Sicherheit durch Überwachung?

Eine Arbeit von Patrick Bucher, Ruedi Hauri, Dominic Kurmann und Philipp Rölli

Inhaltsverzeichnis

Einleitung

Überwachung ist heute allgegenwärtig. An öffentlichen Orten, wie z.B. am Bahnhof wird man von zahlreichen Überwachungskameras verfolgt, in der Migros wird mithilfe des Cumulus-Kärtchens das Konsumverhalten der Kunden aufgezeichnet und am Arbeitsplatz nimmt oftmals eine sog. Controlling-Abteilung die Angestellten genauer unter die Lupe. Meistens weiss man überhaupt nicht, welche Informationen überhaupt erhoben werden, ob und wie eine Speicherung dieser Daten stattfindet und wer überhaupt auf diese Daten zugreifen kann und sie dann auswertet. Dies führt uns bereits zu unserer ersten Hauptfrage:

1. *Mit welchen technischen Mitteln überwacht der Staat seine Bürger, die Wirtschaft die Konsumenten?*

Daten werden mit den verschiedensten technischen Mitteln erhoben, abgespeichert und ausgewertet. Dies geschieht oftmals unter einem grossen Aufwand. So müssen Überwachungskameras nicht nur erworben und angebracht werden, einen viel grösseren Aufwand stellt die Auswertung der Videos – der erhobenen Daten – dar. Auch die Privatwirtschaft lässt sich die Überwachung ihrer Mitarbeiter einiges kosten. Die Angestellten einer Controlling-Abteilung, nicht selten gut ausgebildete Fachkräfte, wollen schliesslich für ihre Arbeit entschädigt werden. Es gibt mittlerweile ganze Wirtschaftszweige, die von der Herstellung von sog. „Sicherheitstechnologie“ leben. Wenn man so einen gewaltigen Aufwand betreibt, möchte man doch etwas dafür zurück bekommen. Wozu betreibt man also diesen ganzen Aufwand? So sind wir bei der zweiten Hauptfrage unserer Arbeit angelangt:

2. *Wozu dient eigentlich Überwachung, was will man damit erreichen?*

Derzeit sind einige Tendenzen zu erkennen, die unsere demokratischen Staaten immer näher an die Welt von Orwell's *1984* (ein totalitärer Polizeistaat) rücken. In den USA ist man seit den Terroranschlägen vom 11. September 2001 besonders vorsichtig, der sog. *Patriot Act* gibt dem Staat mehr Befugnisse zur Überwachung seiner Bürger, letztere verlieren immer mehr von ihrer Privatsphäre. Auch in Deutschland sind solche Tendenzen zu erkennen, jüngst wurde unter Federführung des deutschen Innenministers Wolfgang Schäuble die sog. *Vorratsdatenspeicherung* beschlossen, wonach Verbindungsdaten von Telefon, Internet und E-Mail für eine bestimmte Zeit abgespeichert werden müssen. Dies mag wohl so manchen an die ehemalige DDR und an die Stasi-Zeit erinnern – es geschieht alles im Namen der Sicherheit. Überwachung und Bespitzelung ist also kein Phänomen des hochtechnisierten 21. Jahrhunderts, Überwachung gab es schon früher und wird es wohl auch immer geben. Folge dessen sollte es auch Fälle geben, in denen die Überwachung der Sicherheit gedient hat, Fälle, in denen die Überwachung zur Aufklärung von Verbrechen beigetragen hat. Will man etwas über die Zukunft erfahren (werden durch eine gesteigerte Überwachung mehr Verbrechen aufgeklärt oder verhindert?), lohnt es sich oftmals einen Blick in die Vergangenheit zu werfen. Dies führt uns zu unserer dritten Frage hin:

3. *In welchen konkreten Fällen führt(e) Überwachung zu mehr Sicherheit?*

Betrachten wir die Thematik der Überwachung für einmal ganz naiv; Überwachung dient der Sicherheit, durch Überwachung wird mehr Sicherheit geschaffen. Wir sollten also froh darüber sein, überwacht zu werden, wir sollten uns über jede Überwachungskamera freuen und wir sollten beglückt sein, wenn wir unter unserem Schreibtisch eine Wanze zu Gesicht bekommen – es dient ja schliesslich alles zu unserer Sicherheit, es ist nur zu unserem Besten! Im wirklichen Leben freut sich aber kaum jemand über die Fülle der Überwachungskameras an öffentlichen Plätzen. Auch freut man sich wohl kaum darüber, von einer Wanze abgehört zu werden. Es gibt also irgendetwas, das wir als Preis für eine höhere Sicherheit zu bezahlen haben. An diesem Etwas stören sich viele Bürger, sie wollen nicht in dem Ausmass für die (vermeintliche?) Sicherheit bezahlen, in der sie es tun sollten. In der vierten und somit letzten Frage geht es also darum, was denn dieses Etwas ist, woran sich der überwachte Bürger stört:

4. *Worin besteht eine Bedrohung durch Überwachung, was soll sich der Bürger daran stören?*

Die Beantwortung all dieser Fragen ist unser Ziel für diese Arbeit. Dabei müssen wir realistisch bleiben; so können wir bei der ersten Frage kaum auf alle technischen Mittel eingehen, bei der dritten Frage ist uns nur die Nennung einiger bedeutender Fälle möglich. Auch die Frage nach der Motivation hinter der Überwachung können wir wohl kaum im Rahmen einer Maturaarbeit abschliessend beantworten, für die Beantwortung dieser Frage könnte man ganze Bücher schreiben. Was sich der Bürger an der Überwachung stört, kann ebenfalls nicht pauschal beantwortet werden, hier gibt es eine Vielzahl an Meinungen, wobei wir hoffen, die wichtigsten Bedrohungen, die von Überwachung ausgehen, nennen zu können.

Organisation der Arbeit

Die vier Fragen werden jeweils durch die vier Teammitglieder einzeln bearbeitet, jedes Teammitglied verfasst somit ein Kapitel über seine Frage. Es ergibt sich somit folgende Arbeitsaufteilung:

Teammitglied	Kapitel	Frage
Dominic Kurmann	1 – Technische Mittel zur Überwachung	*Mit welchen technischen Mitteln überwacht der Staat seine Bürger, die Wirtschaft die Konsumenten?*
Ruedi Hauri	2 – Sinn und Zweck der Überwachung	*Wozu dient eigentlich Überwachung, was will man damit erreichen?*
Philipp Rölli	3 – Konkrete Fälle von Überwachung	*In welchen konkreten Fällen führt(e) Überwachung zu mehr Sicherheit?*
Patrick Bucher	4 – Bedrohung durch Überwachung	*Worin besteht eine Bedrohung durch Überwachung, was soll sich der Bürger daran stören?*

Im Verlauf der Arbeit kann es immer wieder vorkommen, dass sich einzelne Inhalte überschneiden. In diesem Fall werden bestimmte Textstellen von einem Kapitel zu einem anderen verschoben. Die obige Arbeitsaufteilung ist somit nicht absolut zu sehen, sondern stellt vielmehr die Hauptverantwortlichkeit der einzelnen Personen für jedes Kapitel dar.

Im Schlussteil geht es darum, dass jede Person die Frage des jeweiligen Kapitels kurz (in 3-4 Sätzen) zu beantworten versucht. Weiter soll hier die Arbeit an den einzelnen Kapiteln durch das jeweilige verantwortliche Teammitglied reflektiert werden. Konnte die Frage beantwortet werden, wie ist man vorgegangen, mit welchen Schwierigkeiten hatte man allenfalls zu kämpfen?

Ganz zum Schluss soll versucht werden, die Hauptfrage dieser Arbeit „*Sicherheit durch Überwachung?*“ zu beantworten.

1 Technische Mittel zur Überwachung

Durch den rasanten Anstieg von elektronischen Geräten, die uns im Alltag umgeben, bieten sich immer mehr Möglichkeiten, persönliche Daten zu erfassen und für verschiedenste Zwecke zu verwenden.

In diesem Kapitel möchten wir die bestehenden technischen Möglichkeiten aufzeigen, die Staat und Wirtschaft besitzen um sein Volk bzw. seine Konsumenten zu überwachen. Die folgenden Überwachungsmethoden haben wir aus verschiedenen Ländern zusammengetragen. Generell könnten wir nach heutigem technischen Stand all diese Methoden auch in der Schweiz vorfinden, was unsere Gesetzeslage glücklicherweise zum grössten Teil noch verhindert. Ein besonderes Augenmerk richten wir dabei auf Deutschland, wo sich in letzter Zeit sehr brisante Gesetzesentscheide zugetragen haben, die unserer Meinung nach mit dem Schutz der Privatsphäre arg in Konflikt stehen.

1.1 Videoüberwachung

Videoüberwachungsanlagen dienen der Beobachtung mittels optisch-elektronischer Einrichtungen. Im englischen Sprachraum sind diese Anlagen unter dem Begriff *Closed Circuit Television* (CCTV) bekannt, was sich vom geschlossenen Benutzerkreis ableitet, der berechtigt ist, die aufgenommenen Bilder und Videosequenzen zu betrachten. So erfolgt innerhalb dieses Begriffs eine Abgrenzung zum öffentlichen Fernsehen. Haupteinsatzgebiet von Videoüberwachungsanlagen ist die Überwachung von öffentlichen und privaten Räumen wie auch die Überwachung des Strassenverkehrs.

Herkömmliche Videoüberwachungsanlagen bestehen aus mindestens einer Überwachungskamera und einem Anzeigemonitor, optional erlauben die Systeme eine Aufzeichnung der Bilder (beispielsweise auf Videoband). Die Übertragung erfolgt oftmals analog, zunehmend jedoch auch digital. Dabei gibt es kabelgebunde sowie kabellose Systeme.

Abbildung 1: Piktogramm Überwachungskamera

Neuere Videoüberwachungsanlagen benutzen oft digitale Kameras, die über ein *TCP/IP*[1]-Netzwerk an einen Computer angeschlossen werden (IP-Kameras). Über eine spezielle Videoüberwachungssoftware können zusätzliche Funktionen, wie beispielsweise Bewegungserkennung, Gesichtserkennung und Speicherung der Bilder vorgenommen werden.

Privatpersonen, Firmen und staatliche Einrichtungen versuchen mittels Videoüberwachungsanlagen ihre Gebäude und Areale vor Übergriffen, wie Einbruch, Diebstahl, Vandalismus und Sabotage zu schützen bzw. bei möglichen Verstössen schnell eingreifen oder im Nachhinein die Täter identifizieren zu können. Auf Motive der (Video-) Überwachung wird im zweiten Kapitel genauer eingegangen.

Des weiteren werden von der Polizei nebst herkömmlichem Filmen und Fotografieren mobile Überwachungskameras eingesetzt, um Demonstrationsteilnehmer zu überwachen, persönlich zu identifizieren und um deren Verstösse gegen Demonstrationsauflagen und Gesetze zu dokumentieren.

Durch die Umstellung von analogen auf digitale Systeme haben sich im Bereich der Videoüberwachung folgende Neuerungen zugetragen:

- Vereinfachte Bildsuchen durch digitale Betrachtungsprogramme
- Vereinfachte Archivierung und Speicherung
- Versand der Bilder an Drittpersonen in Sekundenschnelle (via Internet)
- Automatische Gesichts- und Nummernschilds-Erkennung; CCTV-Bilder werden mit denen aus einer Datenbank verglichen und auf Übereinstimmungen hin überprüft. Besonders die

1 http://de.wikipedia.org/wiki/TCP/IP

Erkennung von Gesichtern ist aber oft sehr schwierig, da viele der Kameras keine klaren Bilder bekommen oder der Gesuchte sich verkleidet hat (Vermummung, Sonnenbrille).

- Automatische Verfolgung; Systeme können Personen und Objekte automatisch von Kamera zu Kamera verfolgen.
- Automatische Erkennung auffälligen Verhaltens; Computersoftware kann sog. „auffälliges Verhalten“ entdecken und melden. Es handelt sich hierbei beispielsweise um schnelle Bewegungen, Menschenansammlungen oder das Abstellen von Gegenständen (potentielle Sprengkörper).

1.2 Telekommunikation

Auch in Zeiten des Internet erfolgt ein grosser Teil unserer Kommunikation via Telefon. Der Trend hin zu Mobiltelefonen erlaubt es uns überall zu telefonieren, ja sogar unterwegs auf das Internet zuzugreifen. Gerade Mobiltelefone haben jedoch einige Konsequenzen im Zusammenhang mit dem Thema Überwachung.

1.2.1 Funkzellenortung

Mit Hilfe der Funkzellenortung kann derjenige Sendemast bestimmt werden, mit dem ein Mobiltelefon zum Ortungszeitpunkt verbunden ist. Durch zusätzliche Massnahmen kann der Standort innerhalb einer Funkzelle noch präzisiert werden (z.B. durch die Bestimmung der Hauptstrahlungsrichtung des Senders). Zur Ortung wird eine Verbindung zum Mobiltelefon aufgebaut, etwa durch den Versand einer SMS. Mittels eines sog. *stealth ping* kann diese Verbindung auch vom Nutzer unbemerkt aufgebaut werden. Die Ortung wird vom jeweiligen Mobilfunkanbieter durchgeführt. Dieser Dienst steht jedem Kunden für sein eigenes Mobiltelefon zur Verfügung. Bei Notrufen, Gefahr im Verzug oder auf richterliche Anordnung hin müssen die Mobilfunkanbieter eine Ortung auch ohne Einwilligung des Inhabers durchführen und die Daten weitergeben. Durch diese Technik lässt sich praktisch von jeder Person zu einem beliebigen Zeitpunkt der Standort bestimmen. Weiter können damit sog. *Bewegungsprofile* erstellt werden.

