

Interdisziplinäre Projektarbeit
zu
Moderne Überwachungsmethoden

—

Terrorverhinderung oder Eingriff in die Privatsphäre?



Verfasser:	Reto Schelbert
Schule:	Berufsmaturitätsschule GIBZ Zug
Klasse:	InfB4b
Betreuungsperson:	Lücking Strankmann Jutta
Eingereicht am:	09.03.2007

Inhalt

1	Abstract.....	3
1.1	Zweck der Arbeit	3
1.2	Ziele	3
1.3	Vorgehensweise.....	3
2	Einleitung	4
3	Hauptteil.....	5
3.1	Terrorismus	5
3.1.1	Das Problem der Definition	5
3.1.2	Entwicklung.....	6
3.1.3	Vorgehensweisen.....	6
3.1.4	Wo sind Gefahren – Wer ist bedroht?	8
3.1.5	Gesetze im Kampf gegen den Terrorismus.....	8
3.1.6	Wie soll man mit dem Terrorismus umgehen – wie verhindern?.....	10
3.2	Privatsphäre	11
3.2.1	Warum die Privatheit wichtig ist	11
3.2.2	Menschenrechte – Freiheitsrechte	12
3.3	Überwachung	14
3.3.1	Totale Informationskenntnis	14
3.3.2	Praktische Schwierigkeiten	14
3.3.3	Neue Gesetze zur staatlichen Überwachung	15
3.3.4	Moderne Überwachungsmethoden	15
3.3.4.1	Biometrische Personenerkennung.....	17
3.3.4.2	Kameraüberwachung / Gesichtserkennung.....	19
3.3.4.3	Profilerstellung von Flugpassagieren.....	20
3.3.4.4	Onyx – Das schweizerische Satellitenabhörsystem	21
3.3.4.5	Echelon.....	23
3.4	Konflikte	25
3.4.1	Bedrohung der Privatsphäre	25
3.4.2	Verhältnismässigkeit und Zweckdienlichkeit	27
3.4.3	Was tun gegen die Bedrohung der Privatsphäre?.....	28
4	Schlusswort.....	30
5	Glossar.....	31
6	Quellenverzeichnis.....	34
7	Erklärung.....	38

Abstract

1.1 Zweck der Arbeit

Viele Sicherheitsmassnahmen im Bereich der Terrorismusbekämpfung sind seit Attentaten wie dem 11. September verschärft oder neu eingeführt worden. Moderne Überwachungsmethoden in der Öffentlichkeit und von Geheimdiensten sollen dem Terror Einheit gebieten. Bei jeder staatlichen Überwachung besteht die Möglichkeit, dass unsere Privatsphäre und das bürgerliche Freiheitsrecht eingeschränkt oder sogar verletzt wird.

1.2 Ziele

In meiner Arbeit möchte ich auf Probleme bei der Terrorismusverhinderung und Bekämpfung eingehen und aufzeigen, ob moderne Überwachungssysteme bei diesen Diensten die Privatsphäre der Bürger verletzen.

1.3 Vorgehensweise

Zu Beginn war mir noch unklar wie wichtig die Privatsphäre und unser bürgerliches Freiheitsrecht für uns sind. Das Thema Überwachung ist sehr weitläufig und ich musste mich auf ein paar wenige Methoden der Überwachung beschränken und wirklich nur Überwachungssysteme nehmen, die zur Terrorverhinderung dienen oder als Sicherheitsmassnahmen zur Vorbeugung von Terrorismus eingesetzt werden. In meiner Arbeit will ich vorerst einmal eine Definition zum Terrorismus abgeben und auf die wirklichen Gefahren des internationalen Terrorismus hindeuten. Weiter werde ich mich mit dem Begriff „Privatsphäre“ und den Gefahren für die Privatsphäre, Freiheit und Demokratie in der heutigen Zeit auseinandersetzen. Zudem kommt die Analyse von ein paar modernen Überwachungsmethoden zur Terrorverhinderung. Dabei helfen mir Meldungen aus Zeitschriften, ein paar interessante Bücher zur Privatsphäre, Terrorismus, Sicherheit und Überwachungssysteme sowie Uni-Arbeiten und Internetwerke.

2 Einleitung

Seit dem 11. September wird vermehrt die Sicherheit bevorzugt, der Schutz des Volkes durch den Staat, Schutz vor Terrorismus und Kriminalität. Dass eine erhöhte Sicherheit die Freiheit des Volkes einschränkt und oft auch Eingriffe und Überwachung unserer Privatsphäre zur Folge hat, darf nicht in Vergessenheit geraten. Der Einsatz neuer Techniken zur Überwachung und Terrorverhinderung wird seit weltbekannten Terrorakten in New York, Madrid und London mit Freuden von Politik und Volk begrüsst. Wie tief schneiden aber moderne Überwachungsmethoden wie Kameraüberwachung auf öffentlichen Plätze und verschärfte Kontrollen an Flughäfen in unsere Privatsphäre ein? Schliesslich werden zur besseren Erkennung möglichst viele Daten über eine Person benötigt. Mit der Erhebung von Daten geht immer auch die Gefahr ihres Missbrauchs einher und je mehr Daten irgendwo gesammelt werden, desto eher können diese auch missbraucht werden. Der liberale Staat präsentiert sich als einer, der unbegrenzten Zugriff auf seine Bürger und Bürgerinnen haben kann und haben will. Die Gefahr liegt auch darin, dass Personen, gerade aufgrund einer strukturellen staatlichen oder gesellschaftlichen Geringschätzung des Schutzes informationeller Privatheit, ihre eigene Autonomie und Privatheit als nicht mehr so relevant begreifen. Konflikte zwischen einerseits der notwendigen Aufgabe des Staates, seine Bürger und Bürgerinnen vor Terrorismus zu schützen, und andererseits der Aufgabe des Staates, die individuelle Freiheit dieser Bürger und Bürgerinnen zu schützen, können natürlich in ihrer Realität nicht einfach bestritten werden. Doch sollte sie richtig beschrieben werden; Stehen Freiheitsrechte und das Interesse an Autonomie auf der einen Seite, so muss für die Einschränkung dieser Rechte nicht nur ein gewichtiger Grund (wie etwa die Terroristenbekämpfung), sondern auch ein hohes Mass an Effektivität bei der Erreichung dieses Ziels in Aussicht gestellt sein. Genau dies scheint jedoch bei den neuen Sicherheitsgesetzen nicht der Fall zu sein.

3 Hauptteil

3.1 Terrorismus

Der Terrorismus bringt die Menschen aus der Fassung. Er tut dies mit Absicht. Darauf legt er es an, und deshalb nimmt er in den ersten Jahren des 21. Jahrhunderts einen so grossen Teil unserer Aufmerksamkeit ein.

Seit dem 11. September befinden wir uns offensichtlich in einem permanenten Notstand, im „Krieg gegen den Terrorismus“, dessen Verästelungen genauso unergründlich sind wie der Terrorismus selbst. Der Terrorismus ist kein Produkt unserer Zeit, sondern hat die Menschheit schon seit vielen Jahrhunderten bewegt und beschäftigt. Seitdem versteht man unter Terrorismus ein System, das auf der Verbreitung von Angst basiert. Die ersten Schritte der Staatengemeinschaft gegen Terrorismus entstanden im Rahmen des Völkerbunds als Reaktion auf die Ermordung des jugoslawischen Königs Alexander 1934.

Als Ergebnis legte ein Expertenausschuss des Völkerbundes am 16. November 1937 die „Genfer Konvention zur Verhütung und Bekämpfung des Terrorismus“ vor. Die Konvention beschreibt den Terrorismus als kriminelle Taten, die gegen Staaten oder geschützte Personen gerichtet sind, um diese in Angst zu versetzen. Nach dem zweiten Weltkrieg wurde die Konvention sinngemäss durch die Etablierung des Völkerrechts 1945 in Form des Gewaltverbots wieder aufgegriffen.¹

3.1.1 Das Problem der Definition

Der Terrorismus muss abgegrenzt werden können von krimineller Gewalt oder militärischen Aktionen. Eine „adäquate“ Definition von Terrorismus gibt es nicht. Kaum eine Person oder Gruppe hat sich jemals selbst als „Terrorist“ bezeichnet. Staaten sind aber schnell einmal bereit, gewalttätige Gegner mit diesem Titel zu brandmarken. Unmenschlichkeit, Kriminalität und Mangel an realer politischer Unterstützung werden oft mit diesem Titel verbunden.

Die USA beschreibt z.B. Terrorismus als „die bewusste Anwendung oder Androhung von Gewalt, um Angst und Schrecken zu verbreiten, in der Absicht, Regierungen oder Gesellschaften zu nötigen oder einzuschüchtern.“ Grossbritannien definiert ihn als „die Anwendung oder Androhung von massiver Gewalt gegen Personen oder Sachen mit dem Ziel, eine politische, religiöse oder ideologische Richtung durchzusetzen.“

Dennoch findet es sich schwierig diese Feststellung genauer zu charakterisieren. Stattdessen werden gewisse Organisationen als „terroristisch“ etikettiert.

Im Kern sind fast alle Terrorismus-Definitionen – wie etwa die der Anwendung von Gewalt zur Erreichung politischer Ziele – der Definition des Krieges zu ähnlich, als dass sie sehr hilfreich sein könnten.

Für den Terrorismus wesentlich ist sicher die Verweigerung des offenen Kampfes. Seine werden so angegriffen, dass eine Selbstverteidigung behindert wird.

¹ Dr. Mir A. Ferdowsi: Maßnahmen im Bereich der Terrorismus-Bekämpfung, Ludwig-Maximilians Universität München 2004

3.1.2 Entwicklung

Das Problem der Geschichte des Terrorismus ist, dass es nicht die eine Geschichte des Terrorismus gibt. Es ist vielmehr die Geschichte einer Unzahl von terroristischen Organisationen und Taten, die sich nur schwer verallgemeinern lässt. Terrorismus ist eine Erscheinung, die es schon immer gab und auch immer geben wird. Letztlich muss jeder Terrorismus in seiner Zeit betrachtet und auch daran gemessen werden.

3.1.3 Vorgehensweisen

Das Wesen des Terrorismus besteht in der Anwendung von bewaffneter Gewalt gegen Unbewaffnete. Doch wie funktioniert der Terrorismus?

In „Der terroristische Prozess“ von Charles Townshend gibt es drei verschiedene Elemente in diesem Prozess:

- **Das Erregen von Aufmerksamkeit: Schock, Horror, Angst oder Abscheu**
Um die Bedürfnisse der Sicherheit zu befriedigen, werden in einer Gesellschaft Regeln aufgestellt und Grenzen gesetzt. Werden diese Grenzen überschritten, bewirkt dies ein Schock. Angriffe auf Wehrlose dramatisieren die schlummernde Sorge der Gesellschaft um ihre eigene Sicherheit.
- **Die Botschaft verstehen; was wollen die Terroristen?**
Terroristische Gruppen fühlen sich keineswegs immer Verantwortlich für ihre Taten, oder, wenn sie sich zu einer Tat bekennen, dann ohne verständliche Begründung oder Forderung. Wenn terroristische Aktionen wie z.B. das Attentat vom 11. September ohne „Unterschrift“ bleiben, müssen die Zuschauer die Leerstellen füllen, wobei die Ergebnisse recht unterschiedlich ausfallen.
- **Kampf oder Flucht? Die Reaktion**
Seltsame Beurteilungen von Motiven sind einige Gründe dafür, warum die Reaktionen auf Attentate unvorhersehbar oder widersprüchlich sein können. Falls die Forderungen verständlich und erfüllbar sind, wird man ihnen vielleicht aus Angst nachgeben. Grössere politische Forderungen können in der Regel nicht sofort eingelöst werden. Terrorismus-Theoretiker unterscheiden zwischen „Zielen“ und „reagierender Masse“. Die reagierende Masse erzeugt vermutlich den massiven politischen Druck, der die Regierung zum Nachgeben zwingen könnte.
Der Terrorismus provoziert den Staat, statt ihn zum Nachgeben zu bewegen, zu gewaltsamen Massnahmen – und diese zerschlagen entweder die terroristischen Organisationen oder zerstören, indem sie den verdeckten Faschismus des Systems aufdecken, die Legitimität des Staates.

