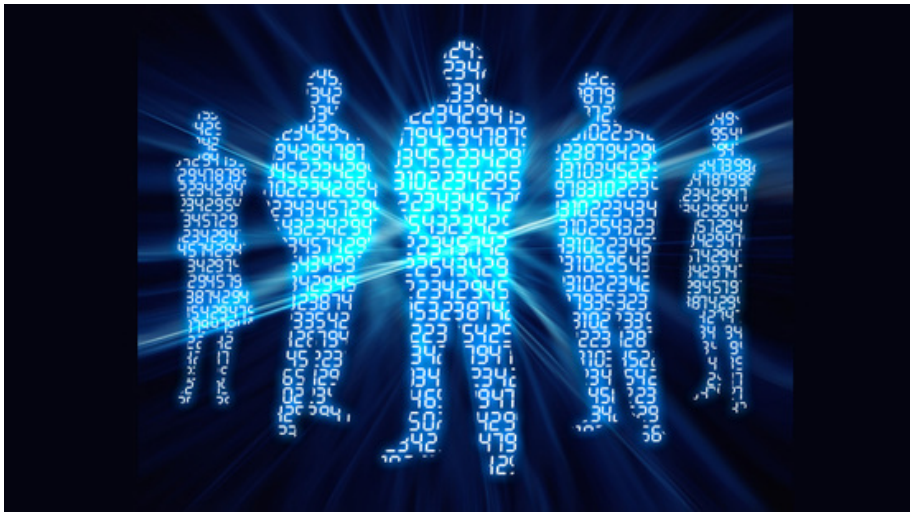


Abbildung 3[36] Durchleuchtete Zukunftsperspektiven

2.2.8. Kundenkarten

Kundenkarten stellen nur bedingt eine kundenorientierte und dienstleistungsfreundliche Maßnahme für Konsumenten dar. Denn für Unternehmen eröffnen sich dadurch neue Vermarktungschancen, da personenbezogene Daten von äußerst ökonomischer Relevanz sind. Als Gegenleistung für die Preisgabe dieser sensiblen Daten erhält man als Kunde, als

[35] Vgl. Albrecht 2008: 133; Schulzki-Haddouti 2007: 25; Schaar 2007: 205.
[36] Quelle: Futurezone

Kundin, beispielsweise Preisnachlässe, ausgewählte limitierte Sortimentsprodukte oder die Teilhabe an Gewinnspielen. Doch die Informationsgesellschaft[37] kennzeichnet sich durch eine neue Form der Entfremdung. Dank der erhobenen Daten durch Kundenkarten werden jedoch nicht selten sogenannte Kundenprofile erstellt, welche sich nach und nach der eigenen Kontrolle der BürgerInnen entziehen (vgl. Schaar 2007:188; Simon/ Simon 2008: 266ff).

> *„Jedes Mal, wenn Sie fortan Ihre Kundenkarte in einer Filiale vorweisen oder mit Ihrer registrierten Geld- oder Kreditkarte zahlen, wird gespeichert, wann, wo und was Sie gekauft haben."* (Simon/ Simon 2008: 266)

Diese Kundenprofile können dazu führen, dass wahre Persönlichkeiten verdunkelt werden. Zu einem Ausschlussmechanismus kommt es oft bei vielen Banken und Versicherungen, die anhand der erhobenen Daten eine Einschätzung nach dem Prinzip des Risikomanagements, basierend auf schubladenartigen Kategorisierungen durchführen und Menschen als geringes oder hohes Risiko einstufen und so unter Umständen Leistungen verweigern (vgl. Simon/ Simon 2008: 261; Schaar 2007: 195ff;Ericson/ Haggerty 1997, zit. nach Ball/ Wood 2006: 6). Kundenprofile erleichtern darüberhinaus immens das Betreiben eines gezielten Marketings. Individuen sind auf diese Art und Weise leichter kontrollierbarer und berechenbarer. Man kennt die Gewohnheiten, Wünsche und Nöte einzelner Konsumenten und kann diese so für kommerzielle Zwecke nutzen (vgl. Schaar 2007: 188; Simon/ Simon 2008: 267). Kundenkarten führen letztendlich nicht nur zu einer Sturmflut zielgruppenspezifischer Werbung im Postkasten oder als Spam im E-Mailordner (vgl. Schaar 2007: 189f), sondern können darüber hinaus auch schlimmere Folgen in sich bergen. Im Sinne einer effizienteren Strafverfolgung gebrauchen Behörden die Konsumentendaten von Supermarktketten, Kreditkartenfirmen, sowie privater Unternehmen zur Ausforschung und Beobachtung Verdächtiger. So wurde im Jahre 2004 der Feuerwehrmann Philip Scott Lyon aus Tukwila (Washington) verhaftet, wegen versuchter Brandstiftung am eigenen Haus. Er war auch Besitzer einer Kundenkarte der Supermarktkette Safeway. Von dieser hatte die Polizei erfahren, dass kurz vor der Brandstiftung Lyon genau dieselbe Art von Zündmaterial gekauft hatte, wie sie der Täter verwendete hatte. Erst als sich der wahre Täter von selbst stellte, wurde der Feuerwehrmann freigesprochen (vgl. Simon/Simon 2008: 244).

[37] Vgl. Schaar 2007: 230

3. Theoretische Ansätze zur Überwachung

Die Herrschenden müssen bewacht werden,
nicht die Beherrschten.
(Friedrich Dürrenmatt[38])

Das Phänomen der Überwachung dehnt sich immer weiter auf gesellschaftliche und wirtschaftliche Lebensbereiche der BürgerInnen aus, indem technische Innovationen weiterführende Ressourcen zur Observation leisten. Als Rechenschaft staatlicher Überwachung fungiert heutzutage immer und überall das „*höhere Ganze*". Anhand von Bedrohungen und Ängsten wird eine Legalität universaler Überwachung geschaffen, mit welcher, Sorgen unterbunden werden sollen (vgl. Coy 2008: 50ff; Gaycken/ Kurz: 2008: 13; Zurawski 2007: 8). Demzufolge kann daraus geschlossen werden, dass Überwachung der Abwehr von Gefahren und dem Schutze der BürgerInnen dienlich sein soll, indem diese, Straftaten aufklärt, verfolgt und im besten Falle gar im Voraus verhindert, mit dem Grundgedanken der Herstellung eines Sicherheitszustandes, welcher aufgrund von Bedrohungen nicht gewährleistet werden kann (vgl. Töpfer 2007: 34). *„Sicherheit hat Vorfahrt" (vgl. Puschke 2006, zit. nach Singelnstein/ Stolle 2007: 47),* das sind jene drei Worte, welche in den Beitrag „Von der sozialen Integration zur Sicherheit durch Kontrolle und Ausschluss", von Tobias Singelnstein und Peter Stolle (2007: 47-66), einleiten. Diese beschreiben Überwachungsinstrumente als Kontrollmaßnahmen für die Herstellung von Sicherheit, nicht nur durch Ahndung divergenter Verhaltensweisen, sondern auch durch Herstellung sozialer Ordnung (vgl. Legnaro 1997: 272, zit. nach Singelnstein/ Stolle 2007: 49). Dr. Hans Zeger, Lektor am Juridicum Wien, Mitglied des Datenschutzrates im Bundeskanzleramt und Geschäftsführer der e-commerce monitoring GmbH, sieht die Ursachen der Überwachung und Kontrolle in der Befriedigung der inneren Bedürfnisse nach Orientierung und Sicherheit (vgl. Vidc). Doch was ist Sicherheit? Ullrich (2005) beschreibt Sicherheit „*als Schutz vor (und Bewältigung von) sozialen Risiken*" (ebd.: 64). Eine anklingende Auslegung findet sich bei Schneier (2006: 11) - „*Security is about preventing adverse consequences from the intentional and unwarrented actions of others.*" Murck (1980: 38) verweist auf die Gegebenheit, dass unerfüllte Sicherheitsbedürfnisse Angst bedingen. Eine unzufrieden stellende, öffentliche Sicherheit erhöhe demnach die Angst, beispielsweise als Opfer einer kriminellen Tat zu verfallen.

[38] www.sevillana.de

Menschen assoziieren Überwachung mit Sicherheit und Schutz, weil sie von der Annahme ausgehen, dass wenn jemand über sie wacht, dieser sie auch beschützt (vgl. Lyon 2001: 3).

> *„The same process, surveillance – watching over – both enables and constrains, involves care and control."* (Lyon 2001: 3)

Wir kennen dieses Gefühl aus der Kindheit, in welcher Eltern über ihre Kinder zum Zweck ihres Schutzes und der Bewahrung vor Dummheiten, wachen. Man könne meinen, der Staat übernähme in späterer Folge diese Funktion– eine Funktion („elterlicher") Fürsorge. So entwickeln sich neuzeitliche Überwachungstechniken nach und nach zu einem Indikator für Sicherheit. Diese Assoziation kann gewissermaßen zu einem Akzeptanzgefühl jener, observationsähnlicher Techniken innerhalb der Bevölkerung beitragen (vgl. Töpfer 2007: 34f). Auch Lyon (2001: 53) sieht in der Sicherheit die Apologie seitens der Bevölkerung. Somit ist „"*Sicherheit" zu einem Lieblingswort der politischen Debatte geworden. Jede zweite Maßnahme wird mit dem Hinweis auf unsere "Sicherheit" begründet.*" (Trojanow/Zeh 2009: 45). Allerdings bedeutet es zu leben, ebenso Risiken einzugehen. Vollkommene Sicherheit hat es nie gegeben und wird es auch nie geben (können) (vgl. Luhmann 2003: 28). Auch Elisabeth Blum (2003) nimmt sich der Thematik Überwachung und Sicherheit in ihrem Band „Schöne neue Stadt. Wie der Sicherheitswahn die urbane Welt diszipliniert", an. Durch ununterbrochene „*Beschwörung*" von Gefährdungen wird ein Schein geschaffen, wonach Maßnahmen eine Sicherheit schaffen, welche sie eigentlich zerstören. Darüberhinaus, wie kann Überwachung „*im Interesse der Öffentlichkeit*" stehen, wenn das, *„was einmal Öffentlichkeit meinte, durch all diese Maßnahmen beschädigt (...) wird"* (vgl. Blum 2003: 47)?

Neben der Funktion des Schutzes und der Sicherheit, soll des Weiteren durch Überwachung gesellschaftliche und wirtschaftliche Ordnung geschaffen, erhalten und zugleich gesteuert werden (vgl. Lyon 2001: 4, zit. nach Zurawski 2007: 9). Demgegenüber steht die Kontrolle und die Voraussetzung ihrer Existenz (vgl. Zurawski 2007: 9). Soziale Kontrolle bezeichnet soziale Beziehungen zwischen Menschen, mit dem Ziel der Achtung der gegenseitigen Erfüllung bestehender Normen (vgl. Malinowski/ Münch 1975: 78, 87ff, zit. nach Grohall 2006: 171f). Grundlage sozialer Kontrolle sind, durch geltende Normen bedingte Verhaltenserwartungen (vgl. Grohall 2006: 171). Die Kontrolle erfolgt dann durch die unterschiedlichen MachtinhaberInnen, welche wiederum verschiedene institutionelle Ziele verfolgen, welche plausibel genug verkauft werden (vgl. Zurawski 2007: 9). Institutionen beispielsweise versuchen mit dem Glauben, je mehr sie wissen, die Risiken durch Informationszufluss zu minimieren. Der Gedanke dahinter ist ein strategischer, wonach mittels Kontrolle Herrschaft hergestellt wird. Durch Kontrolle wird ein gegenwärtiger

Istzustand mit einem zu erwartenden Sollzustand verglichen, um gegebenenfalls bei abweichenden Differenzen notwendige Maßnahmen einzuleiten, welche letztendlich zum angestrebten Ziel führen (vgl. Coy 2008: 47). Doch Becker (2010: 133) argumentiert, dass jene, welche überwachen, demonstrativ ihre Schwächen zeigen, in Verfolgung des Zieles der eigentlichen Manifestation ihrer überlegenen Stärke.

> *„Gerade weil die Überwacher selbst nicht daran glauben, dass ihre Regeln befolgt werden, greifen sie zur Dauerkontrolle.*" (Becker 2010: 133)

Das Prinzip der Dauerüberwachung findet sich auch bei Foucault, wonach bei ihm die Internalisierung von Normen anhand von Disziplinierung erreicht wird. Zur sicheren Erreichung soll das Panopticon[39] beitragen, ein Idealtypus eines Gefängnisses, wonach um einen zentralen Punkt in der Mitte herum, in dem sich ein Wächter befindet, rundherum die Insassen sich in Zellen aufhalten, welche zu jeder Zeit und Gegebenheit vom Wächter beobachtet werden können, ohne dass diese dies jemals wahrnehmen (können). Das damit provozierte Ziel, ist die Sicherstellung eines automatischen Funktionierens der Macht, indem bei den Gefangenen ein Zustand ständiger Transparenz geschaffen wird (vgl. Foucault 1994: 256-259).

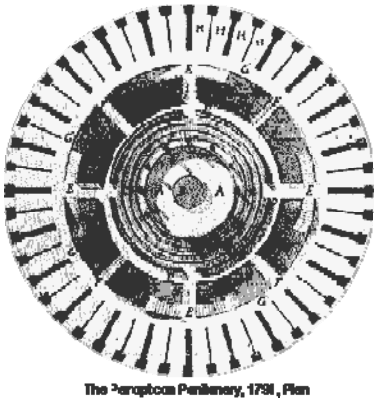


Abbildung 4 Panopticon[40]

> *„Diese Anlage ist deswegen so bedeutend, weil sie die Macht automatisiert und entindividualisiert." (Foucault 1994: 259)*

Francis Bacon[41] beispielsweise betont, dass Wissen Macht sei. Warum? Durch Überwachung entstehen Informationen. Wissen besteht aus Informationen. Wer folglich über dieses Wissen verfügt, besitzt Macht. Müsse dann zunehmende Überwachung demnach nicht zur Verunsicherung, anstatt zu einem erhöhten Sicherheitsgefühl führen? Becker

[39] Kommt aus dem Griechischen: „pan" = alles und „optikós" = optisch. Von Jeremy Bentham entwickelt.
[40] Quelle: Possest
[41] Englischer Philosoph 1561–1626

(2010: 112) hingegen betont, dass jener weltberühmte Satz Bacons nur bei der Anwendung auf das Verhältnis von Mensch und Natur einen Sinn ergäbe. Sobald dieser bei den Machtverhältnissen zwischen den einzelnen Individuen gebraucht wird, verliere dieser seine Substanz. In diesem Falle müsse er umformuliert werden in:*„Das Nicht-Wissen des einen, ist die Macht des anderen“* (Becker 2010: 112). Sprich, das Unwissen der Überwachten ist Voraussetzung für das Funktionieren einer Überwachung mittels Überwachende (vgl. Becker 2010: 112f). Dies spiegelt sich auch in „*Security through obscurity*“ („*Sicherheit durch Unklarheit)*“ wieder, indem die Öffentlichkeit über das tatsächliche Ausmaß der Leistungsfähigkeit der Überwachungstechniken im Unklaren gelassen wird, erhöhe diese Vorgehensweise einerseits die präventiven, als auch andererseits die repressiven Wirkungen überwachungstechnischer Maßnahmen (vgl. Becker 2010: 112). Demzufolge kann ein Durchschnittsbürger/ eine Durchschnittsbürgerin nur wage erahnen, welche Systeme zur Beobachtung im Hintergrund laufen und das soziale Verhalten aufzeichnen, speichern und verwerten. An dieser Stelle betont Zurawski (2007: 8), dass sich die „*Überwachungspraktiken*“ immer mehr zu „*Überprüfungs- und Steuerungsinstrumenten*“ gewandelt haben. Doch,

> *„Überwachung verfolgt nicht immer Ordnung durch Zwang, sondern ermöglicht durchaus auch die Schaffung von Möglichkeiten demokratischer Teilhabe und Kontrolle – und beinhaltet somit beides: Fürsorge und Kontrolle, welche beide oft widerstrebende Aspekte von Überwachung sind.“* (Zurawski 2007: 10)

Peter Schaar (2007: 50) spricht in diesem Zusammenhang von einem Kontrollverlust der einzelnen BürgerInnen. Indem immer mehr personenbezogene Daten erhoben, gespeichert, übermittelt und ausgewertet werden, entziehen sich diese der Kontrolle des Bürgers, der Bürgerin. Diese verlieren in weiterer Folge ihre „*Verfügungsmacht*“ über die eigenen persönlichen Daten und bedrohen somit ihr Recht auf informationelle Selbstbestimmung. Doch Umfragen belegen, dass die Mehrheit der Befragten sich bereit erklären, Einschränkungen der Freiheit im Gegenzug für ein höheres Maß an Sicherheit in Kauf zunehmen (vgl. ebd.: 127). Darüberhinaus werden sinnlich nicht wahrnehmbare Gefahren, sowie unsichtbare Überwachung von Menschen verharmlost (vgl. Simon/ Simon 2008: 105).

Auch Prävention ist eine oft gebrauchte Rechtfertigung für den Einsatz und Nutzen der Überwachungstechnologien (vgl. Purgathofer 2008: 196). An die Stelle des Vertrauens tritt eine neue Form der Kontrolle, die des präventiven Charakters, wonach jedes Individuum als eine potenzielle Gefahrenquelle angesehen wird (vgl. Singelnstein/ Stolle 2007: 51). Diese dienen der Gefahrenabwehr mittels Prävention und Verfolgung von Gesetzeswidrigkeiten im polizeirechtlichen, sowie im geheimdienstlichen Rahmen (vgl. Albrecht 2008: 129). Im Falle

der Videoüberwachung lässt sich feststellen, dass jene zwar im Anschluss an eine erfolgte Straftat zur deren Aufklärung beitragen können, diese jedoch nicht im Vorhinein vereiteln. Der Urglaube, umfassende Überwachung sei mit einem Gewinn an Sicherheit gleichzusetzen, widerstrebt Peter Schaar, Bundesbeauftragten für den Datenschutz, äußerst. Für ihn ist jene durch Videoüberwachung suggerierte Sicherheit, nichts als ein leeres Versprechen. Er bezweifelt beträchtlich, dass es einen signifikanten Zusammenhang zwischen Videokameras und einem erhöhtem Maß an Sicherheit gäbe, denn letztendlich sprechen gegen diese These auch die Kriminalstatistiken. Etliche Studien belegen, dass die erwartete Wirksamkeit von Videoüberwachungen zur Prävention[42] karg ausfällt (Hempel/ Metelmann 2005, zit. nach Schaar 2007: 61). Spürbare Veränderungen der Kriminalstatistiken bleiben aus. Alternative Ansätze werden genauso wenig auf ihre Effektivität geprüft, wie der Erfolg jener Techniken der optischen Überwachung (vgl. Schaar 2007: 59-63).

> *„So kann die Sicherheit in einer dunklen Eisenbahnunterführung möglicherweise durch eine verbesserte Beleuchtung weitaus stärker erhöht werde als durch die Installation einer Videokamera."* (Schaar 207: 60f)

Der präventive Charakter einer Überwachung entfällt ebenfalls, „*wenn der Täter ihre Existenz (...) kennt (...)."* (Bremische Bürgerschaft 2005: 6, zit. nach Hempel 2007: 126). Dazu zählen beispielsweise sichtbar angebrachte Videokameras, jenes allseits bekannte Funktionieren des GPS Aspekts in Mobiltelefonen, sowie Navigationsgeräten, die Datenvorratsspeicherung, die Online-Überwachung, um nur einige Beispiele zu nennen. Im besten Fall können diese retrospektiv zum Einsatz kommen, eine präventive Leistung kann nicht garantiert werden. Möglicherweise wäre eine präventive Schutz- und Sicherheitsfunktion in einem Rundumdauereinsatz der Überwachung aller sämtlicher Lebensbereiche der BürgerInnen mutmaßlicher. Der Preis dafür wäre allerdings unbezahlbar. Fernerhin tendieren Individuen durch Überwachung zu angepasstem Verhalten. So sind beispielsweise die Instrumentarien der Videoüberwachung nicht im Stande zwischen verdächtigen und unverdächtigen Personen zu unterscheiden, wodurch alle Personen mit ihren individuellen Verhaltensweisen aufgezeichnet werden. Das Gefühl der permanenten Beobachtung führt statt der angestrebten Sicherheit, widerwillig zur Verunsicherung (vgl. Schaar 2007: 62).Sandro Gaycken, Wissenschafts- und Technikphilosoph, ist der Auffassung, dass Überwachung eine Gesellschaft verändere und ad hoc Autonomie, Freiheit und Individualität einfordere. Psychologen zeigten, dass sich Menschen, welche sich beobachtet fühlen, anders verhalten und handeln, als wenn dies

[42] „Lediglich in bestimmten besonders gefährdeten und unübersichtlichen Bereichen, etwa in Parkhäusern, lässt sich mittels Videotechnik ein signifikanter Sicherheitsgewinn erzielen." (Schaar 2007: 61; vgl. Gill/Spriggs 2005, zit. nach Töpfer 2007: 36)

nicht der Fall ist. Forscher der Universität Newcastle konnten dieses Phänomen nachweisen. (vgl. Biermann 2009: 1).

> *"Allein das Foto eines Augenpaares über der freiwilligen Kaffeekasse sorgt dafür, dass fast dreimal mehr Geld in der Kasse ist, als wenn ein Blumenposter die Wand schmückt"* (Biermann 2009:1)

Von einem Trugbild der Sicherheit sprechen auch Singelnstein und Stolle (2007: 57), wenn sie darauf verweisen, dass durch keine Sicherheitsvorkehrungen der Welt alle Risiken eleminierbar seien. Zum Einen steigt das Bedürfnis nach Sicherheit stetig, zum Anderen steigt auch das „*Unsicherheit- und Bedrohungsgefühl*". Paradoxerweise produziert eben jenes unersättliche Streben nach Sicherheit jene Verunsicherung, welche es dadurch zu beseitigen gäbe, indem permanent eine nicht erreichbare Sicherheit aufgezeigt wird. Nicht Sicherheit, sondern vielmehr Unsicherheit bildet die grundlegende Voraussetzung der Freiheit. Dadurch, dass Unsicherheit der Freiheit Schranken aufweist, ermöglicht sie diese erst (vgl. Castel 2005: 9ff; Lemke 1997: 187f, zit. nach Singelnstein/ Stolle 2007: 57).

4. Privatsphäre

Freiheit stirbt mit Sicherheit.
(Kurt Tucholsky[43])

Wir leben heutzutage in einer Gesellschaft, in der man sich kaum noch vor den Eingriffen in die Privatsphäre, welche jederzeit und jederorts erfolgen können, bedingt durch technologische Entwicklungen, ökonomische Interessen und staatliche Kontrollen, welche oft auch ohne unser Wissen erfolgen können, schützen kann. Darüberhinaus wächst die Bereitwilligkeit vieler Individuen die „*eigene Privatsphäre nicht mehr ernst zu nehmen*" (vgl. Schaar 2007: 11).

> *„Privatsphäre ist Raum des individuellen Rückzugs und zugleich unverzichtbare Voraussetzung einer freien Meinungsbildung."* (Schaar 2007: 15)

Ihr Gegenstück ist die Öffentlichkeit. Beide entstammen aus der bürgerlichen Gesellschaft (vgl. Schaar 2007: 16). Aus psychologischer Sicht bedeutet Privatsphäre die

> *„ (...) selektive Kontrolle des Zugangs zum Selbst."* (Reinecke 2009: 4)

Wie viel wir von uns preisgeben hängt in erster Linie damit zusammen mit welcher Person bzw. welchen Personen wir gerade verkehren, und/oder in welcher Situation wir uns zurzeit befinden. Es ist somit vom Kontext, von den Rahmenbedingungen, sowie vom Gemütszustand abhängig, wie viel ich will, dass mein Gegenüber über mich weiß (vgl. Heesen 2008:231).Das Wort „privat" kann in unterschiedlichen Kontexten genutzt werden:

> *„Privat ist, mit wem ich zusammenlebe und was ich über meine Kollegen denke. Privat ist mein Tagebuch ebenso wie ein Teil meiner Korrespondenz; meine Privatsache ist, welche Kleidung ich trage, in welche Kirche ich gehe und welchen Beruf ich wähle; privat ist außerdem mein Heim und Herd, privat ist also auch meine Wohnung; privat ist schließlich ebenso die Frage, auf welche Schule ich mein Kind schicke; und wenn ich mit einem Freund im Café sitze, dann ist das zwar ein öffentlicher Ort, aber eine private Angelegenheit."* (Rössler 2001: 10)

Bereits im Staatsgrundgesetz von 1867 findet sich der Verweis auf den Schutz der Privatsphäre (vgl.www.parlament.gv.at). Artikel 12 der Allgemeinen Erklärung der Menschenrechteder UNO-Resolution 217 A (III) vom 10. Dezember 1948 besagt,

[43]www.sevillana.de

> *„Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jede Person hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen*." (vgl. www.un.org)

In der europäischen Menschenrechtskonvention findet sich bei Artikel 8 das Recht auf Achtung des Privat- und Familienlebens, welches am 01.11.1998 in Kraft getreten ist.

> *„(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.*
>
> *(2) Der Eingriff einer öffentlichen Behörde in die Ausübung dieses Rechts ist nur statthaft, insoweit dieser Eingriff gesetzlich vorgesehen ist und eine Maßnahme darstellt, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist."* (vgl. RIS)

Darüberhinaus wird in Österreich die Privatsphäre durch das Datenschutzgesetz (DSG) und durch das Telekommunikationsgesetz (TKG) geregelt und geschützt (vgl. Sterbik-Lamina et al.2009: 19f).

Speziell im Zeitalter der Informationsgesellschaft, wie sie heute besteht, durchdringen innovative technologische Entwicklungen nach und nach das wirtschaftliche und gesellschaftliche Leben und veranlassen so eine wachsende Beeinträchtigung der Privatsphäre durch vermehrte Datenagglomeration (vgl. Ĉas/ Peissl 2000: I).

> *„Ganz allgemein lässt sich eine Dynamisierung feststellen: nicht mehr nur statische Daten in Datensammlungen bilden die Grundlage für eine Bedrohung der Privatsphäre, vielmehr entstehen bei der Nutzung neuer Medien neue, sich bei jeder Mediennutzung verändernde Daten wie Kommunikations- und Inhaltsdaten, die eine umfassende Überwachung bzw. Verhaltensanalyse ermöglichen"* (Čas/Peissl 2000: 4).