1.2.2 Das Handy als Wanze

Durch die technische Entwicklung im Bereich der Mobiltelefone lassen sich nicht nur ein- und ausgehende Telefonanrufe aufzeichnen, auch die Möglichkeit, das Handy als Wanze zu benutzen besteht bereits. Von der Polizei manipulierte Mobiltelefone können zum Abhören Verdächtiger eingesetzt werden. Dabei wird die Software der Mobiltelefone so manipuliert, dass die Freisprecheinrichtung aktiviert wird, ohne dass der Besitzer des Mobiltelefons es merkt.

Abbildung 2: Handy oder Wanze?

Demzufolge ist die Software-Manipulation relativ einfach, wenn die Polizei das Gerät in die Hand bekommt. Möglich ist sie aber auch über Datenschnittstellen wie *Bluetooth*[2] oder *WLAN*[3]. Zudem lassen sich in Spielen, Bilddateien oder Klingeltönen so genannte *trojanische Pferde*[4] verstecken, die entsprechende Änderungen vornehmen.

2 http://de.wikipedia.org/wiki/Bluetooth

3 http://de.wikipedia.org/wiki/WLAN

4 http://de.wikipedia.org/wiki/Trojanisches_Pferd_%28Computerprogramm%29

Die Software des Telefons kann gar so programmiert werden, dass auch ein vermeintlich abgeschaltetes Handy als Wanze fungieren kann. Bei dem manipulierten Gerät erlischt demnach zwar das Display und Anrufe werden nicht mehr angenommen, das Gerät bleibt aber dennoch betriebsbereit und reagiert auf ein bestimmtes Signal der Polizei. Während der Verdächtige glaubt, sein Mobiltelefon sei ausgeschaltet, überträgt es über die Freisprecheinrichtung alle Geräusche aus der Umgebung.

Durch mangelndes Sicherheitsbewusstsein vieler Leute lassen sich so auf einfachem Wege mit geringem Aufwand Lauschangriffe starten.

1.3 Die Online-Durchsuchung

Als Online-Durchsuchung wird der verdeckte, staatliche Zugriff auf fremde, informationstechnische Systeme über Kommunikationsnetzwerke bezeichnet. Der Begriff umfasst dabei sowohl den einmaligen Zugriff, wie auch eine sich über einen längeren Zeitraum erstreckende Überwachung. Als bisher in Deutschland gesetzlich nicht ausdrücklich geregelte Methode staatlicher Informationsgewinnung, soll die Online-Durchsuchung im Rahmen der Strafverfolgung, zur polizeilichen Gefahrenabwehr oder zur nachrichtendienstlichen Informationsbeschaffung eingesetzt werden.

Haben die Ermittler eine Zielperson hinreichend ausgespäht, liegt es an einem Team des BKA (Bundeskriminalamt Deutschlands) einen Weg zum PC des Verdächtigen zu finden. Dies mag in seltenen Fällen tatsächlich ein trojanisches Pferd sein, das dem Verdächtigen als E-Mail zugestellt wird. Aufgrund der mageren Erfolgsaussichten des Weges via E-Mail bevorzugt man jedoch das heimliche Eindringen in die Wohnung des Verdächtigen, worauf Kopien von den lokalen Datenträgern (Festplatten) erstellt werden. Auch kann der Computer des Verdächtigen vor Ort mit einem trojanischen Pferd infiziert werden.

1.3.1 Remote Forensic Software

Im Falle einer Hausdurchsuchung ist es auch möglich, dass eine sog. *Remote Forensic Software* (RFS) ihren Weg auf den Computer des Betroffenen findet. Bei solchen Programmen handelt es sich nicht um standardisierte trojanische Pferde, sondern eher um Wanzen, welche Daten spezialisiert auf die jeweilige Fahndung erheben und an das BKA weiterleiten.

Damit die *Firewall*[5] (Schutzsoftware, die den ein- und den ausgehenden Datenverkehr überwacht) des Betroffenen nicht Alarm schlägt wenn die RFS Daten zum BKA sendet, kann die Untersuchungsbehörde die Sicherheits-Software vor Ort (bei der geheimen Hausdurchsuchung) so einstellen, dass sie die Aktivitäten der „Computer-Wanze“ immer zulässt. Verschlüsselt die Zielperson seine Daten mithilfe eines anderen PCs, bevor er sie über einen das Internet versendet, könnte das Tool den Verschlüsselungscode (per sog. *Keylogging*[6]) abgreifen und an die betreffende Datei anhängen. Gleiches gilt für Passwörter – das BKA bekäme sämtliche Zugangsdaten frei Haus geliefert.

Generell lässt sich somit sagen, dass der physikalische Zugriff auf den PC fast jeden Sicherungsmechanismus umgehbar macht – selbst eine Verschlüsselung per *Smartcard*[7], welche die Zielperson immer bei sich trägt. In so einem Fall könnte die Smartcard mittels *Hardware-Keylogging* mitgelesen werden. Eine technisch einfachere Alternative stellt es dar, einfach das Monitorkabel anzuzapfen und das Bildsignal entsprechend an die Ermittlungsbehörde weiterzuleiten.

Der riesige Aufwand, den das BKA dafür betreiben muss, kann auf den ersten Blick eher positiv wirken, schliesst er doch dadurch einen breit angelegten digitalen Angriff auf die Bevölkerung aus.

5 http://de.wikipedia.org/wiki/Personal_Firewall

6 http://de.wikipedia.org/wiki/Keylogger

7 http://de.wikipedia.org/wiki/Smartcard

Die Zahl der Fälle, in denen ein RFS-Einsatz in Frage käme, liegt derzeit im einstelligen Bereich. Der BKA-Chef fordert ausserdem eine umfassende richterliche Kontrolle der Online-Durchsuchung per Gesetz.

Was kann man gegen solche Remote Forensic Software unternehmen? Wenn das BKA alle Register zieht, gibt es wohl keine praktikable Schutzmöglichkeit. Solange die Online-Durchsuchung aber so aufwendig ist, braucht man sich nicht ernsthaft über eine willkürliche Durchsuchung Sorgen zu machen.

1.3.2 Die Möglichkeit zur Massenüberwachung

Derzeit also birgt die Online-Durchsuchung kein Potential zur Massenüberwachung. Was aber, wenn sich die technischen Möglichkeiten ändern? Wenn ein sog. *Bundestrojaner* in Zukunft tatsächlich zuverlässig und mit geringem Aufwand eingeschleust werden kann, dann wäre ein Orwell-Szenario denkbar, sofern die Datenschutzgesetze weiter aufgeweicht werden.

Sollte diese Praxis bei unserem nördlichen Nachbarn ausgeweitet werden und zu Ermittlungserfolgen führen, so wird wohl auch hierzulande eine Diskussion über den Einsatz einer solchen Technologie entstehen. Die Entwicklung ist somit zu verfolgen, auch wenn sie derzeit auf uns noch keinen direkten Einfluss zu haben scheint.

1.4 Vorratsdatenspeicherung

Vorratsdatenspeicherung bezeichnet die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Registrierung von elektronischen Kommunikationsvorgängen. Dies soll geschehen, ohne dass ein Anfangsverdacht oder konkrete Hinweise auf Gefahren bestehen würden. Die Vorratsdatenspeicherung ist eine Vorstufe der Telekommunikationsüberwachung. Die auf Vorrat zu speichernden Daten erlauben weitgehende Analysen persönlicher sozialer Netzwerke. Mit Hilfe der auf Vorrat zu speichernden Daten lässt sich – ohne dass auf Kommunikationsinhalte zugegriffen wird – das Kommunikationsverhalten jedes Teilnehmers analysieren. Verfassungsrechtlich ist die Vorratsdatenspeicherung umstritten, da sie ohne Anlass in die Privatsphäre sämtlicher Nutzer elektronischer Dienste eingreift. In dem Masse, in dem die Kommunikation über elektronische Medien zunimmt, wird die Bedeutung solcher Analysen für die Erstellung von Persönlichkeitsprofilen wachsen.

Nach dem Gesetz in Deutschland soll nachvollziehbar werden, wer mit wem in den letzten sechs Monaten per Telefon, Handy oder E-Mail in Verbindung gestanden ist oder das Internet genutzt hat. Bei Handy-Telefonaten und SMS soll auch der jeweilige Standort des Benutzers festgehalten werden, sog. *Anonymisierungsdienste* sollen verboten werden.

Mit Hilfe der über die gesamte Bevölkerung gespeicherten Daten können Bewegungsprofile erstellt, geschäftliche Kontakte rekonstruiert und Freundschaftsbeziehungen identifiziert werden. Auch Rückschlüsse auf den Inhalt der Kommunikation, auf persönliche Interessen und die Lebenssituation der Kommunizierenden werden möglich. Zugriff auf die Daten erhalten Polizei, Staatsanwaltschaft und ausländische Ermittlungsbehörden, die sich daraus eine verbesserte Strafverfolgung erhoffen.

Bisher durften Telekommunikationsanbieter nur die zur Abrechnung erforderlichen Verbindungsdaten speichern. Davon ausgeschlossen waren Standortdaten, Internetkennungen und E-Mail-Verbindungsdaten. Der Kunde konnte verlangen, dass Abrechnungsdaten mit Rechnungsversand gelöscht werden. Durch die Benutzung von Pauschaltarifen konnte eine Speicherung zudem gänzlich vermieden werden, was etwa für Journalisten und Beratungsstellen wichtig sein kann. All diese Mechanismen zum Schutz sensibler Kontakte und Aktivitäten beseitigt die Vorratsdatenspeicherung nun. Gegner dieser Praxis nennen unter anderem folgende Gründe für ihre Ablehnung:

- Die Vorratsdatenspeicherung stelle einen Einschnitt in die Privatsphäre dar.
- Die Vorratsdatenspeicherung beeinträchtige berufliche Aktivitäten (z.B. in den Bereichen Medizin, Recht, Kirche, Journalismus) ebenso wie politische und unternehmerische Aktivitäten, die Vertraulichkeit voraussetzen. Dadurch schade sie letztlich unserer freiheitlichen Gesellschaft insgesamt.
- Terrorismus oder Kriminalität könne durch die Vorratsdatenspeicherung nicht verhindert werden. Sie sei unnötig, da sie von „ernsthaften" Kriminellen umgangen werden könne.
- Die Kosten für die Vorratsdatenspeicherung müssen durch die Kommunikationsanbieter getragen werden, sie gefährde somit die Wirtschaft und Arbeitsplätze.
- Die Vorratsdatenspeicherung diskriminiere Nutzer von Telefon, Mobiltelefon und Internet gegenüber anderen Kommunikationsformen.

Zwar hat die Vorratsdatenspeicherung auf uns Schweizer derzeit keinen Einfluss (es sei denn, wir pflegen Kontakt zu den Bewohnern Deutschlands), eine solche Regelung könnte jedoch bald EU-weit gelten. Im Anbetracht eines möglichen Beitritts der Schweiz zur EU müssen wir uns auch hierzulande mit dieser Thematik auseinander setzen!

1.5 Verkehrsüberwachung

Ein Streifenwagen bei der Polizei von Queensland in Australien hat nicht nur eine GPS-Kanone im Kühlergrill, sondern zudem eine hochauflösende Kamera auf dem Dach, die in einer Zehn-Stunden-Schicht zwischen 5'000 und 8'000 Kennzeichen scannen und so zur Fahndung ausgeschriebene Fahrzeuge aus dem fliessenden Verkehr fischen kann. Ausserdem ist das Videoauge so programmiert, dass es Tempoverstösse messen kann. Damit der Sheriff dabei nicht einmal die Hände vom Lenkrad nehmen muss, verfügt sein Streifenwagen über einen leistungsfähigen Zentralrechner, der alle Funktionen per Sprachsteuerung aktivieren kann und zudem Kontakt zur Einsatzzentrale hält.

Ein solcher futuristischer Streifenwagen ist nur eines von vielen Beispielen, wie die Polizei künftig mit noch mehr Hightech Verkehrssündern und Kriminellen nachstellen will. Auch in Europa rüsten die Ordnungsbehörden auf. Durch London zum Beispiel fahren neuerdings zwei Smart-Modelle als elektronische Politessen. In der City of Westminster spielt der Winzling Big Brother und macht mit modernster Technik vor allem Jagd auf Falschparker.

Seine schärfste Waffe ist eine hochauflösende Digitalkamera, die an einem ausfahrbaren Stativ auf dem Dach sitzt. Wie das Periskop eines U-Boots lässt sich das Videoauge vom Beifahrer mittels Joystick ausfahren und in jede Richtung drehen. Dabei liefert es selbst auf grosse Entfernungen gestochen scharfe Vergrösserungen. Die Beamten peilen damit die Nummernschilder von Fahrzeugen an, die im Halteverbot stehen, Einfahrten blockieren, Busse behindern oder den Schulweg versperren.