Thomas P. Thornton unterschied bei der Betrachtung der terroristischen Vorgehensweisen zwei „Typen“ des Terrors, dem „oppressiven“ und dem „agitatorischen“ Terror. Die Funktion des oppressiven Terrors will die Sicherheit der aufständischen Organisationen dadurch wahren, dass sie die Öffentlichkeit davon abschreckt, den Sicherheitskräften Informationen zu liefern. Damit die Organisation in diesem Wesen erfolgreich sein kann, braucht sie ein ausreichend grosses Überwachungssystem, um die Leute davon zu überzeugen, dass eine Unterstützung der Behörden nicht unbemerkt bleibt. Doch die meisten Terrorgruppen haben dafür schlicht zu wenige Mitglieder.

Der agitatorische Terror verfolgt deutlich weiter gestreckte und langfristige Ziele: eine Art „Revolution“ oder „nationale Befreiung“. Eine agitatorische Gewalt wirkt sich stark aus und man schlägt wahllos zu, um den Schock zu maximieren.

Hier hängt der Ausgang des Konflikts davon ab, ob die Terroristen als Feinde der Menschheit betrachtet werden, mit denen eine sinnvolle Interaktion nicht in Frage kommt. Terrorakt können Hilfsfunktionen haben – als ein Element in einer umfassenderen Militär- und Guerilla-Strategie. Sie können auf begrenzte Ziele beschränkt sein (Rache, Gefangenenbefreiung, politische Stellungnahme); oder sie können „absolut“ sein und die Absicht verfolgen, politische Ziele durch den systematischen Gebrauch von blosser Terror durchzusetzen. Nur diese absolute, unabhängige Terrorstrategie, nicht aber die terroristische Aktion als sich, sollte streng genommen als „Terrorismus“ bezeichnet werden.

Johann Mosts legte in seinem Werk „Philosophie der Bombe“ explizit eine spezifische Logik des Terrorismus im letzten Jahrhundert dar. Diese Theorie beruht auf mehreren aufeinander aufbauenden Thesen:

- Extreme Gewalt wird von der Fantasie der Öffentlichkeit Besitz ergreifen.
- So kann die Öffentlichkeit für politische Fragen sensibilisiert werden.
- Gewalt verleiht von sich aus Stärke und wirkt als eine „reinigende Kraft“
- Systematische Gewalt kann den Staat bedrohen und ihn zu unrechtmässigen Reaktionen verleiten.
- Gewalt kann die soziale Ordnung destabilisieren und einen sozialen Zusammenbruch androhen (die „Spirale des Terrors“ und der Gegenterror).
- Schliesslich werden sich die Menschen gegen die Regierung auflehnen und zu den „Terroristen“ übergehen.

Terrorismus im strengen Sinne erschöpft sich also nicht nur in der Anwendung von Gewalt, um politische Ziele zu erreichen. Er ist nicht nur extreme Gewalt; nicht nur Gewaltanwendung von Bewaffneten gegen Unbewaffnete. Er ist vielmehr als eigenständige, hinreichende und ausschlaggebende politische Strategie zu verstehen.²

² Townshend, Charles: Terrorism. Eine kurze Einführung, „Das Problem des Terrorismus“ 2002

3.1.4 Wo sind Gefahren – Wer ist bedroht?

Statistisch gesehen stellt der Terrorismus eine bedeutend geringere Gefahr dar, als ein Verkehrsunfall und lässt sich durch präventive Massnahmen auch viel schlechter in den Griff bekommen.

Doch die Option, den Terrorismus zu ignorieren, ist nicht gegeben. Sie könnte vernünftig sein, ist aber psychologisch und politisch gesehen unmöglich. Der Terrorismus geht ja gerade so vor, dass er mit dem tief sitzenden allgemeinen Bedürfnis nach Sicherheit von Leben und Eigentum und der Sorge darum spielt. Der Terrorismus nahm, und das ist kein Zufall, seinen blühenden Aufschwung gerade in einer modernen westlichen Welt, die seit dem 19. Jahrhundert einen beispiellosen Grad an öffentlicher Sicherheit erreicht hat. Die öffentliche Besorgnis übt in demokratischen Gesellschaften zwangsläufig den grössten Druck aus, denn hier rufen die verschiedenen Repräsentanten der Öffentlichkeit, zusätzlich zu den freien und von Natur aus zur Panikmache neigenden Medien, nach Aktionen, selbst wenn der Mann von der Strasse es nicht tun sollte.

Im Grunde genommen sind „wir alle“ vom transnationalen Terrorismus bedroht. Nach dem 11. September 2001 gab es Anschläge in Bali (Oktober 2002), in Istanbul (Dezember 2003) und in Madrid (März 2004). Diese Anschläge zeigen auch, dass die westliche Welt und Europa von transnationalem Terrorismus (z.B. Terrornetzwerke wie Al-Qaida) genauso bedroht sind wie Länder, in denen nationaler Terrorismus herrscht. Terrorismus wird es geben, solange es menschliche Konflikte gibt.

3.1.5 Gesetze im Kampf gegen den Terrorismus

Das Völkerrecht verbietet bereits seit 1945 die Unterstützung und die Durchführung terroristischer Massnahmen. Ein paar möchte ich hier auflisten.

Die wichtigsten Konventionen der Vereinten Nationen über den Terrorismus in chronologischer Reihenfolge:³

1970: Übereinkommen zur Bekämpfung der widerrechtlichen Inbesitznahme von Luftfahrzeugen. (Inkrafttreten: 14. Oktober 1971).

Es verlangt von den Vertragsstaaten die Verfolgung von Entführern. Die Täter sollen ausgeliefert oder im Festnahme Land bestraft werden.

1979: Internationale Konvention gegen Geiselnahme. (Inkrafttreten: 3. Juni 1983).

Die Vertragsstaaten vereinbaren Geiselnahmen unter Strafdrohung zu stellen, bestimmte Aktivitäten auf ihrem Staatsgebiet zu verbieten, Informationen auszutauschen und Strafverfahren bzw. Auslieferungen durchzuführen.

1980: Übereinkommen über den physischen Schutz von Kernmaterial. (Inkrafttreten 8. Februar 1987)

Vertragsstaaten verpflichten sich jeglichen Transport von nuklearem Material vor dem Zugriff durch Terroristen zu schützen.

³ Dr. Mir A. Ferdowsi: Massnahmen im Bereich der Terrorismus-Bekämpfung, Ludwig-Maximilians Universität München 2004

1988: Übereinkommen über die Kenntlichmachung von plastischen Sprengstoffen zum Zweck ihrer Entdeckung. (Inkrafttreten 21. Juni 1998)

Es dient der Einschränkung des Gebrauchs unmarkierter und unentdeckbarer plastischer Sprengstoffe.

1997: Internationales Übereinkommen zur Bekämpfung terroristischer Bombenanschläge (Inkrafttreten 23. Mai 2001)

Es soll die Möglichkeit „sicherer Basen“ für Bombenleger unterbinden und verpflichtet die Vertragsstaaten zur Verurteilung oder Auslieferung an Drittstaaten.

1999: Internationales Übereinkommen zur Bekämpfung der Finanzierung des Terrorismus. (Inkrafttreten 10. April 2002)

Es verpflichtet die Vertragsstaaten zur Verurteilung oder Auslieferung von Personen, die der finanziellen Unterstützung terroristischer Aktivitäten angeklagt sind. Es fordert Bankinstitute auf, Maßnahmen zur Aufdeckung verdächtiger Transaktionen zu treffen.

Um für zukünftige Aufgaben gewappnet zu sein, arbeitet zurzeit der Rechtsausschuss der UNO-Generalversammlung an einem Übereinkommen zur Bekämpfung des nuklearen Terrorismus, vor allem in Anbetracht der kritischen Sicherheitslage der Atombestände der postkommunistischen Staaten, und an einem umfassenden Übereinkommen zur Beseitigung des Terrorismus. Zusätzlich erforscht die in Wien ansässige Unterabteilung zur Verhütung von Terrorismus aktuelle Entwicklungen und unterstützt Länder bei der Verbesserung ihrer Maßnahmen zur Vermeidung von Terrorakten. Die Abteilung gehört zum Büro der Vereinten Nationen für Drogenkontrolle und Verbrechensverhütung (UNDCP) und wird in Zukunft die Terrorbekämpfung der Staaten intensiver unterstützen.

Gesetzesartikel in der Schweiz:**Terrorismus Art 4. SR 0.361.418.1**

Im Rahmen der Bekämpfung und Verhinderung des Terrorismus tauschen die Vertragsparteien Informationen und Angaben aus:

- a. über geplante oder durchgeführte Terroraktionen, die beteiligten Personen, die Durchführung und die dabei angewendeten technischen Mittel;
- b. über Terroristengruppen und deren Mitglieder, die ihre Straftaten auf dem Hoheitsgebiet der einen Vertragspartei zum Nachteil der anderen Vertragspartei planen, durchführen oder durchgeführt haben, und
- c. über die notwendigen Massnahmen zur Abwehr von Straftaten, die eine grosse Gefahr für die öffentliche Sicherheit darstellen.

3.1.6 Wie soll man mit dem Terrorismus umgehen – wie verhindern?

Für Demokratien ist die Terrorismus-Bekämpfung alles andere als einfach. Welche Grenzen sollte man, wenn überhaupt, im Kampf gegen den Terrorismus ziehen? Um eine Gegenstrategie zum Terrorismus zu finden ist es notwendig den Terrorismus einzuordnen⁴.

Bei der Bekämpfung des internationalen Terrorismus ergeben sich mehrere Probleme.

Definitionsproblematik

Wie schon erwähnt, taucht die Schwierigkeit auf, eine allgemeingültige und akzeptierte Definition von Terrorismus festzulegen.

Reaktion oder kontrollierte Bekämpfung?

Die asymmetrische Strategie terroristischer Netzwerke und ihr asymmetrischer Organisationsaufbau bilden die Kernproblematik bei ihrer Bekämpfung.

Sanktionsproblematik

Es besteht die Gefahr durch übertriebene Sanktionen den Nährboden für Terroristen zu verstärken, da bei der Verfolgung von Einzelntäter ganze Nationen zur Rechenschaft gezogen werden.

Problematik militärischer Maßnahmen

Militärische Aktionen und die Bekämpfung des Terrorismus mit diesen Massnahmen beschäftigen sich mit der Beseitigung aber nicht mit den tieferen Ursachen des Problems. Das Eingreifen von Staaten in die inneren Angelegenheiten anderer Staaten (z.B. US-Engagement in Afghanistan, Irak) droht das geltende Völkerrecht zu erschüttern. Darunter leidet auch unsere Privatsphäre, zu der ich jetzt im nächsten Kapitel schreibe.