Daten werden fast jederorts und jederzeit erhoben, gespeichert, analysiert und so beispielsweise als Verhaltensanalysen genutzt (vgl. Ĉas/ Peissl 2000: I).

Es ist schlichtweg unmöglich die Augen vor den neuen Informationstechnologien zu verschließen und das politische, wirtschaftliche, sowie soziale und kulturelle Umfeld neu zu gestalten. All jene, welche sich dennoch diesem System entziehen, droht der Ausschluss (vgl. Singelnstein/ Stolle 2007: 51).

4.1. Was wird gespeichert?

In der folgenden Tabelle von Čas und Peissl (2000: 15ff) wurde eine Kategorisierung der Daten vorgenommen, die zeigt, welche Einrichtungen welche Art von Daten speichern. Da es unmöglich ist, eine(n) DurchschnittswienerIn zu kreieren, belaufen sich diese Daten auf realistischen Annahmen, welche auf Internetrecherchen und geführten Experteninterviews von Čas und Peissl aufbauen. Ein „X“ bedeutet, dass Daten mit einer sehr hohen Wahrscheinlichkeit gespeichert werden. Ein „O“ bedeutet, dass Daten möglicherweise gespeichert werden, d.h. man kann annehmen, dass die Einrichtungen, auch wenn es nicht publik gemacht wird, diese Art von Daten generieren. Ein leeres Feld hingegen bedeutet nicht automatisch, dass keine Daten gespeichert werden. Die Tabelle zeigt die Speicherung von Daten auf, die offiziell gesammelt werden. Was jedoch noch darüber hinaus recherchiert und gespeichert wird, ist nicht offiziell bekannt. Die Tabelle wurde in veränderter Form übernommen, aus Platzgründen bearbeitet und teilweise aktualisiert.

Tabelle 1 Kategorisierung & Speicherung von Daten

Daten	Kommunale Verwaltung	Polizei/Gericht	Finanzbehörden	Sozialversicherungen	Gesundheitssystem	Statistik AUT (Volksz.)	Arbeitsgeber	Telekommunikation	Kirche	Private Versicherungen	Diverse Branchen, Kundenkarten
Name	X	X	X	X	X	X	X	X	X	X	X
Geschlecht	X	X	X	X	X	X	X	X	X	X	X
Titel	X	X	X	X	X	X	X	X	X	X	X
Postadresse	X	X	X	X	X	X	X	X	X	X	X
Telefonnr. (frei verfügbar)	O	O	O	O	O	O	X	X	O	O	O
Telefonnr. (geheim, Wertkartenhandy)								X			
E-Mailadresse	X	O	X				O	X		O	X
Geburtsdatum	X	X	X	X	X	X	X	X	X	X	X
Geburtsort	X	O				X	X		X	X	X
Familienstand	X	O	X	X	X	X	X		X	X	X
Staatangehörigkeit	X	X	X	X	X	X	X	O	O	X	O
Beruf	X	O	X	X	O	X	X	O	O	X	O
Anzahl Kinder	X		X	X	X	X	X		X	X	O
Bildungsweg			X	X	X	X	X			O	
Konfession							O	X	X		
Daten über Familienangehörige (Name, Adresse, Beruf,..)	X		X	X	X	X	O	O	X	X	
Sozialversicherungsnummer		O	X	X	X		X			O	
Versicherungsdaten (Lebens-, Kranken-, Autoversicherung,..)			X	X	X					X	
Gesundheits-/Krankheitsdaten		O	O	X	X			O		O	
DNA-Daten		O			O						
Bankdaten			X	O			X	X	O	X	O
Einkommen			X	X			X		X	O	
Bonität			X				X	X			O
Immobilien	X		X								
Sonst. nicht monetäres Vermögen			O							X	
Private Kontakte (Zeitpunkt, Häufigkeit, Dauer, Medium, Ort)								X			O
Freizeitverhalten						X	O	O			O
Einkaufsverhalten								O			X
Benutzte Internetseiten/ persönliche Vorlieben								X			O
Politische Einstellungen und Interessen		O				X					O

(Cas/Peissl 2000: 15f [Bearbeitung& Ergänzung, Zamojska 2011])

Die Tabelle zeigt, dass öffentliche Unternehmen durchaus mehr Daten speichern als private. Eine Ausnahme stellt hier der Arbeitgeber dar, da er alleine durch den ausgefüllten Bewerbungsfragebogen eine Vielzahl an persönlichen Daten erhält. Genauso eine Ausnahme stellen auch die Telekommunikationsunternehmen dar, welche private Dinge, wie finanzielle Daten, Kontakte und Gewohnheiten speichern, wie zum Beispiel besuchte Internetseiten. Dabei spielt die Anzahl der gesammelten Daten eine nicht allzu große Rolle, als vielmehr die Daten-Analyseverfahren, wie das Customer Relationship Management (CRM), mit welchen Kundenprofile erstellt werden, um künftige Ereignisse vorherzusagen und Aussagen über das Verhalten eines Individuums zu treffen (vgl. Čas/Peissl 2000: 17, zit. nach Lechner 2000: B1)

Des Weiteren ist aus der Tabelle auch ersichtlich, dass die „Standard Grunddaten“ (Name, Geschlecht, etc. ..) von allen Einrichtungen gespeichert werden und dass die Datenspeicherung mit zunehmender Privatsphäre (sprich von oben nach unten herabgehend) abnimmt. Es ist jedoch anzunehmen, dass „*mit zunehmender Digitalisierung bzw. stärkerem Einsatz von Informations- und Kommunikationsmedien*“ sich dies in naher Zukunft ändern wird (Čas/Peissl 2000: 14ff).

5. Datenschutz

Je korrupter der Staat ist,
desto mehr Gesetze braucht er.
(Tacitus 55-116 n.Chr.[44])

> *„Jedermann hat Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten.“* (Bundeskanzleramt)

Der Datenschutz stellt ein verfassungsrechtliches Grundrecht dar und eine gesetzliche Verankerung des Datenschutzes in Österreich findet sich seit 1978. Seit 1 Jänner 2000 ist das Datenschutzgesetz 2000, BGBl. I Nr. 165/1999 (DSG 2000) in Kraft. Auf europäischer Ebene beinhalten die EG-Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG), die EG-Verordnung über den Datenschutz bei der Datenverarbeitung durch die Organe und Einrichtungen der Gemeinschaft (VO Nr. 45/2001), die Datenschutzkonvention des Europarates (ETS 108) samt Zusatzprotokoll und Bestimmungen bezüglich des Schutzes von Daten. Der Grundrechtsschutz besteht allerdings nur auf personenbezogene Daten, sowie Daten, welche nicht allgemein verfügbar sind. Des Weiteren besteht ein beschränkter Geheimhaltungsanspruch. Im Falle eines lebenswichtigen Interesses des/der Betroffenen, sowie mit seiner/ihrer Zustimmung, wie auch „*zur Wahrung überwiegender berechtigter Interessen eines anderen“*, darf eine Verwendung dieser Daten erfolgen. Staatlichen Behörden darf nur aufgrund der Sicherung eines öffentlichen Interesses ein Zugriffsrecht auf der Grundlage eines Gesetzes gewährt werden. Zu diesen öffentlichen Interessen zählen beispielsweise:

- nationale Sicherheit
- Verhinderung von strafbaren Handlungen
- Schutz der Gesundheit
- Schutz der Rechte und Freiheiten anderer

Datenschutzbrüche können einerseits vor den Zivilgerichten, sowie vor der Datenschutzkommission amtlich ausgetragen werden (vgl. Bundeskanzleramt).

Datenschutz darf allerdings nicht mit Datensicherheit verwechselt werden, was leider oft der Fall ist. Der Datenschutz hat zur Aufgabe die Gewährleistung der Privatsphäre und der individuellen Handlungsfreiheit sowie der Würde, wohingegen Datensicherheit unzulässige Zugriffe auf Daten und deren Verfälschung zu unterbinden hat. Eine weit verbreitete Meinung ist die Behinderung des Datenschutzes bei der Bekämpfung der Kriminalität. Jene mit

[44] www.sevillana.de

Abstand am Häufigsten vorgebrachten Argumentationen gegen den Datenschutz sind einerseits „*Datenschutz sei Täterschutz*“ und andererseits „*Ich habe nichts zu verbergen*“, denn wer nichts zu verbergen hätte, der brauche auch keinen Datenschutz, denn nur wer sich „wehrt“, macht auf sich aufmerksam, macht sich verdächtig, etwas zu verheimlichen, wodurch Menschen regelrecht dazu angespornt werden, sogar freiwillig Privates über sich preiszugeben und einen Überwachungsstaat zu begrüßen. Allerdings belegen Statistiken keinen Zusammenhang zwischen Datenschutz und Kriminalität. Speziell Staaten welche besonders hoch den Datenschutz schätzen, wie Kanada oder Deutschland, weisen deutlich geringere Kriminalitätsstatistiken auf, als jenen Staaten, in welchen mit Datenschutzbestimmungen legerer umgegangen wird bzw. diese kaum vorherrschen, wie Großbritannien, die USA oder Russland[45] (vgl. Schaar 2007: 21-26).

Ein Rechtsstaat unterscheidet sich gegenüber autoritären Regimen durch das Maß der Zulässigkeit des Eingriffes in bürgerliche Staatsrechte (vgl. Schaar 2007: 149). Sowohl über die Einführung als auch über die Anwendung neuer Überwachungsmaßnahmen entscheidet der Gesetzgeber, dessen Entscheidungsfreiheit durch die derzeit gültige Verfassung beschränkt wird. Dieser ist aufgefordert, unter dem Aspekt der Gefahrenabwehr, sachgerecht einen Gleichklang zwischen Freiheit und Sicherheit zu schaffen (vgl. Hornung 2008: 261f).

[45] Laut einer internationalen Hitliste der Bürgerrechtsorganisation „Privacy International“ im Jahre 2006 rücksichtlich des Datenschutzes (vgl. Schaar 2007: 26).

6. Empirische Studie über Einstellungen, Wissen und Akzeptanz von Überwachungsmaßnahmen

Die Freiheit des Menschen liegt nicht darin,
dass er tun kann, was er will,
sondern darin, dass er nicht tun muss,
was er nicht tun will.
(Jean Jacques Rousseau[46])

Im Zuge der vorliegenden Arbeit wurde eine empirische Studie zum Sachverhalt „Überwachung in Wien“ durchgeführt, mit deren Hilfe quantitativ die Einstellungen der WienerInnen bezüglich dieser Thematik erforscht wurden, mit dem Zweck der Durchleuchtung, Bewusstseinsweckung und Näherbringung der zu untersuchenden Problematik. Eingehende Beschäftigung mit diesem Thema brachte die Erkenntnis, dass in regelmäßigen Abständen durchgeführte Befragungen unumgänglich erscheinen, denn die Überwachungstechniken, -möglichkeiten und -maßnahmen stehen in einem engen Zusammenhang mit dem ständig wachsenden technischen Fortschritt und seiner Weiterentwicklung, wodurch sich diese einerseits kontinuierlich wandeln, erweitern und den Rahmen ausweiten und andererseits im Zuge zunehmender Digitalisierung menschlicher Lebensbereiche an Bedeutung und Wichtigkeit, mit steigender Tendenz, erlangen. Dies war unter anderem auch ein ausschlaggebender Punkt warum eine eigene Erhebung diesbezüglich durchgeführt wurde. Im Zentrum des Interesses stand die Frage nach den Gründen der Akzeptanz von Überwachungsmaßnahmen, obwohl diese weitgehende Eingriffe in die Privatsphäre von Individuen vornehmen. Anhand eines zweistufigen Studiendesigns sollten Antworten auf die forschungsrelevanten Fragen gesucht und gefunden werden.

Der Themenkomplex „Überwachung“ vereint interdisziplinäre Aspekte, angefangen bei den rechtlichen Rahmenbedingungen, moralisch, ethischen Grundsatzdiskussionen, technischen Möglichkeiten, politischen Befugnissen, kulturellen Traditionen bis hin zu den sozialen Erwartungshaltungen. Das Hauptaugenmerk dieser Arbeit richtet sich, gemäß einer soziologischen Befassung mit dieser Themenstellung, auf die sozialen Gesichtspunkte, jedoch unter Berücksichtigung weiterer relevanter Themen. Darüberhinaus wird das Forschungsinteresse zu weiten Teilen vom eigenen Interesse am Themengebiet begleitet.

[46] www.sevillana.de

6.1. Forschungsstand

„Surveillance raises some of the most prominent social and political questions of our age. (Haggerty/Ericson 2006: 3).

Der Zugang zu diesem Thema ist groß und interdisziplinär gegeben. Das florierende Forschungsgebiet wurde bereits von verschiedenen Forschern der Ingenieurswissenschaft, über die Jurisprudenz, Soziologie, Psychologie, bis hin zur Geografie und Anthropologie (vgl. Zurawski 2007: 7), um nur einige Beispiele hier zu nennen, versucht zu durchleuchten. Besonders im englischsprachigen Raum ist die Auswahl an literarischer Vielfalt groß.

Es gibt zwei weltbekannte Autoren, welche im Zusammenhang mit „Überwachung" immer, überall und von jedem zitiert werden. Eine Nichterwähnung dieser beiden Persönlichkeiten erscheint fast schon unmöglich. Dabei handelt es sich einerseits um den französischen Philosophen, **Michel Foucault**, welcher nicht „nur" französischer Philosoph war, sondern vielen verschiedenen Wissenschaften angetan war und dort sein Wissen kundtat, und andererseits **George Orwell**[47], britischer Schriftsteller und Journalist. Orwell schuf mit „1984" einen weltberühmten Roman, in welchem er furchteinflößende Szenarien einer zukünftigen totalitären Gesellschaftbeschreibt. Foucault brachte 1976 (deutsche Fassung) den Band „Überwachen und Strafen[48]" heraus. Foucault greift in seinem Buch, das Ende des 18ten Jahrhunderts von Jeremy Bentham entwickelte Modell des Panopticons auf, und demonstriert anhand dessen, dass eine ständige Überwachung nicht von Nöten ist, um sein gewünschtes Ziel, beispielsweise normkonformes Verhalten, zu erreichen. Er zeigt, dass allein die Tatsache, dass eine Möglichkeit zur ständigen Überwachung besteht, auch wenn diese gar nicht genutzt wird, ausreicht, um ein gewünschtes Verhalten zu erzielen. Im Falle des Panopticons wissen die Gefangenen nie wann genau sie beobachtet werden, oder auch nicht. In bestimmten Fällen werden Gefangene permanent überwacht und in anderen wiederum kein einziges Mal. Doch die Furcht dessen, dass sie es nicht wissen, welche dieser beiden Möglichkeit nun zutrifft, treibt sie dazu, nonkonformes Verhalten abzulegen, um weitere Bestrafungen zu umgehen.

Es sollen nun kurz jene Autoren mit ihren Werken vorgestellt werden, welche den Kern der Auseinandersetzung bilden. Der Soziologe **Dr. Nils Zurawski**, Vertretung der Professur für Sicherheit, soziale Konflikte und Regulation an der Universität Hamburg, am Institut für

[47] Eigentlicher Name Eric Arthur Blair.
[48] 1975 unter „*Surveiller et punir" veröffentlicht.*

Soziologie, zeigt beispielsweise in seinem 2007 erschienenen Band „Surveillance Studies“, dass Überwachung ein universelles, soziales Phänomen ist. **Kevin Haggerty**, Kriminologe und Soziologe (University of British Columbia), und **Richard Ericson**, ebenfalls Soziologe und Kriminologe (University of Toronto) befassen sich in ihrem Buch „The New Politics Of Surveillance And Visibility“ (2006) damit, wie die Gesellschaft durch Überwachungssysteme, Technologien und Praktiken organisiert ist und wie sich die Grenze zwischen Öffentlichem und Privaten allmählich verwischt. **David Lyon**, Professor für Soziologie an der Queen´s Universität, Kingston, Ontario, untersucht in „Surveillance Society: Monitoring Everyday Life“ (2001) die computergestützte Kontrolle des alltäglichen Lebens. **Matthias Becker**, studierte Anglistik, Kommunikations- und Medienwissenschaft und Geschichte. 2010 publizierte er „Datenschatten. Auf dem Weg in die Überwachungsgesellschaft?“, welches einen prägnanten Überblick über dieses fachübergreifende Thema bietet.

Ebenfalls von besonderem Interesse ist das Buch „Ausgespäht und abgespeichert“ (2008) von **Anne-Catherine Simon**, Feuilleton-Redakteurin der Österreichischen Tageszeitung „Die Presse“ und **Thomas Simon,** in dem die Autoren auf die neuen Überwachungsmethoden eingehen und ein Ende jeglicher Privatsphäre und eine totale Kontrolle prognostizieren.

Reg Whitaker, Professor für Politikwissenschaften an der York Universität in Toronto, weiß zwar gekonnt in seinem Band „Das Ende der Privatheit“ (1999) die technischen Innovationen gebührend anzuerkennen, und dennoch die damit in Zusammenhang stehenden Probleme und Gefahren zu kennzeichnen. Im Zentrum seiner Betrachtung liegt die Beziehung zwischen politischer Macht und den neuen Informationstechnologien. **Peter Schaar**, Volkswirt und Datenschutzbundesbeauftragter, rekonstruiert in seinem Band, „Das Ende der Privatsphäre“ (2007), die Entwicklung zu einer Überwachungsgesellschaft, sowie die Neigung jedes einzelne Individuum mit einer potenziellen Gefahrenzone gleichzusetzen. And last but not least, „1984.exe“, (2008) von Dr. **Sandro Gaycken**[49] Technik- und Sicherheitsforscher an der Freien Universität Berlin, und **Constanze Kurz**, Aktivistin und Sprecherin des Chaos Computer Clubs (CCC)[50], über gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Hier werden die Auswirkungen technischer Überwachung auf die Bevölkerung beschrieben und dargelegt, dass der Orwell´sche Gedanke eines Überwachungsstaates längst kein Phantasiegebilde mehr darstellt.

Anders als bei der literarischen Vielfalt, zeigt sich im empirischen Bereich ein Mangel an verwertbaren Daten. Dies war der zweite ausschlaggebende Punkt, neben der Notwendigkeit

[49] Darüber hinaus Berater verschiedener ziviler und militärischer Institutionen auf internationaler und nationaler Ebene. Des Weiteren ist Gaycken in Policy-Gremien auf Bundes- und EU-Ebene tätig. Seine Schwerpunkte sind Cyberwarfare, Cybersecurity, Sicherheit und Technik, Datenschutz, sowie gesellschaftliche und ethische Folgen der Informationstechnik.

[50] War Sachverständige bei der Anhörung vor dem Bundesverfassungsgericht zur Vorratsdatenspeicherung.

einer fortwährenden Aktualisierung bereits erhobener Daten auf diesem Gebiet, aufgrund der engen Verflechtung der Überwachung mit dem wachsenden technischen Fortschritt, warum eine eigene quantitative Erhebung durchgeführt wurde. Es lassen sich kaum Daten ausfindig machen, welchen den Bereich Überwachung im Allgemein abdecken und darüber hinaus noch aktuell sind. Beispielsweise weist die Eurobarometerseite[51] vereinzelte Datensätze auf, welche verschiedene Themenbereiche der Überwachung behandeln:

- Eurobarometerumfrage 46.1[52]

Dieser Fragebogen enthält kurz und bündig ein paar Fragen zu den Themen Datensammlung, Datenweitergabe und Datenschutz.

- Eurobarometer 60.0

Hier wurden die Teilnehmer danach gefragt, was und wie sie über den Schutz ihrer personenbezogenen Daten denken. Gefragt wurde ebenso nach dem Grad des Vertrauens in die nationalen Organisationen, was Datenschutzgesetze mit sich bringen sollten und ob sie Tools oder Technologien verwenden (würden), um persönliche Daten zu schützen. Die Probanden wurden auch gefragt, ob sie Produkte im Internet kaufen, wie oft sie dies tun, ob sie Bedenken in Bezug auf Internet-Transaktionen haben, warum sie online einkaufen und auf welchen Websites sie bestellen. Andere Fragen beschäftigen sich mit der Sicherheit von Internet-Transaktionen, einschließlich der Kenntnisse der Befragten über die Rechte der Verbraucher, Internet-Sicherheit, Gesetze über den Schutz der Internet-Käufe und bisherige Erfahrungen mit Beschwerden über Internet-Transaktionen[53].

- Eurobarometer Umfrage 67.2

Beinhaltet nur drei Variablen. Hier wurden die Befragten über ihre Kenntnisse des Datenschutzes personenbezogener Daten; des Rechts, sich vor dem Zugriff der Unternehmer auf sensible Daten zu schützen, und ob Strafverfolgungsbehörden in der Lage sein sollten, auf personenbezogene Daten für Zwecke der Kriminalitäts- und Terrorismusbekämpfungen zugreifen zu können, befragt.

[51] Seit 1973 eine öffentliche Meinungsumfrage zu verschiedenen Themen in der EU. Wird in regelmäßigen Abständen von der Europäischen Kommission in Auftrag gegeben (siehe http://ec.europa.eu/public_opinion/index_en.htm, 17.02.2012)
[52] Alle drei Eurobarometerumfragen wurden das letzte Mal am 17.02.2012 aufgerufen.
[53] Für diese hier durchgeführte Untersuchung boten die durchaus interessanten Fragen allerdings nur wenig Relevanz. Darüber hinaus ist dieser Datensatz acht Jahre alt.

Zwei weiterer Datensätze finden sich auf der Wisdom[54] Homepage unter dem Suchbegriff „Privatsphäre“. Allerdings ist der Zugang kostenpflichtig (ca. 10 Euro):

- Österreichische Tagespolitik (SWT9003)

Die Themen, mit welchen sich dieser Datensatz beschäftigt sind Sicherheit und hauptsächlich polizeiliche Angelegenheiten. Das Manko an diesem Datensatz – er ist aus dem Jahre 1990.

- Neue Ermittlungsmethoden zur Kriminalitätsbekämpfung (SW9911).

Dieser Fragebogen ist aus dem Jahre 1999. Die Zahl der Fragen wurde allerdings auch hier gering gehalten und auch hierdreht sich meistens wieder alles rund um die Polizei und deren Ermittlungsmethoden.

Da hauptsächlich alles seine guten und schlechten Seiten aufweist, so auch die Überwachung, verfolgt diese Arbeit nach bestem Wissen und Gewissen den Versuch, beide Hälften der Medaille aufzuzeigen, sowohl die positiven, als auch die negativen. Ein Staat beispielsweise wäre ohne Überwachung und ohne Kontrolle ohnedies nicht denkbar. Letztendlich bleibt eine Bewertung jedem selbst überlassen.

6.2. Forschungsfragen und Hypothesen

„Доверяй, нопроверяй[55]*.*
Vertrauen ist gut, Kontrolle ist besser.“

Eine allseits weltbekannte Redewendung eines russischen Politikers, Wladimir Iljitsch Uljanow, besser bekannt als der Gründer der Sowjetunion, unter dem Namen Lenin.

Im Regelfall sind Individuen darauf bedacht, ihre Daten vor Dritten zu schützen und geheim zu halten. Einschnitte in die Privatsphäre werden oft als unangenehm empfunden. Die Gründe dafür sind vielfältig. Speziell durch den technischen Fortschritt bieten sich der Gesellschaft immer neuere Möglichkeiten der Überwachung ihrer Mitglieder und deren Handlungen. Es galt nun als Ziel dieser Diplomarbeit die Gründe zu eruieren, warum sich

[54] Das Wiener Institut für sozialwissenschaftliche Dokumentation und Methodik - seit 1985 (siehe www.wisdom.at, 17.02.2012).
[55] www.martin-adler.org

Wienerinnen und Wiener in so vielen Lebenssituationen überwachen lassen, sowohl im öffentlichen, wie auch im privaten Bereich? Warum wird eine Vorratsdatenspeicherung toleriert? Warum werden kaum löschbare Spuren hinterlassen? Ist dies womöglich unumgänglich? Geschieht dies unbewusst oder bewusst? Wie ist die Verteilung des Wissensstandes in der Bevölkerung bezogen auf das Thema Überwachung? Gibt es einen Zusammenhang zwischen mangelndem Wissen darüber, ob Daten gespeichert werden bzw. was für Daten gespeichert werden und der Akzeptanz von Überwachungsmaßnahmen? Besteht womöglich ein signifikanter Zusammenhang zwischen Überwachung und subjektivem Sicherheitsgefühl? Versuchen Individuen mittels Überwachung ihre Ängste zu kompensieren? Kurz gesagt:

Warum lassen wir uns überwachen?

> *„Was, denken Sie, würde geschehen, wenn die Regierung alle Bürger verpflichtet, ab 1. Januar nächstes Jahr ein kleines schwarzes Armband zu tragen, aus nickelfreiem Metall, mit hautfreundlichem Kunststoff ummantelt, das dem Staat vier Möglichkeiten gibt: erstens die ständige Lokalisierung des Bürgers auf einer Landkarte; zweitens die Option, von ihm erfasste Nachrichten zu lesen; drittens die Protokollierung, mit wem und wie lange er telefoniert; und viertens die Möglichkeit, jederzeit unbemerkt den Bürger, seine Gesprächspartner, ja selbst den Raum, in dem er sich befindet, abzuhören. Denken Sie, die Öffentlichkeit würde ein solches Armband akzeptieren? Wenn damit Vermisste gefunden werden könnten, Verbrechen aufgeklärt und Terroristen gefangen? Oder würden Hunderttausende auf die Straße gehen und dagegen rebellieren?“* (Simon/Simon 2008: 15)

So lautet die Einleitung in „Ausgespäht und abgespeichert“ von Simon und Simon (2008). Eine prominente Annahme auf die zentrale Fragestellung dieser Arbeit lautet, dass Individuen sich durch Überwachung sicherer fühlen (siehe Kapitel 3 Theorien). Das würde demnach bedeuten, dass mehr Überwachung, zu mehr Sicherheit führe. Der eigentlich Sinn und Zweck der Überwachung, so eine gängige Meinung, sei die Gewährleistung von Sicherheit und Schutz vor Devianz, sei es in Form von Terroranschlägen oder Gewaltdelikten bzw. generell unerwünschtem Verhalten oder Regelverstoß gegen bestehende Normen. Der französische Philosoph Michel Foucault (1994) betont Überwachung und die daraus resultierenden Informationen und deren strategischen Gebrauch, als Mittel sozialer Kontrolle. Wer Informationen besitzt hat Macht. Müsse demzufolge Überwachung nichtzu Unsicherheit, anstatt zu Sicherheit führen? Folglich dieser Überlegungen ergeben sich untenstehende Hypothesen.