Auch in Österreich hat der Autobahnbetreiber ASFINAG die erste von elf Kameras für jeweils rund 230'000 Euro in Betrieb genommen, die automatisch die Vignetten im fliessenden Verkehr kontrollieren und Mautpreller herausfiltern soll. Dafür nimmt das System von jedem vorbeifahrenden Auto ein Überblicksbild mit Kennzeichen sowie ein Detailbild der Windschutzscheibe auf. In einem zweiten Schritt sucht das Aufnahmesystem die Vignetten und prüft deren Gültigkeit. „Nur im Verdachtsfall werden die Bilder abgespeichert", ist die Aussage des dafür zuständigen Projektleiters. So ganz auf den Computer verlassen wollen sich die Österreicher jedoch nicht: Alle Beweisfotos würden zusätzlich manuell analysiert, beteuert die ASFINAG, die nur eindeutige Verstösse ahnden und „im Zweifel für den Kunden" entscheiden will.

Zwar müssen die Kameras sehr präzise sein um die winzigen Markierungen auf der Vignette zu erkennen, doch nehmen sie künftig noch viel feinere Details ins Visier. So hat das Unternehmen Procontour ein System entwickelt, das mit Hilfe von Lasern, Sensoren und Digitalkameras sogar im

fliessenden Verkehr auf der Autobahn die Profiltiefe eines Reifens bestimmen können soll. Erste stationäre Tests hat der Scanner „H3-D“ bereits bestanden, demnächst soll er auf der Strasse ausprobiert werden. Ziel sei eine Erhöhung der Sicherheit. „Würden auch nur zehn Prozent der Reifenmängel frühzeitig festgestellt und beseitigt, würde dies jährlich bis zu 6000 Unfälle verhindern können“, schreiben die Entwickler auf ihrer Internetseite.

1.6 RFID

Der englische Begriff *Radio Frequency Identification* (RFID) bedeutet zu deutsch „Identifizierung mit Hilfe von elektromagnetischen Wellen“. RFID ist ein Verfahren zur automatischen Identifizierung von Gegenständen und Lebewesen. Neben der berührungslosen Identifizierung und der Lokalisierung von Gegenständen steht RFID auch für die automatische Erfassung und Speicherung von Daten.

Ein RFID-System besteht aus einem *Transponder*, der sich am oder im Gegenstand bzw. Lebewesen befindet und diese kennzeichnet, sowie einem Lesegerät zum Auslesen der Transponder-Kennung. Das Lesegerät enthält eine Software (ein Mikroprogramm), das den eigentlichen Leseprozess steuert.

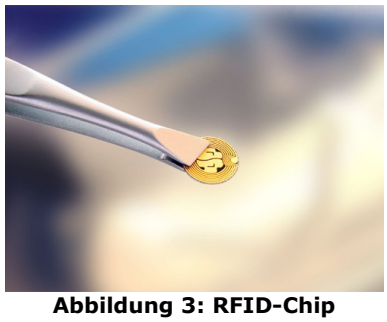

Abbildung 3: RFID-Chip

In der Regel erzeugt das Lesegerät ein elektromagnetisches Hochfrequenzfeld geringer Reichweite, vorzugsweise mit Induktionsspulen. Damit werden nicht nur Daten übertragen, sondern auch der Transponder mit Energie versorgt. Nur wenn grössere Reichweiten erzielt werden sollen und die Kosten der Transponder nicht kritisch sind, werden aktive Transponder mit einer eigenen Stromversorgung eingesetzt.

1.6.1 Einsatzgebiete für RFID

RFID-Transponder können so klein wie ein Reiskorn sein und demnach auch in Lebewesen implantiert werden, wie dies etwa bei Haustieren der Fall ist (in der Schweiz muss beispielsweise jeder Hund einen solchen Chip tragen[8]). Die schnelle Verbreitung dieser Technik ergibt sich aus der Kombination von geringer Grösse der Transponder, unauffälligen Auslesemöglichkeiten (z. B. neuer Pass) und geringem Preis der Transponder. Diese neue Technik verdrängt zunehmend den heute noch weit verbreiteten Barcode.

Die folgende Aufzählung enthält einige wichtige Gebiete für den Einsatz von RFID:

- Fahrzeugidentifikation
- Banknoten
- Identifizierung von Personen
- Echtheitsmerkmal für Medikamente
- Bekleidungssiegel
- Tieridentifikation
- Automobile Wegfahrsperre
- Waren- und Bestandesmanagement
- Positionsidentifikation
- Zutrittskontrolle

8 http://www.admin.ch/aktuell/00089/index.html?lang=de&msg-id=11072

Selbst an Grossanlässen, wie z.B. dem Luzerner Stadtlauf (~15'000 Teilnehmer), kommen RFID-Chips zum Einsatz. So erfolgt die Zeitmessung mithilfe eines RFID-Chips, der an jeder Startnummer angebracht ist.

1.6.2 Das Risiko von RFID

RFID ist eine zurecht als risikobehaftet eingestufte Technologie. Sie erlaubt es, unbemerkt viele Daten exakt personalisierbarer Menschen zu erheben, ihre Angewohnheiten und Lebensumstände sowie die persönlichen Kontakte zu analysieren. Die Erkenntnisse, die sich durch Missbrauch der RFID-Technologie gewinnen lassen, gehen weit über das Mass der „Marktforschung“ hinaus. Einen vernünftigen Umgang vorausgesetzt, bietet RFID jedoch auch ein grosses Nutzungspotential. Um RFID sinnvoll zu nutzen und uns vor dessen Missbrauch zu schützen, müssen wir also wissen, womit wir es zu tun haben. Wir müssen akzeptieren, dass der sinnvolle Einsatz von RFID zu dulden ist, müssen jedoch auch aktiv jedem Missbrauch entgegenwirken.

1.7 Scoring

Scoring beschreibt ein Verfahren, um die Kreditwürdigkeit von natürlichen Personen zu ermitteln. Die grösste Scoring-Gesellschaft ist die deutsche *Schufa*, die „Schutzgemeinschaft für allgemeine Kreditsicherung“. Diese hält für praktisch jeden deutschen Bürger ab 18 Jahren einen Datensatz.

Die Kreditwürdigkeit des einzelnen Bürgers wird anhand eines sog. *Scores*, einem Zahlenwert zwischen 0 und 100, angegeben. Je höher bzw. tiefer dieser Wert ausfällt, desto grösser bzw. kleiner wird die Kreditwürdigkeit des betroffenen Bürgers eingeschätzt. Dieser Score entsteht aufgrund eines statistischen Verfahrens und greift auf komplexe mathematische Algorithmen zurück. Der Scoring-Wert wird anhand 10-20 Variablen errechnet. Dies können einerseits Informationen über die berufliche Ausbildung, das Einkommen, bestehende Insolvenzverfahren oder Haftbefehle sein. Es werden jedoch auch Kriterien wie z.B. die gefahrene Automarke oder die Nachbarschaft, in der man wohnhaft ist, zur Bewertung herangezogen. Ob sich eine Selbstauskunft bei der Schufa ebenfalls negativ auf den Score auswirkt, ist nicht bekannt.

Die Schufa bezieht ihre Daten von mehr als 4'500 Unternehmen. Somit können beispielsweise Versandhäuser auch mit ihren säumigen Kunden Geld verdienen, indem sie die entsprechenden Informationen an die Schufa weiterverkaufen. Auch Finanzinstitute und Betriebe des öffentlichen Nahverkehrs verkaufen Informationen über Kunden an die Schufa weiter.

2 Sinn und Zweck der Überwachung

Wozu dient eigentlich Überwachung, was will man damit erreichen? Diese Frage steht in diesem Kapitel im Mittelpunkt. Oder anders formuliert; warum hat ein Staat oder eine Firma Interesse daran, möglichst viel über seine Bürger/Kunden zu erfahren und welcher Nutzen kann aus den gesammelten Informationen gezogen werden?

Das Sammeln und die Auswertung von Daten basiert auf verschiedenen Grundinteressen. So hat ein Staat ganz sicher andere Motive für eine Überwachungsaktion als dies z.B. die Migros mit ihrem Cumuluskärtchen hat. Die Interessen an personenbezogenen Daten können sich auch überschneiden, dürften doch vor allem private und staatliche Versicherungen ähnliche Motive haben, ihre Kunden zu observieren, um dadurch einen möglichen Versicherungsbetrug aufzudecken. Es lässt sich also hierbei keine klare Grenze zwischen Staat und Wirtschaft ziehen.

Überwachung muss nicht in jedem Fall bedeuten, dass eine Person überwacht wird. Nehmen wir den intelligenten Kühlschrank als Beispiel. Er merkt automatisch wenn ein Lebensmittel sein Verfallsdatum erreicht und meldet dies seinem Hausherrn. Noch praktischer erscheint, dass er Lebensmittel, die ausgehen, automatisch nachbestellt. Es soll uns also mittels Überwachung auch der Alltag erleichtert werden.

2.1 Sicherheits- und sozialpolitische Aspekte

Um die sicherheits- und sozialpolitischen Aspekte der Überwachung zu erläutern, gehen wir von einem demokratischen Staat aus, wie es die Schweiz oder Deutschland ist. Der Einfachheit halber werden sie im weiteren Text als „Staat“ bezeichnet.

Es liegt auf der Hand, dass sich Diktatoren oder Parteien mit allen Mitteln an der Macht halten wollen um so ihre politischen Ziele erreichen zu können. Um politische Gegner ausfindig und unschädlich zu machen, will ein Regime möglichst viel über seine Bürger wissen. Beispiele dafür gibt es mit der Gestapo im 3. Reich oder der Stasi zur Zeit der DDR genug.

2.1.1 Die Aufgaben eines Staats

Die klassische staatliche Aufgabe der „Aufrechterhaltung der öffentlichen Sicherheit und Ordnung“ lässt sich in drei wesentliche Punkte unterteilen. Der Staat übernimmt die Verantwortung für:

1. die äussere Sicherheit
2. die innere Sicherheit
3. die Daseinsvorsorge

Äussere Sicherheit bedeutet den Schutz gegen Feinde von aussen. Dies kann hier vernachlässigt werden, da wir bei der Suche nach Sinn und Zweck der Überwachung von Friedenszeiten ausgehen. Interessanter erscheinen da die beiden letzten Punkte, die innere Sicherheit und Ordnung sowie die Daseinsvorsorge.

Unter innerer Sicherheit versteht man die Erlassung von Gesetzen, den Schutz vor Straftätern, den Schutz vor Terrorismus (wobei dieser Punkt sich mit der äusseren Sicherheit schneidet) und die Rechtsprechung durch Gerichte.

Die Daseinsvorsorge umfasst die Bereitstellung von Infrastruktur (Eisenbahnen, Strassen), die Einrichtung von Bildungsstätten (Schulen, Theater) und natürlich den Aufbau und den Unterhalt von sozialen Einrichtungen (Arbeitslosenkasse, Invalidenversicherung, AHV).

Um die oben genannten Aufgaben erfüllen zu können, muss der Staat zwangsläufig eine grosse Menge an Daten erheben. Von der Geburtsurkunde bis zum Totenschein wird unser Leben in Ur-

kunden und Zeugnissen zusammengefasst. Hinzu kommt die grosse Anzahl von Nummern die unser Dasein dokumentieren, wie z.B. AHV-Nummer, Personalnummer, Versicherungsnummern und Telefonnummern, um nur ein paar zu nennen.

„Von der Wiege bis zur Bahre – Formulare, Formulare."

Deutsches Sprichwort

Staatliche Tätigkeit bedeutet heute mehr denn je Umgang mit Daten. Als Folge dessen sind praktisch alle gesellschaftlichen Bereiche, vom Gesundheitswesen über die Sozialversicherungen bis hin zu Bildung und Wissenschaft, mit staatlichem Handeln verbunden.

Der Bürger nimmt hier eine zentrale Rolle ein und tritt dem Staat in verschiedenen Formen gegenüber. Er ist Verkehrsteilnehmer, Steuerzahler, Sozialhilfeempfänger und kann als Stimmberechtigter die Regierung wählen und politische Vorgänge beeinflussen. Der Bürger kann auch als Verdächtiger einer Straftat ins Visier der Strafverfolgungsbehörden kommen. In den meisten Rollen, die ein Bürger einnimmt, verlangt er vom Staat die Gewährleistung von Sicherheit, sei es auf den Strassen oder zu Hause im eigenen Heim. Der Staat muss nach Rechten und Gesetzen handeln, die nicht als „Gottgegeben" gesehen werden können, sondern hart erkämpft werden mussten. Alle können sich auf ein Grundrecht der Freiheit berufen, das der Staat zu respektieren hat.

Das Verhältnis zwischen Freiheit und Sicherheit ist eine sehr komplexe Angelegenheit, stimmt es doch auch, dass es nur Freiheit geben kann, wenn eine Gesellschaft vor terroristischen, kriminellen und sozialen Gefahren beschützt wird.

2.1.2 Der Kampf gegen die Kriminalität

Gesetze werden durch den Staat erlassen. Somit liegt die Ursache der Kriminalität beim Staat. Ohne Gesetze kann es keine Kriminalität geben und somit auch niemanden, der als kriminell bezeichnet werden kann. Natürlich wäre ein Zusammenleben ohne Regeln unmöglich. Kriminell sein heisst nicht, gegen gesellschaftliche Normen zu verstossen. Kriminalität darf nicht mit Verhalten, das von der Norm abweicht, verwechselt werden. Es ist also nur kriminell, wer gegen die vom Staat erlassenen Gesetze verstösst.