⁴ Dr. Mir A. Ferdowsi: Maßnahmen im Bereich der Terrorismus-Bekämpfung, Ludwig-Maximilians Universität München 2004

3.2 Privatsphäre

Zuerst ein paar Bemerkungen zum Begriff und zur Bedeutung, was wir „privat“ nennen. Von Privatheit oder dem Privaten reden wir nämlich in ganz unterschiedlichen Kontexten: Religion ist Privatsache, ebenso wie bestimmte Daten über mich, etwa medizinische Daten, meine Privatsache sind. Meine Privatsache ist, welche Kleidung ich trage und welchen Beruf ich wähle; und privat ist natürlich auch meine eigene, meine private Wohnung. Prima facie haben all diese Dinge nicht mehr gemeinsam als den Oberbegriff „Privatsache“. Eine Person die Privatheit beansprucht, beansprucht somit etwas wie die Kontrolle über den Zugang – zur Wohnung, aber auch zu persönlichen Daten oder zu Entscheidungen, wie etwa bei der Kontrolle darüber, dass sie selbst entscheiden kann, welcher Religion sie angehören möchte (wenn überhaupt einer). Privat ist etwas dann, wenn ich dazu in der Lage und berechtigt bin, den Zugang – zu Daten, zu Wohnungen, zu Entscheidungen oder Handlungsweisen – zu kontrollieren.

Professor Beate Rössler⁵ fasst die Privatheit in drei verschiedene Dimensionen: Geht es um Daten über eine Person, also generell darum, was andere über mich wissen, dann geht es um meine *informationelle Privatheit*. Geht es um meine privaten Entscheidungen und Handlungen (mit wem will ich zusammenleben; welcher Beruf will ich ergreifen; aber auch: welche Kleidung trage ich), dann geht es um meine *dezisionale Privatheit*, und steht die Privatheit meiner Wohnung zur Debatte, dann rede ich von *lokaler Privatheit*.

3.2.1 Warum die Privatheit wichtig ist

Wir wollen den Schutz des Privaten deshalb, weil wir anders nicht unser Leben so frei und selbstbestimmt wie möglich leben können. Und gerade deshalb sollten wir Privatheit schätzen, denn das Aufgeben von Ansprüchen auf Privatheit ist immer auch zugleich das Aufgeben von bestimmten Ansprüchen, frei und selbstbestimmt zu sein. Die Frage nach dem Wert des Privaten, danach, warum eigentlich Privatheit wichtig ist, der entscheidende Schritt in einer gesellschaftskritischen Theorie des Privaten: Nur wenn man weiss, warum man eigentlich Privatheit für wichtig hält, kann man klarerweise auch kritisieren, wenn Privatheit verletzt wird.

Warum können wir uns eine Gesellschaft ohne Privatheit, wie etwa in Orwells 1984, nicht vorstellen? Es ist die Autonomie die wir brauchen für ein gelungenes Leben. Bei der Autonomie geht es um die grundsätzliche Idee, dass jede Person selbst entscheiden kann und können sollte, wie sie leben will. Autonomie in diesen Sinn bedeutet dann auch, sich selbst für das eigene Leben gut Gründe geben zu können und für Entscheidungen und Lebensweisen sich selbst soweit wir möglich und nötig für verantwortlich zu halten. Ein nichtautonomes Leben in diesem Sinne wäre kein gelungenes Leben. Nun müssen jedoch für ein solches autonomes Leben bestimmte Bedingungen gegeben sein. Dazu gehört eine demokratische Gesellschaft, für die der Respekt vor der Autonomie von Subjekten und ihr Schutz konstitutiv ist, und dazu gehört die Möglichkeit, autonome Entscheidungen und Lebenspläne auch leben zu können; dazu gehört der Schutz von intimen Beziehungen, in denen Autonomie erlernt und gelebt werden kann. Ein solcher Schutz ist deshalb notwendig, weil Personen autonome Entscheidungen nur in einem solche geschützten Umfeld verhandeln können. Für ein solch autonomes Leben sollte also der Schutz von

⁵ Rössler, Beate: Der Wert des Privaten, Suhrkamp Verlag 2001

dezisionaler Privatheit konstitutiv sein. Dezisionale Privatheit deshalb, weil anders Entscheidungen und Lebenspläne nicht gelebt und verfolgt werden können, lokale Privatheit deshalb, weil anders der Schutz intimer Beziehungen und die Rückzugsmöglichkeiten nicht gewährleistet werden können.

Die informationelle Privatheit geht über den Datenschutz gegenüber Staat und Polizei weit hinaus und ist wichtig in allen sozialen Bezügen, in denen Subjekte leben. Der Schutz informationeller Privatheit ist deshalb so wichtig für Personen, weil es für ihr Selbstverständnis als autonome Personen konstitutiv ist, (in ihnen bekannten Grenzen) Kontrolle über ihre Selbstdarstellung zu haben, also Kontrolle darüber, wie sie sich wem gegenüber in welchen Kontexten präsentieren, inszenieren, geben wollen, als welche sie sich in welchen Kontexten verstehen und wie sie verstanden werden wollen, darum also auch, wie sie in welchen Kontexten handeln wollen.

Analysiert man die informationelle Privatheit nach Beate Rössler, dann ist klar, dass es hier nicht nur um Themen wie den Lauschangriff des Staates auf seine Bürger geht, sondern um mögliche Täuschungen in prinzipiell allen Beziehungen, in denen Personen leben.

Informationelle Privatheit kann verletzt werden durch eine Situation des Umbruchs von Normen und Konventionen. Solch eine Veränderung haben wir zum Beispiel dann, wenn staatlicherseits aufgrund neuer Situationen (z.B. terroristischer Aktionen) Massnahmen ergriffen werden, die mit dem Schutz der informationellen Privatheit von Bürgern und Bürgerinnen zu konfliktieren scheinen.

3.2.2 Menschenrechte – Freiheitsrechte

Völkerrechtlich ist die Privatsphäre durch Artikel 8 der Europäischen Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten (EMRK; SR 0.101) und durch Artikel 17 des Internationalen Pakts vom 16. Dezember 1966 über bürgerliche und politische Rechte (UNO-Pakt II; SR 0.103.2) geschützt.

Im Normativen Gehalt der Menschenrechte werden die folgenden Gruppen von Freiheitsrechten bestimmt⁶:

- Recht auf Leben, Freiheit, Eigentum und Sicherheit der Person
- Allgemeine, nur durch Gesetz beschränkbare Handlungsfreiheit
- Freiheit von willkürlichen Eingriffen in die Privatsphäre (Wohnung, Briefgeheimnis etc.)
- Persönlichkeitsrechte
- Meinungsfreiheit
- Gedanken-, Gewissens- und Religionsfreiheit
- Reisefreiheit
- Versammlungsfreiheit
- Informationsfreiheit
- Berufsfreiheit

⁶ Aus <http://de.wikipedia.org/wiki/Menschenrechte#Freiheitsrechte> und http://www.gesetze.ch/sr/131.222.2/131.222.2_002.htm SR 131.222.2

Der Artikel 8 der Europäischen Menschenrechtskonvention von 1950 enthält folgende Gedanken:

- Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.
- Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.

Der Schutz der Privatsphäre umfasst nach Auffassung der Bürgerrechtsorganisation *Electronic Privacy Information Center* folgende vier Bereiche:

- Informationsschutz – d.h. Schutz des Individuums bei der Handhabung, Verbreitung und Verwendung von Informationen;
- Schutz vor körperlichen Übergriffen – d.h. Schutz der Persönlichkeitsrechte bei Leibesvisitationen, Kontrollen usw.;
- Kommunikationsschutz – d.h. Schutz vor Lauschangriffen usw. bei der Benutzung von Telefon, E-Mail und Post;
- Schutz des räumlichen Bereichs – d.h. Unverletzlichkeit der Wohnung oder des persönlichen Bereichs am Arbeitsplatz, Schutz vor Angriffen bei Spaziergängen im Park, auf der Strasse usw.

Panoptikon – die panoptische Gesellschaft

Der Begriff und die Idee des Panoptikons stammen bekanntlich von Bentham und sind über Foucault in die heutigen Debatten zur informationellen Privatheit gelangt.

Im Jahre 1787 entwarf der Philosoph Jeremy Bentham das sogenannte Panopticon (Panoptikon): Ein Gefängnis, das auf der Basis von totaler Überwachung funktioniert. Die Zellen sind kreisförmig um einen einzigen Wachraum angeordnet und vollkommen voneinander isoliert. Der Wachmann kann über Leitungen jederzeit die Gefangen beobachten und gegebenenfalls disziplinieren. Da er jedoch nicht überall gleichzeitig sein kann, ist in Zellen ein künstliches Fenster installiert, hinter dem sich permanent die Silhouette des Wachmanns abzeichnet. Zweck dieses Bauwerks ist jedoch nicht die Besserung der Gefangenen, sondern die Erziehung der normalen Bürger. Indem man ihnen das Panopticon vorführt, soll sich aus Angst davor jede Form von Kriminalität verhindern lassen. Auf den ersten Blick ein verführerischer Gedanke, er hat nur einen Haken: Sollte dieses Prinzip tatsächlich funktionieren, gibt es niemanden mehr, der man im Panopticon einsperren könnte.

Am ehesten mit dem Panopticon zu vergleichen ist die Installierung von Überwachungskameras in den Geschäften, Einkaufszentren und neuerdings auch auf öffentlichen Plätzen. Da man als Normalbürger sich nun vor Räubern und Dieben geschützt wähnt, nimmt man diesen Eingriff in die Privatsphäre gerne in Kauf.⁷ Kommen wir deshalb zum nächsten Kapitel „Überwachung“. Darin möchte ich die Überwachungsmethoden und entstehende Konflikte mit der Privatsphäre aufführen.

⁷ Ralf Grötter: Privat! Telepolis, März 2003

3.3 Überwachung

Überwachung oder **Observation** (v. lat. observare = beobachten) ist das unauffällige, systematische Beobachten einer Person, Sachen und Objekten zur Beschaffung von Beweisen, Ermittlungshinweisen und grundlegenden oder ergänzenden Erkenntnissen für weitere Maßnahmen. Unter anderem unterscheidet man zwischen; technischer Überwachung, Verkehrsüberwachung, medizinische Überwachung, elektronische Überwachung, militärische Überwachung und „low-tech“ Überwachung. Für die Terrorismusverhinderung werden natürlich nicht alle Überwachungsarten eingesetzt. Vielmehr kommen Personenüberwachungen durch elektronische Überwachungen in Frage, wenn es darum geht Terroristen ausfindig zu machen.

3.3.1 Totale Informationskenntnis

Das gigantische Projekt für totale Informationskenntnis in den USA (engl. *Total Information Awareness*, kurz *TIA*, das später *Terrorism Information Awareness* umgetauft wurde) bezweckt die detaillierte elektronische Überwachung der gesamten Bevölkerung im Namen der Terrorismusbekämpfung. So gut wie sämtliche erreichbaren elektronischen Daten von Menschen sollten dabei als Unterlage dienen. Für die Verwirklichung des TIA-Projekts wurde eigens eine neue Behörde ins Leben gerufen, nämlich das Information Awareness Office (IAO – Amt für Informationskenntnis), welches von der DARPA (Defense Advanced Research Projects Agency), einer Agentur des Verteidigungsministeriums der USA, gegründet wurde. Das Projekt startete unmittelbar nach den Terroranschlägen vom 11. September 2001.

Trotz der vollen Unterstützung seitens des amerikanischen Präsidenten und eines Grossteils des amerikanischen politischen Establishments erwies sich TIA schliesslich als zu umstritten. Der US-Kongress untersagte gegen Ende 2003 jegliche weitere Finanzierung des Projekts.⁸

3.3.2 Praktische Schwierigkeiten

Falls es tatsächlich gelänge, Terroristen vor der Ausführung ihrer Anschläge dingfest zu machen, würde dies natürlich grosses Leid ersparen.