► 1. Haupthypothese

Überwachungsmaßnahmen steigern das subjektive Sicherheitsgefühl in der Bevölkerung.

► 2. Haupthypothese

Je größer das Wissen über die verschiedenen Überwachungsmöglichkeiten und je geringer das Institutionsvertrauen, desto größer ist die Verunsicherung und somit auch die Ablehnung von Überwachungsmaßnahmen.

► 3. Haupthypothese

Wird der Öffentlichkeit jedoch die Vielzahl an Überwachungsmöglichkeiten und –arten präsentiert - wird also speziell unsichtbare Überwachung sichtbar gemacht - so bewirkt sie eher Verunsicherung.

►1. Zusatzhypothese

Die Befürwortung von Überwachungsmaßnahmen ist geschlechtsspezifisch.

Es wird davon ausgegangen, dass sich mehr Frauen für Überwachungsmaßnahmen aussprechen werden, als Männer, da sich Frauen womöglich im öffentlichen Raum unsicherer fühlen.

► 2. Zusatzhypothese

Die Zustimmung zu Überwachungsmaßnahmen ist altersspezifisch.

Ältere Menschen, welcher aufgrund ihrer gestiegenen Gebrechlichkeit tendenziell eher den vielfältigen Überwachungsmöglichkeit zu stimmen, als jüngere.

► 3. Zusatzhypothese

Personen, welche öfter Verbrechen ausgesetzt waren als andere, werden sich vermutlich vermehrt für Überwachungsmaßnahmen aussprechen, da das Erinnern an die Verbrechen eine Angst vor Devianz schürt, die mittels Überwachung kompensiert wird.

► **4. Zusatzhypothese**

Personen mit einer rechts gerichteten politischen Anschauung werden sich eher für Überwachungsmaßnahmen aussprechen, als Personen, aus dem linkspolitischen Lager.

Ein Zusammenhang zwischen politischer Einstellung und der Befürwortung von Überwachungsmaßnahmen ergibt sich aus einer Überlegung, dass Personen, welche sich eher im rechten politischen Bereich einordnen, höher die Tugenden, wie Disziplin und Überwachung als Kontrolle zur Einhaltung der Ordnung, einschätzen, teilweise auch durch die geschichtliche Entwicklung bedingt, als jene welche sich mehr dem linkspolitischen Lager zugeordnet fühlen. Auch können sich damit unterschiedliche politische Folgen und Sachverhalte verbinden.

► **5. Zusatzhypothese**

Je geringer das Vertrauen in den Staat und seine Institutionen, desto größer auch die Ablehnung gegenüber Überwachungssysteme.

Da die Angst vor Datenmissbrauch besonders gegeben ist, wenn kein Vertrauen in die Regierung und die verschiedenen Institutionen gegeben ist.

6.3. Untersuchungsgegenstand

Untersuchungsgegenstand sind die mannigfaltigen Möglichkeiten zur Überwachung der BürgerInnen der österreichischen Bundeshauptstadt und in Folge dessen die daraus resultierenden Meinungen der Wiener Bevölkerung zu diesem Thema. Bedingt durch den wachsenden technischen Fortschritt eröffnen sich staatlichen, sowie privaten Institutionen immer mehr Chancen der Überwachung eines Einzelnen. Von bedeutendem Interesse sind daher die Gründe einer Akzeptanz jener Methoden der Überwachung. Der Untersuchungsgegenstand wurde in Kapitel 2 ausführlich beschrieben und dargestellt.

6.4. Stichprobe und Methode

Die Grundgesamtheit der empirischen Studie stellen alle in Wien lebenden Personen, welche mindestens das 16te Lebensjahr begonnen haben, dar. Laut Statistik Austria hatten am 01.01.2011 1. 714.142 Personen einen gemeldeten Wohnsitz in Wien. Hier einbegriffen sind

allerdings alle Personen. Bei der Berechnung des Quotaplanes (siehe dazu Kapitel 6.5. Zweistufiges Studiendesign bzw. Tabelle 2.) für das Kontrollmerkmal „Geschlecht“ wurden die Gruppe der 0 bis 16 Jährigen nicht subtrahiert, da eine 1:1 Abbildung ohnedies mit den Ressourcen einer Diplomarbeit nicht möglich ist und die Abweichung minimal gewesen wäre. Bei der Berechnung der Quoten für das zweite Kontrollmerkmal „Alter“ wurden alle 0 bis 16-jährigen aus der Berechnung ausgeschlossen, da hier eine Unterteilung in Altersgruppen durchgeführt wurde.

Als Erhebungsinstrument wurde die standardisierte schriftliche Befragung mit einem standardisierten Fragebogen gewählt. Dieser untergliedert sich in eine standardisierte internetgestützte Befragung in Form eines E-Mail Surveys und in standardisierte face-to-face Interviews. Im Zuge der Online-Befragung wurde nach dem Schneeballverfahren vorgegangen, da keine vollständige E-Mail Adressliste der in Wien wohnhaften Personen existiert, obwohl dieses Verfahren eine bewusste Auswahl (vgl. Schnell et al. 2005) darstellt. Durch die standardisierten face-to-face Interviews wurde für die älteren Generationen ein Zugang in die Stichprobe geschaffen (siehe Kapitel 6.5.3.). Durch Kombination dieser beiden Methoden wurde versucht, eine möglichst genaue Repräsentation der Grundgesamtheit zu erzielen, d.h., dass die Quoten etwa der Grundgesamtheit entsprechen.

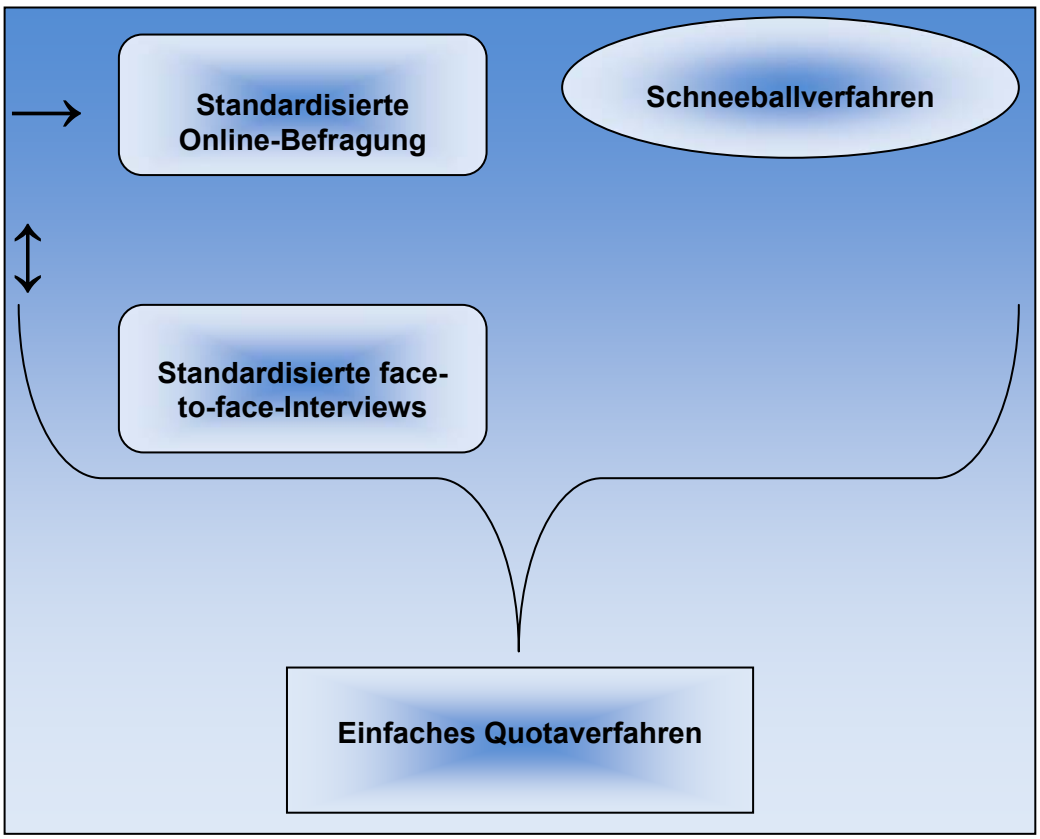


Abbildung 5 Verwendete Methodik

6.5. *Aufbau der Untersuchung*

Um die Repräsentativität[56] dieser Untersuchung bestmöglich garantieren zu können, wurde ein Methoden-Mix[57] durch Variationen der Befragung angewendet, bestehend aus einem standardisiertem Online-Fragebogen (Kapitel 6.5.2), welcher online per E-Mail an die Probanden verschickt wurde, und standardisierten face-to-face-Interviews zufällig ausgewählter Probanden ab 60+ (Kapitel 6.5.3.).

> *„Die Befragung gilt nach wie vor als das Standardinstrument empirischer Sozialforschung bei der Ermittlung von Fakten, Wissen, Meinungen, Einstellungen oder Bewertungen im sozialwissenschaftlichen Anwendungsbereich." (Phillips 1971: 3; Kaase/ Ott/ Scheuch 1983: 17, zit. nach Schnell et al. 2005: 321).*

Durch diesen Methoden-Mix sollte so, dank der face-to-face-Interviews, den älteren Mitgliedern unserer Gesellschaft die Chance gegeben werden, in die Stichprobe einbezogen zu werden, da erfahrungsgemäß die ältere Generation ab 60+ kaum[58], bis sehr selten (je älter die Probanden werden) das Internet nutzt. Die Grundgesamtheit umfasst alle in Wien[59] lebenden Personen ab 16 Jahren, ohne einer Altersbegrenzung nach oben hin. Als weiterer Garant, um die Repräsentativität dieser Stichprobe zu gewährleisten, wurden sogenannte Quoten festgehalten (einfaches Quotaverfahren). Der Quotenplan wurde so berechnet, dass die Verteilung der quotierten Merkmale in der Stichprobe der Verteilung in der Grundgesamtheit entspricht (vgl. Schnell et al.). Zur Berechnung der Quoten diente die Homepage der Statistik Austria als Informations- und Zahlenlieferant für das Bundesland Wien. Hierbei spielte die Verteilung des Geschlechts, des Alters und des Bildungsstandes der Bevölkerung Wiens die wesentliche Rolle, welche mit den Häufigkeitsauszählungen der Stichprobe verglichen wurde (siehe Tabelle 2 – Quotenplan Wien). Abhängig von der Rücklaufquote, welche auf Grund des Schneeballverfahrens nicht festgestellt werden kann, wurde mit zwischen 200 und 300 Fragebögen gerechnet. Weit überschritten wurde diese Marke in 12 Wochen Erhebungsdauer, angefangen von Anfang März 2011 bis Ende Mai 2011, mit 324 ausgefüllten Fragebögen.

---

[56] *„Der Begriff (...) sollte, wenn er für Zufallsstichproben verwendet wird, in dem eingeschränkten Sinn verwendet werden, dass mit diesen statistisch begründete Schlussfolgerungen auf die Grundgesamtheit möglich sind." (Diaz-Bone 2006: 133).*

[57] Auch Mixed-Mode-Methode genannt – Anwendung verschiedener Methoden.

[58] Bei einer 2009 durchgeführten Studie vom GFK Austria im Auftrag des Österreichischen Seniorenbundes gaben all jene 60 plus Probanden zu 49% an „Ja, sie haben die Möglichkeit auf Internet zuzugreifen" und 50% gaben „Nein" an (1% keine Meinung)
Quelle: www.besserlaengerleben.at.

[59] Im Fragebogen wurde der Wohnsitz nicht abgefragt. Es kann allerdings davon ausgegangen werden, da die Erhebung in Wien durchgeführt wurde, dass die Mehrheit der befragten Probanden in Wien wohnhaft ist. Auch wenn eine Online- Befragung den Kern dieser Studie bildet, ist zu großen Teil zu erwarten, dass weite Kreise der Verwandtschaft, sowie des Arbeits- und Freundeskreises ihren dauerhaften Wohnsitz in der Bundeshauptstadt haben. Kleinere Abweichungen und Ausnahmen sollten zudem auch zu keinen erwähnenswerten Verzerrungen im Ergebnis führen. Daher wurde auch der Quotenplan für das Bundesland Wien berechnet, da hier die Erhebung im Jahr 2011stattfand.

Bevölkerung WIEN am 1.1.2011 nach GESCHLECHT			
Insgesamt	1. 714 142	**Wien**	**Stichprobe**
Männer	821 605	48%	46%
Frauen	892 537	52%	54%

Bevölkerung WIEN am 1.1.2011 nach Alter - Insgesamt		
16 bis 24	11,0%	20,1%
25 bis 39	22,7%	27,2%
40 bis 49	16,3%	22,5%
50 bis 59	12,3%	11,1%
60 und älter	22,4%	19,1%

Q: STATISTIK AUSTRIA[60]

Bevölkerung WIEN 2001 nach BILDUNG - Insgesamt		
Pflichtschule	33,2%	25,3%
Lehrling	28,6%	23,1%
Berufsbildende mittlere Schule	10,6%	14,2%
Höhere Schule/Matura	15,8%	22,5%
Universität/Fachhochschule	11,8%	11,7%

Q:STATISTIK AUSTRIA[61]

Tabelle 2 Quotenplan[62] Wien, n = 324

Nachdem die forschungsrelevanten Daten erhoben wurden, wurden diese in einer SPSS Datenmatrix eingegeben und anhand einer quantitativen statistischen Analyse anschließend ausgewertet. Bei der univariaten Analyse wurden zunächst die Verteilungen aller Variablen mittels Häufigkeitstabellen untersucht und mittels statistischer Maßzahlen beschrieben. Darüberhinaus wurde auch mit graphischen Darstellungen, zur besseren Veranschaulichung, gearbeitet. In der bivariaten Analyse wurde der statistische Zusammenhang ausgewählter Variablen, welche aufgrund vorher durchdachter Überlegungen in einer Beziehung

[60]http://www.statistik.at/web_de/statistiken/bevoelkerung/bevoelkerungsstruktur/bevoelkerung_nach_alter_geschlecht/index.html, 21.05.2011.

[61]http://www.statistik.at/web_de/statistiken/bevoelkerung/volkszaehlungen_registerzaehlungen/bevoelkerung_nach_dem_bildungsstand/index.html, 21.05.2011

[62]Die Daten für den Bevölkerungsbildungsstand beziehen sich auf die Volkszählung von 2001, da auf Statistik Austria im Moment noch keine neueren Daten bezüglich dessen zu finden sind, wonach die Bevölkerung im Alter von 15 und mehr Jahren nach der höchsten abgeschlossenen Ausbildung und den Bundesländern untergliedert wird. 2011 wird die nächste Volkszählung erfolgen.

zueinander stehen könnten, untersucht und auf Abhängigkeit / Unabhängigkeit getestet. Mittels statistischer Maßzahlen, wurde im Falle eines Zusammenhangs, die Stärke dieser Beziehung ausgedrückt. In der multivariaten Analyse wurde hauptsächlich mit der Faktorenanalyse, zur Skala- bzw. Indexbildung, und der multiplen Regressionsanalyse der Einfluss mehrerer unabhängiger Variablen auf eine abhängige Variable analysiert.

6.5.1. Fragebogenaufbau

Die Erhebung zum Thema „Überwachung in Wien" wurde mit einem standardisierten Fragebogen durchgeführt. Dies bedeutet, dass allen befragten Probanden der gleiche Fragebogen, mit den gleichen Fragen, den gleichen Formulierungen und in der gleichen Reihenfolge gehalten (vgl. Schnell et al. 2005), zum Ausfüllen per E-Mail zugeschickt bzw. im Falle der face-to-face Interviews, zur Beantwortung überreicht wurde. Insgesamt wurden 19 Fragen zum Thema gestellt, wofür eine Ausfüllzeit von maximal 15 Minuten in Anspruch genommen wurde. Bei den Fragen handelt es sich um geschlossene Fragen, mit vorgegeben Antwortkategorien. Der Fragebogen beinhaltet neben Einstellungsfragen, Wissensfragen, Meinungsfragen, abschließend Fragen zur Demographie der Person. Um die verschiedenen Meinungen der befragten Personen zum Themengebiet „Überwachung in Wien" zu erfassen, wurden Likert-Skalen verwendet. Dazu wurden zu den verschiedenen Themenbereichen der Überwachung unterschiedliche Statements formuliert, denen die Probanden entweder zustimmen, oder diese ablehnen konnten. Die Möglichkeiten (4-stufige Antwortskala) zu antworten waren von „trifft sicher zu" bis „trifft überhaupt nicht zu" bzw. „stimme sehr zu" bis „stimme überhaupt nicht zu".

6.5.2. Online Befragung

Ein Spezialfall der schriftlichen Befragung ist die Online-Befragung. Hierbei werden die Fragebögen entweder per E-Mail verschickt oder im Internet auf einer Website hochgeladen (vgl. Schnell et al. 2005). Ersteres wurde gewählt, da diese Art der Befragung in einer relativ schnellen Zeit kostengünstig Ergebnisse liefert. Ein weiterer positiver Effekt schriftlicher Befragungen ist auch die Minderung der sozialen Erwünschtheit[63].

> *„Die Befragungen sind schneller durchführbar, man benötigt keine Interviewer (...) Von besonderer Bedeutung sind die im Vergleich zu anderen Erhebungsmodi vernachlässigten Erhebungskosten." (Schnell et al. 2005: 377)*

[63] Ein Störfaktor bei Befragungen, wenn die Befragten jene Antworten geben, von denen sie glauben, man wolle diese hören, eben sozial erwünscht (vgl. Schnell et al. 2005).

Bei dem Versand per E-Mail wurde nach dem Schneeballverfahren vorgegangen. Dieses Verfahren wird besonders gerne für seltene Subpopulationen verwendet, wenn die zu Untersuchenden schwer bis kaum erfassbar sind. Dabei wird *„ausgehend von einer [Start-; DZ]Person die von dieser benannten Personen befragt (...).“ (Schnell et al. 2005: 300).*Zwar handelt es sich hier nicht um eine schwer erreichbare Gruppe, vielmehr liegt die Begründung in der Auswahl dieses Verfahrens darin, dass dadurch versucht wurde, eine möglichst repräsentative Zufallsstichprobe zu ziehen, da keine vollständige E-Mail Liste der Wien Bevölkerung vorlag bzw. vorliegt.

Anhand einer standardisierten schriftlichen Befragung, wurde per Mail ein selbst konzipierter Fragebogen an die Probanden verschickt, wodurch die Einstellung der Wienerinnen und Wiener zum Thema Überwachung und Datenschutz im Jahre 2011 erforscht wurde. Als einziges Kriterium wurde ein unterstes Alterslimit von 16 Jahren festgelegt. Bevor die ersten Fragebögen verschickt wurden, wurden in den Monaten Jänner und Februar 2011 zwei Pretests[64] durchgeführt, um den vorherrschenden Fragebogen zu testen und gegebenenfalls zu verfeinern. Der erste Pretest wurde zur leichteren Erstellung des Fragebogens mit Studienkolleginnen und -kollegen, Freunden und Bekannten durchgeführt (n=15). Getestet wurden unter anderem die Verständlichkeit der Fragen, sowie der sinnvolle Aufbau des Fragebogens. Um Ergänzungen, Kritik und Verbesserungsvorschläge wurde ebenfalls gebeten. Der zweite und letzte Pretest wurde mit zwei Studienkolleginnen und drei zufällig ausgewählten Passanten durchgeführt[65] (n=5). Dabei wurde gefragt, ob man kurz Lust und Zeit hätte, ein Urteil über den Fragebogen zu fällen, denn es stand vielmehr die Bewertung des Fragebogens im Vordergrund, als die Beantwortung der Fragen. Nach den neu gewonnenen Eindrücken wurde zum letzten Mal der Fragebogen überarbeitet und mit Ende Februar 2011 stand die finale Version fest. Anfang März 2011 wurden dann die ersten Bögen per Mail an Personen aus meinem eigenen Bekannten-, Freundes-, Studium-, und Arbeitskreis verschickt (ca. 250 E-Mailadressen), mit der Bitte, jenen Fragebogen an Personen des eigenen Familien- , Bekannten- , Freundes- , Studium- und Arbeitskreises, weiterzuleiten und diese wiederum freundlicherweise zu bitten, sie mögen ihn wieder an Personen des eigenen Familien- , Bekannten- , Freundes- und Arbeitskreises weiterleiten, und so weiter und so fort. Es wurde ein Ausmaß zwischen 200 und 300 Fragebögen angestrebt. Summarisch kamen 305 Fragebögen zurück. Zusammen mit den 19 face-to-face durchgeführten Interviews wurde eine Fallzahl von insgesamt 324 Fragebögen erreicht.

[64] Sie dienen der Überprüfung von Fragebögen, bevor diese endgültig in Umlauf gebracht werden.
[65] Einmal im Donauzentrum, einmal auf der Favoritenstraße und einmal in einem Wartezimmer einer Frauenärztin im 21ten Wiener Gemeindebezirk.

6.5.3. Face-to-face-Interviews

Ergänzend zur computergestützten Online-Befragung wurden 19 standardisierte face-to-face Interviews, im Zeitraum Ende März bis Ende Mai 2011, durchgeführt, um so die ältere Population zu erreichen, da vermutet wurde, dass die Altersgruppe der 60+ sonst in der Stichprobe unterrepräsentiert gewesen wäre. Bei den Befragungsorten wurde darauf geachtet, Plätze aufzusuchen, an welchen sich vermehrt ältere Personen aufhalten (beispielsweise in Parks). Die Befragungen wurden hauptsächlich vormittags, sowie an Wochenenden gestartet, da auch hier wieder die Chance größer gegeben war, genau jene Passanten anzutreffen, welche ins Untersuchungsdesign passen. Neben etlichen Verweigerungen, traten besonders bei den älteren Probanden immer wieder Verständigungsprobleme bzw. Missverständnisse auf. Die mit Abstand am häufigsten gestellte Frage war, was denn eine IP-Adresse sei. Ein weiteres Problem bei der Befragung der 60+ Probanden, waren immer wieder, „das weiß ich nicht"-Antworten, obwohl diese wiederholt bei Meinungs- und Einstellungsfragen auftraten. Hier wurde betont, dass es nicht um das Wissen, sondern um die Meinung und die Einstellung ginge, was man denn glaube, dass zutreffen würde. Diese aufgetretenen Probleme bestärkten im Nachhinein noch einmal die Entscheidung, mit den face-to-face-Interviews die älteren Probanden einzubeziehen, da so Missverständnisse aufgeklärt, Hilfestellungen beim Ausfüllen gegeben und Zwischenfragen beantwortet werden konnten.

7. Diskussion der Ergebnisse und Interpretation

7. 1. Stichprobenbeschreibung

Wer Sicherheit der Freiheit vorzieht,
ist zu Recht ein Sklave.
(Aristoteles[66])

Die Ergebnisse der vorliegenden Arbeit beruhen auf einer Stichprobe von N=324 Personen ab 16 Jahren. Davon sind 54% weiblich und 46% männlich. Mit 27% ist die Altersgruppe der 25 bis 39 Jährigen am Stärksten vertreten, gefolgt von den 40 bis 49 Jährigen mit knapp 23%. 20% sind zwischen 16 und 24 Jahre alt, 19% sind 60 oder älter und 11% sind zwischen 50 und 59 Jahre (Tabelle 4). 30% der befragten Personen sind verheiratet und fast genauso viele, nämlich 29%, sind ledig. 26% leben in einer festen Partnerschaft bzw. Lebensgemeinschaft. Summa summarum lässt sich festhalten, dass die Mehrheit der befragten Probanden in einer festen Partnerschaft lebt. 11% sind geschieden und 3% sind verwitwet (Tabelle 3).

Tabelle 3 Familienstand der Probanden in %

Familienstand	Anzahl	%
Ledig (ohne feste Partnerschaft)	94	29
In fester Partnerschaft/ Lebensgemeinschaft	85	26
Verheiratet	98	30
Geschieden	37	11
Verwitwet	10	3
Gesamt	**324**	**100**

Tabelle 4 Alter der Probanden in %

Alter	Anzahl	%[67]
16 bis 24	65	20
25 bis 39	88	27
40 bis 49	73	23
50 bis 59	36	11
ab 60	62	19
Gesamt	**324**	**100**

[66] www.sevillana.de
[67] Gerundete Prozent

Tabelle 5 Höchste abgeschlossene Schulbildung der Probanden in %

Ausbildung	Anzahl	%
Ohne Abschluss	3	1
Noch Schüler	7	2
Pflichtschule	82	25
Lehre	75	23
Berufsbildende mittlere Schule	46	14
Höhere Schule/Matura	73	23
Universität/Fachhochschule	38	12
Gesamt	**324**	**100**

Ein Viertel der befragten Personen haben einen Pflichtschulabschluss. Jeweils 23% geben als höchste abgeschlossene Ausbildung entweder einen Lehrabschluss oder die Matura an. 14% haben eine berufsbildende mittlere Schule abgeschlossen und 11% besitzen einen Universitäts- bzw. einen Fachhochschulabschluss (Tabelle 5).

Tabelle 6 Derzeitige Beschäftigung der Probanden in %

Ich bin zurzeit ...	Anzahl	%
Arbeitslos/Arbeitsunfähig	15	5
Hausfrau/Hausmann, in Karenz	27	8
Schüler/Schülerin	7	2
Student/Studentin	29	9
In Ausbildung/Lehrling	20	6
Präsenzdienst/Zivildienst	10	3
Hauptberuflich erwerbstätig	183	57
In Pension	33	10
Gesamt	**324**	**100**

Deutlich mehr als die Hälfte der befragten Probanden, nämlich 57%, sind hauptberuflich erwerbstätig. 10% sind in Pension, 9% studieren, 8% befinden sich zurzeit in Mutter- bzw. Vaterkarenz, oder sind „hauptberuflich“ Hausfrau oder Hausmann. 6% absolvieren noch eine Ausbildung bzw. eine Lehre und knapp 5% sind arbeitslos oder arbeitsunfähig (Tabelle 6). Mit 37% sind die einfachen Angestellten am Häufigsten in der Stichprobe vertreten, mittlere und höhere Angestellte zu 12%. Den zweiten Platz belegen die an- sowie ungelernten ArbeiterInnen mit 22%. 10% sind einfache Beamte und 8% sind mittlere bzw. höhere Beamte.10% sind FacharbeiterInnen und 2% sind selbstständig bzw. frei beruflich (Tabelle 7).