Die Verfolgung einer Person, die einer Straftat verdächtigt wird, unterliegt der Polizei. Sie muss beweisen können, dass ein Verdächtiger eine Tat auch tatsächlich begangen hat. Um dies beweisen zu können steht ihr eine grosse Anzahl von Möglichkeiten, wie z.B. die DNA-Analyse oder der althergebrachte Fingerabdruck, zur Verfügung. Die Daten von überführten Straftätern werden, je nach Ausmass der Straftat, in so genannten „Täterdatenbanken" gespeichert um Wiederholungstäter schnell und effizient ausfindig machen zu können. Dies ist das klassische Vorgehen bei der Verbrechensbekämpfung.

Ein anderer Weg im Kampf gegen die Kriminalität besteht darin, Verbrechen zu verhindern. Der Staat versucht dieses Ziel mittels Abschreckung zu erreichen. So lässt er auf öffentlichen Plätzen Videokameras aufstellen oder genehmigt gross angelegte Abhöraktionen.

Bei dieser Art der Verbrechensbekämpfung wird ganz bewusst in die Privatsphäre der Bürger eingedrungen um gewisse Verhaltensweisen zu ändern oder zu unterbinden. Was dabei auf der Strecke bleibt ist die Unschuldsvermutung (siehe Abschnitt 4.2.3). Ein anderes Mittel der Abschreckung ist der sog. „Internet- Pranger" (siehe Abschnitt 4.3.4). Dabei werden die vollen Anschriften und Photos von Verbrechern ins Internet gestellt und so der Öffentlichkeit preisgegeben.

2.1.3 Der Sozialstaat als Überwacher

Der Sozialstaat soll die soziale Sicherheit der Bevölkerung gewährleisten. Mit seinen verschiedenen Institutionen wie der AHV, der IV oder der Arbeitslosenversicherung soll uns in verschiedensten

Lebenssituationen geholfen werden. Sie haben die Aufgabe, uns in persönlichen Notlagen zu unterstützen – uns „aufzufangen“.

Obwohl man die beiden Begriffe „Sozialstaat“ und „Überwachung“ nicht auf Anhieb miteinander in Verbindung bringt, handelt es sich bei den sozialstaatlichen Einrichtungen um den Teil im Staat, der am meisten über seine Bürger weiss.

Immer wenn jemand die Leistungen einer staatlichen Sozialeinrichtung in Anspruch nimmt, fallen automatisch Daten über die betreffende Person an, die in Datenbanken gespeichert werden. So entstehen mit der Zeit tausende von Datensätzen. Diese reichen vom Stipendien- bis hin zum IV- oder AHV-Bezüger. Wie überall gibt es auch hier Personen, die versuchen das System auszunutzen. Um unrechtmässigen Bezug von mehreren Sozialleistungen zu verhindern, werden die Daten von den verschiedenen Ämtern untereinander abgeglichen. Dabei werden nicht nur Daten von Sozialämtern verwendet, sondern es wird auch auf Datenbanken von Steuerämtern zurückgegriffen. Die Problematik besteht auch hier darin, dass man willkürlich Daten durchforstet, ohne dass je ein Verdachtsmoment bestanden hätte.

2.2 Der Kampf gegen den Terrorismus

Seit dem 11. September 2001 ist der „Kampf gegen den Terrorismus“ ein Dauerthema. Dieser Ausdruck wurde vor allem durch die Bush-Regierung geprägt und ist zum Oberbegriff für eine Reihe von Massnahmen gegen den internationalen Terrorismus geworden. Seither wurden unter dem Deckmantel der Terrorbekämpfung eine Reihe von neuen Gesetzen erlassen. Antreibende Kraft ist die USA aber auch in Europa wird munter an neuen Gesetzen gebastelt. So erhält der Staat immer mehr Befugnisse um personenbezogene Daten zu erheben.

2.2.1 Der Patriot-Act

In den USA wurde als Reaktion auf die Anschläge vom 11. September der *Patriot-Act*[9] verabschiedet. „USA Patriot“ ist eine Abkürzung und steht für: ***U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism*. Auf Deutsch bedeutet dies in etwa: „Gesetz zur Stärkung und Einigung Amerikas durch Bereitstellung geeigneter Werkzeuge um Terrorismus aufzuhalten und zu blockieren“.

Abbildung 4: Unterzeichnung des Patriot-Act (2001)

Dieses, im Eilverfahren verabschiedete Gesetz weitet die Befugnisse des amerikanischen Staats, seine Bürger zu überwachen massiv aus. So werden beispielsweise Buchhandlungen und Bibliotheken dazu gezwungen, Daten über das Leseverhalten ihrer Kunden an staatliche Ermittler weiterzugeben.

Die Erlaubnis für solche Nachforschungen wird nicht mehr durch einen zivilen Richter, sondern durch ein 1978 geschaffenes Geheimgericht erteilt. Diesem Geheimgericht wird nachgesagt, noch nie eine Erlaubnis verweigert zu haben. Es erscheint natürlich, dass die Polizei bei einer Anfrage nicht nachweisen muss, dass ein konkreter terroristischer Tatverdacht vorliegt. Weit schlimmer ist hingegen, dass den Firmen, die intimste Kundendaten preisgeben mussten, unter Strafe verboten wird, ihre Kunden über diese Ermittlungen zu informieren.

Der Patriot-Act ist erst der Anfang zu weit tiefschürfenderen Massnahmen. Gleich nach dem Inkrafttreten des Patriot-Act begann die Forschungsabteilung des US-Verteidigunsministeriums DAR-

9 http://de.wikipedia.org/wiki/Patriot_Act

PA mit der Forschung an einem Programm namens „Terrorist Information Awareness“ (TIA). Ziel war es, eine Datenbank zu schaffen, mit deren Hilfe terroristische Machenschaften aufgedeckt werden können. In der Datenbank sollten öffentliche und private Informationen über Bürger enthalten sein. Es sollten Daten über Internet-Verkehr, komerzielle und staatliche Datenbanken von Finanzinstituten, von Reiseunternehmen sowie Informationen von Gesundheits- und Verkehrsbehörden erhoben werden. 2003 wurden keine Gelder mehr für TIA gesprochen, was sogleich das Ende für das Projekt bedeutete. Kurz danach wurde von der DARPA ein Projekt namens „ADVISE“ ins Leben gerufen, welches ähnliche Ziele verfolgt wie das TIA-Projekt. Über ADVISE ist sehr wenig bekannt, ausgenommen, dass es ein Jahresbudget von rund 47 Millionen Dollar haben soll.

2.2.2 Vorratsdatenspeicherung

Auch in Europa wurden kurz nach den Anschlägen vom 11. Septembers 2001 Anti-Terror Gesetze verabschiedet. In Deutschland wurde das Terrorbekämpfungsgesetz (TBG) am 2. Januar 2002 und das Luftsicherungsgesetz am 11. Januar 2005 in Kraft gesetzt.

Momentan sorgt vor allem die Vorratsdatenspeicherung für Diskussionsstoff. Die Vorratsdatenspeicherung ist im deutschen Gesetz für Telekommunikation verankert, welches am 9. November 2007 vom Bundestag gutgeheissen wurde. Unter anderem zum Zweck der Strafverfolgung werden Telekommunikationanbieter und Internetprovider dazu verpflichtet, sämtliche bei Telekommunikation anfallenden Verkehrsdaten für sechs Monate zu speichern. Das bedeutet, dass während sechs Monaten festgestellt werden kann, wer mit wem und wann per Telefon, SMS oder E-Mail in Kontakt gestanden hatte. Bei Handy-Telefonaten und SMS soll ausserdem der Standort zum Zeitpunkt der Kommunikation gespeichert werden.

Die so gesammelten Daten können leicht zur Erstellung von Persönlichkeitsprofilen missbraucht werden, ohne dass die betroffenen Personen davon Kenntnis haben.

2.3 Wirtschaftliche Aspekte

Die Überwachung im Gebiet der Wirtschaft ist gegenüber der Überwachung von Seiten des Staats aus nicht zu unterschätzen. Die Interessen, möglichst viel über seine Angestellten oder Kunden zu erfahren, sind vielfältig, steht doch in der Wirtschaft nicht zuletzt der Profit im Vordergrund. Was die Menge der beschafften Daten betrifft, stehen Firmen in nichts den staatlichen Institutionen nach, wenn sie den Staat nicht sogar noch übertreffen. Vielfach sind Daten, die von privaten Gesellschaften gesammelt werden, weitaus tiefschürfender und sensibler als diejenigen, die von staatlichen Einrichtungen erhoben werden.

2.3.1 Ausschluss potentiell zahlungsunfähiger Kunden

Ein grosses finanzielles Risiko für die Wirtschaft stellen Kunden dar, die ihre Rechnungen nicht bezahlen können. Mahnverfahren sind aufwändig und stellen, gerade bei kleineren Beträgen, einen grossen Mehraufwand dar. Im Falle eines Privatkonkurs ist zwar die Ware verkauft, das Geld dafür hat der Verkäufer jedoch nicht erhalten.

Nicht nur im Bereich des Warenhandels stellen insolvente Kunden ein Problem dar, besonders Finanzinstitute sind auf zahlungsfähige Kunden angewiesen. Kann der Kunde einen Kredit oder eine Hypothek nicht mehr zurückzahlen, wird die Bank ihr Geld nicht wieder sehen. Dies ist auch ein Grund für die aktuelle Finanzkrise (auch als „Subprime-Krise“ oder „US-Immobilien-Krise“ bekannt), wobei hier teilweise bewusst Hypotheken mit grossem Risiko vergeben worden sind (man konnte die Kredite ja schliesslich weiterverkaufen). Finanzinstitute machen somit immer mehr vom Scoring (siehe Abschnitt 1.7) Gebrauch, womit potentielle „Risikokunden“ ausgeschlossen werden können.

Nicht nur im Finanzsektor verzeichnet das Scoring eine immer höhere Beliebtheit; immer mehr Firmen handeln nach dem Motto; *Vertrauen ist gut, Kontrolle ist besser*. Telefongesellschaften vergeben Festnetzanschlüsse oder Handyverträge nur noch an Leute mit einem guten Scoring-Wert. Zahnärzte informieren sich vor aufwändigen Behandlungen über den Scoring-Wert ihrer Patienten. Auch beim Auto-Leasing, beim Antrag auf eine Tankkarte oder bei Internetbestellungen wird vom Scoring Gebrauch gemacht. Häufig entscheidet ein Scoring-Wert darüber, ob man eine Ware per Rechnung bezahlen kann oder ob man per Vorkasse bezahlen muss.

2.3.2 Überwachung am Arbeitsplatz

Natürlich wird auch am Arbeitsplatz munter überwacht, sei es nun der Büroangestellte oder der Fliessbandarbeiter – überall möchten Arbeitgeber wissen, was ihre Angestellten so treiben.

Dies ist kein neues Phänomen; bereits Henry Ford, der berühmte Automobilhersteller aus den USA, hat seine Mitarbeiter penibel überwachen lassen. Dabei geholfen hat ihm Frederick Winslow Taylor. Zusammen setzten sie sog. Effizienzexperten ein. Diese registrierten, mit Notizbuch und Stoppuhr bewaffnet, jede Bewegung eines Arbeiters wie die eines seelenlosen Apparats. Diese Vorgehensweise, *Taylorismus* genannt, hat Charlie Chaplin in seinem Film „Modern Times“ eindrücklich parodiert. Vor diesem Hintergrund erstaunt es nicht, dass Ford und Taylor in den Romanen von Aldous Huxley (*Brave New World*) und Jewgeni Samjatin (*Wir*) erwähnt werden.

Wussten die Angestellten von Ford noch, dass sie überwacht wurden, so ist es im Zeitalter der Computertechnik zunehmend schwieriger zu merken, ob und wann man beobachtet wird. So haben Arbeitgeber die Möglichkeit, jegliche verwendeten Kommunikationsmittel, sei es nun das Internet, das Telefon oder den E-Mail-Verkehr, zu überwachen.

Ein Arbeitgeber hat das Recht, die Benutzung von Internet, E-Mail und Telefon für den privaten Gebrauch einzuschränken oder ganz zu verbieten. Merkt er, dass die Regeln nicht eingehalten werden, darf er seine Mitarbeiter überwachen. Natürlich darf die Observierung eines Angestellten nicht zu weit gehen (siehe Abschnitt 3.3.2, die Lidl-Affäre). Auf der Homepage des eidgenössischen Datenschutzbeauftragten (EDÖB) finden wir dazu folgende Aussage:

> *„Selbst wenn die private Nutzung von World Wide Web und E-Mail grundsätzlich verboten ist, hat der Arbeitgeber nicht unbeschränkte Überwachungsrechte. Die systematische Überwachung des Verhaltens eines Arbeitnehmers ist in jedem Fall verboten, ebenso das Lesen von als privat gekennzeichneten oder erkennbaren E-Mails. Punktuelle Überwachungen sind erlaubt, müssen aber in einem Überwachungsreglement klar umschrieben sein und in einer ersten Phase anonym erfolgen. Dieses Reglement muss allen Angestellten zugänglich sein.“*

Auszug aus EDÖB-Information „Nutzung von Kommunikations- und Informationsmitteln“[10]

Die Überwachung von Büroangestellten beschränkt sich nicht nur auf die Kommunikationsmittel. Für einen Arbeitgeber ist es kein Problem herauszufinden, wie viele Tastaturanschläge seine Angestellten erreichen, wie hoch die Qualität einer Arbeit ist und in welcher Geschwindigkeit sie ausgeführt wird.