Viele Überwachungsprogramme (wie einst das TIA) stossen aus folgenden Gründen aber auf starke Kritik:

- Der Erfolg eines Erkennungssystems ist ungewiss, da auch Terroristen lernen, die Spuren, auf deren ein Entdeckungssystem und Programm geeicht ist, zu verwischen bzw. zu vermeiden.
- Die Funktionalität eines Systems macht die fortlaufende, detaillierte Überwachung sämtlicher Bürger – d.h. der grossen, unbescholtenen Mehrheit der Bevölkerung – erforderlich, was zum Polizeistaat führt.
- Ein System kann nie so genau kalibriert werden, dass es 100-prozentige Treffsicherheit erzielt. Eine Anzahl „falscher positiver“ Ergebnisse ist die Folge, d.h. es werden Unschuldige verdächtigt, möglicherweise in beträchtlicher Anzahl.

⁸ Aus http://de.wikipedia.org/wiki/Total_Information_Awareness

3.3.3 Neue Gesetze zur staatlichen Überwachung

Die Terrorschläge vom 11. September führten zu einer grundsätzlichen Sinneswandlung von Regierung und Behörden, was sich weltweit in neuen Gesetzestexten niederschlug. Einige Beispiele hier:⁹

- Die Europäische Union hat eine Regelung erlassen, nach der alle Mitgliedsstaaten verpflichtet sind, Informationen über die Anrufe, e-Mails und SMS ihrer Bürger für 6 bis 24 Monate zu speichern, inklusive Informationen über den Aufenthaltsort von Mobiltelefonbenutzern.
- Die Europäische Union hat ebenfalls beschlossen, biometrische Pässe einzuführen, die digitale Informationen über das Gesicht und eventuell auch die Fingerabdrücke enthalten.
- In Grossbritannien hat man ein stark kritisiertes Gesetz erlassen, das Behörden das Recht einräumt, von Privatanwendern die Auslieferung von Schlüsseln für Chiffrierprogramme zu erzwingen.
- In den Vereinigten Staaten haben die Behörden mittlerweile wesentlich erweiterte Befugnisse, Gespräche zu belauschen, von den Bibliotheken Informationen über ausgeliehene Bücher zu fordern etc.
- In Ungarn muss man sich bei Käufen, deren Wert ein bestimmtes Limit übersteigt, mit seinem Ausweis registrieren lassen. In Italien müssen Internetcafés ihre Kunden um den Ausweis bitten und Listen von den besuchten Seiten jedes Benutzers an die Polizei weitergegeben werden.
- In Schweden hat das Verteidigungsministerium vorgeschlagen, alle E-Mails, die über die Landesgrenze verschickt werden, zu lesen.
- Das neue dänische Antiterrorismugesetz gibt der Polizei in Dänemark das Recht, so genannte Spyware in den Computern verdächtiger Personen zu installieren.

3.3.4 Moderne Überwachungsmethoden

Wir wollen uns die Aufgabe des IAO etwas veranschaulichen, obwohl diese Agency nicht mehr existiert, sind die entwickelten Prototypen eines globalen Super-Lauschsystems sicherlich eine Grundlage für zukünftige Projekte.

Das IAO hatte die Aufgabe, den Prototyp eines Systems zu entwickeln, das private Kommunikationen und kommerzielle Transaktionen nach Mustern durchsuchen kann, die auf terroristische Aktivitäten hinweisen könnten. Die Agency hat sich das anspruchsvolle Big-Brother-Ziel einer "totalen Informationskenntnis" - ein bisschen wie ein irdisches Auge Gottes - gesetzt, für die jede Informationsquelle in der Welt (siehe Abb.3.3.4: Transactional Data), die irgendwie zugänglich ist, berücksichtigt werden soll, um Terroristen oder Verdächtige zu entdecken. Zu diesen Quellen zählen natürlich auch Telefone und das Internet.

⁹ Ström Pär: Die Überwachungsmafia, Heyne Verlag 2006

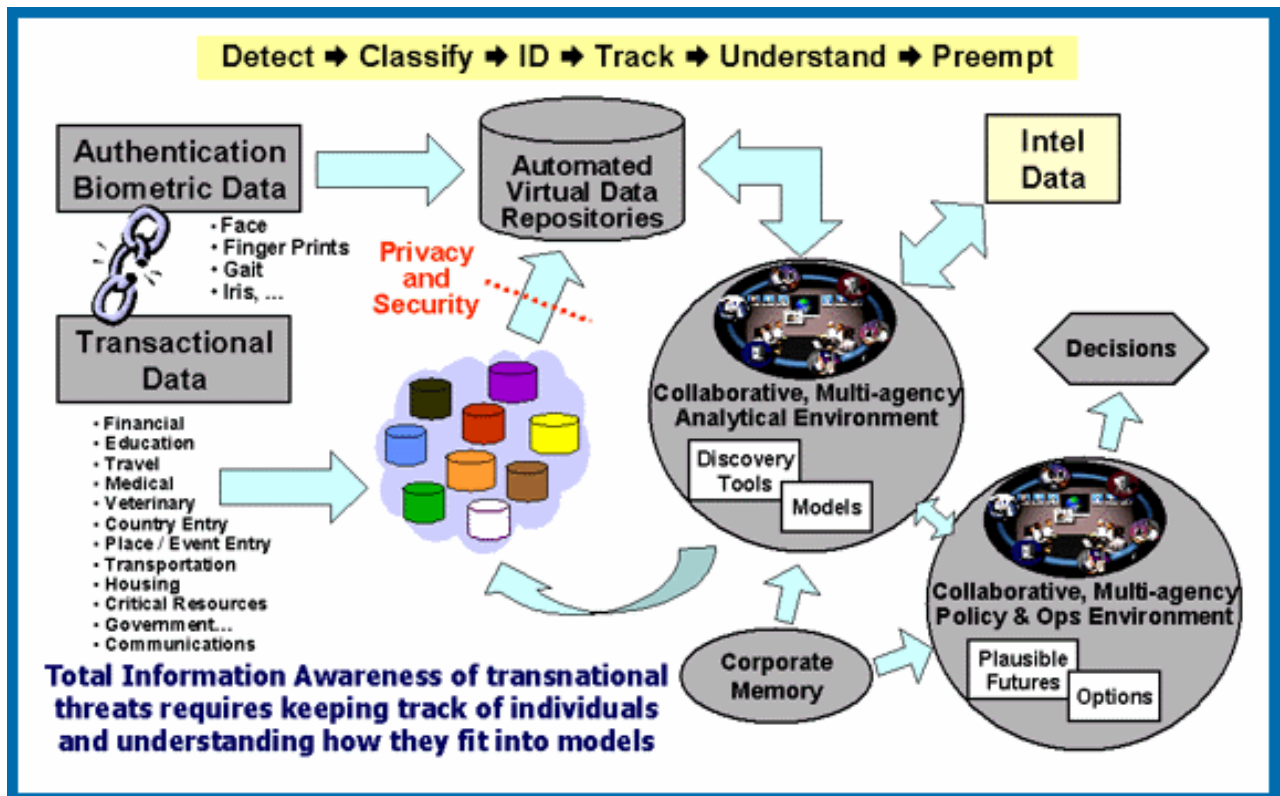


Abb3.3.4: Data Mining und Informationsbeschaffung, wie es das AIO entwickelte

Begründet wird die Schaffung des globalen Super-Lauschsystems, das Informationen nicht nur zusammen führen und bewerten, sondern auch Voraussagen und Handlungsvorschläge machen soll, mit der üblichen "asymmetrischen Bedrohung der Vereinigten Staaten" durch den Terrorismus, der von lose organisierten, schwer zu identifizierenden Menschen ausgeübt wird, die unregelmäßig in einem "low-intensity/low-density form of warfare" zuschlagen. Zu deren Identifizierung muss man eben über alles Bescheid wissen, also wer was mit Kreditkarten einkauft, wer einen akademischen Abschluss erhält, einen Führerschein für Piloten oder einen anderen Ausweis beantragt, wer Geld überweist, Informationen über Email verschickt oder unvorsichtigerweise am Telefon plaudert.

„Wenn Terrororganisationen Angriffe auf die USA planen und durchführen, müssen deren Mitglieder Transaktionen vornehmen. Dabei hinterlassen sie Spuren in diesem Informationsraum.“ - John Poindexter

Weil "Information der Schlüssel zur Bekämpfung des Terrorismus" ist, sollen natürlich auch alle verfügbaren biometrischen Daten zur Identifizierung von Personen zur Durchsuchung verfügbar sein. Zugreifen sollen auf das Data-Mining-System mit den unerschöpflich großen Informationsquellen die Geheimdienste und Strafverfolger - auch ohne richterliche Genehmigung im Hinblick auf die Daten der amerikanischen Bürger (der Rest der Welt ist sowieso Freiwild für die Geheimdienste - nicht nur der USA). Und dafür müssen eben auch die hinderlichen Barrieren zwischen den staatlichen und privaten Datenbanken fallen. Und das System muss auch schon deswegen besonders ausgeklügelt sein, weil die Terroristen ja gerade versuchen, möglichst keine Hinweise auf sich und ihre Aktivitäten zu hinterlassen.

Der Anschlag in London hat zu den üblichen Verurteilungen und Gesten der Einheit im Kampf gegen den Terrorismus sowie zu den erwartbaren Forderungen nach

erhöhten Sicherheitsmaßnahmen und neuen Gesetzen geführt. Aber die Bomben in London lehren vermutlich gerade, dass die meisten Sicherheits- und Überwachungsmaßnahmen entschlossene und einigermaßen intelligente Terroristen, auch wenn sie mit wenig ausgeklügelten Strategien und relativ primitiven Mitteln vorgehen, nicht daran hindern können, Anschläge im öffentlichen Raum von Städten auszuführen. Um das Risiko wirklich zu minimieren, wäre schon ein Überwachungsapparat Orwellscher Dimension oder ein Repressionsregime notwendig, wie man es etwa in Nordkorea findet.¹⁰

3.3.4.1 Biometrische Personenerkennung

Biometrie bedeutet die Identifizierung von Menschen mittels körperlichen Kennzeichen. Die Begriffe Biometrie, Biometrik und biometrische Identifikation werden häufig synonym verwendet.

Die üblichsten Methoden zur Personenerkennung sind: Gesichtserkennung, Gangidentifizierung, Fingerabdrücke, Abdrücke der Hand, Erkennung der Iris oder Retina des Auges, Analyse der Stimme oder der Schrift, Analyse des Eingaberhythmus an Tastaturen sowie DNA-Informationen aus menschlichen Gewebe. Eine weitere Methode ist die Erkennung von Blutgefäßsmustern am Handgelenk bzw. am Ohr.

Im Rahmen der Diskussion über Maßnahmen zur Erhöhung der inneren Sicherheit nach den terroristischen Anschlägen in den USA im September 2001 hat der Einsatz biometrischer Systeme neue Aufmerksamkeit auch in Europa erfahren¹¹. Die Einsatzfelder können grob in fünf unterschiedliche Gruppen unterteilt werden. Die meisten biometrischen Systeme dienen zur Zugangskontrolle und Sicherheit. Im Bezug zur „Terrorverhinderung“ ist für uns nur die „Personenidentifikation durch biometrische Systeme“ interessant.

Bei der eindeutigen Identifikation einer Person werden gegenüber der bloßen Verifikation weitaus höhere Anforderungen an ein biometrisches Systeme gestellt. Es fallen weitaus größere Datenmengen an, die an einer zentralen Stelle gespeichert und verarbeitet werden müssen.