Tabelle 7 Probanden nach Berufe in %

Beruf	**Anzahl**	**%**
Angelernte(r)/Ungelernte(r) ArbeiterIn	43	21
FacharbeiterIn	21	10
einfache(r) Angestellter/Angestellte	74	37
mittlere(r)/höhere(r) Angestellter/Angestellte	24	12
einfache(r) Beamter/Beamtin	20	10
mittlere(r)/höhere(r) Beamte/Beamtin	16	8
Selbstständige(r) oder Frei beruflich	5	3
Gesamt	**203**	**100**

7.2. *Einstellung zur Bedeutung des Themas*

Die Frage nach der Wichtigkeit dieses Themas für die Befragten wurde von allen Probanden (N=324) beantwortet. Am Häufigsten, mit knapp 50%, wurde die Antwortkategorie „eher wichtig“ gewählt. Für fast 46% aller Befragten ist das Thema Überwachung und Datenschutz sogar sehr wichtig. Insgesamt lässt sich sagen, dass knapp 95% der Probanden das Thema als wichtig einstufen.

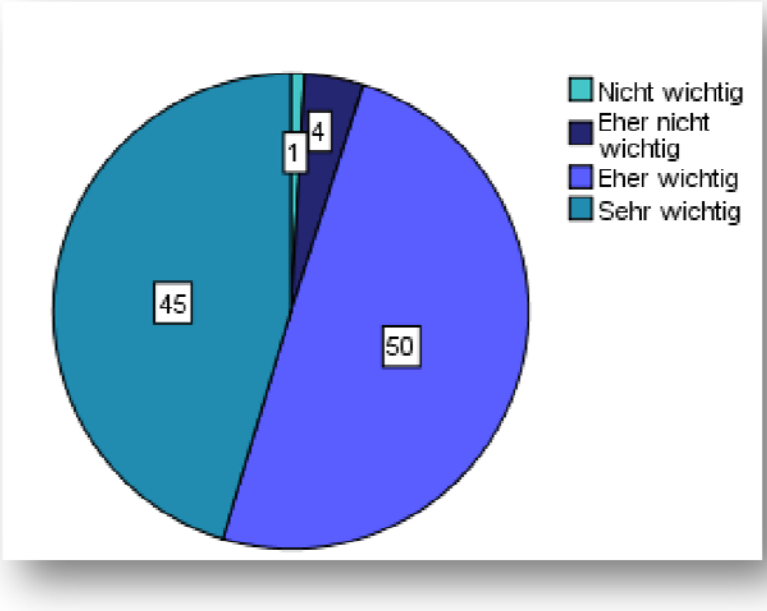


Abbildung 6 Wichtigkeit des Themas Überwachung & Datenschutz[68] in %

[68] Der Datenschutz stellt eine Folge der Überwachung dar und ist eng mit diesem Themenkomplex verbunden. Aufgrund einer Sensibilisierung wurde dieser Sachverhalt in die Einleitungsfrage aufgenommen.

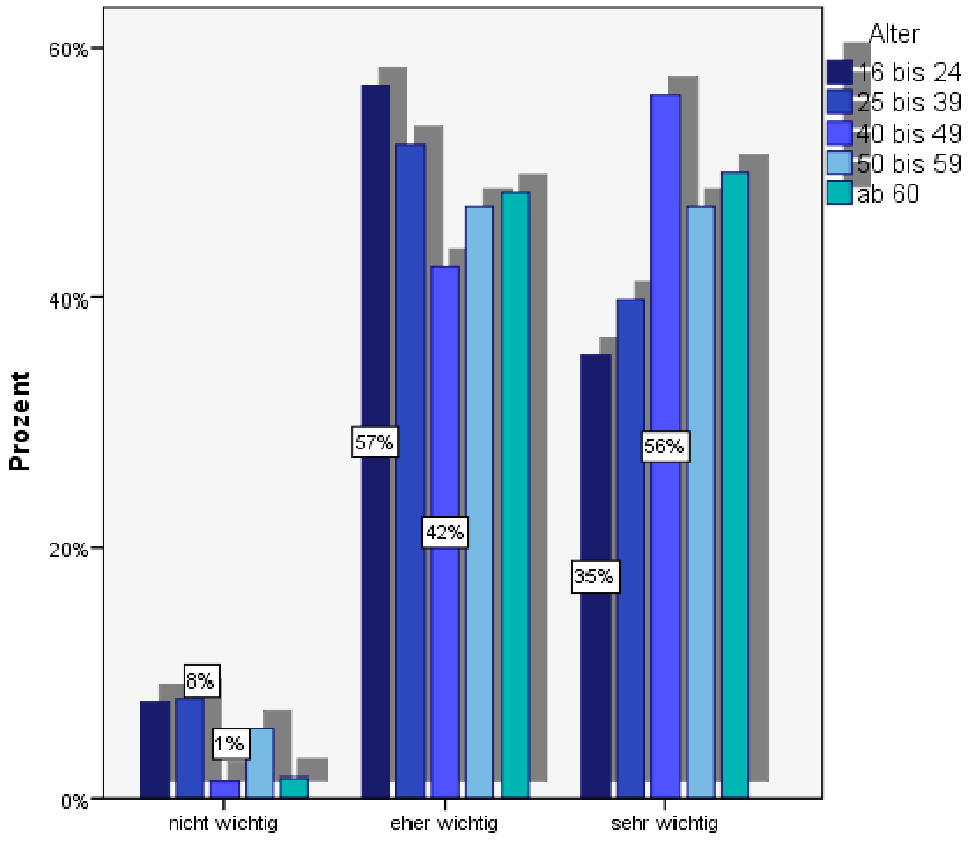


Abbildung 7 Wichtigkeit des Themas Überwachung & Datenschutz nach Alter in % $n_{weiblich}$=175 $n_{männlich}$=149 (χ^2=16,293; df=12; p=0,178[69])

57 % der 16 bis 24 Jährigen sind der Meinung, das Thema „Überwachung und Datenschutz“ sei eher wichtig. Diese Meinung teilen zu 52% auch die 25 bis 39 Jährigen. Doch mit zunehmendem Alter steigt auch die Wichtigkeit des Themas. Mehr als die Hälfte, knapp 56%, der 40 bis 49 Jährigen sind der Ansicht, das Thema sei sehr wichtig, im Gegensatz zu den Jungen (16 bis 24), welche nur zu 35% angeben, dass dieses Thema ihnen sehr wichtig sei. Bei jenen ab 60-Plus gibt jeder Zweite an, das Thema sei sehr wichtig für ihn oder sie (50%). Diesen Zusammenhang bestätigt auch das Korrelationsmaß, welches einen signifikanten und mittleren Zusammenhang zwischen den beiden Variablen Alter und Wichtigkeit des Themas zeigt (Gamma=0,179; p<0,05). Es handelt sich somit um einen positiven Zusammenhang, woraus man schließen kann, dass wenn das Alter steigt, auch die Relevanz der BürgerInnen bezüglich der Wichtigkeit des Themas „Überwachung und Datenschutz“ steigt.

[69] *„Bei Tabellen mit vielen Zellen und nicht sehr großen Fallzahlen kann es geschehen, dass auch bei erwartungsgemäßem Zusammenhang der Chi²-Test nicht signifikant ausfällt, der Test eines geeigneten Assoziationsmaßes jedoch schon. Wenn tatsächlich ein Zusammenhang (...) vermutet wurde, ist (...) in dieser Situation dem Test des Assoziationsmaßes mehr Glauben zu schenken.“* (Ludwig-Mayerhofer: 25).

Es ergeben sich keine signifikanten Zusammenhänge zwischen der Wichtigkeit des Themas und dem Geschlecht der Probanden, dem Familienstand, sowie der höchsten abgeschlossenen Schulbildung, der Position im Beruf der hauptberuflich Tätigen oder dem persönlichen Nettoeinkommen. Auch die derzeitige Beschäftigung aller nicht hauptberuflich Erwerbstätigen, wie beispielsweise Schüler, Studenten, Hausfrauen und Hausmänner, sowie Pensionistinnen und Pensionisten, um nur einige zu nennen, hat keinen Einfluss darauf, ob die Befragten die Wichtigkeit des Themas höher oder niedriger einschätzen.

Personen, welche jedoch angeben sie hätten große Besorgnis über die verschiedenen Überwachungsmaßnahmen, stufen zu 60% das Thema „Überwachung und Datenschutz“ als sehr wichtig ein (siehe Tabelle 8). Hingegen geben Personen, welche sich durch die Überwachungsmaßnahmen keine besonders großen Sorgen machen, nur zu 32% an, dass ihnen das Thema sehr wichtig sei. Somit stellt die Tatsache, wie man Überwachungsmaßnahmen bewertet, einen Einfluss auch auf die Relevanz des Themas dar. Für Personen, welche das Thema „Überwachung und Datenschutz“ keine besonders hohe Wichtigkeit einnimmt, erscheinen auch Überwachungsmaßnahmen als nicht besonders besorgniserregend. Die Signifikanz des Chi^2-Test, fällt höchst signifikant aus χ^2=24,657; df=3; p<0,001). Auch das Korrelationsmaß (Phi=0,276; p<0,001) legt einen mittleren Zusammenhang zwischen den beiden Variablen auf höchst signifikantem Niveau dar.

Tabelle 8 Kreuztabellierung Besorgnis * Wichtigkeit des Themas gerundet in %

			Besorgnis		Gesamt
			Nein	*Ja*	
Wichtigkeit des Themas	*nicht wichtig*[70]	Anzahl	10	6	16
		% innerhalb von Besorgnis	6%	4%	5%
	eher wichtig	Anzahl	104	57	161
		% innerhalb von Besorgnis	**62%**	**37%**	50%
	sehr wichtig	Anzahl	54	93	147
		% innerhalb von Besorgnis	**32%**	**60%**	45%
Gesamt		Anzahl	168	156	324
		% innerhalb von Besorgnis	100%	100%	100%

[70] Die beiden Kategorien „nicht wichtig“ und „eher nicht wichtig“ wurden aufgrund geringer Fallzahlen zu einer gemeinsamen Kategorie zusammengeschlossen.

7.2.1. Akzeptanz eines „Regierungsarmbands“

Auf die Frage hin, wie die Probanden auf ein Regierungsarmband reagieren würden, welches „ab 1. Jänner nächsten Jahres (...) dem Staat vier Funktionen biete: erstens (1) die ständige Lokalisierung des Bürgers auf einer Landkarte; zweitens (2) die Option, von ihm erfasste Nachrichten zu lesen; drittens (3) die Protokollierung, mit wem und wie lange er telefoniert; und viertens (4) die Möglichkeit, jederzeit unbemerkt den Bürger, seine Gesprächspartner abzuhören“, antworteten mehr als $^{2}/_{3}$ (69%) aller befragten Personen, sie würden gar keine dieser genannten Funktionen akzeptieren, auch „wenn damit Vermisste gefunden, Verbrechen aufgeklärt und Terroristen gefangen“[71] werden könnten.

Tabelle 9 Ergebnisse Regierungsarmband gerundet in %

Akzeptanz der 4 Funktionen	Anzahl	%
Ich würde gar keine Funktion akzeptieren.	225	69
Ich würde Funktion 1 akzeptieren.	81	25
Ich würde Funktionen 1& 2 akzeptieren.	3	1
Ich würde Funktionen 1 & 2 & 3 akzeptieren.	2	1
Ich würde alle 4 Funktionen akzeptieren.	13	4
Gesamt	**324**	**100**

Diese Tatsache widerspricht der Annahme, dass Personen generell Überwachungsmaßnahmen zustimmen, die die Sicherheit erhöhen. Zu groß muss hierbei wohl der Eingriff in die Privatsphäre sein. Man kann davon ausgehen, dass Kontroll- und Überwachungsmechanismen nur bis zu einem gewissen Grad erduldet werden. Wird die Trennlinie zwischen öffentlich und privat zu stark überschritten, bringen auch dadurch erhöhte Sicherheitsmaßnahmen keine positive Akzeptanz der besagten Instrumentarien einer Überwachungsgesellschaft.

Interessant, dass weitaus mehr Personen (13) alle 4 Funktionen akzeptieren würden, als jene die die Funktionen 1 und 2 (3), oder jene, die die Funktionen 1,2 und 3 (2) billigen würden. Dies deutet darauf hin, dass diese prinzipiell zustimmen, ohne auf eine Differenzierung zu achten. Vielmehr müsse man davon ausgehen, da die Bedingungen immer extremer werden, dass die Zustimmung mit der Zunahme der Extremität abnimmt. Hingegen ist die „Mitte“ eher spärlich vertreten, das Extremmaß, gleich alle vier Funktionen zu akzeptieren, liegt im Vergleich zu dessen um einiges höher, welches zwar noch immer beträchtlich unter der Nichtakzeptanz liegt (225 vs. 13), aber weitaus über den mittleren (13 vs. 3 und 13 vs. 2) Ausprägungen. Ein Viertel (genau 25%) würden die erste Funktion, das ständige Lokalisieren auf einer Landkarte genehmigen, womit eine

[71] siehe dazu Simon/ Simon 2008: 15.

ständige Identifikation des Bestimmungsortes, solange das Mobiltelefon in Betrieb ist, erfolgen könne. Rund 67% geben an, dass sie glauben, dass ihr Handy die erste Funktion, eine ständige Lokalisierung der BürgerInnen auf einer Landkarte durch den Staat, besitzt. Knapp 80% verneinen die Aussage, dass ihr Mobiltelefon über die zweite Funktion, die Option, dass der Staat von ihm erfasste Nachrichten zu lesen, verfüge. Die dritte Funktion, die Protokollierung, mit wem und wie lange er telefoniert, bejahen immerhin fast die Hälfte aller Probanden (41%), rund 59%. Wobei hier ein anderes Ergebnis zu erwarten gewesen wäre, bedenkt man die ausführlichen Handyrechnungen mit exakten Auflistungen aller gewählten Nummern, den dazugehörigen genauen Uhrzeiten und der Dauer der Telefonate. Die vierte Funktion, dass der Staat die Möglichkeit besäße, jederzeit unbemerkt seine BürgerInnen und seine GesprächspartnerInnen abzuhören, wird von 19% der befragten Personen als eine Funktion ihres Handys erachtet und von 81% nicht. 30% glauben, dass ihr Handy gar keine dieser Optionen besäße, immerhin knapp $^1/_3$.

7.3. Zentrale Einstellungsdimensionen und Hintergrund

Alle Fragen bzw. Items mit Likertskalierung wurden einer Faktorenanalyse[72] unterzogen, um zugrunde liegende Einstellungen herauszufinden. Auf der Basis der Reliabilitätsanalyse wurden die so erstellten Skalen geprüft. „Als „*Reliabilität*" oder „Zuverlässigkeit" kann das Ausmaß bezeichnet werden, in dem wiederholte Messungen eines Objekts mit einem Messinstrument die gleichen Werte liefern. (...) *„Reliabilität" wird in der klassischen Testtheorie als der Quotient der Varianz der wahren Werte und der Varianz der beobachteten Werte definiert."* (Schnell et al. 1999: 145). Dank dieser Itemanalyse sollten ungeeignete Items aus der Rohskala eliminiert werden, um so die Zuverlässigkeit der Messung zu verbessern (vgl. Schnell 1999: 182-183).

7.3.1.Law & Order

Die Items des Fragenblocks Nummer 5 im Fragebogen spiegeln die Dimension des Wirkungsbereichs staatlicher Kontrolle wieder. Sie implizieren Ordnung im Zuge gesetzlicher Zensur. Nach der durchgeführten Faktorenanalyse, erklären die extrahierten Hauptkomponenten in Summe knapp 80% der Varianz.

[72] Hauptkomponentenanalyse

Tabelle 10 Verwendete Items zur Skalenkonstruktion Law & Order[73]

Fragebogenfrage	$\bar{x}$	σ
5.1 Der Staat sollte Zeitungen und Fernsehen kontrollieren, um Moral und Ordnung sicher zu stellen.	**2,04**	**1,018**
5.3 In unserem öffentlichen Leben gibt es zu viel Kritik und zu wenig Ruhe und Ordnung.	**2,34**	**0,934**

Dabei ließen sich nach der Varimaxrotation zwei Komponenten mit sehr hohen Faktorladungen bündeln. Nach der durchgeführten Reliabilitätsanalysen an beiden Faktoren, wurde nur der erste Faktor[74] zur Bildung der Skala[75] „Law&Order" herangezogen.

Die gebildete Skala „Law & Order" zeigt den Zustimmungsanteil in Prozent der Probanden zu mehr Kontrolle und Einfluss des Staates auf das öffentliche Leben der BürgerInnen (siehe Abbildung 7). 57% verneinen einen größeren Einfluss und ausgedehntere Kontrolle des Staates auf das öffentliche Leben der BürgerInnen. Doch knapp die Hälfte, 43%, sprich, fast jeder zweite Bürger und jede zweite Bürgerin, wünschen sich mehr behördliche Beobachtung und Willenslenkung des Staates, im Zuge der Gewährleistung von Ordnung und Moral.

Die Kreuzung des Index mit den demographischen Variablen lieferte keine signifikanten Ergebnisse, jedoch die Kreuztabellierung (siehe Tabelle 11) mit der Frage nach der Wichtigkeit des Themas innerhalb der Bevölkerung, wonach sich ergab, dass all jene Bürger und Bürgerinnen, für welche das Thema eher nicht so wichtig ist, zu knapp 70% mehr staatliche Kontrolle befürworten. Umgekehrt verneinen ca. 62% der BürgerInnen mehr staatlichen Einfluss auf ihr öffentliches Leben, sobald sie die Wichtigkeit des Themas „Überwachung und Datenschutz" als sehr wichtig einschätzen (χ^2=8,733; df=3; p<0,05). Diesen Zusammenhang bestätigt auch das Korrelationsmaß (Phi=0,164; p<0,05).

[73] Vierstufige Antwortkategorie: 1=Stimme überhaupt nicht zu; 4=Stimme sehr zu.
[74] Erklärt 52,77% der Varianz vor der Rotation und 47,85% nach der Rotation. Zwar erklärt der zweite Faktor nach der Rotation immerhin 31,89% der Varianz, allerdings führt die Reliabilitätsanalyse zu einem viel zu geringen Cronbachs Alpha (α=0,498), wonach dieser zweite Faktor zur Skalenkonstruktion nicht herangezogen wird.
[75] α=0,852.

Tabelle 11 Kreuztabellierung Wichtigkeit des Themas * Law & Order gerundet in %

			Wichtigkeit des Themas				Gesamt
			Nicht wichtig	*Eher nicht wichtig*	*Eher wichtig*	*Sehr wichtig*	
Law & Order	*Nein*	Anzahl	3	4	85	91	183
		% innerhalb von Wichtigkeit des Themas	100%	31%	53%	**62%**	57%
	Ja	Anzahl	0	9	76	55	140
		% innerhalb von Wichtigkeit des Themas	0%	**69%**	47%	38%	43%
Gesamt		Anzahl	3	13	161	146	323
		% innerhalb von Wichtigkeit des Themas	100%	100%	100%	100%	100%

7.3.2. Terrorangst

Die abgefragte Dimension hier war die Angst vor terroristischen Anschlägen radikaler Gruppen und deren Einfluss auf das öffentliche Leben der WienerInnen. Erhoben wurde Daten bezüglich einer gesteigerten Verunsicherung aufgrund des Anschlages 9/11 in den USA. Des Weiteren wurde untersucht inwieweit die Angst, Opfer eines Terroranschlages in Österreich zu werden, gegeben ist und ob dies, zu vermeintlichen Vermeidungsaktionen, wie dem Nichtbesuch kultureller und/oder sportlicher Großveranstaltungen, führe.

Tabelle 12 Verwendete Items zur Skalenkonstruktion Terrorangst[76]

Fragebogenfrage	$\bar{x}$	σ
9.1 Ich fühle mich seit den Anschlägen vom 11. September generell unsicherer.	**2,08**	**0,906**
9.2 Ich halte es für möglich, in den nächsten Jahren Opfer eines Terroranschlages in Österreich (z.B. Flughafen, U-Bahn,...) zu werden.	**2,21**	**0,981**
9.3 Seit den Terroranschlägen meide ich kulturelle und/oder sportliche Großveranstaltungen.	**1,38**	**0,644**

Eine Faktorenanalyse extrahierte eine Hauptkomponente[77]. Aus folgenden Items (siehe Tabelle 12) wurde die Skala „Terrorangst“ gebildet[78]. 72% der befragten Probanden geben an, keine Terrorgefahr für sich in Österreich zu sehen. 28% hingegen sehen eine erhöhte Wahrscheinlichkeit selbst einmal Opfer eines terroristischen Anschlages in Österreich zu werden. Interessant an dieser Stelle war auch die Untersuchung einer möglichen Abhängigkeit zwischen der Terrorangst und der Befürwortung von Überwachungsmaßnahmen, ob eine erhöhte Angst vor terroristischen Aktivitäten, die Akzeptanz überwachungstechnischer Strategien zur Bekämpfung des Terrorismus zur Folge

[76] Vierstufige Antwortkategorie: 1=Stimme überhaupt nicht zu; 4=Stimme sehr zu.
[77] Erklären insgesamt 60% der Varianz.
[78] α=0,651.

hätte. Allerdings brachte die Kreuztabellierung dieser beiden Dimensionen nicht signifikante Unterschiede hervor, woraus geschlossen werden kann, dass die Angst vor Terrorismus keinen Einfluss auf die Zustimmung von Überwachung ausübt. Somit scheint eine Rechtfertigung seitens des Staates und der Politik, Überwachung unter dem Aspekt der Bekämpfung des Terrorismus voranzutreiben, als wenig zielführend, besonders wenn die Mehrheit der WienerInnen von keiner akuten Gefahr, terroristischer Anschläge in Österreich, ausgeht.

7.3.3. Autoritarismus

Die Dimension welche hier abgebildet wird, ist die Einstellung bezüglich des Verhältnisses der BürgerInnen zum politischen System des Staates. Diese Einstellungsskala setzt sich, nach einer an vier Items durchgeführten Faktorenanalyse[79], aus zwei Statements zusammen[80].

Tabelle 13 Verwendete Items zur Skalenkonstruktion Autoritarismus[81]

Fragebogenfrage	$\bar{x}$	σ
11.2Sicherheit ist wichtiger als Freiheit.	**2,22**	**0,846**
11.4Wo strenge Autorität herrscht, dort ist auch Gerechtigkeit.	**1,73**	**0,787**

Diese zwei beinhalten die Konzepte, wonach Sicherheit wichtiger sei als Freiheit (39% stimmen dieser Aussage sehr zu bzw. nur zu) und das überall, wo strenge Autorität herrsche, auch Gerechtigkeit walte (insgesamt 13% Zustimmung innerhalb der Bevölkerung). Darüber hinaus geben 95% der Wiener und Wienerinnen an, dass BürgerInnen mehr Einfluss auf Regierungsentscheidungen haben sollten und 87% heben die Demokratie als die beste Staatsform hervor. Die Skala bildet somit die Zustimmung zu einer bedeutend autoritären Staatsführung ab, wobei jedoch 62% der Bevölkerung solch ein Herrschaftsmodell ablehnen. Allerdings befürworten 38% einen totalitären Handlungsspielraum politischer Akteure.

[79] Erklärter Varianzanteil 40%.
[80] α = 0,704.
[81] Vierstufige Antwortkategorie: 1=Stimme überhaupt nicht zu; 4=Stimme sehr zu.

7.4. Hypothesentestung

7.4.1. Subjektives Sicherheitsgefühl

Die erste Haupthypothese lautet, dass *Überwachungsmaßnahmen, das subjektive Sicherheitsgefühl in der Bevölkerung steigern*. Die erste Forschungsfrage zielt auf eine mögliche Abhängigkeit des Sicherheitsgefühls in der Bevölkerung von den verfügbaren Überwachungstechniken in einer Gesellschaft ab. Hierbei wurden die Skalen „Sicherheitsgefühl“ und „Pro-Überwachung“ aus dem Fragenblock Nummer 6 (siehe Fragebogen im Anhang) gebildet.

7.4.1.1. Skala Sicherheitsgefühl

Nach einer Faktorenanalyse[82] wurden die extrahierten Items einer Reliabilitätsanalyse[83] unterzogen, um so in weiterer Folge die Skala „Sicherheitsgefühl“ zu bilden.

Tabelle 14 Verwendete Items zur Skalenkonstruktion Sicherheitsgefühl[84]

Fragebogenfrage	$\bar{x}$	σ
6.4 Videoüberwachung schreckt potenzielle Täter ab.	**2,78**	**0,802**
6.6Videoüberwachung verringert die Kriminalität nicht, sondern verlager diese auf andere Orte.	**2,14**	**0,770**
6.1. Je mehr überwacht und kontrolliert wird, desto sicherer ist es auch.	**2,45**	**0,814**
6.14 Überwachungssysteme schaffen in der Bevölkerung mehr Verunsicherung als Sicherheitsgefühle.	**2,59**	**0,878**

Diese bildet die Zustimmung der WienerInnen ab, wonach Überwachungsmaßnahmen das subjektive Sicherheitsgefühl steigern. Entgegen der Hypothese, geben gerundet 58% der Befragten an, Überwachungsmaßnahmen würden demnach nicht zu einem gesteigerten Sicherheitsgefühl führen. 42% hingegen fühlen sich dank der innovativen Techniken der Dauerbeobachtung sicherer.