Überwachung am Arbeitsplatz muss nicht in jedem Fall negative Folgen für den Arbeitnehmer haben. In Bereichen der Industrie, wo Gefahren für Arbeitnehmer auftreten können, erscheint es sinnvoll, wenn gewisse Risikofaktoren mittels Überwachung abgeschwächt werden. Als Beispiel kann man hier die Überwachung der Luftqualität in einem Labor nennen. Diese Angestellten werden sich wohl kaum daran stören, wenn sie ihrer Gesundheit wegen überwacht werden.

10 http://www.edoeb.admin.ch/dokumentation/00612/00614/00619/index.html?lang=de

2.4 Überwachung im Alltagsleben

Nachdem staatliche und wirtschaftliche Aspekte der Überwachung schon beleuchtet wurden, soll in diesem Unterkapitel geschildert werden, wo wir in unserem Alltag mit Überwachung in Kontakt kommen können. Dies bedeutet nicht in jedem Fall, dass wir diejenigen sind, die überwacht werden, genauso gut kann das Interesse an jemand anderem von uns aus kommen. Ebenso gibt es mehr und mehr „intelligente" Geräte, auch von diesen soll hier die Rede sein.

2.4.1 Private Überwachung

Private Überwachung kann aus verschiedenen Motivationen heraus entstehen. Man ist beispielsweise eifersüchtig auf seinen Ehepartner, möchte wissen wo seine Kinder sind oder man ist daran interessiert zu wissen, wo sich denn der Nachbar wieder herumtreibt.

Früher wie heute wird häufig ein Privatdetektiv zur Hilfe gezogen wenn man der Meinung ist, dass z.B. der Ehepartner nicht mehr treu ist. Auch Privatdetektive behelfen sich bei der Observierung ihrer Zielperson modernster Technik. Die meisten Errungenschaften dieser neuen Techniken können allerdings auch ganz leicht selbst beschafft werden. Als Beispiel nehmen wir die Handy-Ortung. Das Angebot für Handy-Ortung ist gross, wer im Internet danach sucht merkt schnell, dass neben Mobilfunkanbietern auch viele private Firmen existieren, die mit diesem Service ihr Geld verdienen. So auch die Firma *Track your kid*[11]. Auf Deutsch: „Verfolge dein Kind."

Bei „Track your kid" handelt es sich um eine Firma, die anbietet, dass Eltern ihre Kinder mittels Handy-Ortung überwachen können. Damit soll die Sicherheit der Liebsten erheblich erhöht werden. Ein anderer Zweig der Firma bietet auch diverse Programme an, mit denen sich Lastwagen oder Handwerker überwachen lassen.

Dass mit dem „Track your kid" Service nicht nur Kinder, sondern auch Ehepartner überwacht werden können, liegt auf der Hand. Allerdings muss man zuerst das Handy der zu überwachenden Person in die Hände bekommen. Für Ortsabfragen muss in jedem Fall das Einverständnis des Überwachten eingeholt werden.

Handy-Ortung kann auch positive Seiten haben, dies zeigt sich bei der „Björn Steiger"-Stiftung die in Deutschland aktiv ist. Wer bei ihr registriert ist und einen Notruf tätigen muss, kann sein Handy orten lassen. So kann verhindert werden, dass Rettungskräfte auf der Suche nach der Unfallstelle wichtige Zeit verlieren. Das Einverständnis zur Ortung wird dabei erst abgegeben, wenn es auch wirklich nötig ist.

2.4.2 Intelligente Dinge

Überwachung muss nicht in jedem Falle störend sein. Immer mehr helfen uns intelligente Dinge bei ganz alltäglichen Sachen. Basistechnologie für intelligente Dinge ist das sog *ubiquitous computing* (UC). „Ubiquitous" heisst auf Deutsch „allgegenwärtig". Erst diese Technologie lässt Dinge intelligent, „smart" werden.

> *„Intelligente Dinge setzen sich aus klassischen physischen Produkten (Atomen) und darin integrierten und weitgehend unsichtbaren Minicomputern, wie z.B. Sensoren, Sendern und Smart Labels mit Daten und Software (Bits) zusammen"*

Definition von „ubiquitous computing" der ETH Zürich[12]

11 http://www.trackyourkid.de/

12 http://fm-eth.ethz.ch/eth/media/FMPro?-db=pressemitteilungen.fp5&-lay=html&-format=pr_detail_de.html&pr_id=2001-38&-find

So werden „dumme Dinge“ in „intelligente, aufmerksame Dinge“ umgewandelt. Das bedeutet, dass die mit Minicomputern ausgestatteten Dinge zu „denken“ beginnen. Je nach dem, für welchen Verwendungszweck sie programmiert wurden, entnehmen sie Informationen über Temperatur, Haltbarkeitsdatum oder Lagerort aus ihrer Umwelt. Die gesammelten Daten werden automatisch weitergeleitet. Es findet also eine Verbindung zwischen der virtuellen Welt, die automatisch Daten erfasst, und des reellen Lebens statt. Bereits bekannt sind der intelligente Kühlschrank und das intelligente Haus, doch gehen die Forscher viel weiter. Weitere Anwendungen könnten sein:

- Ein Spitalbett, das die tatsächliche Medikamentierung registriert, mit der gewollten Dosis vergleicht und bei Unstimmigkeiten Alarm schlägt.
- Maschinen, die dem Handwerker melden, wann der nächste Service fällig ist.
- Blutkonserven, die merken, sobald die Temperatur zu hoch ist oder das Ablaufdatum bald erreicht ist.
- Supermarktregale, die merken, wann eine Ware ausgeht und diese dann selbstständig nachbestellen.
- Kleider, die sich an Umweltbedingungen anpassen und Körperfunktionen, wie Herzfrequenz, Blutdruck oder Körpertemperatur messen können.

Diese Aufzählung kann noch weitergeführt werden. Bis in ein paar Jahren werden intelligente Dinge wohl in allen Sparten anzutreffen sein. Durch diese Technologie eröffnen sich tausende von neuen Anwendungsfeldern, die, wie so oft wenn es um Überwachung geht, im Guten wie im Schlechten eingesetzt werden können.

3 Konkrete Fälle von Überwachung

Wurde in den bisherigen zwei Kapiteln einerseits auf die technischen Möglichkeiten und andererseits auf die Motive hinter der Überwachung eingegangen, werden an dieser Stelle konkrete Fälle von Überwachung geschildert. Es geht dabei um die Frage, wie und wo man durch Überwachung die Sicherheit erhöhen kann. Auf die Videoüberwachung wird dabei ein besonderer Fokus gelegt, da durch diese Form der Überwachung wohl jeder betroffen ist.

3.1 Videoüberwachung

Politisch gesehen ist das Thema der Videoüberwachung in Luzern momentan hochaktuell, denkt man nur an die Abstimmung über das neue Reglement der Videoüberwachung vom 1. Juni 2008. Kameras gelten gemeinhin als Wundermittel zur Kriminalitätsbekämpfung, ein tolles, magisches Ding, das die Kriminalität leicht beseitigt. Dafür, dass kaum aussagekräftige Untersuchungen existieren, ist diese Meinung ziemlich stark in der Bevölkerung verankert. In der Praxis sieht es natürlich ein wenig komplizierter aus.

3.1.1 Fehlen aussagekräftiger Untersuchungen

Die Frage, wie effektiv Videoüberwachungssysteme sind, erweist sich als problematisch. Momentan werden leider kaum Gelder für die Evaluation solcher Projekte eingesetzt. Die Behörden wollen schnelle Lösungen und ziehen aus Einzelfällen, wo die Videoüberwachung erfolgreich war, voreilige Schlüsse. Ob die Systeme überhaupt miteinander vergleichbar sind, wird dabei häufig ausser Acht gelassen. Sind die Kameras erst einmal montiert, werden Kriminalitätsstatistiken analysiert, inwiefern die Überwachung erfolgreich ist. Diese verlieren aber aus verschiedenen Gründen an Glaubwürdigkeit:

- Wenig aussagekräftige Untersuchungen der Wirksamkeit von Videoüberwachung, da die Untersuchungen von Befürwortern oder Betreibern der Videoüberwachungen statt durch unabhängige Organisation durchgeführt werden.
- Oftmals ist kein Vergleich zu einem ähnlichen Gebiet vorhanden, wo keine Videoüberwachungsanlage installiert wurde (das sog. *Kontrollgebiet*).
- Die Zeiträume für die Untersuchungen sind oftmals zu kurz gewählt.
- Saisonale Schwankungen werden nicht berücksichtigt.
- Gleichzeitige Massnahmen werden ausgeklammert und alles wird den Kameras zugeschrieben. Eine bessere Beleuchtung oder eine geöffnete Bar im Bereich der Überwachungskameras sorgt ebenfalls für mehr Sicherheit.

Abbildung 5: Hinweisschild für Videoüberwachung

- Fehlen eines Kosten-Nutzen-Vergleichs; Einbeziehung von alternativen Massnahmen wie z.B. eine bessere Beleuchtung, sonstigen baulichen Massnahmen wie Zäune etc. fehlt.
- Die Verlagerung der Kriminalität in unbewachte Zonen wird nicht untersucht.

3.1.2 Verbesserte Sicherheit durch Videoüberwachung

Der Bürger will beschützt werden, er will das Gefühl von Sicherheit. Gerade auch im Namen der jüngsten Terrorismusbekämpfung wird aber häufig eher unmittelbare Bedürfnisbefriedigung vorge-

nommen, als für wirklich langfristige Lösungen zu sorgen. Unter dem Strich ist aber die tatsächliche Sicherheit entscheidend, nicht das Gefühl von Sicherheit. Gerade das lässt sich nicht so einfach feststellen.

3.2 Fallbeispiel Grossbritannien

Die Bevölkerung in England hegt grosse Hoffnung und Vertrauen in die Wirksamkeit der Videoüberwachung zur Reduzierung der Kriminalität. Die Medien spielen dabei eine sehr wichtige Rolle, indem Fälle, bei denen ein starker Rückgang der Kriminalität verzeichnet werden konnte, medial gross inszeniert werden. Einzelfälle, wie der vom Bombenleger „David Copeland", der dank dem CCTV identifiziert werden konnte, sind dem Ansehen der Videoüberwachungsanlage sehr dienlich und rechtfertigen für einen grossen Teil der Bevölkerung die grossen Investitionen. Dabei geht meist die Fragestellung unter, ob diese Reduktion über einen langfristigen Zeitrahmen hinweg gehalten werden kann oder ob dieser Erfolg wirklich nur dem CCTV zu verdanken ist.

In Grossbritannien werden auch Fahndungsfotos, die auf Videoüberwachungsbildern basieren, in den Zeitungen abgedruckt. Auch die Hysterie im Rahmen der Terrorismusbekämpfung wird genutzt, um die Kameras zu rechtfertigen. Gerade aber die organisierte Kriminalität wird eher einen Weg finden, dem Netz der Überwachung zu entgehen. Ein Selbstmordattentäter profitiert im Grunde auch von den Überwachungsmassnahmen, weil er sich so sicher sein kann, dass das Attentat bildlich festgehalten und so medienwirksam „inszeniert" wird.

Abbildung 6: CCTV-Anlage in London

3.2.1 Wissenschaftliche Studie von Gill/Spriggs

Im Gegensatz zum deutschsprachigen Raum sind in Grossbritannien einige Studien zur Videoüberwachung durchgeführt worden, wenn auch dort nur ein sehr kleiner Teil des Geldes für die Untersuchungen von Videoüberwachungssystemen eingesetzt wird. Martin Gill, Professor der Kriminologie, und Angela Spriggs von der Universität Leicester untersuchten in ihrer, vom britischen Innenministerium in Auftrag gegebenen Studie „Assessing the impact of CCTV[13]" die Wirksamkeit von Videoüberwachungsmassnahmen.

Grundlage der Analyse sind 14 unterschiedliche CCTV-Systeme, die über ganz England verteilt sind. Dabei wurden Kriminalitätsstatistiken vor und nach der Installation der Videokameras analysiert und dabei mit einem unüberwachten Kontrollgebiet verglichen. Um das Ausmass der Verlagerung der Kriminalität zu untersuchen, wurde die Umgebung ebenfalls miteinbezogen. Auch wurde die Bevölkerung vor und nach Installation der Videokameras bezüglich ihres Sicherheitsgefühls befragt.

Dabei zeigte sich, dass die Wirksamkeit sehr systemabhängig ist. Es gibt Fälle, da sinkt die Kriminalität, in anderen steigt sie sogar. Generell ist die Auswirkung auf die Gesamtkriminalität aber eher klein.

3.2.2 Globaler Effekt

Vor allem in einer gesamthaften Reduzierung der Kriminalität liegt sehr viel Hoffnung. Die Studie von Gill/Spriggs fällt gerade hier sehr ernüchternd aus, da die Reduktion von Delikten insgesamt nur sehr gering war. Von den zwölf untersuchten CCTV-Systemen (bei zwei Systemen waren keine Daten vorhanden) konnte lediglich in fünf Fällen ein Rückgang der Kriminalität festgestellt werden.