Die Anwendungskontexte erfordern z.T. eine Verbindung zu hochsensiblen Informationen z.B. polizeilicher Art, so dass Fragen des Datenschutzes hier eine besondere Rolle spielen. Wegen der Größe der Nutzergruppen und der Bedeutung der Zwecke bzw. der Missbrauchspotenziale sind höchste Anforderungen an die technische Ausgereiftheit der biometrischen Systeme zu stellen.

Drei zentrale Zwecke der Personenidentifikation sind die - polizeiliche - Überwachung öffentlicher Orte (zu Abschreckungs- wie zu Fahndungszwecken), die Verbesserung des Identitäts- bzw. Legitimationsnachweises (z.B. Führerschein, aber auch Personalausweise o.ä.) sowie die Kontrolle der Gewährung bzw. die Vermeidung des Missbrauchs von staatlichen (Sozial-)Leistungen oder von Leistungen im Rahmen der Gesundheitsversorgung.

¹⁰ Florian Rötzer, Telepolis Artikel „Politiker fordern mehr Überwachung zur Verhinderung von Terror“, Juli 2005

¹¹ Petermann Thomas & Sauter Arnold, Biometrische Identifikationssysteme, TAB Februar 2002

Der Einsatz von Gesichtserkennungssystemen im Rahmen der Überwachung öffentlicher Straßen und Plätze wird in Europa vor allem aus Großbritannien berichtet. Für Schlagzeilen gesorgt hat das Beispiel des Londoner Stadtteils Newham, in dessen Einkaufszone weit über 100 Kameras aufgestellt worden sind, deren Bilder einem ständigen Abgleich durch ein Gesichtserkennungssystem (siehe Bsp. Abb.3.3.4.1) mit einer Datenbank Verdächtiger oder ehemaliger Krimineller unterzogen werden. Diese datenschutzrechtlich hochumstrittene Maßnahme soll zumindest anfangs die Kriminalitätsrate in dem überwachten Gebiet um 40 % gesenkt haben.

Zur Identifikation und vereinfachten Abfertigung von Vielfliegern werden Handerkennungssysteme seit Jahren an den Flughäfen von New Jersey, New York, Miami und Washington D.C. sowie in Kanada und Singapur eingesetzt.

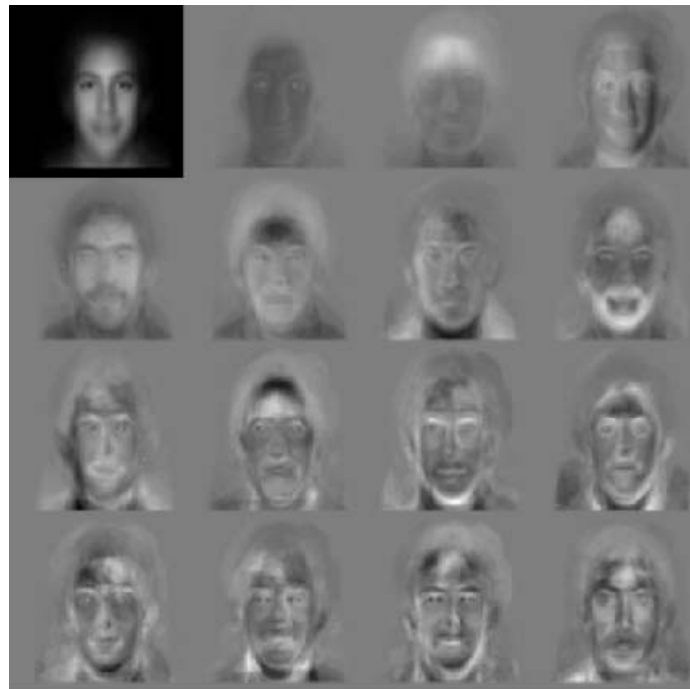


Abb.3.3.4.1:MIT Gesichtserkennung Demonstration

Im Zuge der intensiven Diskussionen um Maßnahmen zur Verbesserung der Sicherheitslage nach dem 11.09.2001 wurde auch der Einsatz biometrischer Verfahren erörtert. Mit dem kürzlich verabschiedeten "Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz)" ist der Gesetzgeber entsprechend tätig geworden. Insbesondere im Pass- und Personalausweisrecht wird die Möglichkeit computerunterstützter Identifizierung von Personen durch biometrische Daten in Ausweisdokumenten eröffnet.

Mithilfe der Biometrie soll deren Fälschung erschwert bzw. unterbunden und es soll verhindert werden, "dass Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen können". Entsprechend werden zweifelsfreie Feststellungen der Echtheit von Dokumenten und der Identität von Personen erwartet.

Datenverarbeitung mittels biometrischer Verfahren greift in einen speziellen Aspekt des Allgemeinen Persönlichkeitsrechts ein: das Recht auf informationelle Selbstbestimmung. Dieser Eingriff ist durch die Datenschutzgesetzgebung erfasst. Auch die Menschenwürde kann als herausragendes Schutzgut betroffen sein. Das Grundrecht auf informationelle Selbstbestimmung garantiert die Befugnis des Einzelnen, prinzipiell selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Die Problematik der möglichen Aufnahme von biometrischen Daten in den Pass ist eine mögliche Verletzung informationeller Privatheit.

3.3.4.2 Kameraüberwachung / Gesichtserkennung

Das Zentrum von London ist der am dichtesten mit Überwachungskameras ausgestattete Ort auf der Welt, was offenbar die Täter nicht davon abhalten konnte, die Anschläge "erfolgreich" durchzuführen. Untersuchungen haben allgemein gezeigt, dass die Präsenz von Überwachungskameras langfristig Kriminalität nicht reduziert. Kameras befinden sich in London an zahlreichen Häusern, Plätzen, Parkplätzen, Straßen, auch zur Mauterfassung, und an und in allen U-Bahn-Stationen, auch in vielen U-Bahn-Wägen. Über 6.000 Kameras überwachen das U-Bahn-Netz.

Insgesamt soll es im Zentrum von London mehr als 500.000 Überwachungskameras geben (in ganz Großbritannien sollen es um die 7 Millionen Kameras sein, Tendenz steigend). Nach einer Untersuchung wird jeder Passant, der sich im Zentrum Londons bewegt, an einem einzigen Tag durchschnittlich von 300 Kameras erfasst. Große Erkenntnisse wird man daraus vermutlich aber nicht gewinnen. Dies nicht nur wegen der Bilderflut aus den zahlreichen Kameras, sondern vor allem deswegen, weil die Täter eben womöglich völlig unauffällig sind und das Tragen einer Aktentasche oder einer anderen Tasche im Berufsverkehr nicht gerade besonders auffällig ist. Weiß man nicht, wen man sucht, dann könnte man die Nadel im Heuhaufen nur aufgrund von vermeintlichen Verhaltensauffälligkeiten entdecken. In den USA ist es sogar üblich, dass Privatpersonen ihren Garten, ihr Haus, ihr Kindermädchen, die Kindertagesstätte usw. per Videokamera überwachen. Häufig sind die Videokameras ans Breitband-Telefonnetz angeschlossen, was eine Überwachung via Internet möglich macht.

Die Überwachungskameras der neusten Generation erkennen Gesichter. Zum Beispiel das von Identix entwickelte System analysiert ein mittels Digitalkamera oder Videokamera fotografiertes Gesicht anhand eines mathematischen Algorithmus, der 80 Kontrollpunkte misst: z.B. Grösse und Form von Augen, Nase, Mund, Ohren, Kinn usw. sowie deren Verhältnis zueinander. Das Resultat dieser Analyse ist eine mathematische Formel, die einen sog. „Gesichtsabdruck“ darstellt. Die Formel wird in einer Datenbank gespeichert bzw. mit anderen, bereits gespeicherten „Gesichtsabdrücken“ verglichen. Das System ist darauf geeicht, bei zwölf übereinstimmenden Merkmalen (von insgesamt 80 Merkmalen) Alarm zu geben.

Automatische Gesichtserkennung bedroht in allerhöchstem Masse die Privatsphäre, da sie zwei bereits an sich sensitive Technologien kombiniert, nämlich Kameraüberwachung in der Öffentlichkeit und Biometrie.

Ausserdem erfordert sie nicht – wie z.B. beim Fingerabdruck oder bei der Messung der Iris – die aktive Mitwirkung des Betroffenen; sie lässt sich anwenden, ohne dass wir etwas bemerken.



Abb.3.3.4.2: Nackte Sicherheit – Kleidung von Passanten werden durchleuchtet

Angeblich sollen in London aber dennoch zur Beruhigung oder zum Testen einige dieser "Passive Millimetre-wave Scanner" im Eingangsbereich der U-Bahn aufgebaut werden, die die Kleidung der Passanten durchleuchten und versteckte Gegenstände sichtbar machen können (aber dementsprechend auch Nacktbilder erstellen, was nicht allen Menschen gefallen dürfte, siehe Abb.3.3.4.2). Bislang hat man sie nur zum Aufspüren von illegalen Immigranten in Lastwagen, an Häfen und am Flughafen Heathrow benutzt, da die Nacktbilder einen Eingriff in die Privatsphäre darstellen und die Geräte auch ziemlich teuer sind. Pro Station würden bis zu drei Millionen Euro erforderlich sein. Aber Schutz der Privatsphäre und hohe Geldausgaben scheinen keine Einwände mehr darzustellen.¹²

3.3.4.3 Profilerstellung von Flugpassagieren

CAPPS II (Computer Assisted Passenger Prescreening System) wurde von der neu gebildeten amerikanischen Behörde für Transportsicherheit (Transportation Security Administration) entwickelt und bis zum Sommer 2004 erarbeitet.

Es funktioniert folgendermassen: Jede Person, die ein Flugticket in die USA bzw. für den Transit durch die USA kauft, wird erst einmal überprüft. Dies erfolgt durch eine Software, die den Namen des Passagiers anhand einer Reihe von staatlichen kommerziellen Datenbanken kontrolliert. Die Unterlage für die Kontrolle sollte ursprünglich genauso umfassend sein wie für die TIA, was bedeutet hätte, dass sämtliche denkbaren digitalen Fingerabdrücke relevant gewesen wären. Da aber Kritik laut wurde, dass die Persönlichkeitsrechte verletzt werden, lenkte die Behörde ein und versicherte, dass sie bestimmte Informationsquellen nicht benutzen würde. Die Quellen selbst sollten jedoch geheim bleiben.

¹² Aus Ström Pär: Die Überwachungsmafia, Heyne Verlag 2006 und Florian Rötzer, Telepolis Artikel „Politiker fordern mehr Überwachung zur Verhinderung von Terror“ Juli 2005

Die Software komprimiert die aus den Datenbanken gewonnenen Informationen zu einem farblichen Gefahrencode, der jedem Passagier zugeteilt wird. Der grüne, gelbe oder rote Code wird in chiffrierter Form auf der Bordkarte eingetragen (der Code ist nur vom Flugpersonal erkennbar). Grün bedeutet, dass die Person kein Risiko darstellt, gelb heisst verschärfte Kontrolle und rot bedeutet, dass der Betroffene die Reise nicht antreten darf. Ein Passagier ist selbst also völlig unwissend, welcher Farbcode ihm zugeteilt wurde und es bestand keine Möglichkeit des Einspruchs. Falsche Regierungsangaben können also nicht berichtigt werden. Auch steht das System willkürlichen Schnüffelaktionen aller möglichen Behörden offen. Dank starkem Widerstand von amerikanischen Bürgerrechtsorganisationen wie EPIC wurde das System im Sommer 2004 fallen gelassen. Stattdessen hat man ein anderes System namens Secure Flight eingeführt. Die Informationen sollen nur noch aus streng geheimen Listen des amerikanischen Terrorist Screening Center geschöpft werden. „Falsche Alarme“ sind damit aber immer noch möglich, ebenso wie die Schwierigkeit, Unschuldige von der Liste entfernen zu lassen. Schlussendlich handelt es sich um ein ähnliches System wie das CAPPS II.¹³

3.3.4.4 Onyx – Das schweizerische Satellitenabhörsystem

Onyx ist ein Schweizer Satellitenabhörsystem des militärischen Nachrichtendienstes der Schweiz. Onyx ermöglicht eine Massenüberwachung von Kommunikationen. Es erleichtert die Beschaffung nutzdienlicher Informationen, beispielsweise bei der Bekämpfung der Proliferation von Massenvernichtungswaffen (Weapons of Mass Destruction [WMD]) oder des internationalen Terrorismus, wobei die diesbezüglichen Kapazitäten der Nachrichtendienste um ein Vielfaches erhöht werden.