[82] Zwei Hauptkomponenten wurden extrahiert. Erste Komponente erklärt 35% der Varianz, zweite Komponente zu 21% nach der Varimaxrotation. Cronbachs Alpha für den ersten Faktor =0,695; für den zweiten Faktor=0,247. Da dieser viel zu gering ausfällt, belaufen sich weitere Berechnungen nur anhand des ersten Faktors.
[83] α =0,695.
[84] Vierstufige Antwortkategorie: 1=Stimme überhaupt nicht zu; 4=Stimme sehr zu.

7.4.1.2. Skala Pro-Überwachung

Die Skala[85] „Pro-Überwachung“ wurde mit Hilfe von Items gebildet, welche *für*, wie auch *gegen,* Überwachungsmaßnahmen sprechen, welche in weiterer Folge dementsprechend negativ codiert wurden.

Tabelle 15 Verwendete Items zur Skalenkonstruktion Pro-Überwachung[86]

Fragebogenfrage	$\bar{x}$	σ
6.1 Datenschutz ist Täterschutz. Wer nichts zu verbergen hat, hat auch nichts zu befürchten.	**2,64**	**0,969**
6.3 Überwachungssysteme greifen in meine Privatsphäre ein.	**1,98**	**0,801**
6.5Ich fühle mich durch die Kameras beobachtet.	**2,73**	**0,854**
6.8Verbotene Gegenstände werden Dank Nacktscanner schneller gefunden.	**2,76**	**0,710**
6.11 Biometrische Pässe (beinhalten Fingerabdrücke, Iriserkennung und Personaldaten) schützen uns besser vor Datenmissbrauch und Fälschungen, als die alten Pässe.	**2,97**	**0,692**
6.12 Terroristen können anhand biometrischer Pässe schneller identifiziert werden.	**1,96**	**0,682**

[85] α=0,665
[86] Vierstufige Antwortkategorie: 1=Stimme überhaupt nicht zu; 4=Stimme sehr zu.

Diese Einstellungsskala spiegelt den Sachverhalt wieder, ob die Wiener und Wienerinnen für oder gegen Überwachungsmaßnahmen plädieren.

Tabelle 16 Kreuztabellierung Pro-Überwachung * Sicherheitsgefühl gerundet in %

			Pro-Überwachung		Gesamt
			Nein	*Ja*	
Sicherheitsgefühl	*Nein*	*Anzahl*	132	52	184
		% innerhalb von Pro-Überwachung	71%	39%	58%
	Ja	*Anzahl*	54	81	135
		% innerhalb von Pro-Überwachung	**29%**	**61%**	42%
Gesamt		*Anzahl*	186	133	319
		% innerhalb von Pro-Überwachung	100%	100%	100%

Es konnte hiermit die Hypothese bestätigt werden, dass Probanden, welche Überwachungsmaßnahmen zustimmen, sich (61%) durch diese sich auch sicherer fühlen (χ^2=32,268; df=1; p<0,001).Auf einen großen Zusammenhang auf höchst signifikantem Niveau innerhalb dessen, deutet auch das Korrelationsmaß hin (Phi=0,318, p<0,001).

7.4.2. Wissen vs. Institutsvertrauen vs. Sicherheitsgefühl

Die zweite Haupthypothese besagt, dass *je größer das Wissen über die verschiedenen Überwachungsmöglichkeiten und je geringer das Institutionsvertrauen, desto geringer das subjektive Sicherheitsgefühl (desto größer die Verunsicherung) und somit auch die Ablehnung von Überwachungsmaßnahmen*. Hier wird unterstellt, dass Personen mit einem größeren Wissen im Bereich der Überwachung und des Datenschutzes im Allgemeinen über einen breiteren Fundus der möglichen Gefahren für die Privatsphäre verfügen und aufgrund dessen, eher dazu tendieren werden, Überwachungsarten abzulehnen, als diese zu befürworten. Unterstellt wird dabei auch, dass hier Drittvariablen, wie das subjektive Sicherheitsgefühl und das Vertrauen in die österreichischen Institutionen (Staat, Polizei, Telekommunikationsanbieter, Medien, etc. ...) einen Einfluss auf die Ablehnung ausüben. Zur Veranschaulichung der zweiten Haupthypothese siehe folgende graphische Darstellung der Vermutungen (siehe Abbildung 12).

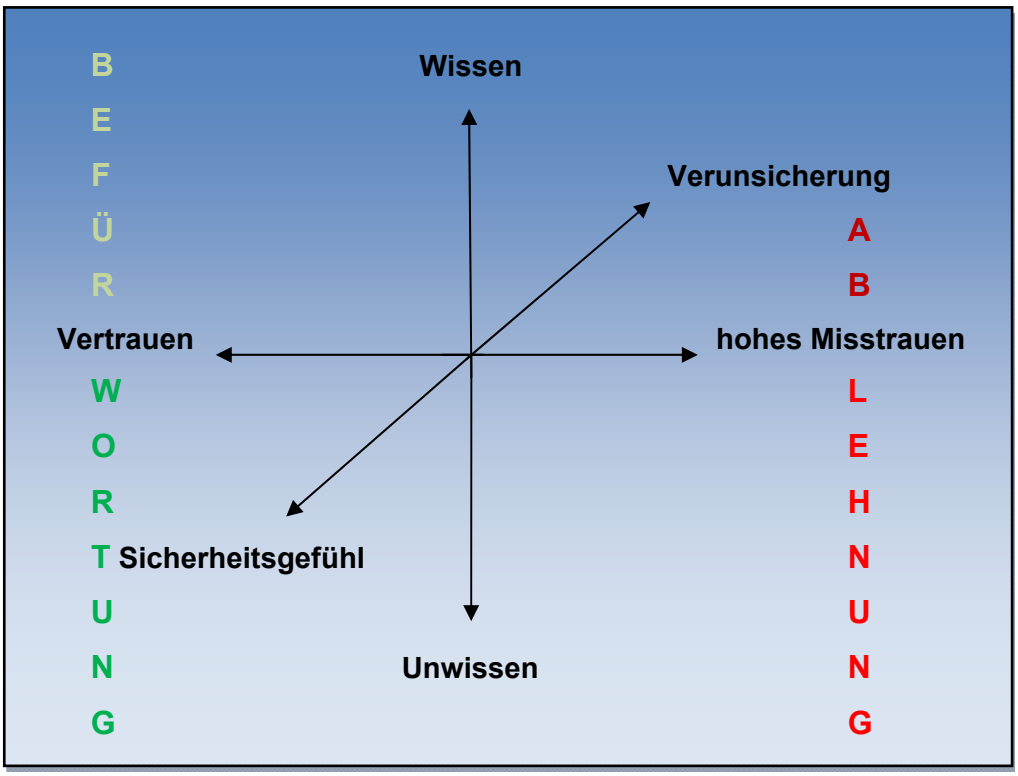


Abbildung 8 Grafische Darstellung der Hypothese

Abbildung 12 spiegelt graphisch die zweite Haupthypothese wieder, wonach ein hoher Wissensstand (bezüglich der mannigfaltigen Überwachungsmaßnahmen) und ein hohes Misstrauen gegenüber österreichischen Behörden, zur Verunsicherung (einem negativen Sicherheitsgefühl) führen, anstatt zum angestrebten höheren Sicherheitsgefühl. Die intervenierende Variable ist das Sicherheitsgefühl aufgrund der Überwachungsmaßnahmen. Die Konsequenz daraus ist eine Ablehnung observationsähnlicher Techniken. Ein niedriger Wissensfundus und ein hohes Vertrauen in die staatlichen Institutionen, führen demnach zu einem positiven Sicherheitsgefühl, was eine Akzeptanz bzw. Befürwortung der Überwachungsarten zur Folge hat. Zur Überprüfung dieser Hypothese werden 3 Skalen herangezogen, bestehend aus dem Wissensindex, der Sicherheitsgefühlskala[87] und der Institutionenvertrauensskala.

7.4.2.1. Wissensindex

Es sollte zuerst der Wissensstand der Probanden zu den verschiedenen Überwachungsmöglichkeiten (Videoüberwachung, Google und Google Street View, Vorratsdatenspeicherung, Kundenkarten und Kundenprofile, Nacktscanner und last but not least GPS Geräte) erhoben werden. Bei fast allen Statements zeigte sich, dass die Meisten der befragten Probanden ganz gut über die erdenklichen Überwachungsmöglichkeiten

[87] Zur Bildung dieser Skala siehe 7.4.1.1.

Bescheid wissen. Eine Ausnahme bilden Telefonie- und Internetdatenspeicherung, sowie Kundenkartenverwendung. Folgende Tabelle liefert eine Zusammenfassung der Ergebnisse des Fragenblocks Nr. 2:

Tabelle 17 Darstellung Ergebnisse Wissensfrage[88]

Fragebogenfrage	*Erste vs. letzte Antwortkategorie*	$\bar{x}$	σ
2.1 Die immer mehr lückenloser werdende Videoüberwachung nimmt zu.	Trifft sicher zu 33% Trifft überhaupt nicht zu 0,3%	**3,19**	**0,672**
2.2 Die Suchmaschine Google speichert alle von Ihnen jemals eingegebenen Suchanfragen mit dazugehöriger IP-Adresse.	Trifft sicher zu 35% Trifft überhaupt nicht zu 4%	**3,16**	**0,774**
2.3 Seit 2007/2008 werden alle Telefonie- und Internetdaten verdachtsunabhängig gespeichert.	Trifft sicher zu 19% Trifft überhaupt nicht zu 7%	**2,30**	**0,852**
2.4 Dank Google Street View werden Adressen demnächst in einer 360° Ansicht sichtbar, somit auch ihr Haus / ihre Wohnung, wenn sie dem nicht widersprechen.	Trifft sicher zu 37% Trifft überhaupt nicht zu 5%	**3,08**	**0,878**
2.5 Die anhand von Kundenkarten (z.B. Billa, Libro…) erstellten Kundenprofile dienen auch dem Risikomanagement, z.B. bei Banken als Entscheidungsgrundlage für die Kreditwürdigkeit.	Trifft sicher zu 14% Trifft überhaupt nicht zu 12%	**2,37**	**0,869**
2.6 Nacktscanner sind nicht im Stande wahrheitsgetreue Körperbilder zu liefern.	Trifft sicher zu 12% Trifft überhaupt nicht zu 14%	**2,51**	**0,876**
2.7 Selbst Geräte mit GPS Funktionen, wie z.B. Navigationsgeräte oder Handys, ermöglichen keine Ortung des Aufenthaltes.	Trifft sicher zu 2% Trifft überhaupt nicht zu 64%	**3,55**	**0,678**

Die Beantwortung der sieben Statements erfolgte über vier Antwortkategorien, beginnend mit „Trifft überhaupt nicht zu“ und endend mit „Trifft sicher zu“. Richtige Antworten wurden mit der „4“ vercodet und „falsche“ Antworten mit der „1“. Somit liegt der Minimalwert, welcher

[88] Antwortskala 1bis 4, wobei 1 = Trifft überhaupt nicht zu; 4= Trifft sicher zu.

erreicht werden konnte, bei 7 und der höchste bei 28. Aus den Antworten heraus lässt sich schlussfolgern, dass kaum jemand über weniger als die Hälfte der Überwachungsmöglichkeiten Bescheid wusste. Die Meisten, nämlich ein Viertel der befragten Personen, haben einen Wert von 20 erreicht. Nach Zusammenfassung der Kategorien in „kein Wissen“ (0-7), „niedriges Wissen“ (8-14), „mittleres Wissen“ (15-20) und „hohes Wissen“ (21-28), ergibt sich, dass mehr als die Hälfte (60%) ein mittleres Wissen in Bezug auf die verschiedenen Überwachungsmaßnahmen, was stimmt bzw. was zutrifft, haben. 40%, also fast knapp die Hälfte, haben ein hohes Wissen. Keiner/Keine hat kaum einen bzw. einen niedrigen Wissensstand bezüglich der Möglichkeiten der Überwachungspraktiken.

Die Kreuztabellierung (siehe Tabelle 18) des Wissens mit der höchsten abgeschlossenen Schulbildung[89] ergab, dass die Ausbildung einen Einfluss auf den Wissensstand der Probanden hat. Je höher die Ausbildung, desto größer auch der Wissensstand der befragten Personen zur Thematik „Überwachungsmöglichkeiten“ (χ^2=5,760; df=1; p=0,05). Das Wissen all jener mit einem Maturaabschluss bzw. einem Universitäts- oder Fachhochschulabschluss, verteilt sich auf die beiden Kategorien mittleres und hohes Wissen, gleichmäßig zu je ca. 50%. Bei all jenen ohne Matura nimmt der Wissensanteil bei der Kategorie „hohes Wissen“ um knapp die Hälfte ab (65% zu 36%). Diesen Zusammenhang belegt auch das Korrelationsmaß (Phi=0,136; p<0,05).

Tabelle 18 Kreuztabellierung höchste abgeschlossene Schulbildung * Wissensstand gerundet in %

			Ausbildung dichotom		Gesamt
			ohne Matura	*Matura + Hochschulabschluss*	
Wissen	*mittleres Wissen*	*Anzahl*	131	54	185
		% innerhalb von Ausbildung dichotom	**65%**	51%	60%
	hohes Wissen	*Anzahl*	72	53	125
		% innerhalb von Ausbildung dichotom	36%	**50%**	40%
Gesamt		*Anzahl*	203	107	310
		% innerhalb von Ausbildung dichotom	100%	100%	100%

[89]Es wurden Personen mit Matura + Hochschule zusammengefasst und den Personen mit niedriger Bildung gegenüber gestellt.

Auch die Position im Hauptberuf übt einen Einfluss auf den Wissensstand der Probanden aus (χ^2=13,926; df=3; p<0,01). In die Berechnung der Werte gingen jedoch nur 200 der 324 Fälle ein, da 124 der Befragten noch Schüler, Student / Studentin, Hausmann / Hausfrau, in Pension etc. waren. 73% der ArbeiterInnen[90] und 62% der Angestellten[91] verfügen über ein mittleres Wissen, Selbstständige bzw. Freiberufliche besitzen zu 60% und Beamte[92] zu 64% ein hohes Wissen (siehe Tabelle 19). Auch das Korrelationsmaß denunziert einen sowohl großen, als auch hoch signifikanten Zusammenhang zwischen diesen beiden Variablen (Gamma=0,413; p<0,001). Es zeigt sich, dass dieses Ergebnis eng mit jenem der höchsten abgeschlossenen Schulbildung zusammenhängt. Einerseits steigt mit der Höhe der Ausbildung und mit der Höhe der Berufsposition also auch der Wissensstandüber die mannigfaltigen Überwachungsmöglichkeiten.

Tabelle 19 Kreuztabellierung Beruf * Wissensstand gerundet in %

			Beruf				Gesamt
			ArbeiterInnen	*Angestellte*	*Beamte*	*Selbstständige & Freiberufliche*	
Wissen	*mittleres Wissen*	*Anzahl*	46	59	13	2	120
		% innerhalb von Beruf	**73%**	**62%**	36%	40%	60%
	hohes Wissen	*Anzahl*	17	37	23	3	80
		% innerhalb von Beruf	27%	39%	**64%**	**60%**	40%
Gesamt		*Anzahl*	63	96	36	5	200
		% innerhalb von Beruf	100%	100%	100%	100%	100%

[90] Dazu zählen an- sowie ungelernte ArbeiterInnen und FacharbeiterInnen.
[91] Einfache, mittlere und höhere Angestellte.
[92] Einfache, mittlere und höhere Beamte.

7.4.2.2. Skala Institutionenvertrauen

Folgende Tabelle zeigt tabellarisch die Verteilung des Vertrauens der Wiener Bevölkerung in die unterschiedlichen Institutionen.

Tabelle 20 Vertrauen der Wiener Bevölkerung in österreichische Institutionen gerundet in %

Institutionen	*Vertrauen*				
	Groß bis sehr groß	*Mittel*	*Gering bis kein Vertrauen*	$\bar{x}$	σ
Regierung	27%	51%	22%	3,06	0,802
Glaubenseinrichtungen (z.B. Kirche,…)	8%	22%	**70%**	2,13	0,921
Polizei	36%	47%	18%	3,20	0,884
Parlament	34%	**53%**	13%	3,21	0,754
Justiz	33%	43%	24%	3,13	0,845
Medien	52%	35%	13%	3,46	0,898
Banken	41%	45%	15%	3,32	0,931
Telekommunikationsanbieter	21%	50%	29%	2,88	0,835
Gesundheitssystem	**64%**	29%	8%	3,62	0,744
Private Versicherungen	27%	39%	35%	2,93	0,933
Private Unternehmen	22%	49%	30%	2,94	0,858

Dabei genießt das größte Vertrauen der Wiener Bevölkerung das Gesundheitssystem mit 64%, dicht gefolgt vom Parlament, welchem 53% mittleres Vertrauen entgegen gebracht wird. Am Schlechtesten schneiden die Glaubenseinrichtungen ab. Diesen wird zu 70% nur geringes bis gar kein Vertrauen geschenkt. Eine durchgeführte Faktorenanalyse extrahierte drei Hauptkomponenten.

Der erste Faktor[93] wurde in „Vertrauen in staatliche Institutionen“ benannt[94]. Diesen wird zu 44% hohes und zu 56% niedriges Vertrauen entgegen gebracht. Folgende Kreuztabellierung der beiden Skalen „Vertrauen in staatliche Institutionen“ als unabhängige Variable, mit der Skala „Pro-Überwachung“ als abhängige Variable, zeigt tabellarisch eine Abhängigkeit dieser beiden Indizes auf höchst signifikantem Niveau (siehe Abbildung 14).

Tabelle 21 Kreuztabellierung Vertrauen in staatliche Institutionen * Verunsicherung gerundet in %

			Vertrauen in staatliche Institutionen		Gesamt
			niedrig	*Hoch*	
Verunsicherung	*Nein*	*Anzahl*	80	88	168
		% innerhalb von Vertrauen in staatliche Institutionen	44%	**62%**	52%
	Ja	*Anzahl*	102	54	156
		% innerhalb von Vertrauen in staatliche Institutionen	56%	38%	48%
Gesamt		*Anzahl*	182	142	324
		% innerhalb von Vertrauen in staatliche Institutionen	100%	100%	100%

Personen, welche staatlichen Institutionen ein hohes Vertrauen entgegen bringen, fühlen sich zu 62% durch diese auch nicht verunsichert. Hingegen empfinden 56% aller Wiener und Wienerinnen, sobald diese ein niedriges Vertrauen in staatliche Institutionen setzen, Überwachungsmaßnahmen als besorgniserregend. Demgegenüber stehen 38%, welche ebenfalls Techniken der Überwachung als besorgniserregend einstufen, und dennoch ein hohes Vertrauen in den Staat und seine Einrichtungen legen (χ^2=10,370; df=1; p≤0,001; Phi= -0,179; p≤0,001).

Der zweite Faktor[95] wurde in „Vertrauen in intermediäre Institutionen“ benannt[96]. Diesen wird zu 45% hohes und zu 55% niedriges Vertrauen geschenkt. Auch hier ergibt sich eine signifikante Abhängigkeit der beiden Skalen „Vertrauen in intermediäre Institutionen“ und „Pro-Überwachung“ (siehe Abbildung 15).

[93] Beinhaltet das Vertrauen in die österreichische Regierung, das Parlament, die Polizei und die Justiz.
[94] α = 0,812.
[95] Beinhaltet das Vertrauen in die österreichischen Banken, Medien, Telekommunikationsanbieter und das Gesundheitssystem.
[96] α = 0,705

Der dritte Faktor wurde in „Vertrauen in private Institutionen[97]“ benannt[98]. Diesen wird zu 27% hohes und zu 73% niedriges Vertrauen entgegen gebracht. Auch hier wurde untersucht ob dieser Tatbestand – Vertrauen in private Institutionen – eine Wirkung auf die Zustimmung zu Überwachungstechniken ausübt (siehe Abbildung 16).

Tabelle 22 Kreuztabellierung Vertrauen in private Institutionen * Verunsicherung gerundet in %

			Vertrauen in private Institutionen		Gesamt
			niedrig	*Hoch*	
Verunsicherung	*Nein*	*Anzahl*	108	60	168
		% innerhalb von Vertrauen in private Institutionen	46%	67%	52%
	Ja	*Anzahl*	127	29	156
		% innerhalb von Vertrauen in private Institutionen	**54%**	**33%**	48%
Gesamt		*Anzahl*	235	89	324
		% innerhalb von Vertrauen in private Institutionen	100%	100%	100%

Wenn Probanden privaten Institutionen ein niedriges Vertrauen entgegen bringen, dann fühlen sich diese zu 54% durch Überwachungsmaßnahmen verunsichert (χ^2=11,906; df=1; p≤0,001; Phi=-0,192; p≤0,001). Je höher das Vertrauen in private Institutionen, desto geringer die Verunsicherung (33%).

[97] Beinhaltet das Vertrauen in private Unternehmen und private Versicherungen.
[98] α = 0,631

Tabelle 23 Kreuztabellierung Vertrauen in staatliche Institutionen * Wissensstand der Probanden * Sicherheitsgefühl durch Überwachungsmaßnahmen gerundet in %

Sicherheitsgefühl durch Überwachungsmaßnahmen				Wissen		Gesamt
				Niedriges[99] *bis mittleres Wissen*	*Hohes Wissen*	
Nein	**Vertrauen in staatliche Institutionen**	*Niedrig*	*Anzahl*	71	43	114
			% innerhalb von Wissen	**72%**	51%	62%
		Hoch	*Anzahl*	28	41	69
			% innerhalb von Wissen	28%	49%	38%
	Gesamt		*Anzahl*	99	84	183
			% innerhalb von Wissen	100%	100%	100%
Ja	**Vertrauen in staatliche Institutionen**	*Niedrig*	*Anzahl*	42	20	62
			% innerhalb von Wissen	46%	47%	46%
		Hoch	*Anzahl*	49	23	72
			% innerhalb von Wissen	54%	54%	54%
	Gesamt		*Anzahl*	91	43	134
			% innerhalb von Wissen	100%	100%	100%
Gesamt	**Vertrauen in staatliche Institutionen**	*Niedrig*	*Anzahl*	113	63	176
			% innerhalb von Wissen	60%	50%	56%
		Hoch	*Anzahl*	77	64	141
			% innerhalb von Wissen	41%	50%	45%
	Gesamt		*Anzahl*	190	127	317
			% innerhalb von Wissen	100%	100%	100%

Die Hypothese besagt, dass Probanden, je größer ihr Wissensstand bezüglich der mannigfaltigen Möglichkeiten zur Observation der BürgerInnen und je geringer deren Vertrauen in staatliche Institutionen, desto geringer ihr individuelles Sicherheitsgefühl. Dies bedeutet, dass ein hohes Wissen und ein niedriges Vertrauen in den Staat und seine Institutionen ein verringertes Sicherheitsgefühl auslöst. Doch wie aus der Tabelle zu entnehmen ist, ist jedoch Gegensätzliches der Fall. Je niedriger der Wissensstand und je geringer das Vertrauen, desto niedriger auch das Sicherheitsgefühl[100] (χ^2=8,152; df=1; p<0,01). Einen mittleren Zusammenhangbekundet auch das Zusammenhangsmaße (Phi=0,211; p<0,01).

[99] Wie in Tabelle 17 bereits gezeigt wurden, verfügen nur sehr wenige über ein geringes Wissen, so dass praktisch mittleres Wissen, hohem Wissen gegenüber gestellt wird.
[100] Für 72% der befragten Personen.

7.4.3. Verunsicherung

Durch Überwachung werden Informationen über BürgerInnen generiert. Dadurch entstehen unterschiedliche Machtverhältnisse, denn wer Informationen besitzt, besitzt auch Macht. Macht bedeutet allerdings auch Kontrolle. Die Frage dahinter lautet nun, *ob Überwachung zu einem Kontrollverlust und somit zur Verunsicherung führt, anstatt des angestrebten Sicherheitsgefühls*. Kontrollverlust ist hier in jenem Sinne zu verstehen, dass das Individuum nur noch indirekt bis kaum einen Einfluss darüber erhält, wem es welche Informationen zuteilwerden lässt. Untenstehende Tabelle zeigt die Verteilung des Besorgnisses innerhalb der Wiener Bevölkerung aufgrund vorgestellter Überwachungsmaßnahmen.

Tabelle 24 Besorgnis innerhalb der Bevölkerung bezüglich Überwachungsmaßnahmen gerundet in %

Institutionen	*Ein wenig bis sehr besorgt*	*Kaum bis überhaupt nicht besorgt*	$\bar{x}$	σ
GPS Ortungen	48%	52%	2,41	0,915
Vorratsdatenspeicherung	61%	39%	2,72	0,884
Kundenprofile	51%	49%	2,47	0,939
Risikomanagement	58%	42%	2,75	0,908
Kommerzielle Zwecke	58%	42%	2,68	0,928
Google	**68%**	32%	2,94	0,880
Google Street View	59%	41%	2,80	0,877
Zunehmende Videoüberwachung	45%	**55%**	2,40	0,933
Lückenloser werdende Videoüberwachung	64%	**56%**	2,41	0,925
Einführung von Nacktscannern	45%	**55%**	2,44	0,843
Online Durchsuchungen	57%	43%	2,77	0,921
Lausch- und Abhörservice	**66%**	34%	2,83	0,897

Am Meisten von allen genannten Überwachungsmaßnahmen, fürchten die Wiener und Wienerinnen zu 68% die Suchmaschine Google, welche jede jemals eingegebene Suchanfrage mit der dazugehörigen IP-Adresse speichert. Auf dem zweiten Rang platzieren die befragten Probanden zu 66% den Lausch- und Abhörservice der Polizei. Am wenigsten Sorgen bereiten der Bevölkerung die immer lückenloser werdende Videoüberwachung (56%), sowie die Einführung von Nacktscannern (55%).

Die Faktorenanalyse extrahierte aus den Variablen der Fragenbogennummernserie sieben, einen Faktor[101], welcher in „Verunsicherung“ benannt wurde. Die dazu verwendeten Items sind in nachfolgender Tabelle ersichtlich. Diese Einstellungsskala[102] misst den Grad der Besorgnis der befragten Probanden im Hinblick auf die verschiedenen Überwachungsmaßnahmen. Für 52% der Wiener Bevölkerung sind Überwachungsmaßnahmen nicht sonderlich besorgniserregend. 48% hingegen haben hinsichtlich dieser Überwachungsstrategien große Bedenken und Sorgen. Zusammenfassend lässt sich eine geteilte Meinung in der Wiener Bevölkerung feststellen, ob Überwachungsmaßnahmen, sobald diese der Öffentlichkeit präsentiert, sichtbar, gemacht werden, Verunsicherung statt Sicherheit, auslösen. Demgegenüber herrscht ein heterogenes Bild zu je knapp 50%.