13 http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf

In nur einem Fall konnte ein signifikanter Rückgang beobachtet werden, der neben anderen Massnahmen auch dem CCTV zu verdanken war. In sieben Fällen stieg die Kriminalität sogar an, was aber nicht heisst, dass die Überwachungsmassnahmen ineffektiv wären. Eher ist dieser Anstieg auf eine verbesserte Registrierung von Delikten zurückzuführen.

3.2.3 Eigentums- und Affektdelikte

Delikte werden unterschieden in *Affektdelikte* und Eigentumsdelikte. Affektdelikte sind Gewaltdelikte, sowie Vergehen, die im Zusammenhang mit Alkohol und Drogen stehen. Vergehen wie Raub, Einbruch oder Sachbeschädigung hingegen werden als Eigentumsdelikte bezeichnet.

Auf Affektdelikte scheint die Videoüberwachung nur eine geringe Auswirkung zu haben. Von 19 untersuchten Fällen konnte lediglich in vier Fällen ein Rückgang festgestellt werden. In 15 Fällen stieg die Rate gar an. Lediglich vier von diesen 15 Fällen sind auf eine grössere Erfassung von solchen Straftaten zurückzuführen.

Wirksamer scheint der Einfluss von CCTV auf Eigentumsdelikte zu sein. In 16 von insgesamt 23 untersuchten Fällen sank die Zahl solcher Delikte. Besonders auf Grossparkplätzen erzielten die Kameras eine sehr gute Wirkung, was auch auf die gute Übersichtlichkeit und Abgrenzung zu anderen Gebieten zurückzuführen ist. Auf Parkplätzen hat jeder meist ein ganz klares Ziel, nämlich das Auto zu parkieren bzw. damit wieder wegzufahren. In leeren, übersichtlichen Räumen sind aussergewöhnliche Verhaltensweisen sehr auffällig, weshalb die Abschreckung durch Videokameras als sehr gross eingeschätzt werden kann.

3.2.4 Der Verlagerungseffekt

Die Theorie, dass die Kriminalität aus den überwachten Gebieten in unüberwachte Gebiete verdrängt wird, ist eines der Hauptargumente gegen eine Installation von Videoüberwachungsanlagen. Dabei ist es sehr gut möglich, dass die Kriminalität vermehrt in ärmere, sozial schlechter stehende Gebiete verdrängt wird, wo auch die statistische Erfassung von Straftaten geringer ausfällt. Auch eine Verdrängung innerhalb des Zielgebiets an Orte, die von den Kameras nicht eingesehen werden können, klingt durchaus plausibel. Dies ist insofern problematisch, dass auch dieser unbewachte Bereich überwacht werden sollte, was rein theoretisch zu einer flächendeckenden Überwachung führen würde.

Die Studie von Gill/Spriggs untersuchte auch den Effekt der Verlagerung. In fünf Fällen konnte eine mögliche Verlagerung der Kriminalität festgestellt werden. Etwa beim „Eastcap Estate“, eines der untersuchten Gebiete, konnte innerhalb eines Radius von 100 Metern um die Kameras ein Rückgang der Delikte im Zusammenhang mit Fahrzeugen („Vehicle Crime“) von 38% verzeichnet werden. Ausserhalb dieses 100-Meter-Radius hingegen stieg die Kriminalität um 94% an.

3.2.5 Alternativmassnahmen

Die Videoüberwachung ist bei weitem nicht die einzige Möglichkeit um im öffentlichen Raum mehr Sicherheit zu schaffen. Kameras sind nicht generell ein Garant für mehr Sicherheit, sondern lediglich Bestandteil eines Sicherheitskonzepts. In bestimmten Situationen ist Videoüberwachung gar relativ wirkungslos, wie die Studie von Gill und Spriggs belegt. Deswegen ist es sinnvoll, die Wirksamkeit und Kosten von Alternativmassnahmen mit denen einer Überwachung durch Videokameras abzuwägen. Des weiteren wird bei Alternativmassnahmen die Privatsphäre weniger stark beeinträchtigt.

Als Alternative bietet sich zum Beispiel die Schaffung von kulturellen Möglichkeiten innerhalb des gefährdeten Gebiets, wie etwa eine Bar, die bis lange in die Nacht geöffnet hat. So kann aus einem menschenleeren Gässchen ein Gebiet mit regem Betrieb entstehen. Es bietet sich auch an, im Zielgebiet einen grossen Bereich auf grosse Entfernung einsehbar zu gestalten, um so eine bessere

Überblickbarkeit zu schaffen. Dunkle Ecken und Nischen können besser ausgeleuchtet werden, um das Sicherheitsgefühl weiter zu stärken. Aber auch bauliche Massnahmen, wie etwa die Errichtung von Zäunen um damit einem potentiellen Täter das Auflauern eines Opfers zu erschweren, kommen in Frage.

Es besteht die Möglichkeit, dass bei grossflächiger Videoüberwachung die Zivilcourage weiter sinken könnte. Selbst ohne Kameras verlässt sich die einzelne Person am ehesten auf einen eingreifenden Mitmenschen. Wenn dann aber überall Kameras hängen, vertraut bestimmt so manch einer auf eine sofortige Intervention der Polizei. Gerade aber mit mehr Zivilcourage könnte man Verbrechen im öffentlichen Raum – sehr kostengünstig – reduzieren.

3.2.6 Bewertung der Videoüberwachung

Von Videokameras auf heutigem technischen Niveau sollte man sich nicht zu viel erhoffen. Gemäss der Studie von Gill/Spriggs ist deren Wirksamkeit deutlich niedriger als weithin angenommen, zudem fällt der Effekt von System zu System sehr unterschiedlich aus. Die Auswirkung auf die Gesamtkriminalität ist eher bescheiden, gegenüber Affektdelikten (Gewaltdelikte und Delikte in Zusammenhang mit Alkohol und Drogen) scheint Videoüberwachung kaum wirksam zu sein. Jedoch scheint Videoüberwachung in einigen CCTV-Systemen relativ wirksam zu sein, wenn es darum geht, in klar abgeschlossener Umgebung Eigentumsdelikte (Sachbeschädigung, Diebstahl) zu senken. Das trifft am meisten auf Grossparkplätze zu, wo unübliches Verhalten sehr auffällig ist.

Kameras gelten gemeinhin als etwas gutes, sicherheitsschaffendes und werden viel zu wenig aus einem kritischen Blickwinkel betrachtet. Behörden greifen viel zu schnell auf die Installation einer Videoüberwachungsanlage zurück, ohne eine genaue Vorstellung davon zu haben. In Anbetracht der grossen Summen, die rein für die technische Anlagen investiert werden, scheint unklar zu sein, welche Rolle die Kameras im Gesamtsystem spielen und wie sie sich auf die Bevölkerung auswirken. Als Argument für die Überwachung werden häufig eher fadenscheinige Vergleiche herbeigezogen, teils von Systemen mit einer völlig anderen Ausgangssituation. So etwa wird im Fall von Luzern, wo 300'000 Fr. in die Überwachung des Bahnhofplatzes, der Kappel- und der Spreuerbrücke investiert werden möchten, ein Vergleich mit Olten herbeigezogen[14], wo in einer Unterführung innerhalb von einem halben Jahr drei Fälle mithilfe von Videoüberwachung aufgeklärt werden konnten.

Unserer Meinung nach reicht es nicht aus von Einzelfällen, wo Videokameras zur Aufklärung eines Kriminalfalles beigetragen haben, gleich auf einen kriminalitätsmildernden und sicherheitserhöhenden Effekt zu schliessen. Gerade weil die Überwachung einen Eingriff in die Privatsphäre der Menschen darstellt und zu angepasstem Verhalten führen kann (siehe Abschnitt 4.3.2), ist ein wissenschaftlicher Nachweis der Auswirkungen solcher Überwachungsmassnahmen zwingend notwendig. Dazu müssten aber mehr Gelder in die Erforschung der Sicherheit solcher Systeme eingesetzt werden. Schlussendlich sind Kameras lediglich ein möglicher Bestandteil eines Gesamtkonzeptes, weshalb auch die soziokulturellen Verhaltensweisen miteinbezogen werden müssen.

3.3 Weitere konkrete Fälle

Konkrete Fälle von Überwachung könnte man zu tausenden aufzählen, denkt man nur an „prominente“ Geheimdienste der Vergangenheit (Gestapo, KGB, Stasi) und an solche der Gegenwart (CIA, NSA, BND, Mossad usw.). Darum wollen wir zum Ende dieses Kapitels nur noch kurz auf einige weitere (teils aktuelle) Fälle von Überwachung eingehen.

Einerseits ist dies ein Fall, der gerade uns Schweizer betrifft (bzw. betroffen hat) und andererseits ein Fall hoher Aktualität – die Fichenaffäre und die Bespitzelung in der Supermarktkette „Lidl“. Des weiteren wird ein aktueller Fall aus Deutschland erwähnt, bei welchem ein klarer Eingriff in

14 Neue Luzerner Zeitung, Ausgabe vom 19.05.2008, „Vergleich mit Olten“

die Pressefreiheit stattgefunden hat. Hier fällt auf, dass Überwachung oft sehr willkürlich stattfindet und kaum etwas zur Sicherheit beiträgt.

3.3.1 Die Fichenaffäre

Zur Zeit des kalten Kriegs überwachte die schweizerische Bundespolizei systematisch über 700'000 Personen und Organisationen, indem über sie die sog. *Fichen* angelegt wurden. Das entspricht mehr als 10% der schweizerischen Gesamtbevölkerung. Im Jahre 1989 wurden diese Dokumente von einer parlamentarischen Untersuchungskommission gefunden. Überwacht wurden in erster Linie linke Politiker, Gewerkschaften und Kommunisten, um das System vor einer Unterwanderung solcher Kräfte zu schützen und Stabilität zu bewahren.

3.3.2 Die Lidl-Bespitzelungsaffäre

Bei Lidl, einer deutschen Supermarktkette mit Plänen, flächendeckend in die Schweiz zu expandieren, ist ein Überwachungsskandal aufgeflogen. Vergangenes Jahr wurden die Mitarbeiter von Lidl systematisch überwacht, wie hunderte Seiten an Protokollen belegen.

Mittels versteckter Kameras, die eigentlich Ladendiebstähle aufklären und verhindern sollten, wurde das Verhalten der Mitarbeiter nach Datum und Uhrzeit genaustens festgehalten. Protokolliert wurde alles, was man sich so vorstellen kann; von Toilettenbesuchen bis hin zu Pausengesprächen von Mitarbeitern über das jeweilige Gehalt. Selbst vor dem Privatleben machten die Lidl-Überwacher keinen Halt, wenn es etwa darum ging, private Telefonate zu protokollieren und Schlüsse über die Struktur des Beziehungsnetzes zu ziehen. Auch Äusserlichkeiten, wie z.B. Tätowierungen, wurden protokolliert. Das stellt einen massiven Eingriff in die Persönlichkeitsrechte dar und hat nichts mehr mit legitimer Arbeitskontrolle zu tun. Gemäss Lidl dienen die Protokolle „nicht der Mitarbeiterüberwachung“, sondern der „Feststellung eventuellen Fehlverhaltens“.

3.3.3 Bespitzelung einer SPIEGEL-Journalistin

Im Jahr 2006 überwachte der Bundesnachrichtendienst (BND, der Auslandsnachrichtendienst der Bundesrepublik Deutschland) den E-Mail-Verkehr zwischen der Spiegel-Journalistin Susanne Koelbl und dem afghanischen Handelsminister Amin Farhang.[15] Dazu drangen BND-Mitarbeiter auf die Rechner des afghanischen Ministeriums für Handel und Industrie ein und infizierten diese mit sog. trojanischen Pferden (siehe Abschnitt 1.3, Online-Durchsuchung). In den darauf folgenden Monaten wurden zahlreiche private E-Mail-Nachrichten zwischen der deutschen Journalistin und dem afghanischen Minister mitgelesen. Da in Deutschland die Kommunikationsüberwachung – in diesem Fall das Mitlesen der privaten E-Mail-Inhalte – grundrechtswidrig ist, wurde eine interne Untersuchung eingeleitet. Diese kam zum Schluss, dass es sich in diesem Fall nicht um eine eigentliche Kommunikationsüberwachung handle, da die Kommunikation zum Zeitpunkt der Auswertung bereits abgeschlossen sei – die E-Mail-Nachricht wurde schliesslich zu einem früheren Zeitpunkt verfasst und versendet. Eine solche fadenscheinige Begründung zeigt deutlich, wie wenig ernst der Datenschutz in der Zeit nach dem 11. September 2001 oftmals genommen wird.

15 DER SPIEGEL, Ausgabe 18/2008 – „Ausser Kontrolle“, S. 22

4 Bedrohung durch Überwachung

In diesem Kapitel geht es um die Frage, was sich denn der Bürger an der Überwachung störe. Gleich zu Beginn muss jedoch erwidert werden, dass scheinbar immer weniger Bürger die Überwachung für ein ernstzunehmendes Problem halten. Auf die Verabschiedung der sog. Vorratsdatenspeicherung[16] in Deutschland hielten sich die Proteste in Grenzen.