Die Geschäftsprüfungsdelegation GPDel übt im Auftrag der Eidgenössischen Räte die Oberaufsicht über die Tätigkeit des Bundes im Bereich des Staatsschutzes und der Nachrichtendienste aus. Unter «Staatsschutz» sind sämtliche Aktivitäten des Bundes zu verstehen, die einen repressiven oder präventiven Charakter aufweisen und die dazu beitragen, die «innere Sicherheit» der Schweiz zu gewährleisten. Dabei handelt es sich insbesondere um den Kampf gegen den Terrorismus, gegen gewalttätige Gruppierungen von Extremisten, gegen das organisierte Verbrechen, gegen die Spionage und gegen die Weiterverbreitung von WMD.

¹³ Aus Ström Pär: Die Überwachungsmafia, Heyne Verlag 2006 und Florian Rötzer, Telepolis Artikel „US-Regierung bewertet das Risikopotenzial aller Ein- und Ausreisenden“ Dezember 2006



Abb.3.3.4.4: Onyx-Lauschzentrale in Zimmerwald, Schweiz

Onyx ist ein COMINT-System (Communications Intelligence, direkte Abhörmaßnahmen) zur Erfassung von durch Satelliten übertragenen militärischen und zivilen Kommunikationen. Es ermöglicht den Empfang gewisser Daten wie Telefonanrufe, Fax, Telex, E-Mail und Informatikdaten. Dieses System ergänzt die Aufklärung von Kurzwellensignalen, die während langer Zeit die einzige von den schweizerischen Behörden verwendete Form der elektronischen Nachrichtenbeschaffung darstellte.

Das Onyx-System darf nur für Abhöraktionen ausserhalb der Landesgrenzen verwendet werden.

Im Verlauf des Jahres 2004 hat das System an den Standorten Zimmerwald, Heimenschwand und Leuk den operationellen Betrieb aufgenommen.¹⁴

¹⁴ Bericht der Geschäftsprüfungsdelegation der Eidgenössischen Räte, November 2003

Aufklärungssysteme andere Länder

Laut bestimmten Quellen besitzen rund 30 Staaten eine bedeutsame Abhörkapazität. Die Vereinigten Staaten sind das Land, das im Bereich des elektronischen Nachrichtendienstes über die höchstentwickelten Kapazitäten verfügt. Das für die Abhörung zuständige Zentralorgan ist die *National Security Agency* (NSA), die im In- und Ausland gegen 40 000 Mitarbeiter beschäftigt und über ein Jahresbudget in der Grössenordnung von 4 Milliarden Franken verfügt. Die NSA ist vor der CIA (*Central Intelligence Agency*) und dem FBI (*Federal Bureau of Investigations*) die grösste nachrichtendienstliche Institution der Vereinigten Staaten.

Sie stützt sich auf ein weltweites Netzwerk zur Kommunikationsaufklärung, das nebst den Abhörsatelliten auch elektronische Abhörstationen, terrestrische Funknetze sowie Kabelnetze umfasst. Gemäss zahlreichen übereinstimmenden Quellen betreibt die NSA in Zusammenarbeit mit Grossbritannien, Kanada, Australien und Neuseeland auch ein multinationales Abhörnetz: das Echelon-Netz.

3.3.4.5 Echelon

Echelon ist der Name eines Spionagenetzes. Die Staaten USA, Vereinigtes Königreich, Kanada, Australien und Neuseeland sind daran beteiligt.

War Echelon zunächst nur dazu gedacht, die militärische und diplomatische Kommunikation der Sowjetunion und ihrer Verbündeten abzuhören, so wird es heute angeblich zur Suche nach terroristischen Verschwörungen, Aufdeckungen im Bereich Drogenhandel und als politischer und diplomatischer Nachrichtendienst benutzt. Seit Ende des Kalten Krieges dient dieses System auch der Wirtschaftsspionage.



Menwith Hill, Grossbritannien, fast 30 Parabolantennen, wichtigster Knotenpunkt des Systems

Echelon basiert auf einem gigantischen Netzwerk von Abhöranlagen unterschiedlicher Art: riesige Parabolantennen auf Stützpunkten in sämtlichen fünf Erdteilen, Satelliten (Anzahl: ca. 120), Abhörsysteme auf Schiffen, die vor der Küste der betroffenen Länder kreuzen, Abhörgeräte an Unterwasserkabeln sowie Antennen an Botschaften und Konsulaten.

Die Existenz des Echelon-System war bis 2001 noch heiss umstritten, einige teilnehmende Länder haben nie seine Existenz bestätigt.

In einer Resolution¹⁵ des Europaparlaments im September 2001 heisst es:

- Über die Existenz eines solchen Systems bestehe „kein Zweifel mehr“, auch wenn einige Behauptungen in der Presse über den Umfang des Systems übertrieben sein dürften.
- Das System diene der Überwachung privater und kommerzieller, nicht aber militärischer Kommunikation.
- Das Abhören privater Mitteilungen sei „eine ernste Verletzung der Privatsphäre von Menschen, deren Schutz im Artikel 8 der Europäischen Menschenrechtskonvention garantiert ist“ (dieser Schutz darf nur unter besonderen Umständen – z.B. aus Gründen der nationalen Sicherheit – ausser Kraft gesetzt werden).
- Es kann angenommen werden, dass Echelon „gegen die Grundsätze des Schutzes der Privatsphäre verstösst, die vom Europäischen Gerichtshof für die Menschenrechte in Strassburg beschlossen“ wurden.

James Bamford schreibt in seinem Buch „Body of Secrets“¹⁶:

Ohne politische und rechtliche Kontrolle, ohne Gerichte und Geschworenen oder irgendein Recht des Individuums auf Verteidigung kann Echelon zu einer Art Geheimpolizei des Cyberspace werden.

Wegen der extrem geheimen Art der Tätigkeit ist es schwer zu sagen, wie umfassend die Überwachungskapazität von Echelon ist.

Im Prinzip wird sämtliche Kommunikation, die über Satelliten läuft, überwacht. Die Fähigkeit automatischer Spracherkennung ermöglicht, dass Telefongespräche per Computer nach bestimmten Stichwörtern überwacht werden können.

Es gibt auch Anzeichen dafür, dass es den beteiligten Nachrichtendiensten gelungen ist, Unterwasserkabel (Transatlantikleitung) und auch Glasfaserkabel „anzuzapfen“ Normalerweise erfolgt die elektronische Kommunikation in einem Land via Mikrowellenübertragung. Funkwellen eines Mikrowellentypes werden in einer geraden Linie von einer Parabolantenne zur nächsten gesendet. Dies nutzt z.B. auch unsere eidgenössische Landesverteidigung bei der Luftwaffe, welche über mehrere Richtstrahlnetze mit Knotenpunkten auf Höhen-Anlagen für die Datenvermittlung verfügen. Mikrowellenübertragung ist schwierig abzuhören, da die Signale genau gerichtet sind und aus physikalischen Gründen in einer geraden Linie weiterlaufen, ohne auf die Erdkrümmung Rücksicht zu nehmen.¹⁷

¹⁵ EU Resolution Nr. A5-0264/2001

¹⁶ Bamford, James: Body of Secrets, Trade Paperback April 2002

¹⁷ Aus „Bericht des nichtständigen Ausschusses des EP über das Abhörssystem Echelon“ (A5-0264/2001, Berichterstatter: Gerhard Schmid) vom 11. Juli 2001

3.4 Konflikte

„Diejenige, die bereit sind,
wesentliche Freiheit aufzugeben,
um zeitweilig Sicherheit zu erlangen,
verdienen weder Freiheit noch Sicherheit“
Benjamin Franklin (1706 – 1790)

3.4.1 Bedrohung der Privatsphäre

Die Bedrohung der Privatsphäre kommt von drei Seiten: vom Staat, von Unternehmen und von Einzelnen. Im Kampf gegen den Terrorismus werden neue Sicherheitsmassnahmen staatlicherseits bestimmt, deswegen schauen wir uns die Bedrohung der Privatsphäre durch den Staat etwas genauer an. Der öffentliche Sektor hat die Kraft des Gesetzes auf seiner Seite und kann daher Bürger zwingen, bestimmte Informationen zu liefern. Ausserdem können staatliche und kommunale Stellen die aus verschiedenen Quellen stammenden Informationen miteinander abgleichen, was eine Verletzung des Schutzes der Privatsphäre noch gravierender macht, da die Informationen zu einem nahezu lückenlosen Bild des Menschen zusammengefügt werden können. Auf der anderen Seite ist (in einer Demokratie) der Zweck des Staates gut, d.h. er soll zum Wohle der Bürger tätig sein, was jedoch nicht Machtmissbrauch und andere Fehler bei der Handhabung persönlicher Informationen ausschliesst.

Betrachten wir die Informationsbeschaffung durch staatliche und kommunale Stellen etwas näher. Grundsätzlich kann man sagen, dass diese Tätigkeit insgesamt einem guten Zweck dient. Nur die misstrauischen Personen dürften dahinter einen bösen Plan, eine böse Absicht vermuten.

Der Kampf gegen den Terrorismus ist wichtig. Die Profilerstellung von Flugpassagieren will vermeiden, dass erneut Tausende unschuldiger Opfer an einem neue 11. September zu Tode kommen. Die Gesichtserkennung mittels Kameras an Strassen und öffentlichen Plätzen will verhindern, dass friedliche Bürger bei ihrem Abendspaziergang überfallen, beraubt oder gar ermordet werden. Die elektronische Überwachung des Verkehrs zielt auf die Vermeidung von Staus und will somit den Bürgern Zeit sparen, die Umwelt zu schützen usw., usf.

Der Staat erfüllt also etwas vereinfacht gesagt zwei Hauptaufgaben mit der Beschaffung persönlicher Daten:

- Schaffung einer effizienten, „schlanken“ öffentlichen Verwaltung
- Gewährleistung der Sicherheit der Bürger und des Landes

Beide Aufgaben sind höchst legitim. Hocheffiziente Verwaltung und totale Sicherheit würden aber einen Kontroll- und Überwachungsstaat ungeahnten Ausmasses erfordern – also einen reinen Polizeistaat. Die Abwägung eines angemessenen Kompromisses zwischen beiden Extremen – totale Überwachung oder totaler Schutz der Privatsphäre – ist äusserst schwierig.

Manche sind davon überzeugt, dass wir uns bereits auf einem falschen Gleis befinden.