[101] Erklärt 44,11% der Varianz.
[102] α=0,825.

Tabelle 25 Verwendete Items für Skalenkonstruktion Verunsicherung[103]

Fragebogenfragen	$\bar{x}$	σ
7.1 Geräte mit GPS Funktionen, wie z.B. Handys, Navigationsgeräte, ermöglichen eine Ortung des Aufenthaltes.	2,41	0,914
7.3 Anhand von Kundenkarten (z.B. Billa, Bipa,...) werden Kundenprofile erstellt, die für gezieltes Marketing genutzt werden.	2,47	0,941
7.5 Private Unternehmen, wie Autovermieter oder Telekom-Anbieter, speichern personenbezogene Daten und verarbeiten diese später für kommerzielle Zwecke.	2,68	0,927
7.7 Mit Google Street View werden Adressen bald in einer 360° Ansicht sichtbar, somit auch ihr Haus/ihre Wohnung, wenn sie dem nicht widersprechen.	2,80	0,878
7.11 Mögliche Online-Durchsuchungen staatlicher Stellen in Österreich.	2,76	0,922

Die Kreuztabellierung der beiden Skalen „Pro-Überwachung“ und „Verunsicherung“ ergab eine höchst signifikante Abhängigkeit zwischen diesen beiden Dimensionen (χ^2=50,863; df=6; p<0,001). All jene, welche Überwachungsmaßnahmen als besorgniserregend einstufen, lehnen diese zu 79% ab. Probanden, welche hingegen keine Sorgen aufgrund der mannigfaltigen Möglichkeiten zur Überwachung äußern, befürworten diese zu 61%. Phi(-0,399) bezeugt einen starken Zusammenhang auf höchst signifikantem Niveau (p<0,001). Daraus lässt sich schlussfolgern, dass je besorgniserregender Überwachungsmaßnahmen wahrgenommen werden, aufgrund dessen die Akzeptanz jener Strategien sinkt.

[103] Antwortskala bezüglich der Besorgtheit im Bezug auf folgende Tatsachen von 1 bis 4, wobei 1 = überhaupt nicht besorgt; 4 = sehr besorgt.

Tabelle 26 Kreuztabellierung Verunsicherung * Pro-Überwachung gerundet in %

			Verunsicherung		Gesamt
			Nein	*Ja*	
Pro-Überwachung	Nein	Anzahl	65	122	187
		% innerhalb von Verunsicherung	**39%**	**79%**	58%
	Ja	Anzahl	100	33	133
		% innerhalb von Verunsicherung	**61%**	**21%**	42%
Gesamt	Anzahl		165	155	320
	% innerhalb von Verunsicherung		100%	100%	100%

7.4.4. Akzeptanz von Überwachung nach Geschlecht

Die Zusatzhypothese dass die Befürwortung von Überwachungsmaßnahmen geschlechtsspezifische Unterschiede aufweisen würde, musste aufgrund nicht signifikanter Ergebnisse verworfen werden (siehe Tabelle 38 im Anhang). Das Geschlecht der befragten WienerInnen übt keinen Einfluss auf die Akzeptanz der Überwachung aus.

7.4.5. Akzeptanz von Überwachung nach Alter

Eine weitere Zusatzhypothese unterstellte einen Zusammenhang zwischen Alter der Probanden und Zustimmung zur Überwachung, doch auch hier konnten keine altersspezifischen Besonderheiten aufgedeckt werden (siehe Tabelle 39 im Anhang).

7.4.6. Befürwortung von Überwachung als Verbrechensopfer

Bei einer weiteren Zusatzhypothese wurde unterstellt, dass *Personen, welche öfter Verbrechen ausgesetzt waren als andere, sich vermutlich vermehrt für Überwachungsmaßnahmen aussprechen werden, da das Erinnern an die Verbrechen, eine Angst vor Devianz schürt, die mittels Überwachung kompensiert wird.* Dies bedeutet, dass die Zustimmung zu Überwachungsmaßnahmen mit der Opferhäufigkeit steigt. Abgefragte Verbrechensarten waren Diebstahl, Raub, Einbruch, Überfall, Körperverletzung, Nötigung, Erpressung und Stalking. Die Kategorie „Sonstiges“ wurde von keinem der Probanden zur Anführung weiterer Verbrechensformen genutzt.37% der befragten Personen gaben an, noch nie Opfer eines Verbrechens gewesen zu sein. Knapp $^{1}/_{3}$, nämlich 26%, sind schon Opfer eines Verbrechens geworden. 23% geben an, Opfer zweier Verbrechen gewesen zu sein. 14% sind schon drei oder mehrere Verbrechen widerfahren (siehe Tabelle 40). Insgesamt fielen 63% der Wiener Bevölkerung einem oder mehrerer Verbrechen zu Opfer.

Tabelle 27 Opferanzahl der befragten Probanden gerundet in % nach Verbrechenshäufigkeit

	Anzahl	%
Noch nie Opfer eines Verbrechens	120	37
Opfer eines Verbrechens	85	26
Opfer zweier Verbrechen	75	23
Opfer dreier oder mehrerer Verbrechen	44	14
Gesamt	324	100

Es wurde ebenfalls danach gefragt, wie oft Familienangehörige und Verwandte Opfer eines oder mehrerer Verbrechen wurden, da dies auch einen Einfluss zur Akzeptanz der Überwachungsmaßnahmen haben könnte (siehe Tabelle 28). Genauso wie die Tatsache, dass Freunde und Bekannte Leittragende krimineller Handlungen wurden (siehe Tabelle 29).

Tabelle 28 Familienangehörige und Verwandte der Probanden welche Opfer eines oder mehrerer Verbrechen wurden gerundet in %

	Anzahl	%
Noch nie Opfer eines Verbrechens	127	39
Opfer eines Verbrechens	102	32
Opfer zweier Verbrechen	60	19
Opfer drei oder mehrerer Verbrechen	35	11
Gesamt	324	100

Die Mehrheit der Familienangehörigen und Verwandten der Probanden fiel zu 39% noch nie einem Verbrechen zu Opfer. Freunde und Bekannte der befragten Personen wurden jedoch zu 41% Leittragende eines Verbrechens.

Tabelle 29 Freunde und Bekannte der Probanden welche einem oder mehrerer Verbrechen zu Opfer fielen gerundet in %

		Anzahl	%
Noch nie Opfer eines Verbrechens		94	29
Opfer eines Verbrechens		133	41
Opfer zweier Verbrechen		65	20
Opfer drei oder mehrerer Verbrechen		31	10
Gesamt		323	100
Fehlend	**System**	1	
Gesamt		324	

Tabelle 30 Kreuztabellierung Probanden Opfer eines oder mehrerer Verbrechen * Pro-Überwachung in %

			Probanden Opfer eines oder mehrerer Verbrechen		Gesamt
			Nein	*Ja*	
Pro-Überwachung	*Nein*	*Anzahl*	62	125	187
		% innerhalb von Probanden Opfer eines oder mehrerer Verbrechen	52%	63%	58%
	Ja	*Anzahl*	58	75	133
		% innerhalb Probanden Opfer eines oder mehrerer Verbrechen	**48%**	**38%**	42%
Gesamt		*Anzahl*	120	200	320
		% innerhalb von Probanden Opfer eines oder mehrerer Verbrechen	100%	100%	100%

Hier zeigt sich, anders als erwartet, dass Personen, welche noch nie Opfer eines Verbrechens wurden, zu 48% Überwachungsmaßnahmen begrüßen, anders als Personen, welche Leittragende einer oder mehrere krimineller Handlungen wurden, lehne diese zu 63% ab (χ^2=3,624; df=1; p<0,05).Der Zusammenhang ist allerdings nur schwach signifikant. Eine mögliche Erklärung könne darin liegen, dass der Sinn und Zweck von Überwachungsmaßnahmen in erster Linie dem Schutz vor kriminellen Handlungen dienen solle, Verbrechensopfer können diese aber nicht als Präventionsmittel empfinden (da sie sonst keinem Verbrechen zu Opfer gefallen wären) und somit keinen Nutzen in Überwachungsmaßnahmen sehen (Phi= -0,106; p<0,05).

Die Kreuztabellierung der beiden Indizes, dass entweder Familie und/oder Verwandte Opfer von Verbrechen wurden, bzw., dass Freunde und/oder Bekannte, Opfer von Verbrechen wurden, mit der Zustimmung zu Überwachungsmaßnahmen, lieferte in keinem der beiden Fälle signifikante Zusammenhänge, woraus sich ableiten lässt, dass die Tatsache, dass nahestehende Personen Leittragende einer oder mehrerer krimineller Handlungen wurden, keinen Einfluss auf die Zustimmung bzw. die Ablehnung bezüglich Überwachungsmaßnahmen einnimmt.

7.4.7. Befürwortung von Überwachung nach politischer Anschauung

Auf die Frage hin, wie sich die befragten Personen auf einer Skala von Eins (sehr links) bis Zehn (sehr rechts) einstufen würden, gaben am Häufigsten mit 38% der befragten Personen den Wert Fünf an, welcher eventuell als die neutrale Mitte verstanden wurde, wobei bei einer

10er Skala keine Mitte existiert, da die beiden Kategorien 5 und 6 das Zentrum bilden. Die Abbildung veranschaulicht, dass sich mehr als die Hälfte im mittleren Bereich um die Werte 4 bis 6 aufteilt und das zu den beiden Enden der Skala (1 und 10) die Prozentwerte abnehmen.

Folgende Abbildung beleuchtet eine Abhängigkeit zwischen politischer Einstellung und höchster abgeschlossener Schulbildung. Personen mit einem Matura oder Hochschulabschluss orientieren sich politisch eher im neutralen (44%), sowie im linken Bereich (45%). Probanden ohne Maturaabschluss ordnen sich zu 63% der politisch neutralen Domäne zu (χ^2=15,592; df=2; p<0,001). Diesen ansehnliche Beziehung auf höchst signifikantem Niveau bestätigt auch das Korrelationsmaß (Phi=0,225; p<0,001).

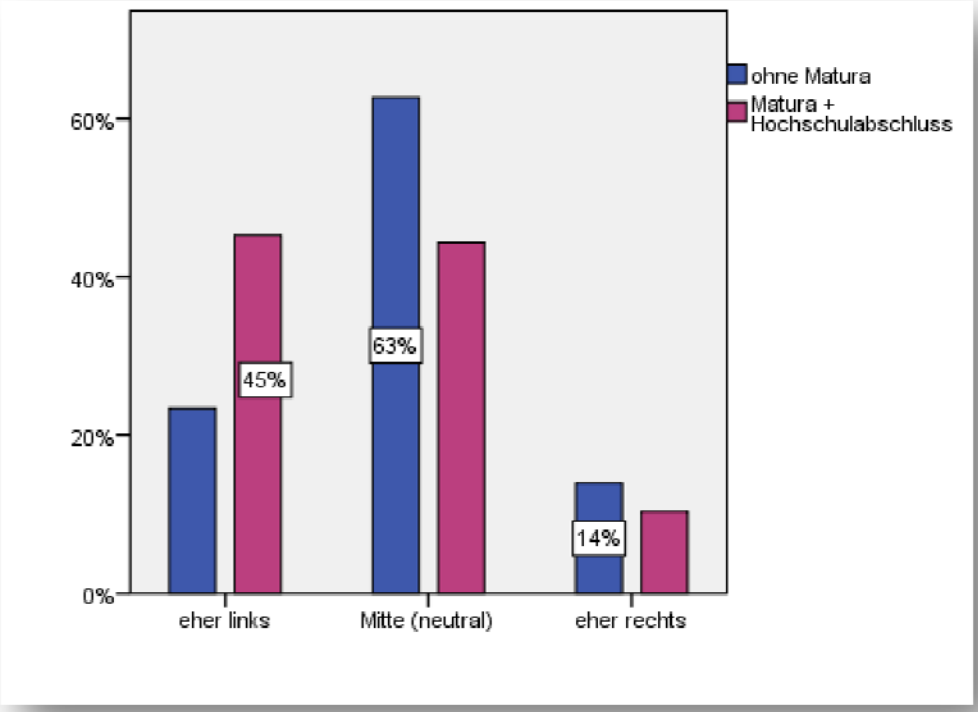


Abbildung 9 Politikskala nach höchster abgeschlossener Schulbildung[104] in %

Die vierte Zusatzhypothese postulierte eine Abhängigkeit zwischen der politischen Anschauung der Probanden und der Befürwortung von Überwachungsmaßnahmen. Allerdings konnte diese Hypothese, dass die politische Anschauung der Probanden einen

[104]Es wurden Personen mit Matura + Hochschule zusammengefasst und den Personen mit niedriger Bildung gegenüber gestellt.

Einfluss auf die Befürwortung von Überwachungsmaßnahmen ausübe, nicht bestätigt werden. Bei einer Kreuztabellierung dieser beiden Variablen wurden keine zufriedenstellenden und signifikanten Ergebnisse erzielt (siehe Tabelle 37 im Anhang).

7.4.8. Akzeptanz von Überwachung nach Institutionenvertrauen

Die fünfte Zusatzhypothese besagt, dass *je geringer das Vertrauen in den Staat und seine Institutionen, desto größer ist auch die Ablehnung gegenüber Überwachungssystemen.*

Tabelle 31 Kreuztabellierung Vertrauen in staatliche Institutionen * Pro-Überwachung gerundet in %

			Vertrauen in staatliche Institutionen		Gesamt
			Niedrig	*Hoch*	
Pro-Überwachung	*Nein*	*Anzahl*	123	64	187
		% innerhalb von Vertrauen in staatliche Institutionen	69%	45%	58%
	Ja	*Anzahl*	56	77	133
		% innerhalb von Vertrauen in staatliche Institutionen	**31%**	**55%**	42%
Gesamt		*Anzahl*	179	141	320
		% innerhalb von Vertrauen in staatliche Institutionen	100%	100%	100%

Erkenntlich ist auf den ersten Blick, dass die Zustimmung bzw. die Akzeptanz von Überwachungsmaßnahmen vom Vertrauen in staatliche Institutionen abhängt. Personen, welche staatlichen Institutionen, wie der österreichischen Regierung, dem Parlament, der Polizei und der Justiz, ein hohes Vertrauen entgegen bringen, befürworten zu 55% Überwachungsmaßnahmen und lehnen diese nur zu 31% ab. Probanden, welche hingegen ein niedriges Vertrauen in staatliche Institutionen setzen, lehne zu 69% Überwachungstechniken ab, sprich fast jede(r) 7te WienerIn (χ^2=17,667; df=1; p<0,001). Diesen Zusammenhang hebt auch das Korrelationsmaß auf höchst signifikantem Niveau hervor (Phi=0,235; p<0,001).

Tabelle 32 Kreuztabellierung Vertrauen in intermediäre Institutionen * Pro-Überwachung gerundet in %

			Vertrauen in intermediäre Institutionen		Gesamt
			niedrig	*Hoch*	
Pro-Überwachung	*Nein*	*Anzahl*	110	76	186
		% innerhalb von Vertrauen in intermediäre Institutionen	63%	52%	58%
	Ja	*Anzahl*	64	69	133
		% innerhalb von Vertrauen in intermediäre Institutionen	**37%**	**48%**	42%
Gesamt		*Anzahl*	174	145	319
		% innerhalb von Vertrauen in intermediäre Institutionen	100%	100%	100%

Ähnlich wirkt sich auch das Vertrauen in intermediäre Institutionen aus. Personen, welche intermediären Institutionen ein hohes Vertrauen entgegen bringen, befürworten zu 48% Überwachungsmaßnahmen und lehnen diese zu 37% ab. Probanden, welche hingegen ein niedriges Vertrauen in private Institutionen setzen, lehne diese zu 63% ab (χ^2=3,798; df= 1; p<0,05). Diesen Zusammenhang bestätigt auch das Korrelationsmaß auf höchst signifikantem Niveau (Phi=0,109; p<0,05).

Tabelle 33 Kreuztabellierung Vertrauen in private Institutionen * Pro-Überwachung gerundet in %

			Vertrauen in private Institutionen		Gesamt
			niedrig	*Hoch*	
Pro-Überwachung	*Nein*	*Anzahl*	148	39	187
		% innerhalb von Vertrauen in private Institutionen	64%	44%	58%
	Ja	*Anzahl*	83	50	133
		% innerhalb von Vertrauen in private Institutionen	**36%**	**56%**	42%
Gesamt		*Anzahl*	231	89	320
		% innerhalb von Vertrauen in private Institutionen	100%	100%	100%

Auch die Befürwortung von Überwachungsmaßnahmen ist vom Vertrauen in private Institutionen abhängig. Personen, welche privaten Institutionen, wie privaten Unternehmen, sowie privaten Versicherungen, ein hohes Vertrauen entgegen bringen, befürworten zu 56% Überwachungsmaßnahmen und lehnen diese zu 36% ab. Probanden, welche hingegen ein niedriges Vertrauen in private Institutionen setzen, lehne zu 64% Überwachungstechniken ab (χ^2=10,846; df=1; p<0,001). Diesen Zusammenhang bestätigt auch das Korrelationsmaß auf höchst signifikantem Niveau (Phi=0,184; p<0,001).

Zusammenfassend lässt sich sagen, dass das Vertrauen einen signifikanten Einfluss auf die Befürwortung von Überwachungsmaßnahmen ausübt. Je größer das Vertrauen in die österreichischen Institutionen, desto größer ist auch die Bereitschaft der Wiener Bevölkerung Überwachungsmaßnahmen zu akzeptieren. Allerdings genießen die Institutionen in Österreich bei den Wienern und Wienerinnen kein besonders hohes Vertrauen. Am Schlechtesten schneiden zusammengefasst private Institutionen ab, inklusive Glaubenseinrichtungen. Nichtsdestotrotz konnte die Hypothese, *je geringer das Vertrauen in den Staat und seine Institutionen, desto größer ist auch die Ablehnung gegenüber Überwachungssystemen*, bestätigt werden.

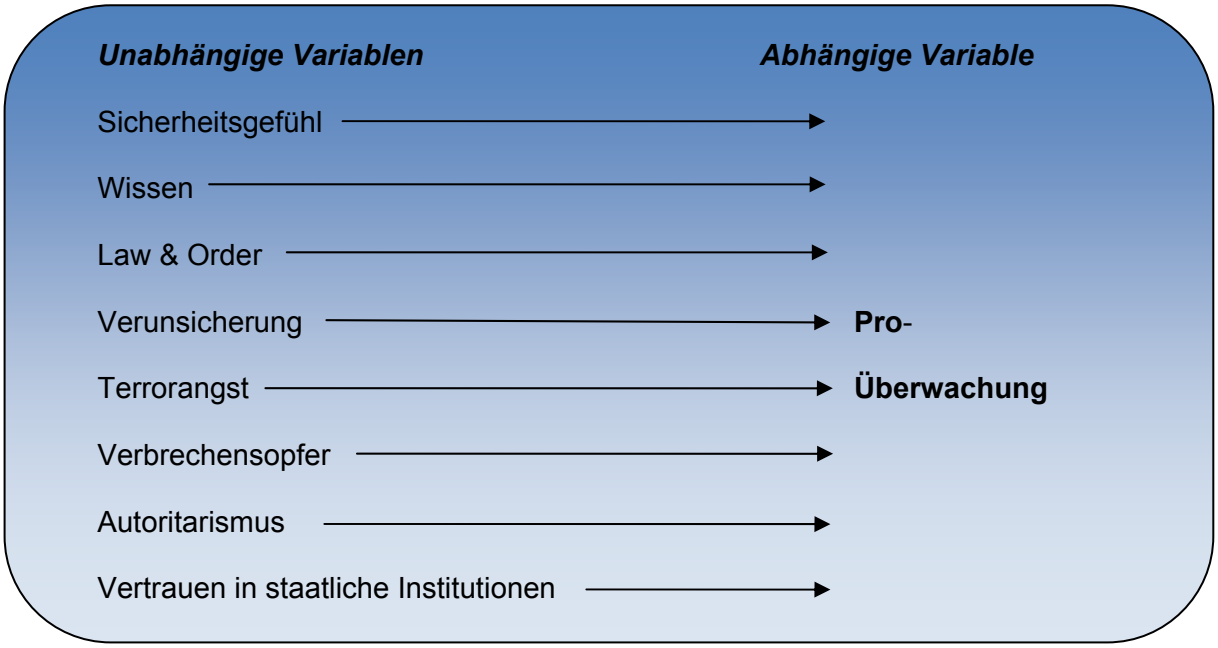
7.4.9. Zentrale Einflüsse (Regressionsanalyse)

> *„In der **multiplen Regressionsanalyse** wird der gerichtete Einfluss **mehrerer** unabhängiger Variablen auf eine abhängige Variable untersucht.“* (Diaz-Bone 2006: 185)

Mithilfe der multiplen Regressionsanalyse[105] sollte der Einfluss mehrere unabhängiger Variablen auf eine abhängige Variable untersucht werden (siehe Abbildung 10). Es wurde getestet, welche Dimensionen die Akzeptanz von Überwachungsmaßnahmen beeinflussen. Was sind die Hauptgründe, dass Probanden einer Observation ihrer Tätigkeiten zustimmen? Mögliche Einflussvariablen wurden in folgender Abbildung dargestellt.

[105] Schrittweise

Abbildung 10 Darstellung der Einflussvariablen in der multiplen Regressionsanalyse



Eine zunächst durchgeführte Korrelationsanalyse, welche Aufschluss über mögliche Beziehungen zwischen den Items liefern sollte, ergab folgendes Ergebnis.

Tabelle 34 Korrelationsanalyse metrischer Variablen nach Pearson, Signifikanz (2-seitig)

	Pro-Überwachung
Vertrauen in staatliche Institutionen	**,317**
	,000
Sicherheitsgefühl	**,636**
	,000
Verunsicherung	**-,448**
	,000
Autoritarismus	**,231**
	,000
Verbrechensopfer	-,085
	,128
Terrorangst	,001
	,983
Law & Order	,095
	,091
Wissen	**-,248**
	,000
Höchste abgeschlossene Schulbildung	-,104
	,067
Position im Hauptberuf	,025
	,729
Persönliches Nettoeinkommen	,010
	,860

Die Korrelationsanalyse ergab, dass das Sicherheitsgefühl am Stärksten mit der Akzeptanz von Überwachungsmaßnahmen korreliert (r=0,636; p<0,001). Diese beiden Themenaspekte hängen dicht miteinander zusammen, wie dies bereits auch aus der Literatur ersichtlich wurde. Am zweit stärksten korrelieren Verunsicherung und die Befürwortung von Überwachungsmaßnahmen, jedoch ist ihre Beziehung negativ, wonach wenn das eine Item zunimmt, in Folge dessen das andere abnimmt (r=-0,448; p<0,001). Eine möglich Annahme wäre, dass wenn die Verunsicherung zunimmt, die Bereitschaft der Probanden zur Akzeptanz der Überwachungsmaßnahmen abnimmt. Des Weiteren besteht eine Wechselbeziehung, mittlerer Stärke, zwischen Vertrauen in staatliche Institutionen und der Akzeptanz von Überwachung, sowohl als auch zwischen Wissen und Überwachung und Autoritarismus und Überwachung.

Im Zuge der multiplen Regressionsanalyse wurden das Sicherheitsgefühl, die Verunsicherung und das Vertrauen in staatliche Institutionen in das Modell aufgenommen. Dieses Ergebnis stimmt mit jenem der Korrelationsanalyse überein.

Tabelle 35 Modellzusammenfassung multiple Regressionsanalyse

Modell	R	R^2	Korrigiertes R^2	Standardfehler des Schätzers	Änderungsstatistiken				
					Änderung in R^2	*Änderung in F*	*df1*	*df2*	*Sig. Änderung in F*
1	,636[a]	,405	,403	2,265	,405	211,280	1	311	,000
2	,689[b]	,475	,472	2,130	,071	41,783	1	310	,000
3	**,694[c]**	,482	,477	2,120	,007	3,877	1	309	**,050**

a. Einflussvariablen : (Konstante), Sicherheitsgefühl

b. Einflussvariablen : (Konstante), Sicherheitsgefühl, Verunsicherung

c. Einflussvariablen : (Konstante), Sicherheitsgefühl, Verunsicherung, Vertrauen in staatliche Institutionen

Wie bereits aus der Modellzusammenfassung ersichtlich, sind die größten Einflussvariablen auf die Akzeptanz der Überwachung seitens der Bevölkerung, das Sicherheitsgefühl, die Verunsicherung und das Vertrauen in staatliche Institutionen ($p \geq 0{,}05$). R^2 verändert sich spürbar durch die Aufnahme des zweiten Items „Verunsicherung“ in das Model um 0,071. Die Hinzunahme des dritten Items „Vertrauen in staatliche Institutionen“ bewirkt nur mäßige Veränderung in R^2 (0,007), nichtsdestotrotz sind diese weiterhin signifikant. Eine multiple Regressionsanalyse mit den demographischen Merkmalen Bildung, Einkommen und Beruf lieferte keine signifikanten Ergebnisse, wonach daraus geschlossen werden kann, dass die Demographie einer Person keinen bedeutsamen Einfluss auf die Zustimmung zur Überwachung ausübt. Wie bereits bei der Zusatzhypothesentestung dargestellt wurde, ergeben sich des Weiteren auch keine geschlechts-, sowie altersspezifischen Unterschiede in Bezug auf die Akzeptanz von Überwachungsmaßnahme. Die Angst vor terroristischen Angriffen radikaler Gruppen, sowie der Wissensstand der Probanden, ob diese nun gut informiert sind oder nicht, spielt keine Relevanz bei der Entscheidung für oder gegen Überwachungsmaßnahmen. Auch das Item „Law & Order“ spiegelt keinerlei Einwirkung auf die Zustimmung wieder. Ob die befragten Personen dem Staat mehr Macht und Einfluss auf das öffentliche Leben der BürgerInnen zusprechen würden oder nicht, übt keinerlei Einfluss auf die Akzeptanz oder Befürwortung von Überwachungsmaßnahmen aus.