Auch hierzulande scheint man die langsam, jedoch kontinuierlich fortschreitende Ausbreitung der Überwachungsmassnahmen zu akzeptieren. Es stellt sich die Frage, ob denn so ein Gesetz der Vorratsdatenspeicherung auch in der Schweiz möglich wäre.

Der Ausbau der Überwachungsmassnahmen geschieht zumeist unter dem Vorwand einer erhöhten Sicherheit. So erhofft man sich aus der Videoüberwachung einerseits abschreckende Wirkung auf potentielle Gewalttäter und andererseits eine grössere Chance um allfällige Verbrechen einfacher aufklären zu können.

Obwohl Überwachungskameras und andere „Sicherheitsmassnahmen“ auf eine immer höhere Akzeptanz zu stossen scheinen, gibt es noch einige Interessensgruppen, die dem Ausbau der Überwachungsmassnahmen im Weg stehen. Prominentestes Beispiel dafür ist wohl der deutsche *Chaos Computer Club* (CCC), der die Vorratsdatenspeicherung bis zu deren Verabschiedung stark bekämpft hat und dies noch immer tut. Auch staatliche Organe haben den Auftrag, ihre Bürger vor immer mehr Überwachung zu schützen bzw. auf diese Thematik zu sensibilisieren. In der Schweiz ist dies der *eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte* (EDÖB).

Nun könnte man meinen, diese Interessensgruppen seien darauf bedacht, einer Erhöhung der Sicherheit im Wege zu stehen, wollen sie doch „sicherheitsschaffende“ Überwachungsmassnahmen vehement verhindern. Vielmehr geht es diesen Organisationen jedoch um den Schutz der sog. „Privatsphäre“. Doch was bedeutet der Begriff „Privatsphäre“ eigentlich?

4.1 Privatsphäre

Seit Jahrhunderten unterscheidet man zwischen einer öffentlichen und einer privaten Sphäre. Die öffentliche Sphäre könnte man (stark vereinfacht) als all das bezeichnen, was sich jenseits der eigenen Haustüre befindet. Somit wäre die Privatsphäre in den eigenen vier Wänden anzusiedeln (obwohl moderne Informationstechnik, wie z.B. das Internet, diese Grenzen stark verwischt und selbst im öffentlichen Raum noch eine Privatsphäre besteht).

Diskutiert man nun über diese Privatsphäre, bekommt man immer wieder die folgende, etwas einfältige Antwort zu hören:

> *„Aber ich habe doch gar nichts zu verbergen!“*

Antwort auf die Frage; „Warum schützen Sie denn Ihre Privatsphäre nicht?“

Nun könnte man eine ebenso einfältige Gegenfrage stellen; „Wenn Sie wirklich gar nichts zu verbergen haben, warum schliessen Sie dann die Türe hinter sich, wenn sie auf der Toilette sind?“

Auf diese Gegenfrage fällt eine Antwort schwer. Grund dafür ist, dass jeder Mensch eine Privatsphäre kennt und diese keinesfalls preisgeben möchte. Auch wenn man auf der Toilette nichts kriminelles tut, möchte man dabei keinesfalls beobachtet werden. Auch beim Abendessen mit der Familie, wo in der Regel weder kriminellen Pläne noch terroristische Anschläge ausgebrütet werden, möchte man lieber ungestört bleiben.

16 http://www.sueddeutsche.de/deutschland/artikel/181/149816/

Richtig; man hat zwar überhaupt nichts zu verbergen, wofür man strafrechtlich verfolgt werden könnte, man will sein Privatleben aber trotzdem nicht preisgeben. Unsere Verfassung räumt uns dieses Recht sogar ein:

> *„Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs."*

Bundesverfassung der Schweizerischen Eidgenossenschaft – Art.13: Schutz der Privatsphäre

Die Bundesverfassung (als Inbegriff der Rechtsstaatlichkeit) spricht uns also das Recht auf eine Privatsphäre zu. Der Staat hat somit Vertrauen in seine Bürger, dass diese sich auch im privaten Bereich – ohne jegliche Überwachung – an die geltenden Gesetze halten. Dabei endet die Privatsphäre nicht an der Haustüre, auch unser Brief- und Fernmeldeverkehr unterliegt dem Schutz der Privatsphäre.

Die *„Wer nichts zu befürchten hat, der hat auch nichts zu verbergen"*-Haltung scheint jedoch selbst in Kreisen von Politikern weit verbreitet zu sein. Dies belegt z.B. ein Artikel aus der monatlichen FDP-Zeitung *Freisinn*[17] (letzter Satz; Begründung der Ja-Parole):

Jungfreisinnige kritisieren JUSO

Mit einem Leserbrief äusserte Maurus Zeier, Präsident der Jungfreisinnigen der Stadt Luzern, seine Meinung zum Vorgehen der JUSO, die in private Videoüberwachungssysgteme eingedrungen war und die Bilder im Internet veröffentlicht hatte.

Von Maurus Zeier, Präsident Jungfreisinnige Stadt Luzern

Videokameras sind ein bewährtes Mittel zur Überwachung, Verfolgung und Fahndung von Übeltätern. Nicht zuletzt deshalb gibt es an unzähligen Orten solche Kameras, und die Tendenz dieses Einsatzes ist steigend. Die Stadtbevölkerung kann am 1. Juni einen elementaren Schritt für die Sicherheit vollziehen. Mit Kameras haben wir die Möglichkeit, kriminellen Personen das Handwerk zu legen und die gesamte Hemmschwelle für Gewaltverbrechen um ein entscheidendes Stück zu heben.

Die Gegner haben das Referendum ergriffen und bekommen nun eine Chance, gegen dieses Reglement über die Videoüberwachung zu kämpfen. So soll es auch sein, das ist faire Politik. Was nun aber die Jungsozialisten vollzogen haben, ist weder fair noch erlaubt. Sie haben sich an privaten Videodaten von Firmen bedient, diese ins Netz gestellt und stehen auch noch stolz dazu. Das ist politische Polemik ohne Substanz und Niveau, mal abgesehen davon, dass all diese Firmen unverdient einen Imageschaden davontragen müssen. Mit aus der Luft gegriffenen Behauptungen bezüglich der Polizeikameras zeigen sie gleich selbst, wie haltlos diese Aktion war. Ich möchte nicht wissen, in wie vielen Firmen dieses Experiment gescheitert ist, bis die JUSO endlich eine Firma gefunden hat, bei der man die Kameras anzapfen konnte.

Die Kameras alleine genügen der Sicherheit noch nicht, aber sie sind eine Massnahme dazu. Nehmen wir die Chance wahr und sagen am 1. Juni JA zur Videoüberwachung und zur Sicherheit (oder haben Sie etwas zu verbergen?).

Abbildung 7: Beitrag aus dem Magazin "Freisinn"

„Ja zur Videoüberwachung und zur Sicherheit (oder haben Sie etwas zu verbergen?)." Diese, bei Politikern durchaus verbreitete Haltung setzt nicht nur den Begriff der Überwachung mit demjenigen der Sicherheit gleich, er verträgt sich auch nicht so ganz mit unserer Vorstellung von Demokratie. Die Gründe dafür sollen in den folgenden Abschnitten behandelt werden.

17 Luzerner Freisinn – Nr. 5 / 28. Mai 2008

4.2 Überwachung und Demokratie

Der Staat muss seinen Bürgern nicht blind vertrauen. Wie wir in den vorhergehenden Kapiteln gesehen haben, schreitet der Staat hin und wieder über die Grenze zwischen öffentlicher und privater Sphäre – *Vertrauen ist gut, Kontrolle ist besser*. Doch kann dies im Interesse eines demokratischen Staats liegen?

4.2.1 Freie Meinungsbildung

Ein wichtiges Element eines jeden demokratischen Staats ist die *freie Meinungsbildung*. Der Bürger soll die Möglichkeit haben, sich unabhängig von Staat, Wirtschaft und Medien eine Meinung über Personen, Gesetze, gesellschaftliche Tendenzen usw. zu bilden. Hierbei wird der Bürger jedoch stark beeinflusst (vor allem von den Medien, wie aber auch von Einzelpersonen und Interessensgruppen). Der Bürger bleibt aber grundsätzlich in seiner Meinungsbildung „frei".

Aufgrund der so gefundenen Meinung kann der Bürger dann seine demokratischen Pflichten wahrnehmen. Er kann die Politiker wählen, die seine Meinung am besten vertreten, er kann für und gegen bestimmte Geschäfte der Regierung stimmen und er kann sich zu politischen Entwicklungen äussern. Ohne die freie Meinungsbildung ist eine „echte" Demokratie somit unmöglich.

Totalitäre Systeme haben stets versucht, diese freie Meinungsbildung zu unterdrücken oder so stark zu beeinflussen, dass sie überhaupt nicht mehr „frei" ist. Das wohl wichtigste Instrument dafür ist die Überwachung. So zeichnen sich totalitäre Systeme stets durch sehr mächtige Geheimdienste aus, die sehr eng mit der Polizei in Verbindung stehen. Im dritten Reich war dies die Gestapo, in Russland der KGB und in der DDR die Stasi. Auch in China greift der Staat durch Überwachung in die freie Meinungsbildung seiner Bürger ein, z.B. durch Medienzensur und die Unterdrückung der Pressefreiheit (beides Instrumente der Überwachung).

Ein weiteres, wenn auch fiktives totalitäres System ist die Regierung von Ozeanien in George Orwell's Roman *1984*. In dieser Welt unterdrückt die Regierung die freie Meinungsbildung, indem sie ihre Bürger auf Schritt und Tritt überwacht. Jede noch so kleine Abweichung von der vorgeschriebenen Meinung wird mit Folter und schliesslich dem Tod bestraft. Im Laufe des Romans versucht der Protagonist *Winston* eine freie Meinung zu finden. Dies geschieht jeweils in einer Ecke in Winston's Wohnung, welche nicht durch Überwachungskameras erfasst werden kann. Dort hat Winston ein Tagebuch versteckt, wo er seine Eindrücke und systemkritische Gedanken festhält. In dieser Ecke fühlt sich Winston unbeobachtet, hier kann er die Gelegenheit zur freien Meinungsbildung wahrnehmen. In Tat und Wahrheit weiss die Regierung jedoch sehr wohl über Winston's Tagebuch und somit über seine Meinung Bescheid, diese lässt ihn jedoch vorerst noch im Glauben, unbeobachtet zu sein.

Die freie Meinungsbildung kann somit nur stattfinden, wenn der Bürger dabei unbeobachtet bleibt bzw. sich dabei unbeobachtet fühlt.

4.2.2 Pressefreiheit

Wie bereits angesprochen, wird der Bürger in der Meinungsbildung stark durch die Medien beeinflusst. Darum ist es wichtig, dass Medien nicht im Sinne der Regierung zensiert werden. Die Berichterstattung muss stets frei sein, man spricht hierbei von der sog. *Pressefreiheit* – ein weiteres Grundelement eines jeden demokratischen Staats.

Für eine gründliche Berichterstattung ist oft die Verwendung von Informationen notwendig, deren Urheber aus Gründen der Sicherheit lieber anonym bleiben. Erhält ein Journalist beispielsweise von einem Mitglied einer kriminellen Organisation „heikle" Informationen über Vorgänge innerhalb derselben, so könnte die Nennung der Informationsquelle für den Informanten eine lebensgefährli-

che Situation schaffen. Das Beispiel unter Abschnitt 3.3.3 belegt jedoch, dass es die Geheimdienste mit der Pressefreiheit nicht immer sehr genau nehmen.

In Orwell's 1984 ist die Pressefreiheit gänzlich ausgelöscht; das *Ministerium für Wahrheit* verfasst Meldungen gemäss den Weisungen der Partei. Nachrichten werden zensiert, nachträglich geändert und wenn nötig ganz ausgelöscht. Nötigenfalls wird die Geschichte einfach neu geschrieben, so wie es den aktuellen Umständen am besten entgegenkommt.

> *„Wer die Macht über die Geschichte hat, hat auch Macht über Gegenwart und Zukunft."*

Grundsatz des Ministeriums für Wahrheit in Orwell's Roman 1984

Die Pressefreiheit ist für die freie Meinungsbildung äusserst wichtig und somit ernst zu nehmen!

4.2.3 Demokratisches Rechtssystem

In westlichen Rechtssystemen wird stets von der Unschuld des Menschen ausgegangen. Bestraft wird nur, wessen Schuld als bewiesen gilt. Der Angeklagte muss demnach eigentlich nicht seine Unschuld beweisen, das Gericht muss die Schuld des Angeklagten nachweisen können, um ihn verurteilen zu können. Zum Angeklagten wird man erst, wenn man der Begehung eines bestimmten Verbrechens verdächtigt wird. Angeklagt werden auch nicht eine Reihe von möglichen Tatverdächtigen, sondern nur diejenigen Person (oder Gruppe von Personen), bei denen sich der Verdacht erhärtet hat.

Weiter gilt in unserem Rechtssystem der Grundsatz, dass nur verurteilt werden kann, wer angeklagt ist. Begeht der Bürger ein Verbrechen/ein Vergehen, so muss er zunächst angeklagt werden, bevor er verurteilt werden kann. Bei leichteren Vergehen, wie z.B. bei übler Nachrede oder leichter Körperverletzung, klagt der Geschädigte den Täter an. Bei schwereren Vergehen, wie z.B. Mord oder Brandstiftung, wird der Verdächtige durch die Staatsanwaltschaft angeklagt. Hier mag es Unterschiede zwischen den Rechtssystemen einzelner westlicher Staaten geben, es gilt aber trotzdem immer der Grundsatz; *wo kein Kläger ist, ist kein Richter*.