Im September 2002 verabschiedeten die Leiter von mehr als 50 Datenschutzbehörden aus aller Welt eine Erklärung, die mit folgender Formulierung endete:

Die Tageszeitungen einigten sich darauf, dass der an sich notwendige Schutz vor Attentaten (wie die des 11. September 2001) in vielen Ländern bereits zu übertriebenen Reaktionen gegenüber der Terrorismusgefahr geführt hat, was ernste Folgen für den Schutz der Privatsphäre hatte. [...] Wenn die Regierungen nicht dazu übergehen, die Belange des Datenschutzes und des Schutzes der Privatsphäre zu berücksichtigen, besteht die Gefahr, dass sie die grundlegende Freiheiten, die sie zu schützen versuchen, ins Gegenteil verkehren.

Tony Bunyan von der Bürgerrechtsorganisation Statewatch drückt sich ähnlich aus:

Der Krieg gegen den Terrorismus hat sich in einen ständigen Krieg gegen Freiheit und Demokratie verwandelt, wobei neue Normen errichtet werden – Normen, die bedeuten, dass politische Verantwortung, kritische Prüfung sowie Garantie der Einhaltung der Menschenrechte zu Luxuserscheinungen geworden sind, auf die wir zum Zwecke der Verteidigung der Demokratie verzichten können.

Überwachungsmethoden sollten eine fundamentale ethische Norm erfüllen. Natürlich muss die Polizei die Möglichkeit haben, über die gleichen Werkzeuge zu verfügen wie Straftäter, sonst werden ja unsere Gesetze wirkungslos. Jedoch muss die polizeiliche Anwendung unter genauer demokratischer Kontrolle stehen. Grundlegende Bürger- und Menschenrechte müssen beachtet werden. Auch die „Überwacher“ sind zu überwachen. Dies wird häufig vergessen, was schwere Folgen für Rechtsstaatlichkeit und Schutz der Privatsphäre haben kann.¹⁸

Auch terroristische Anschläge rechtfertigen nicht, die zum Teil hoch sensitiven Daten aller EU-Bürger über Jahre dem potentiellen Zugriff interessierter Stellen auszusetzen. Nils Leopold, Mitglied HU-Bundesvorstand

¹⁸ Vgl. Ström Pär: Die Überwachungsmafia, Heyne Verlag 2006, S. 267ff

3.4.2 Verhältnismässigkeit und Zweckdienlichkeit

Von den rund 10 Millionen alltäglich aus und nach Deutschland getätigten internationalen Kommunikationsverbindungen wickeln sich rund 800 000 oder 8 % über Satelliten ab. Knapp 10 % davon (75 000 Kommunikationen) werden durch eine Suchmaschine gefiltert. Es scheint, dass von diesen Gesprächen nur etwa 700 Informationen beinhalten, die möglicherweise Anhaltspunkte für eine Gefährdung der nationalen Sicherheit enthalten, und dass von diesen 700 höchstens 15 Gegenstand einer eingehenden Überprüfung sein können. Das Verhältnis liegt demnach bei 15 auf 10 Millionen oder 0,00015 %.¹⁹

Ich möchte hier ein paar Erkenntnisse meiner Arbeit festhalten. Diese Tabelle soll eine Verhältnismässigkeit zwischen Nutzen und Gefahren von den behandelten Überwachungsmethoden darstellen.

Überwachungsmethode	Gefahr für die Privatsphäre	Effektivität der Terrorverhinderung
Echelon/Onyx – elektronische Überwachung und Abhörsysteme	Zugriff zu privaten Daten, welche elektronisch übertragen werden sind jederzeit, überall (transnational) und völlig unbemerkt möglich. Durch Automatisierung und Geheimhaltung der ganzen Prozesse ist keine politische und rechtliche Kontrolle vorhanden.	Enormer Aufwand ist erforderlich für das Aufspüren möglicher Gefahrenquellen. Falschdeutung möglich. Der Nutzen zur Terrorverhinderung kann nicht ganz klar festgelegt werden.
Profilerstellung von Flugpassagieren	Nationalübergreifende Datenbanken und Ansammlung von verschiedensten Daten können gegen das Datenschutzgesetz verstossen und greifen die informationelle Privatheit an.	Nur durch eine genaue und säuberlich geführte Liste können Terroristen an Flughäfen gestoppt werden. Fehlanzeigen sind schnell möglich, Unschuldige können nicht von der Liste genommen werden, da auch hier die rechtliche Kontrolle fehlt.
Biometrische Datenerfassung und Personenerkennung	Verletzung informationeller Privatheit. Preisgebung von persönlichen Daten auf biometrischem Pass.	Nützlich bei der Verhinderung von gefälschten Papieren. Für die Kontrolle von Terroristen muss man wissen, wen man sucht, um ihn auf zuhalten. Terroristen mögen vielleicht nun biometr. kontrollierte Gebiete und Landesübergänge meiden, zur Verhinderung trägt dies aber nicht viel bei.
Überwachungskameras und Gesichtserkennung	Durch übertriebene Überwachung (siehe London) ist man in der Öffentlichkeit extrem eingeschränkt, Gefahr der panoptischen Gesellschaft.	Durch Verhaltensmuster, Gangart oder tragen einer auffälligen Tasche lassen sich keine Terroristen aufspüren. Nur wenn man weiss, wen man sucht, hilft diese Massnahme.

¹⁹ Vom deutschen Koordinator der Nachrichtendienste vor dem Nichtständigen Ausschuss der Europäischen Parlaments abgegebenen Erklärungen vom 21.11.2000

3.4.3 Was tun gegen die Bedrohung der Privatsphäre?

Nach Par Ström²⁰ gibt grundsätzlich vier verschiedene Arten des Schutzes persönlicher Daten und der eigenen Privatsphäre:

- **Flächendeckende Gesetzgebung**
Innerhalb der EU deckt ein umfassendes Gesetz den Schutz der Privatsphäre sowohl im öffentlichen wie im privaten Bereich. Dies kann als wirksamster Schutz der Privatsphäre betrachtet werden.
- **Gesetze für bestimmte Bereiche**
Es gibt Länder, die kein umfassendes Gesetz zum Datenschutz haben. Stattdessen hat man Gesetze für verschiedene wirtschaftliche und gesellschaftliche Bereiche geschaffen. Dieser Weg wurde in den USA beschritten. Dort gibt es ein Gesetz für den Schutz der Privatsphäre beim Verleih von Videofilmen, bei der Beantragung einer Bankkredits, bei der telefonischen Werbung usw. Der Nachteil ist, dass jeder neue technische Bereich auch ein neues Gesetz erfordert; die Gesetze hinken also stets den Entwicklung hinterher. Auch kann ein bestimmter Bereich sozusagen „zwischen den Stühlen“ landen, und das Fehlen von Kontrollinstanzen kann zu Problemen führen.
- **Selbstregelung des Marktes**
Ein dritter Weg wäre der Verzicht auf jegliche Gesetzgebung, also das Vertrauen auf die „selbstregulierende Kräfte“ des Marktes. In den USA sind weite Bereiche der Selbstregulierung überlassen. Die wirtschaft entwickelt auf freiwilliger Basis einen bestimmten Verhaltenskodex, häufig unter Zuhilfenahme ihrer Branchenverbände. Wie die berichtsbezogene Gesetzgebung bietet auch die Selbstregulierung einen schwächeren Schutz der Privatsphäre, und auch hier kann das Fehlen von Kontrollinstanzen Probleme mit sich führen.
- **Technische Lösungen**
Der Einzelne kann sich selbst mittels geeigneter Technologie schützen. Beispiele für diese Technik sind Programme für Chiffrierung, für anonyme E-Mail-Beförderung sowie für anonyme Finanztransaktionen. Diese rein technischen Lösungen haben mehrere Nachteile: Sie erfordern einen gewissen Zeitaufwand, sie bieten manchmal nur unzureichend Schutz und sie stehen nicht überall zur Verfügung, wo heute eine Bedrohung der Privatsphäre vorliegt.

²⁰ vgl. Ström Pär: Die Überwachungsmafia, Heyne Verlag 2006, S. 290ff

Folgende Massnahmen könnten also von einer Regierung, die es wirklich ernst meint mit dem Schutz der Privatsphäre, in Betracht genommen werden:

- Abstandnahme von jeglicher Informationsbeschaffung, die nicht dem Verhaltenskodex zur Handhabung der Informationstechnologie entspricht.
- Abstandnahme von Zusammenarbeit mit anderen Ländern im IT-Bereich, falls diese Länder nicht den genannten Verhaltenskodex anwenden.
- Schaffung eines Gesetzes, das den Transfer von digitalen Fingerabdrücken ohne Zustimmung der betroffenen Person verbietet.
- Abstandnahme von der Einführung eines „automatischen Gesetzesvollzuges“.
- Kein Abgleich zwischen öffentlichen (obligatorischen) Datenbanken und privaten bzw. halb privaten (freiwilligen) Datenbanken.
- Jährliche Überprüfung der Gesamtsituation für Datenschutz und Schutz der Privatsphäre in einem Land seitens einer unabhängigen Ombudstelle.
- Informierung der Öffentlichkeit über die Risiken der Verletzung der Privatsphäre und über die Möglichkeit von Gegenmassnahmen.
- Schaffung technischer und politischer Mittel, um die Bürger des eigenen Landes vor den im Ausland stationierten Überwachungssystemen wie Echelon, TIA usw. zu schützen, sowie Informierung der Öffentlichkeit über solche Systeme.
- Technische Verfahren wie Chiffrierung, Anonymisierung usw. sind mit der Rede- und Pressefreiheit gleichzustellen und im Grundgesetz zu schützen. Erwägung eines Gesetzes für den IT-Bereich, das Internet- und Telekomfirmen dazu verpflichtet, ihr Dienstleistungsangebot mit solchen Verfahren zu ergänzen.

4 Schlusswort

Mit Erstaunen entdeckt man, wie gering viele Menschen offenbar ihre Privatsphäre schätzen (Beispiel in Grossbritannien, London). Es darf nicht sein, dass in der heutigen Überwachungsmethoden als „Nutzen zur Terrorverhinderung“ geltend gemacht werden, damit Politiker und Mitmenschen keinen grossen Einwand mehr haben bei einem Eingriff in ihre und „unsere“ Privatsphäre. Das ist eine „Politik der Angst“ und schlussendlich eine bewusste Folge des Terrorismus. Durch mangelndes Problembewusstsein opfern diese Menschen gern ihre Anonymität und setzen sich für digitale Überwachungssysteme ein. Die Aufgabe, die Privatsphäre zu bewahren, wird durch Annehmlichkeiten wie unsere Bequemlichkeit erschwert. Protest ist immer unbequem, deshalb akzeptieren wir leicht das, was uns geboten wird. Die neue Technik bietet uns ausserdem in bestimmten Fällen ein stromlinienförmiges, reibungsloses Dasein, falls wir unsere Anonymität aufgeben und Informationen über uns zugänglich machen. Mehr Sicherheit, ein wachsendes Bedürfnis des Schutzes vor Kriminalität und Terroranschlägen ist festzustellen. Finanzielle Vorteile und auch eine Art imaginäre „Gerechtigkeit“ verlocken uns ebenfalls, ein Teil unserer Privatsphäre herzugeben.

Die Bücher von Pär Ström und Christiane Schulzki-Haddouti haben mich wirklich beeindruckt und mein vorerst enthusiastisches Denken gegenüber neuen Massnahmen zur Terrorverhinderung stark beeinflusst. Ich kann den Lesern meiner Arbeit nur empfehlen sich über solche Massnahmen und Überwachungssysteme ausgiebig zu informieren. Telepolis und andere Netz-Magazine behandeln solche Themen und sind eine gute Ergänzung zur alltäglichen Lesezeitschrift. Die Wichtigkeit der Privatsphäre darf nicht in Vergessenheit geraten, denn die Privatsphäre ist wie Sauerstoff; erst wenn er weg ist, bemerkt man, dass er fehlt.