Tabelle 36 Koeffizienten (abhängige Variable: Pro-Überwachung)

Modell		Nicht standardisierte Koeffizienten		Standardisierte Koeffizienten	T	Sig.
		Regressionskoeffizient B	*Standardfehler*	*Beta*		
1	*(Konstante)*	8,025	,556		14,423	,000
	Sicherheitsgefühl	,787	,054	,636	14,535	,000
2	*(Konstante)*	12,039	,812		14,827	,000
	Sicherheitsgefühl	,689	,053	,557	12,963	,000
	Verunsicherung	-,231	,036	-,278	-6,464	,000
3	*(Konstante)*	10,959	,977		11,218	,000
	Sicherheitsgefühl	,664	,054	,537	12,214	,000
	Verunsicherung	-,223	,036	-,267	-6,204	,000
	Vertrauen in staatliche Institutionen	,096	,049	,084	1,969	,050

Aus dieser Tabelle ist ersichtlich, dass das Sicherheitsgefühl, die Verunsicherung, sowohl als auch das Vertrauen in staatliche Institutionen den größten Einfluss auf die Akzeptanz von Überwachungsmaßnahmen ausüben ($p \leq 0,05$). Dies bedeutet, dass sobald Überwachungsmaßnahmen zu einem gesteigerten Sicherheitsgefühl beitragen, Verunsicherung reduzieren und ein hohes Vertrauen in die Regierung gegeben ist, diese Strategien zur Observation der BürgerInnen von der Bevölkerung auch akzeptiert werden. Es kann davon ausgegangen werden, dass die befragten Probanden aufgrund wünschenswerter Leistungen, wie beispielsweise ein erhöhtes Sicherheitsgefühl, sich bereit erklären, Einbußen bezüglich der Privatsphäre zu erdulden.

8. Resumée

Was man zu verstehen gelernt hat,

fürchtet man nicht mehr.
(Marie Curie[106])

Zusammenfassend lieferte die empirische Studie, dass für 95% aller Wiener und Wienerinnen das Thema „Überwachung & Datenschutz“ wichtig sei. Diesbezüglich ergaben sich altersspezifische Unterschiede, wonach die Wichtigkeit dieser Thematik mit dem Alter der Probanden steigt. Signifikante Zusammenhänge ergaben sich des Weiteren auch im Bezug auf die besorgniserregende Wirkung von Überwachungsmaßnahmen. Für Personen, welche das Thema „Überwachung & Datenschutz“ keine besonders hohe Wichtigkeit einnimmt, erscheinen auch Überwachungsmaßnahmen als nicht besonders besorgniserregend. Ein mögliches „Regierungsarmband“ würde mehr als die Hälfte der Bevölkerung (69%) ablehnen, wonach dieses dem Staat vier Funktionen zur Überwachung seiner Bürger bieten würde, wie die ständige Lokalisierung des Aufenthaltsortes des Probanden, das Erfassen sämtlicher erhaltener Nachtrichten, die Protokollierung des gesamten Telefonverkehrs, sowie das Abhören der geführten Gespräche, selbst wenn damit Vermisste gefunden, Verbrechen aufgeklärt und der Terrorismus dadurch besser bekämpft werden könnte. Ein Viertel aller Wiener und Wienerinnen würden jedoch die ständige Lokalisierung auf einer Landkarte akzeptieren.

57% der Bevölkerung wünschen sich keinen größeren Einfluss und mehr Kontrolle des Staates auf das öffentliche Leben der BürgerInnen zur Gewährleistung von Ordnung und Moral, 43% hingegen schon. Knapp jeder dritte Proband und jede dritte Probandin (28%) sehen eine erhöhte Wahrscheinlichkeit Opfer eines terroristischen Anschlages in Österreich zu werden. 62% geben an, Überwachungsmaßnahmen steigern das subjektive Sicherheitsgefühl. Des Weitern sprechen sich 58% für Überwachungsmaßnahmen aus. Die Hypothese, dass Probanden, welche Überwachungsmaßnahmen zustimmen, sich durch diese auch sicherer fühlen (61%), konnte bestätigt werden.

Das Vertrauen der Wiener Bevölkerung in staatliche Institutionen ist zu 44% hoch, in intermediäre Institutionen zu 45%. Privaten Institutionen wird zu 73% ein niedriges Vertrauen entgegen gebracht. Am schlechtesten schneiden die Glaubenseinrichtungen ab, welchen zu 70% ein geringes bis kein Vertrauen seitens der Bevölkerung erhalten. Das beste Ergebnis

[106] www.sevillana.de

erzielte das Gesundheitssystem in Österreich. Wiener und Wienerinnen hegen zu 64% ein großes bis sehr großes Vertrauen in diese Einrichtung. Personen, welche staatlichen Institutionen ein hohes Vertrauen entgegenbringen, befürworten vermehrt Observationsmaßnahmen, als jene, welche ein niedrigeres Vertrauen in den Staat und seine Institutionen setzen. Gleiches gilt sowohl für das Vertrauen in intermediäre, wie auch in private Institutionen. Somit übt das Vertrauen in die unterschiedlichsten Institutionen einen bedeutsamen Einfluss auf die Befürwortung von Überwachungsmaßnahmen aus.

Die Überprüfung des Wissenstandes der Probanden zur Thematik Überwachungsmaßnahmen ergab, dass mehr als die Hälfte (60%) über ein mittleres Wissen verfügt. Knapp die Hälfte, 40%, haben sogar ein solides hohes Wissen diesbezüglich. Kaum jemand hat ein niedriges Wissen, wonach daraus schlussgefolgert werden kann, dass die Wiener Bevölkerung gut bis sehr gut über die mannigfaltigen Möglichkeiten zur Observation der BürgerInnen Bescheid weiß. Eine Kreuztabellierung des Wissenstandes mit der Ausbildung einer Person lieferte das Ergebnis, dass das Wissen mit der Höhe des Abschlusses zunimmt. Die Überprüfung der Hypothese der Abhängigkeit zwischen dem Wissensstand, dem Vertrauen in staatliche Institutionen und dem subjektiven Sicherheitsgefühl, führte zu der Einsicht, dass je niedriger der Wissensstand und je geringer das Vertrauen, desto niedriger ist aufgrund dessen das subjektiv empfundene Sicherheitsgefühl der Probanden. 48% der befragten Personen vertreten die Annahme, Überwachungsmaßnahmen lösen vermehrt Verunsicherung, anstatt des eigentlich angestrebten Sicherheitsgefühls hervor. Doch 52% empfinden Techniken zur Überwachung der BürgerInnen als nicht besorgniserregend.

Die Annahme, wonach Probanden vermehrt Überwachungsmaßnahmen zustimmen, welche schon einmal Opfer eines oder mehrerer Verbrechen wurden, konnte nicht bewiesen werden. Anders als erwartet, begrüßen vermehrt Personen Überwachungsstrategien, welche noch nie Leittragende einer kriminellen Tat wurden.

Die Regressionsanalyse führte zu dem Ergebnis, dass die Akzeptanz zur Überwachungsmaßnahmen innerhalb der Bevölkerung in erster Linie vom Sicherheitsgefühl, in zweiter Linie von der Verunsicherung und in dritter Linie, vom Vertrauen in staatliche Institutionen abhängig ist. Die Demographie, wie das Alter oder das Geschlecht der befragten Personen, wie deren Ausbildung, der Beruf und das Einkommen haben keinerlei Wirkung auf die Befürwortung von Überwachungstechniken. Ebenfalls wirken, wenn auch nur schwach, der Wissensstand der Probanden, sowie die Bereitschaft der Bevölkerung zu

einer autoritäreren Staatsmacht schwach auf die Zustimmung zu observationsähnlichen Maßnahmen. Die Angst vor Terrorismus, sowohl als auch die Tatsache, ob Personen schon einmal ein oder mehrere Verbrechen zuteil wurden, wie die Bereitwilligkeit zu mehr Kontrolle des Staates, üben keinerlei Einfluss auf die Befürwortung von Überwachungsmaßnahme aus. Summa summarum lässt sich festhalten, dass eine Akzeptanz von Überwachung innerhalb der Bevölkerung am Stärksten unter dem Aspekt „Sicherheit“ vorangetrieben werden kann. Es kann davon ausgegangen werden, dass Wiener und Wienerinnen sich im Zuge einer Überwachungsgesellschaft bereit erklären, Einbußen der eigenen Privatsphäre im Gegenzug für eine erhöhte Sicherheit zu erdulden. Doch heutzutage birgt schon das Verlassen des Hauses hohe Risiken: sei es ein Terroranschlag feindseliger Truppen, ein Entgleisen der U-Bahn, oder sei es ein durchdrehender Amokläufer, der unerwartet eine Pistole aus seiner Jackentasche zieht, was selten aber überall und jederzeit passieren kann. Nur was wollen Staat und Politik gegen das zuletzt genannte Beispiel unternehmen?

Um uns vor Terrorismus und Kriminalität zu schützen, werden alle erdenklichen Daten, unter dem Vorwand Sicherheit herstellen zu wollen - sie gar garantieren zu wollen, auf Vorrat gespeichert, verarbeitet und ausgewertet. Nur wie wollen Staat und Politik gegen psychosoziale Aussetzer vorgehen. Ein plötzlicher unkontrollierbarer Gefühlsausbruch könnte möglicherweise das Leben unzähliger Menschen kosten. Sollten wir uns unter diesen Umständen nicht sicherheitshalber einen Chip implantieren lassen, welcher jederzeit und jederorts den Gefühlszustand misst, sowie sonstige gesundheitlich relevanten Daten erfasst, speichert und verarbeitet, um einerseits so die Sicherheit vor Amokläufen zu erhöhen, sowie die subjektive Gesundheit zu fördern und/oder einen höheren Lebensstandard zu garantieren? Wer würde da noch Nein sagen?

Sie?

Völlig außer Acht gelassen wird die Tatsache, dass die Sammlung der Daten nicht ausschließlich auf der Grundlage von Sicherheit geschieht, welche ohne Zweifel nicht einfach so hergestellt oder gar gesichert werden kann. Der eigentliche Grund der Datensammlung, Datenverarbeitung und Datenspeicherung, ist die Kontrollierbarkeit der Geschehnisse und somit deren Berechenbarkeit und in gewissem Grade dadurch deren Manipulation. Selbst in totalitären Staaten ist es schlichtwegunmöglich Sicherheit durch Überwachung zu garantieren. Im Grunde lässt sich Sicherheit durch nichts und niemanden zu 100% garantieren, da ja Sicherheit an sich als etwas Relatives und nicht als etwas

Absolutes anzusehen ist (vgl. Luhmann 2003: 28). Es steht außer Frage jedes Risiko kalkulierbar machen zu können.

Schlussendlich ist Risiko nicht „das“, was das Leben ausmacht? Warum sonst setzen sich Individuen gezielt einem Adrenalinkick[107] aus, wie beispielsweise Fallschirmspringen? Wohl gemerkt, dass Fallschirmspringen nicht jedermanns („jederfraus[108]“) Sache ist.

Der springende Punkt ist, dass die Menschheit wohl nie im Stande sein wird, in die Zukunft zu blicken und schon im Vorfeld ungewollte Geschehnisse einzudämmen. Der Aspekt der Sicherheit ist weder simple herstellbar noch garantierbar. Dieser Tatsache gilt es in die Augen zu sehen. Wie bereits erwähnt, weißt jede Medaille zwei Seiten auf, so auch die Überwachung. Wovor sich die Menschheit schützen muss, ist die Tendenz völliger Paranoia gegenüber allem und jedem. Hart erkämpfte Grundrechte der Freiheit dürfen einer totalitären Überwachung nicht weichen, welche wohlgemerkt nicht im Stande ist, jenes zu leisten, was sie verspricht.

[107] Adrenalin ist ein Hormon, welches in Stresssituationen in der Nebenniere gebildet und ins Blut ausgeschüttet wird. Seine Wirkung war von besonderer Wichtigkeit für unsere Vorfahren. Durch die Freisetzung von Adrenalin gelangt der Körper schneller an seine Energiereserven, was ihn wiederum zu Höchstleistungen antreibt (vgl. Heinisch 2011).
[108] Im Sinne einer geschlechtsneutralen Sprache.

9. Quellenangabe

- ✓ **ADLER**, Martin: Management Mitarbeitergespräch und Führungstechniken - Vertrauen ist gut, Kontrolle ist besser? http://www.martin-adler.org/TI/FUH/VertrauenIstGutKontrolleIst Besser.htm, 07.10.2011.
- ✓ **ALBRECHT**, Hans-Jörg, 2008: Kosten und Nutzen technisierter Überwachung. In: Gaycken, Sandro; Kurz, Constanze (Hg.), 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologie. Bielefeld: transcript Verlag, 129-147.
- ✓ **ARGEDATEN**, 2002: Schaffung geeigneter Regelungen zur Videoverwendung (Aufzeichnung/Überwachung) und zur Biometrie. http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=64742izc, 18.02.2012.
- ✓ **ARGEDATEN**, 2006: EG-Richtlinie 2006/24/EG - VORRATSDATENSPEICHERUNG von EU beschlossen. http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=11563vpp, 03.10.2010.
- ✓ **ARGEDATEN**, 2009: Großer Lauschangriff und Co – Das Konzept ist offenbar gescheitert. http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=05364auv, 01.03.2012.
- ✓ **ARGEDATEN**, 2010: Darf zum Eigentumsschutz mittels Video überwacht werden?http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=89079api, 23.02.2012.
- ✓ **BALL**, Kirstie; **WOOD**, Murakami David, 2006: Ein Bericht zur Überwachungsgesellschaft. Für den Datenschutzbeauftragten. Vom Surveillance Studies Network. http://www.privacyconference2006.co.uk/files/report_ger.pdf, 20.02.2012.
- ✓ **BECKER**, Matthias, 2010: Datenschatten. Auf dem Weg in die Überwachungsgesellschaft? Hannover: Heise Zeitschriften Verlag GmbH & Co KG.
- ✓ **BESSER LÄNGER LEBEN**, 2010: Generation 60 plus und das Internet.http://www.besserlaengerleben.at/dies-und-das/generation-60-plus-und-das-internet.html, 18.02.2012.
- ✓ **BIERMANN**, Benno; **BOCK-ROSENTHAL**, Erika; **DOEHLEMANN**, Martin; **GROHALL**, Karl-Heinz; **KÜHN**, Dietrich, 2006: Soziologie. Studienbuch für soziale Berufe. 5. Auflage. München: Reinhardt.

- ✓ **BIERMANN**, Kai, 2009: Datenschutz. Überwachung macht unsicher. http://www.zeit.de/online/2007/41/Datenschutz-Freiheit, 23.02.2012.
- ✓ **BIERMANN**, Kai, 2009: Überwachung. Indect – der Traum der EU vom Polizeistaat. http://www.zeit.de/digital/datenschutz/2009-09/indect-ueberwachung/seite-1, 26.03.2012.
- ✓ **BLUM**, Elisabeth, 2003 : Schöne neue Stadt. Wie der Sicherheitswahn die urbane Welt diszipliniert. Basel: Birkhäuser – Verlag für Architektur.
- ✓ **BUNDESKANZLERAMT**: Datenschutz. http://www.bka.gv.at/site/5808/default.aspx, 04.03.2012.
- ✓ **ČAS**, Johann, **PEISSL**, Walter, 2000: ITA. Beeinträchtigung der Privatsphäre in Österreich. Teil I Bestandsaufnahme: Datensammlung über ÖsterreicherInnen. http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a24.pdf, 13.02.2011.
- ✓ **CASTEL**, Robert, 2005: Die Stärkung des Sozialen. Leben im neuen Wohlfahrtsstaat. Hamburg: Hamburger Edition.
- ✓ **COMETO EDUHI**: Hintergrund: Überwachung in Österreich. Telefon, Video, Raster und Lauschen. http://cometo.eduhi.at/standings/Artikel%20IKT/Hintergrund%20-%20%C3%9Cberwachung%20in%20%C3%96sterreich%20(St,%2018.10.07).pdf, 27.02.2012.
- ✓ **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. Bielefeld: transcript Verlag, 47-52.
- ✓ **DANDEKER**, Christopher, 1990: Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day. New York: St. Martin´s Press.
- ✓ **DATENSCHUTZBERICHT**, 2009.https://www.dsk.gv.at/DocView.axd?CobId=40344, 23.02.2012.
- ✓ **DIAZ-BONE,** Rainer, 2006: Statistik für Soziologen. Konstanz: UVK Vertragsgesellschaft mbH.
- ✓ **DIE PRESSE**, 2007:EU-Experten: Speicherung von Verbindungsdaten "bedenklich“. http://diepresse.com/home/techscience/internet/sicherheit/305640/EUExperten_Datenspeicherung-bedenklich (18.02.2012).
- ✓ **DSK**: Österreichische Datenschutzkommission. Neue Entwicklungen betreffend Google Street View.https://www.dsk.gv.at/site/6733/default.aspx, 03.03.2012.

- ✓ **FAZ**, 2011: Aktuell. Gesellschaft. Kriminalität. London: Sechs Morde in zwei Wochen. http://www.faz.net/s/Rub77CAECAE94D7431F9EACD163751D4CFD/Doc~E42C690AC86B24953922C046182D1E891~ATpl~Ecommon~Scontent.html, 26.10.2010.
- ✓ **FAZ**, 2012:Google und der Datenschutz. Wer hier sucht, wird entmündigt. Artikel von 29.02.2012. http://www.faz.net/aktuell/feuilleton/google-und-der-datenschutz-wer-hier-sucht-wird-entmuendigt-11665354.html, 03.03.2012.
- ✓ **FOUCAULT**, Michel, 1976; 1994: Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt am Main: Suhrkamp.
- ✓ **FUTUREZONE**, 2011: Globaler Rückschritt der Bürgerrechte. Abbildung. http://futurezone.at/netzpolitik/6056-globaler-rueckschritt-der-buergerrechte.php, 25.02.2012.
- ✓ **GAYCKEN**, Sandro; **KURZ**, Constanze (Hg.), 2008: 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld: transcript Verlag.
- ✓ **GIDDENS**, Anthony, 1985: The Nation-State and Violence. Volume Two of A Contemporary Critique of Historical Materialism. Cambridge: Polity Press.
- ✓ **GILL**, Martin; **SPRIGGS**, Angela, 2005: Home Office Research Study 292. Assessing the impact of CCTV.http://webarchive.nationalarchives.gov.uk/20110218135832/http://rds.homeoffice.gov.uk/rds/pdfs05/hors292.pdf, 05.03.2012.
- ✓ **GOOGLE**, 2012: Datenschutzerklärung und Nutzungsprinzipien. http://www.google.com/intl/de/policies/privacy/, 03.03.2012.
- ✓ **GROHALL**, Karl-Heinz, 2006: Soziologie abweichenden Verhaltens und sozialer Kontrolle. In: Biermann, Benno; Bock-Rosenthal, Erika; Doehlemann, Martin; Grohall, Karl-Heinz; Kühn, Dietrich, Soziologie. Studienbuch für soziale Berufe. München: Reinhardt, 156-203.
- ✓ **GSPURNIG**, Stefan : Bezahlen mit dem Finger - Fiktion oder bald Realität. http://www.marketmentor.at/wissensbasis/2618-bezahlen-mit-dem-finger-fiktion-oder-bald-realitaet.html, 20.02.2012.
- ✓ **HAGGERTY**, Kevin D.; **ERICSON**, Richard, 2006: The new politics of surveillance and visibility. Toronto: University of Toronto Press.
- ✓ **HANDELSBLATT**, 2011: Bundestrojaner. Friedrich verteidigt Spionagesoftware. Artikel vom 15.10.2011. Letztes Update 15.10.2011. http://www.handelsblatt.com/politik/deutschland/bundestrojaner-friedrich-verteidigt-spionagesoftware/4893366.html, 03.03.2012.

- ✓ **HEMPEL**, Leon, 2007: Zur Evaluation von Videoüberwachung. Methoden, Standards und Beispiele aus der Bewertungspraxis. In: Zurawski, Nils (Hrsg.), Surveillance Studies. Perspektiven eines Forschungsfeldes. Opladen: Verlag Barbara Budrich.
- ✓ **HEMPEL**, Leon; **METELMANN**, Jörg (Hg.), 2005: Bild-Raum-Kontrolle. Frankfurt/M.
- ✓ **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. Bielefeld: transcript Verlag, 231-246.
- ✓ **HEINISCH**, Daniela, 2011: Adrenalin. http://www.gesundheit.de/krankheiten/druesen-und-hormone/nebenniere/adrenalin, 21.02.2012.
- ✓ **HORNUNG**, Gerrit, 2007: Über Möglichkeiten und Grenzen der rechtlichen Bewertung neuer Überwachungstechnologien. In: Zurawski, Nils (Hrsg.), Surveillance Studies. Perspektiven eines Forschungsfeldes. Opladen: Verlag Barbar Budrich, 149-166.
- ✓ **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. Bielefeld: transcript Verlag.
- ✓ **INTERNET 4 JURISTS**: Sicherheitspolizeigesetz – SPG. §24. http://www.internet4jurists.at/ges/spg2008.htm#§_24., 02.03.2012.
- ✓ **KAASE**, M.; **OTT**, W.; **SCHEUCH,** E. K. (Hrsg.), 1983: Empirische Sozialforschung in der modernen Gesellschaft. Frankfurt.
- ✓ **KAMMERER**, Dietmar, 2008: Bilder der Überwachung. Frankfurt am Main: Suhrkamp.
- ✓ **KLAß**, Christian, 2007: Videoüberwachung keine große Hilfe bei Verbrechensbekämpfung. London: Aufklärungsrate steigt durch mehr Kameras nicht. http://www.golem.de/0709/54913.html, 26.10.2010.
- ✓ **KREMER**, Annika, 2009: Indect: Wie die EU die Überwachung vernetzen will. http://www.gulli.com/news/248-indect-wie-die-eu-die-ueberwachung-vernetzen-will-2009-09-24, 26.03.2012.
- ✓ **KUBE**, Edwin, 2003: Polizeiliche Videoüberwachung von Straßen und Plätzen – vorrangig Präventionsmittel oder Gefahrenpotenzial? In: Kuratorium der Polizei-Führungsakademie (Hrsg.). Angewandte Kriminologie und Kriminalprävention; Entwicklungen, Sachstand und Perspektiven. Schriftenreihe Heft 2, Jg. 2003. Dresden: Sächsisches Drucks- und Verlagshaus AG, S. 118-126.

- ✓ **KURIER**, 2011: „Bundestrojaner“ auch in Österreich? Deutsche Spionage-Software angeblich an heimische Behörden geliefert. Innenministerium bestreitet Einsatz.Artikel vom 13.10.2011. Letztes Update 05.12.2011.http://kurier.at/techno/4306000-bundestrojaner-auch-in-oesterreich.php, 03.03.2012.
- ✓ **LUDWIG-MAYERHOFER**, W.: Statistik – Kreuztabellen. Zusammenhänge zwischen nominalen (und/ oder ordinalen) Merkmalen: Kreuztabellenanalyse und Assoziationsmaße II: Signifikanztests und Maße der Assoziation. Universität Siegen. http://www.uni-siegen.de/phil/sozialwissenschaften/soziologie/mitarbeiter/ludwig-mayerhofer/statistik/statistik_downloads/statistik_i_5b.pdf, 16.03.2012.
- ✓ **LECHNER**, 2000: Konsumentenwünsche sind vorhersehbar. Der Standard, 12.10.00, B1.
- ✓ **LEGNARO**, Aldo (2000): Aus der neuen Welt: Freiheit, Furcht und Strafe als Trias der Regulation. Leviathan 2000, 202-220.
- ✓ **LEMKE**, Thomas, 1997: Eine Kritik der politischen Vernunft. Foucaults Analyse der modernen Gouvernementalität. Hamburg: Argument.
- ✓ **LUHMANN**, Niklas, 2003: Soziologie des Risikos. Berlin: Walter de Gruyter GmbH & Co. KG.
- ✓ **LYON**, David, 1994: The Electronic Eye: The Rise of Surveillance Society. Cambridge: Polity Press.
- ✓ **LYON**, David, 2001: Surveillance Society. Monitoring everyday life. Buckingham: Open University.
- ✓ **MALINOWSKI**, Peter; **MÜNCH**, Ulrich, 1975: Soziale Kontrolle: soziologische Theoriebildung und ihr Bezug zur Praxis der sozialen Arbeit. Neuwied: Leuchterhand.
- ✓ **MURCK**, Manfred, 1980: Soziologie der öffentlichen Sicherheit. Frankfurt: Campus Verlag.
- ✓ **NEWS**, 2011: Eurofighter. Lobbyisten abgehört. Format: Verdacht auf Schmiergeldzahlungen an Beamte und Politiker. http://www.news.at/articles/1135/30/305898/eurofighter-lobbyisten, 01.03.2012.
- ✓ **NOGALA**, Detlef, 2000: Gating the Rich – Barcoding the Poor. Konturen einer neoliberalen Sicherheitskonfiguration. Ludwig-Mayerhofer, Wolfgang (Hrsg.): Soziale Ungleichheit, Kriminalität und Kriminalisierung. Opladen: Leske + Budrich, 49-83.
- ✓ **PARLAMENT**: Das Bundes-Verfassungsgesetz.http://www.parlament.gv.at/PERK/VERF/BVG/, 03.03.2012.
- ✓ **PASSENHEIM**, Antje, 2008: Vor 25 Jahren das erste Handy. http://sciencev1.orf.at/science/news/151782, 15.02.2012.