5 Glossar

A

agitatorisch (abwertend) aggressiv [für politische Ziele] tätig, hetzerisch	6
asymmetrische Asymmetrische Strategie oder Organisationsaufbau beruhen nicht auf klassischen Methoden sondern sind ungleichmässig und unregelmässig	10
Autonomie Unabhängigkeit, Selbstverwaltung	11

B

Biometrie Die Biometrie (auch Biometrik,) beschäftigt sich mit Messungen an Lebewesen.....	17
--	----

C

CAPPS II Computer Assisted Passenger Prescreening System.....	21
chiffriert verschlüsselt	22
CIA Central Intelligence Agency, Zentraler Nachrichtendienst.....	24
COMINT Communications Intelligence	23

D

DARPA Defense Advanced Research Projects Agency.....	14
Data-Mining-System Unter Data-Mining versteht man die Anwendung von (statistisch-mathematischen) Methoden auf einen Datenbestand mit dem Ziel der Mustererkennung.....	16
Datenschutz Schutz personenbezogener Daten vor Missbrauch.....	27
<i>dezisionale</i> private Entscheidungen und Handlungen.....	11

E

<i>Eletronic Privacy Information Center</i> EPIC ist eine Bürgerrechtsorganisation in Washington D.C. die unter anderem für den Schutz der Privatheit kämpft.....	13
---	----

F

FBI Federal Bureau of Investigations, Bundesuntersuchungsamt	24
---	----

G

Genfer Konvention internationale vertragliche Vereinbarung.....	5
--	---

GPDeI	
Geschäftsprüfungsdelegation	22
Guerilla	
Kleinkrieg mit nichtregulären Kombattanten.....	7

I

IAO	
Information Awareness Office	14
Identix	
Hersteller von biometr. Erkennungssystemen.....	20
Ideologie	
eine Denkweise über Mensch und Gesellschaft.....	5

K

konfliktieren	
widerstreiten, widersprechen.....	12
konstitutiv	
wesentlich, grundlegend.....	12

L

legitim	
legal, rechtmäßig, im Rahmen der Gesetze erlaubt	6
low-intensity/low-density form of warfare	
niederschweilliger Krieg gegen das "Reich des Bösen"	16
low-tech	
wenig Technologie, bei der Überwachung z.B. Beschattung durch eine andere Person	14

M

Mikrowellen	
elektromagnetische Wellen, deren Wellenlänge zwischen 100 cm und 1 mm liegt.....	25

N

nationaler Terrorismus	
Nationaler Terrorismus beschränkt sich in Zielsetzung und Aktionsradius auf das Territorium eines Staates....	8
NSA	
National Security Agency, Nationale Sicherheitsbehörde	24

O

Onyx	
(griechisch = Krallen) Satellitenabhörsystem des schweizerischen Nachrichtendienstes	22
oppressiv	
unterdrückend, bedrückend.....	6
Orwells 1984	
ist ein Roman von George Orwell (eigentlich Eric Blair), erschienen im Juni 1949, in dem die negative Utopie (auch als Dystopie oder Anti-Utopie bezeichnet) eines totalitären Überwachungs- und Präventionsstaates im Jahre 1984 dargestellt wird.....	11

P

Parabolantenne	
bündelt Mikrowellenstrahlung im Brennpunkt eines Parabolspiegels.....	24
präventiv	

vorbeugend, verhütend	8
vorbeugend	8
Prima facie (lat. „auf ersten Blick“) bedeutet „bis auf Widerruf“	11
Proliferation Proliferation bedeutet die Weiterverbreitung von Massenvernichtungswaffen bzw. der zu ihrer Herstellung benötigten Produkte einschließlich des dafür erforderlichen Know-hows sowie von entsprechenden Waffenträgersystemen.....	22

S

Statewatch Bürgerrechtsbewegung mit Sitz in London.....	27
--	----

T

Terror Schreckensherrschaft, systematische Verbreitung von Angst und Schrecken.....	7
TIA Terrorism Information Awareness	14
Transportation Security Administration	22
transnationalen Terrorismus Transnationaler Terrorismus hat weite Teile der Welt als Ziele im Visier und will die Änderung der internationalen Ordnung erreichen. Der transnationale Terrorismus wird oft auch als <i>internationaler</i> <i>Terrorismus</i> bezeichnet	8

V

Vereinten Nationen United Nations, UN	8
--	---

W

WMD Weapons of Mass Destruction	22
--	----

6 Quellenverzeichnis

Literatur

Privat! Telepolis Kontrollierte Freiheit in einer vernetzten Welt

Ralf Grötter

Erschienen: März 2003

ISBN: 3936931011

Erschienen bei: Heise Heinz

Im Netz der inneren Sicherheit. Die neuen Methoden der Überwachung

Christiane Schulzki-Haddouti

Erschienen: September 2004

ISBN: 3434505822

Verlag: Europäische Verlagsanstalt

Vom Ende der Anonymität. Die Globalisierung der Überwachung

Christiane Schulzki-Haddouti

Erschienen: Auflage 2, 2001

ISBN: 3882291850

Verlag: Europäische Verlagsanstalt

Die Überwachungsmafia. Das lukrative Geschäft mit unseren Daten-

Pär Ström

Erschienen: August 2006

ISBN: 3453620100

Verlag: Heyne

Unter Kontrolle

Gerald Reischl

Erschienen: 2002

ISBN: 3832308857

Verlag: Ueberreuter Wirtschaft

Terrorismus. Eine kurze Einführung

Charles Townshend

Erschienen: Februar 2004

ISBN: 3150183014

Verlag: Reclam, Ditzingen

Universitätsarbeiten (veröffentlichte):

Gunther Tichy und Walter Peissl
Beeinträchtigung der Privatsphäre in der Informationsgesellschaft
<http://www.oeaw.ac.at/ita/ebene5/GTWPweissenbach.pdf>
Mai 2001

PD Dr. Mir A. Ferdowsi
Maßnahmen im Bereich der Terrorismus-Bekämpfung
http://www.forschungsstelle-dritte-welt.de/Dokumente/paper/SS04_UN_Ue/HA_VNTerror_TK.pdf
2004

Dominik Prosenjak
Völker- und europarechtliche Regelungen zum Problem des Terrorismus
<http://www.uni-koeln.de/jur-fak/ostrecht/WS2005-06/dt-ru-Seminar/Prosenjak.pdf>
2004

Thomas Petermann. Arnold Sauter
Biometrische Identifikationssysteme
<http://www.tab.fzk.de/de/projekt/zusammenfassung/ab76.pdf>
2002

Hans-Joachim Heintze
Völkerrecht im Anti-Terror-Kampf
<http://scholar.google.com/url?sa=U&q=http://www.ruhr-uni-bochum.de/ifhv/red/heintzereferendar.pdf>
2002

Jaumann
Möglichkeiten des Strafrechts zur Bekämpfung des neuen Terrorismus
http://scholar.google.com/url?sa=U&q=http://homepages.uni-tuebingen.de/student/daniel.jaumann/terrorismus_strafrecht_jaumann.pdf
2004

Gesetzesartikel in der Schweiz

Überwachung
http://www.gesetze.ch/SR/780.1/780.1_001.htm

Terrorismus
http://www.gesetze.ch/sr/0.361.418.1/0.361.418.1_001.htm

Grundrechte Freiheit/Privatsphäre
http://www.gesetze.ch/sr/131.222.2/131.222.2_002.htm

Bekämpfung des Terrorismus in der EU
<http://europa.eu/scadplus/leg/de/lvb/l33219.htm>
<http://europa.eu/scadplus/leg/de/lvb/l33220.htm>

Thesepapiere:

Menschenrechtskonvention/Konvention zum Schutz der Menschenrechte und Grundfreiheiten/4.
November 1950

http://members.aon.at/sources/f_WAT/assets/pdf/emrk.pdf

Zugriff am 13.1.2004

Florentine Barckhausen

Ist die Privatsphäre noch zu retten?

Vor- und Nachteile von Data Mining, Videoüberwachung und Biometrie

http://viadrina.uni-frankfurt-o.de/~sk/diges/privacy_the.html

1999

Catherine Weber

Überwachung ist der falsche Weg

http://www.raben-net.ch/ficherman/neue_texte/ueberwachung_der_falsche_weg.htm

2001

Stefan Krempf

Überwachungsstaat

<http://www.heise.de/tp/r4/artikel/9/9914/1.html>

2001

Herbert Huber

Überwachung des Bürgers durch den Staat

<http://www.gavagai.de/gg/HHD91GB.htm>

Bis 2006

Meldungen:

Privacy International:

About Anti-Terrorism Policies and the Open Society

[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-65421&als\[theme\]=Anti%20Terrorism](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65421&als[theme]=Anti%20Terrorism)

September 2001

Terrorism Profile - EU

[http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-508362&als\[theme\]=Anti%20Terrorism](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-508362&als[theme]=Anti%20Terrorism)

Oktober 2005

Telepolis (Magazin für Netzkultur)

<http://www.heise.de/tp/r4/artikel/23/23941/1.html>

<http://www.heise.de/tp/r4/artikel/20/20677/1.html>

<http://www.heise.de/tp/r4/artikel/20/20490/1.html>

<http://www.heise.de/tp/r4/artikel/16/16994/1.html>

<http://www.heise.de/tp/r4/artikel/17/17006/1.html>

<http://www.heise.de/pda/newsticker/m73450.html>

<http://www.heise.de/tp/r4/artikel/19/19543/1.html>

<http://www.heise.de/tp/r4/artikel/21/21853/1.html>

Weitere Internetadressen:

<http://www.3sat.de/3sat.php?http://www.3sat.de/nano/cstuecke/24567/index.html>

http://www.mitmischen.de/article_detail.php?reportId=3493&sumMsg=6¤tReportPage=1&topicId=3447

<http://www.gulli.com/netzwelt/ueberwachung/emailueberwachung/>

<http://www.taz.de/blogs/paranoia/>

http://www.computerwoche.de/produkte_technik/netzwerke/544015/

<http://www.3sat.de/3sat.php?http://www.3sat.de/nano/cstuecke/24567/index.html>

http://www.bpb.de/publikationen/TLP3LA,0,0,Neue_Gefahren_verlangen_neue_Politik_Multilateralism_us_statt_Dominanz.html

<http://www.european-security.com/index.php?id=4009>

<http://www.european-security.com/index.php?lg=DE>

http://www.admin.ch/cp/d/436b64d4_1@fwsrvg.html

http://www.bpb.de/themen/38L6XK,0,0,Terror_und_Sicherheit.html

http://www.bpb.de/veranstaltungen/DXKVCA,1,0,Erscheinungsformen_Wurzeln_und_aktuelle_Entwicklungslinien_im_Terrorismus.html#art1

http://scholar.google.com/scholar?hl=de&lr=&client=firefox-a&q=cache:ZurHaXbMhHYJ:www.cx.unibe.ch/krim/Vorlesungen/W2044_Arbeiten_4.pdf+terrorismus+gefahren

Mit Biometrie gegen den Terrorismus

http://www.nadir.org/nadir/initiativ/kombo/k_47/k_47biomet.htm

Panoptikon

<http://www.bleyenberg.de/panoptikon/main.htm>

Gefundene Interviews:

<http://www.gulli.com/news/kai-raven-im-gespraech-wenn-du-2007-02-10/>

<http://www.gulli.com/news/was-tun-gegen-die-2007-02-11/>

7 Erklärung

Hiermit erkläre ich, dass ich diese Arbeit selbst und nur mit den aufgeführten Quellen sowie den zugelassenen Hilfsmitteln verfasst habe.

Ried-Muotathal, März 2007

Reto Schelbert