- ✓ **PETERS**, Helge, 1995: Devianz und soziale Kontrolle. Eine Einführung in die Soziologie abweichenden Verhaltens. 2. Aufl. Weinheim/München: Juventa.
- ✓ **PHILLIPS**, D. L., 1971: Knowledge from what? Chicago.
- ✓ **POSSEST**: The Panopticon Penitenary, 1791, Plan. http://www.possest.de/sascha_is/learning_about/the_limitation_of/this_world/by_observing/the_observer.html, 24.02.2012.
- ✓ **PURGATHOFER**, Peter, 2008: Eine kleine Geschichte der Überwachung. In: Gaycken, Sandro; Kurz, Constanze (Hg.), 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld: transcript Verlag, 195-208.
- ✓ **PUSCHKE**, Jens (2006): Die Vorratsdatenspeicherung als Instrument der Strafverfolgung. Datenschutz Nachrichten 2006. 65-73.
- ✓ **REINECKE**, Leonard, 2009: Das Ende der Privatheit? Zum Stellenwert der Privatsphäre und Selbstoffenbarung im Social Web.

  http://www.fsm.de/inhalt.doc/Praesentation_Reinecke_2009-06-23.pdf, 26.04.2010.
- ✓ **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. Bielefeld: transcript Verlag, 53-66.
- ✓ **RIS**, 2012: Bundesrecht konsolidiert: Gesamte Rechtsvorschrift für Sicherheitspolizeigesetz. Fassung vom 20.02.2012. §17. http://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792, 20.02.2012.
- ✓ **RIS**, 2012: Bundeskanzleramt Rechtsinformationssystem. Bundesrecht konsolidiert. http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12016939, 03.03.2012.
- ✓ **RÖSSLER**, Beate, 2001: Der Wert des Privaten. Frankfurt am Main: Suhrkamp.
- ✓ **SCHAAR**, Peter, 2007 : Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft. 1. Auflage, München: C. Bertelsmann Verlag.
- ✓ **SCHEERER**, Sebastian, 2000: „Soziale Kontrolle“ – schöner Begriff für böse Dinge? Peters, Helge (Hrsg.): Soziale Kontrolle. Zum Problem der Nonkonformität in der Gesellschaft. Opladen: Westdeutscher Verlag, 153-169.
- ✓ **SCHNEIER**, Bruce, 2006: Beyond Fear. Thinking Sensibly About Security in an Uncertain World. New York: Copernicus Books.

- ✓ **SCHNELL**, Rainer; **HILL**, Paul B.; **ESSER**, Elke, 1999: Methoden der empirischen Sozialforschung. 6., völlig überarb. Und erw. Aufl., München: Oldenbourg.
- ✓ **SCHNELL**, Rainer; **HILL**, Paul Bernhard; **ESSER**, Elke, 2005: Methoden der empirischen Sozialforschung. 7. Auflage, München: Oldenbourg.
- ✓ **SCHULZKI-HADOUTI**, Christiane, 2007: Gläserner Bürger 2.0. In: Zurawski, Nils (Hrsg.), Surveillance Studies. Perspektiven eines Forschungsfeldes. Opladen: Verlag Barbara Budrich, 25-32.
- ✓ **SEVILLANA**: Weise Welt. Freiheit. http://www.sevillana.de/weise-welt/freiheit.htm, 15.02.2012.
- ✓ **SIMON**, Anne-Catherine; **SIMON**, Thomas, 2008: Ausgespäht und abgespeichert. Warum uns die totale Kontrolle droht und was wir dagegen tun können. München: F. A. Herbig.
- ✓ **SINGELNSTEIN**, Tobias; **STOLLE**, Peter, 2007: Von der sozialen Integration zur Sicherheit durch Kontrolle und Ausschluss. Zum Wandel sozialer Kontrolle und seinen gesellschaftlichen Grundlagen. In: Zurawski, Nils (Hrsg.), Surveillance Studies. Perspektiven eines Forschungsfeldes. Opladen: Barbara Budrich Verlag, 47-66.
- ✓ **SPIEGEL**: RFID-Technik.http://www.spiegel.de/netzwelt/tech/0,1518,430138,00.html, 19.02.2012.
- ✓ **STERBIK-LAMINA**, Jaro; **PEISSL**, Walter; **CAS**, Johann, 2009: PRIVATSPHÄRE 2.0. Beeinträchtigung der Privatsphäre in Österreich - neue Herausforderungen für den Datenschutz. Studie im Auftrag der Bundesarbeitskammer. http://www.arbeiterkammer.at/bilder/d89/Studie_Datenschutz.pdf, 03.03.2012.
- ✓ **TÖPFER,** Eric, 2007: Videoüberwachung – Eine Risikotechnologie zwischen Sicherheitsversprechen und Kontrolldystopien. In: Zurawski, Nils (Hrsg.), Surveillance Studies. Perspektiven eines Forschungsfeldes. Opladen: Verlag Barbara Budrich, 33-46.
- ✓ **TROJANOW**, Ilija; **ZEH**, Juli, 2010: Angriff auf die Freiheit. Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte. München: Deutscher Taschenbuchverlag GmbH & Co. KG.
- ✓ **ULLRICH**, Carsten, 2005: Soziologie des Wohlfahrtsstaates: Eine Einführung. Frankfurt am Main: Campus Verlag.
- ✓ **UN**: Allgemeine Erklärung der Menschenrechte. http://www.un.org/depts/german/grunddok/ar217a3.html, 03.03.2012.

- ✓ **UNWATCHED**, 2007: Vorratsdatenspeicherung: Österreich auf dem Weg zur digitalen Überwachungsgesellschaft. Artikel vom 31.05.2007. http://www.unwatched.org/node/495, 03.10.2010.
- ✓ **VIDC**, 2009: News 5/2009. Überwachung und Kontrolle. Vom Überwachungsstaat zur Scoringgesellschaft.http://www.vidc.org/index.php?id=563, 20.02.2012.
- ✓ **WEBER**, Karsten, 2008: Informationsethik und technisierte Überwachung. In: Gaycken, Sandro; Kurz, Constanze (Hg.), 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Bielefeld: transcript Verlag, 283-302.
- ✓ **WHITAKER**, Reg, 1999: Das Ende der Privatheit. Überwachung, Macht und soziale Kontrolle im Informationszeitalter. München: Verlag Antje Kunstmann.
- ✓ **WIKIMEDIA**, 2005: Überwachungsstaat-Adler.jpg.http://upload.wikimedia.org/wikipedia/commons/f/fa/Ueberwachungsstaat-Adler.jpg, 15.02.2012.
- ✓ **ZURAWSKI**, Nils (Hrsg.), 2007: Surveillance Studies. Perspektiven eines Forschungsfeldes. Opladen: Verlag Barbara Budrich.

Ich habe mich bemüht, sämtliche Inhaber der Bildrechte ausfindig zu machen und ihre Zustimmung zur Verwendung der Bilder in dieser Arbeit eingeholt. Sollte dennoch eine Urheberrechtsverletzung bekannt werden, ersuche ich um Meldung bei mir.

9.1. Weiterführende Literatur

- ✓ **BANISAR**, David; **DAVIES**, Simon: Privacy and Human Rights. An International Survey of Privacy Laws and Practice. Zeit und Ort unbekannt. In: http://www.gilc.org/privacy/survey/intro.html. Heruntergeladen am 23.04.2010
- ✓ **DARNSTÄDT**, Thomas, 2009: Der globale Polizeistaat. 1. Auflage, München: Deutsche Verlags-Anstalt.
- ✓ **DIEKMANN,** Andreas (2009): Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen. 20. Auflage, Hamburg: Rowohlt.
- ✓ **GARLAND**, David, 2008 : Kultur der Kontrolle. Verbrechensbekämpfung und soziale Ordnung in der Gegenwart. Band 12, Frankfurt: Campus Verlag.

- ✓ **GERGELY**, Stefan M., 1984 : Überwachungsstaat Österreich? Der Mensch im Würgegriff des Computers. Wien: ORAC Verlag.
- ✓ **REISCHL,** Gerald, 2002 : Unter Kontrolle. Die fatalen Folgen der staatlichen Überwachung für Wirtschaft und Gesellschaft. Frankfurt: Wirtschaftsverlag Carl Ueberreuter.
- ✓ **WINKELMANN**, Arne; **FÖRSTER**, Yorck (Hrsg.) 2007 : Gewahrsam. Räume der Überwachung. Frankfurt am Main: Kehrer Verlag Heidelberg.
- ✓ **ZANKL**, Wolfgang (HG.) 2009 : Auf dem Weg zum Überwachungsstaat?

  Neue Überwachungsmaßnahmen im Bereich der Informations- und Kommunikationstechnologie. Wien: Facultas Verlags- und Buchhandels AG

9.2. Abbildungsverzeichnis

9.3. Tabellenverzeichnis

10. Anhang

10.1. Tabellen

Tabelle 37 Kreuztabellierung politische Anschauung * Pro-Überwachung gerundet in % (χ^2=0,096; df=2; p=0,953; Phi=0,018; p=0,953)

			Politische Anschauung			Gesamt
			eher links	*Mitte (neutral)*	*eher rechts*	
Pro-Überwachung	*Nein*	*Anzahl*	56	102	22	180
		% innerhalb von politische Anschauung	57%	59%	56%	58%
	Ja	*Anzahl*	42	72	17	131
		% innerhalb von politische Anschauung	43%	41%	44%	42%
Gesamt		*Anzahl*	98	174	39	311
		% innerhalb von politische Anschauung	100%	100%	100%	100%

Tabelle 38 Kreuztabellierung Geschlecht * Pro-Überwachung gerundet in % (χ^2=0,945; df=1; p=0,331; Phi=0,054; p=0,331)

			Geschlecht		Gesamt
			Männlich	*Weiblich*	
Pro-Überwachung	*Nein*	*Anzahl*	89	98	187
		% innerhalb von Geschlecht	61%	56%	58%
	Ja	*Anzahl*	56	77	133
		% innerhalb von Geschlecht	39%	44%	42%
Gesamt		*Anzahl*	145	175	320
		% innerhalb von Geschlecht	100%	100%	100%

Tabelle 39 Kreuztabellierung Alter * Pro-Überwachung gerundet in % (χ^2=7,242; df=4; p=0,124; Phi=0,150; p=0,124)

			Alter					Gesamt
			16 bis 24	*25 bis 39*	*40 bis 49*	*50 bis 59*	*ab 60*	
Pro-Überwachung	*Nein*	*Anzahl*	35	55	49	17	31	187
		% innerhalb von Alter	56%	64%	67%	47%	50%	58%
	Ja	*Anzahl*	28	31	24	19	31	133
		% innerhalb von Alter	44%	36%	33%	53%	50%	42%
Gesamt		*Anzahl*	63	86	73	36	62	320
		% innerhalb von Alter	100%	100%	100%	100%	100%	100%

Tabelle 40 Kreuztabellierung Opfer Familienangehörige und/oder Verwandte gerundet in % (χ^2=2,303; df=3; p=0,512; Phi=0,085; p=0,512)

			Opfer Familienangehörige und/oder Verwandte				Gesamt
			0	*1*	*2*	*3*	
Pro-Überwachung	*Nein*	Anzahl	67	62	38	20	187
		% innerhalb von Opfer Familienangehörige & Verwandte	54%	61%	64%	59%	58%
	Ja	Anzahl	58	40	21	14	133
		% innerhalb von Opfer Familienangehörige & Verwandte	46%	39%	36%	41%	42%
Gesamt		Anzahl	125	102	59	34	320
		% innerhalb von Opfer Familienangehörige & Verwandte	100%	100%	100%	100%	100%

Tabelle 41 Kreuztabellierung Opfer Freunde und/oder Bekannte gerundet in % (χ^2=2,641; df=3; p=0,450; Phi=0,091; p=0,450)

			Opfer Freunde und/oder Bekannte				Gesamt
			0	*1*	*2*	*3*	
Pro-Überwachung	*Nein*	Anzahl	53	79	40	14	186
		% innerhalb von Opfer Freunde und/oder Bekannte	56%	60%	64%	47%	58%
	Ja	Anzahl	41	53	23	16	133
		% innerhalb von Opfer Freunde und/oder Bekannte	44%	40%	37%	53%	42%
Gesamt		Anzahl	94	132	63	30	319
		% innerhalb von Opfer Freunde und/oder Bekannte	100%	100%	100%	100%	100%

10.2. Erhebungsinstrument standardisierte Fragebogen

Universität Wien

Institut für Soziologie

Fragebogen zum Thema „Überwachung in Wien“

März 2011

Liebe Teilnehmerin! Lieber Teilnehmer!

Durch das Ausfüllen des Fragebogens unterstützen Sie mich beim Verfassen meiner Diplomarbeit, in der ich eine Erhebung über das Thema „Überwachung in Wien“ durchführe. Der Fragebogen beinhaltet 19 Fragen und dauert nicht länger als 15 Minuten. Selbstverständlich werden alle Daten anonym ausgewertet und vertraulich behandelt.

Der von Ihnen ausgefüllte Fragebogen wird unter einer Zahlenkombination abgespeichert, wobei Ihre E-Mail Adresse gelöscht wird und jeder Rückschluss auf Ihre Person im Nachhinein, wie auch währenddessen, unter Einhaltung der sozialwissenschaftlichen Regeln, nicht möglich und auch untersagt ist. Die Ergebnisse dieser Befragung, sowie der Umfang der ganzen Studie, werden sich anschließend in meiner Diplomarbeit wiederfinden.

Vielen herzlichen Dank für Ihre Mithilfe!

Dagmara Zamojska

1. **Wie wichtig ist Ihnen das Thema Überwachung (Videoüberwachung, biometrische Pässe, etc. ...) und Datenschutz?**

   ☐ Sehr wichtig

   ☐ Eher wichtig

   ☐ Eher nicht wichtig

   ☐ Nicht wichtig

2. **Wie sehr treffen folgende Aussagen ihrer Meinung nach zu, oder nicht zu?**

	Trifft sicher zu	Trifft eher zu	Trifft eher nicht zu	Trifft überhaupt nicht zu
2.1 Die immer mehr lückenloser werdende Videoüberwachung nimmt zu.	☐	☐	☐	☐
2.2 Die Suchmaschine Google speichert alle von Ihnen jemals eingegebenen Suchanfragen mit dazugehöriger IP-Adresse.	☐	☐	☐	☐
2.3 Seit 2007/2008 werden alle Telefonie- und Internetdaten verdachtsunabhängig gespeichert.	☐	☐	☐	☐
2.4 Dank Google Street View werden Adressen demnächst in einer 360° Ansicht sichtbar, somit auch ihr Haus / ihre Wohnung, wenn sie dem nicht widersprechen.	☐	☐	☐	☐
2.5 Die anhand von Kundenkarten (z.B. Billa, Libro…) erstellten Kundenprofile dienen auch dem Risikomanagement, z.B. bei Banken als Entscheidungsgrundlage für die Kreditwürdigkeit.	☐	☐	☐	☐
2.6 Nacktscanner sind nicht im Stande wahrheitsgetreue Körperbilder zu liefern.	☐	☐	☐	☐

2.7 Selbst Geräte mit GPS Funktionen, wie z.B. Navigationsgeräte oder Handys, ermöglichen keine Ortung des Aufenthaltes.	☐	☐	☐	☐

3. **Was würden Sie tun, wenn die Regierung alle Bürger verpflichtet, ab 1. Jänner nächsten Jahres, ein kleines schwarzes Armband zu tragen, aus nickelfreiem Metall, mit hautfreundlichem Kunststoff ummantelt, das dem Staat vier Funktionen bietet : erstens (1) die ständige Lokalisierung des Bürgers auf einer Landkarte; zweitens (2) die Option, von ihm erfasste Nachrichten zu lesen; drittens (3) die Protokollierung, mit wem und wie lange er telefoniert; und viertens (4) die Möglichkeit, jederzeit unbemerkt den Bürger, seine Gesprächspartner abzuhören. Würden Sie ein solches Armband akzeptieren? Wenn damit Vermisste gefunden werden könnten, Verbrechen aufgeklärt und Terroristen gefangen?**

   ☐ Ich würde Funktion 1 akzeptieren.

   ☐ Ich würde Funktionen 1 + 2 akzeptieren.

   ☐ Ich würde Funktionen 1+ 2 + 3 akzeptieren.

   ☐ Ich würde alle 4 Funktionen akzeptieren.

   ☐ Ich würde gar keine Funktion akzeptieren.

4. **Über welche der oben genannten Funktionen, glauben Sie, verfügt Ihr Handy?? (Mehrfachnennung möglich)**

   ☐ Funktion 1

   ☐ Funktionen 2

   ☐ Funktionen 3

   ☐ Funktionen 4

   ☐ Gar keine dieser Funktion

5. Wie sehr stimmen Sie folgenden Aussagen zu oder nicht zu?

	Stimme sehr zu	Stimme zu	Stimme nicht zu	Stimme überhaupt nicht zu
5.1 Der Staat sollte Zeitungen und Fernsehen kontrollieren, um Moral und Ordnung sicher zu stellen.	☐	☐	☐	☐
5.2. Eine möglichst straffe politische Führung scheint mir das Beste zu sein.	☐	☐	☐	☐
5.3 In unserem öffentlichen Leben gibt es zu viel Kritik und zu wenig Ruhe und Ordnung.	☐	☐	☐	☐
5.4 Streiks und Demonstrationen gefährden die öffentliche Ordnung und sollten verboten werden.	☐	☐	☐	☐

6. Wie sehr stimmen Sie folgenden Aussagen zu?

	Stimme sehr zu	Stimme zu	Stimme nicht zu	Stimme überhaupt nicht zu
6.1 Ich bemerke die Überwachung kaum.	☐	☐	☐	☐
6.2 Datenschutz ist Täterschutz. Wer nichts zu verbergen hat, hat auch nichts zu befürchten.	☐	☐	☐	☐
6.3 Überwachungssysteme greifen in meine Privatsphäre ein.	☐	☐	☐	☐
6.4 Videoüberwachung schreckt potenzielle Täter ab.	☐	☐	☐	☐
6.5 Ich fühle mich durch die Kameras beobachtet.	☐	☐	☐	☐
6.6 Videoüberwachung verringert die Kriminalität nicht, sondern verlagert diese auf andere Orte.	☐	☐	☐	☐

6.7 Die Sicherheit an Bord von Passagierflugzeugen wird durch Nacktscanner verstärkt.	☐	☐	☐	☐
6.8 Verbotene Gegenstände werden Dank Nacktscanner schneller gefunden.	☐	☐	☐	☐
6.9 Der Staat ist dazu verpflichtet seine Bürger zu schützen.	☐	☐	☐	☐
6.10 Je mehr überwacht und kontrolliert wird, desto sicherer ist es auch.	☐	☐	☐	☐
6.11 Biometrische Pässe (beinhalten Fingerabdrücke, Iriserkennung und Personaldaten) schützen uns besser vor Datenmissbrauch und Fälschungen, als die alten Pässe.	☐	☐	☐	☐
6.12 Terroristen können anhand biometrischer Pässe schneller identifiziert werden.	☐	☐	☐	☐
6.13 Irrtümer oder geklonte Chips bei biometrischen Pässen sind nie ganz ausgeschlossen.	☐	☐	☐	☐
6.14 Überwachungssysteme schaffen in der Bevölkerung mehr Verunsicherung als Sicherheitsgefühle.	☐	☐	☐	☐

7. Wie besorgt sind Sie über folgende Tatsachen?

	Sehr besorgt	Ein wenig besorgt	Kaum besorgt	Überhaupt nicht besorgt
7.1 Geräte mit GPS Funktionen, wie z.B. Handys, Navigationsgeräte, ermöglichen eine Ortung des Aufenthaltes.	☐	☐	☐	☐
7.2 Seit 2007/2008 werden alle Telefonie- und Internetdaten verdachtsunabhängig gespeichert.	☐	☐	☐	☐
7.3 Anhand von Kundenkarten (z.B. Billa, Bipa,...) werden Kundenprofil erstellt, die für gezieltes Marketing genutzt werden.	☐	☐	☐	☐
7.4 Die so erstellten Kundenprofile dienen auch dem Risikomanagement, z.B. bei Banken als Entscheidungsgrundlage für die Vergabe von Krediten (Kreditwürdigkeit).	☐	☐	☐	☐
7.5 Private Unternehmen, wie Autovermieter oder Telekom-Anbieter, speichern personenbezogene Daten und verarbeiten diese später für kommerzielle Zwecke.	☐	☐	☐	☐
7.6 Die Suchmaschine Google speichert alle von Ihnen jemals eingegebenen Suchanfragen mit dazugehöriger IP-Adresse.	☐	☐	☐	☐
7.7 Mit Google Street View werden Adressen bald in einer 360° Ansicht sichtbar, somit auch ihr Haus / ihre Wohnung, wenn sie dem nicht widersprechen.	☐	☐	☐	☐
7.8 Die Zunahme der Videoüberwachung.	☐	☐	☐	☐

7.9 Die immer mehr lückenloser werdende Videoüberwachung.	☐	☐	☐	☐
7.10 Die mögliche Einführung von Nacktscanner an österreichischen Flughäfen.	☐	☐	☐	☐
7.11 Mögliche Online-Durchsungen staatlicher Stellen in Österreich.	☐	☐	☐	☐
7.12 Lausch- und Abhörservices der Polizei	☐	☐	☐	☐

8. **Sind Sie selbst, oder ein Mitglied ihrer Familie / Verwandtschaft, ihres Freundes- oder Bekanntenkreises, schon einmal Opfer eines Verbrechens geworden?**

	Sie selbst	Familie / Verwandtschaft	Freunde / Bekannte
Diebstahl	☐	☐	☐
Raub	☐	☐	☐
Einbruch	☐	☐	☐
Überfall	☐	☐	☐
Körperverletzung	☐	☐	☐
Nötigung	☐	☐	☐
Erpressung	☐	☐	☐
Stalking	☐	☐	☐
Sonstiges			

9. Wie beurteilen Sie die Terrorgefahr in Österreich für sich selbst?

	Stimme sehr zu	Stimme zu	Stimme nicht zu	Stimme überhaupt nicht zu
9.1 Ich fühle mich seit den Anschlägen vom 11. September generell unsicherer.	☐	☐	☐	☐
9.2 Ich halte es für möglich, in den nächsten Jahren, Opfer eines Terroranschlages in Österreich (z.B. Flughafen, U-Bahn,...) zu werden.	☐	☐	☐	☐
9.3 Seit den Terroranschlägen meide ich kulturelle und/oder sportliche Großveranstaltungen.	☐	☐	☐	☐

10. Wie groß ist Ihr Vertrauen in folgende Institutionen?

	Sehr groß	Groß	Mittel	Gering	Kein Vertrauen
10.1 Regierung	☐	☐	☐	☐	☐
10.2 Glaubenseinrichtungen (z.B. Kirche,etc...)	☐	☐	☐	☐	☐
10.3 Polizei	☐	☐	☐	☐	☐
10.4 Parlament	☐	☐	☐	☐	☐
10.5 Justiz	☐	☐	☐	☐	☐
10.6 Medien	☐	☐	☐	☐	☐
10.7 Banken	☐	☐	☐	☐	☐
10.8 Telekommunikationsanbieter	☐	☐	☐	☐	☐
10.9 Gesundheitssystem	☐	☐	☐	☐	☐

10.10 Private Versicherungen	☐	☐	☐	☐	☐
10.11 Private Unternehmen	☐	☐	☐	☐	☐

11. Wie beurteilen Sie folgende Aussagen?

	Stimme sehr zu	Stimme zu	Stimme nicht zu	Stimme überhaupt nicht zu
11.1 Demokratie ist die beste Staatsform.	☐	☐	☐	☐
11.2 Sicherheit ist wichtiger als Freiheit.	☐	☐	☐	☐
11.3 BürgerInnen sollten mehr Einfluss auf Regierungsentscheidungen haben.	☐	☐	☐	☐
11.4 Wo strenge Autorität herrscht, dort ist auch Gerechtigkeit.	☐	☐	☐	☐

Abschließend noch ein paar Fragen zu Ihrer Person:

12. Geschlecht

☐ Männlich

☐ Weiblich

13. Alter

☐ 16 bis 24

☐ 25 bis 39

☐ 40 bis 49

☐ 50 bis 59

☐ Ab 60

14. Welchen Familienstand haben Sie zurzeit?

- ☐ ledig (ohne feste Partnerschaft)
- ☐ in fester Partnerschaft /Lebensgemeinschaft
- ☐ verheiratet
- ☐ geschieden
- ☐ verwitwet

15. Höchste abgeschlossene Schulbildung

- ☐ Ohne Abschluss
- ☐ Noch Schüler
- ☐ Pflichtschule
- ☐ Lehre
- ☐ Berufsbildende mittlere Schule (HASCH, ...)
- ☐ Höhere Schule/ Matura (AHS, HAK, HTL, HBLA,...)
- ☐ Universität/Fachhochschule

16. Ich bin zur Zeit ... (bitte nur eines ankreuzen)

- ☐ Arbeitslos / Arbeitsunfähig *(weiter zu Frage 18)*
- ☐ Hausfrau / Hausmann, in Karenz *(weiter zu Frage 18)*
- ☐ Schüler / Schülerin *(weiter zu Frage 19)*
- ☐ Student / Studentin *(weiter zu Frage 18)*
- ☐ In Ausbildung / Lehrling
- ☐ Präsenzdienst / Zivildienst *(weiter zu Frage 18)*
- ☐ Hauptberuflich erwerbstätig
- ☐ In Pension *(weiter zu Frage 18)*

17. Welche Position nehmen Sie in Ihrem (Haupt-)Beruf ein?

☐ Angelernte(r) / Ungelernte(r) ArbiterIn

☐ FacharbeiterIn

☐ einfache(r) Angestellter/Angestellte

☐ mittlere(r) oder höhere(r) Angestellter/Angestellte

☐ einfache(r) Beamte/ Beamtin

☐ mittlere(r) oder höhere(r) Beamter/Beamtin

☐ Selbstständiger / Selbstständige oder Frei beruflich

18. Ihr persönliches Nettoeinkommen

☐unter 1000 EUR

☐ 1000 EUR bis unter 2000 EUR

☐ 2000 EUR bis unter 3500 EUR

☐ 3500 EUR bis unter 5000 EUR

☐ 5000 EUR und mehr

19. Wie würden Sie sich auf einer Skala von (1) sehr links bis (10) sehr rechts einstufen?

1	2	3	4	5	6	7	8	9	10
☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Sehr links Sehr rechts

10.3. Curriculum Vitae

Personal Data

Name	Dagmara Anna Zamojska
Date of Birth	22.10.1987
Nationality	Poland

Education

2006 - today	UNIVERSITY VIENNA Dr. Karl-Lueger Ring 1 , 1010 Wien Graduate studies in Sociology of the legal, socio-economic and scientific study branch
1998 – 2006	HIGH SCHOOL Franklinstrasse 26, 1210 Wien School-leaving-exam with success on the 20th of July 2006
1994 - 1998	ELEMANTERY SCHOOL Herzmanovsky Orlando Gasse 11, 1210 Wien