Moderne Überwachungstechnologie scheint aber unser Rechtssystem in einigen Fällen aushebeln zu können. Dazu zwei (fiktive) Beispiele:

1. **Automatisierter Strafvollzug:** Moderne Automobile sind mit viel Elektronik ausgestattet. Technische Daten, wie z.B. die Fahrgeschwindigkeit, könnten so protokolliert werden. Eine Versicherungsgesellschaft könnte so z.B. auf verunfallte Temposünder Regress nehmen, indem sie das Geschwindigkeitsprotokoll eines Fahrzeugs auswertet. Überwachung soll ja angeblich einer erhöhten Sicherheit dienen, so wäre es doch schön, wenn man solche Unfälle gar nicht erst stattfinden liesse. Warum soll also bei einer übersetzten Geschwindigkeit nicht einfach die Benzinzufuhr abgedreht werden bis sich die Geschwindigkeit wieder im legalen Bereich befindet (siehe dazu auch Abschnitt 4.2.5)? Finanziell wäre es noch attraktiver, wenn man so z.B. den Temposünder gleich automatisch büssen könnte. Bei jeder Tempoüberschreitung erhält der Fahrer automatisch eine entsprechendes Busse, die Abwicklung könnte automatisch erfolgen, Zeit und somit Geld sparen. Das Problem an diesem fiktiven, jedoch technisch durchaus realisierbaren Szenario ist nun, dass es unser Rechtssystem untergräbt. Hier fehlt nicht nur ein Kläger, das Recht wird auch automatisch gesprochen. Dies ist mit unserem Rechtssystem, wo Richter abwägen und Tatumstände berücksichtigen müssen, nicht vereinbar.
2. **Der Bürger unter Generalverdacht:** Bei schweren Sexualdelikten kommen immer öfters Gentests zum Einsatz, womit man den Täter anhand winzigster Spuren am Tatort oder am Opfer (z.B. Haaren oder Blutflecken) überführen kann. Gentests gelten als eine sehr genaue Methode zur Überführung von Verbrechern, mit Hilfe von Gentests konnten so einige Täter überführt werden, denen man diese Verbrechen mit althergebrachten Fahndungsmethoden

wohl nicht hätte nachweisen können. Somit sind Gentests grundsätzlich positiv zu bewerten. Problematisch wird es jedoch, wenn sog. Massengentests durchgeführt werden. Hier könnte von einem bestimmten Personenkreis verlangt werden, dass sie eine DNA-Probe abgeben müssen. Die Eingrenzung des Personenkreises kann dabei mehr oder weniger stark sein, so könnten bei einer Vergewaltigung mit anschliessendem Mord ein Gentest sämtlicher Personen menschlichen Geschlechts ab 18 Jahren erfolgen. Selbst wenn diese DNA-Tests freiwillig sind, ist de facto jeder „Verdächtige" dazu verpflichtet, einen entsprechenden Gentest über sich ergehen zu lassen. Wer seine DNA aus Gründen des Datenschutzes nicht offenbaren will, der könnte sich so leicht verdächtig machen. Grund dafür ist das leidige „*Wer nichts zu befürchten hat, der hat auch nichts zu verbergen*". Es werden somit zusätzliche Verdachtsmomente geschaffen. Obwohl bei einem solchen Verbrechen in der Regel nur ein Einzeltäter zu suchen ist, wird von einer grossen Anzahl von Personen verlangt, dass sie ihre Unschuld nachweisen sollen. Ungeachtet dessen, ob die DNA-Informationen vertraulich behandelt und nach erfolgter Ermittlung wieder gelöscht werden, verträgt sich diese Art der Fahndung nicht mit unserem Rechtssystem.

4.2.4 Vertrauen gegenüber dem Bürger

In jeder Beziehung – gerade in der Beziehung zwischen dem Staat und seinen Bürgern – ist gegenseitiges Vertrauten unbedingt notwendig. Die Redewendung *„Vertrauen ist gut, Kontrolle ist besser."* schliesst ein, dass sich Kontrolle (Überwachung) über das Vertrauen hinweg setzt. Wer glaubt, er müsse kontrollieren, der vertraut nicht. Ein Überwachungsstaat vertraut seinen Bürgern nicht, er hält sie für potentiell kriminell, er sieht sie als Gegner des Regimes, als Staatsfeind.

Nimmt der Bürger nun eine starke Überwachung wahr, so nimmt er den Überwachenden (den Staat) als übergeordnete Kontrollinstanz wahr, der seinen Bürgern nicht vertraut. Infolge dessen steigt das Machtgefälle zwischen Bürger und Staat – der Staat ist dem Bürger übergeordnet, der Bürger sieht sich nicht mehr als Teil des Staats.

Jedoch lebt ein jeder demokratischer Staat von seinen Bürgern. Schliesslich muss die Regierung von seinen Bürgern gewählt werden, in der Schweiz können die Bürger sogar sehr direkten Einfluss auf die Regierungsgeschäfte nehmen (Referenden, Volksinitiativen). Bürger, die dem Staat nicht mehr vertrauen, nehmen sich nicht mehr als Teil des Staats wahr. Dies kann sich zum Beispiel dadurch äussern, dass der Bürger nicht mehr an Wahlen und Abstimmungen teilnehmen möchte. Da eine Regierung stets das ganze Volk vertreten soll, müssen die Interessen möglichst aller Bürger berücksichtigt werden. Dies ist nur bei einer hohen Wahlbeteiligung möglich. Wer nicht wählt, dessen Interessen können gar nicht demokratisch vertreten werden.

Eine Staatsform kann sich nur halten, wenn sie stark ist. Wird die Demokratie (durch sinkenden Wähleranteil) immer schwächer, ist sie in Gefahr. Es könnte so die Machtübernahme eines nicht demokratischen Regimes folgen. In Europa halten wir unsere Demokratien zwar für „gesichert", dies muss aber kein zwingender Endzustand sein. Es liegt nur gerade 60 Jahre zurück, dass die Diktatur eine in Europa gebräuchliche Staatsform war (deutsches Reich, Italien, Spanien).

Überwachung soll zwar Sicherheit schaffen und somit unsere Demokratie stärken. Übertreibt man es jedoch mit der Überwachung, so kann als Folge daraus eine geschwächte Demokratie resultieren.

4.2.5 Der unmündige Bürger

Um auf das Beispiel des tempobegrenzten Autos zurückzukommen; würde der Staat in sämtliche Autos seiner Bürger Steuerungen einbauen, die eine Überschreitung der Mindestgeschwindigkeit verhindern würden, so würde möglicherweise mehr Sicherheit geschaffen, der Bürger wird aber in seiner Entscheidung eingeschränkt, sich gesetzeskonform zu verhalten. Greift eine solche *Bevormundung* in immer mehr Bereiche des Lebens ein, so muss der Bürger gar nicht mehr entscheiden, was er nun tun soll – er kann ja schliesslich nur noch das tun, was ihm der Staat zu tun erlaubt. Es

wäre dem Bürger somit nicht mehr möglich, eine eigene Moralvorstellung auszubilden. Lässt man die Bürger nur noch in einem Gängelwagen laufen, so werden sie das selbständige Gehen nie richtig erlernen können (siehe dazu auch den Aufsatz „*Beantwortung der Frage: Was ist Aufklärung?*“[18] von Immanuel Kant).

Sollten wir für ein bisschen mehr Sicherheit wirklich wieder in das Zeitalter vor der Aufklärung zurück kehren?

4.3 Weitere Gefahren

Bisher wurde in diesem Kapitel die Überwachung in den Kontext zwischen Staat und Bürger gestellt. Wie die vorhergehenden Kapitel jedoch aufgezeigt haben, geht ein Grossteil der heutigen Überwachung nicht vom Staat, sondern von der Wirtschaft oder sogar vom einzelnen Bürgern aus. Es sind somit nicht nur die Gefahren für die demokratische Rechtsordnung zu beachten, sondern auch diejenigen, die sich dort bemerkbar machen, wo wir keinen Staat wahrnehmen.

In den folgenden Abschnitten geht es um allgemeinere Gefahren der Überwachung, ungeachtet dessen, ob der Staat, die Wirtschaft oder der einzelne Bürger der Überwacher ist. Dabei geht es vor allem darum, wie sich die Gefahren auf den einzelnen Bürger auswirken können.

4.3.1 Missbrauch erhobener Daten

Bereits im Mittelalter wurden Daten erhoben, gesammelt und ausgewertet – Überwachung ist kein Phänomen des hochtechnisierten 21. Jahrhunderts. Gerade die heutige Technik birgt jedoch grosse Risiken, indem sie einen grossen Einfluss auf den Umgang mit Daten hat:

- **Daten können einfacher erhoben werden.** Vorbei sind die Zeiten, in denen Informationen mit Tinte und Feder zu Papier gebracht werden mussten, um festgehalten werden zu können. Überwachungskameras mit Gesichtserkennung, RFID-Chips, Sensoren in Automobilen wie auch andere, in Kapitel 1 vorgestellte Technologien vereinfachen die Erhebung der Daten massiv. Die Folge daraus ist nicht nur eine grössere Datenmenge, sondern auch die Erhebung von Daten aus praktisch sämtlichen Lebensbereichen.
- **Daten haben „Flügel“.** Die Verteilung von Informationen war bis im Mittelalter ein mühsames Unterfangen, musste doch alles von Hand abgeschrieben werden. Seit dem Buchdruck ist dies deutlich einfacher geworden. Dennoch waren Daten zu diesem Zeitpunkt noch an ihr Trägermedium gebunden. Für die Weitergabe von Informationen war somit die physische Weitergabe des ganzen Trägermediums notwendig. Heutzutage, da Daten digital vorliegen, können sie in kürzester Zeit über die ganze Welt transportiert werden – verlustfrei und sooft man will.
- **Datenbestände werden abgeglichen.** Daten liegen heute zumeist digital, in der Regel in sog. relationalen Datenbanken[19] vor. In solchen Datenbanken stehen die Daten in bestimmten Beziehungen (in Relationen) zueinander. Eine Zusammenführung von Datenbeständen schafft in diesem Fall eine Vergrösserung des Informationswerts. Dieser Informationswert ist grösser als die Summe der einzelnen Datenbestände, da aufgrund der neuen Beziehungen zwischen den Daten neue, aus dem Kontext erschliessbare Informationen zu erkennen sind. Eine grosse, zusammengeführte Datenbank hat somit einen grösseren Wert als zehn kleinere Datenbanken, auf denen die gleichen Informationen verteilt sind.
- **Daten bleiben „haften“.** Nicht nur die Übertragung ist heute wenig aufwändig, auch die dauerhafte (persistente) Speicherung der Daten wird immer einfacher und günstiger. Den Informationsgehalt, den man im 19. Jahrhundert in riesigen Aktenschränken halten musste,

18 http://de.wikisource.org/wiki/Beantwortung_der_Frage:_Was_ist_Aufkl%C3%A4rung

19 http://de.wikipedia.org/wiki/Relationale_Datenbank

kann man sich heute bequem als digitales Speichermedium in die Hosentasche stecken. Papier ist im Vergleich zu digitalem Speicherplatz ein sehr teures Medium, betrachtet man dies im Verhältnis „speicherbare Information pro Geldeinheit". Daten können somit äusserst günstig abgespeichert werden. Der Preis für digitale Speichermedien sinkt unaufhörlich. Heute bezahlt man für eine DVD ungefähr den gleichen Preis, wie man vor 10 Jahren für eine Diskette bezahlt hat. Die DVD verfügt jedoch über eine mehr als 3'000 mal grössere Speicherkapazität als die Diskette. Es macht somit keinen Sinn, alte Daten (die sich gerade auf älteren Medien befinden) zu löschen. Der daraus gewonnene Speicherplatz kann kaum in Geld aufgewogen werden. Im Zweifelsfall lässt man Daten also einfach bestehen, Daten werden somit kaum gelöscht. Ein anderes Beispiel dazu ist das Internet. Selbst wenn Information aus dem Internet (d.h. vom entsprechenden Webserver) gelöscht werden, können diese noch lokal bei Internet-Nutzern vorhanden sein und dies auch bleiben. Sind die Daten erst einmal erhoben, können sie kaum mehr gelöscht werden.

Erhobene (und auf ewig gespeicherte) Daten stellen zwar an und für sich keine Gefahr dar. Problematisch wird die Situation erst, wenn die Daten verwendet werden. Diese Verwendung befindet sich oftmals in einer rechtlichen Grauzone, da die Gesetzgebung mit der technischen Entwicklung kaum Schritt halten kann. Dies birgt für den Einzelnen einige Gefahren, hier einige Beispiele dazu:

- **Falschinformationen:** Nicht alle erhobenen Daten müssen notwendigerweise korrekt sein. So entstehen einige Daten durch Interpretation aus bestehenden Datenbeständen, werden ungenau aufgenommen oder es passieren Fehler bei der Überführung von analogen Daten in digitale Systeme (ein Sachbearbeiter tippt die Angaben aus einem Formular falsch ein). Daten werden für eine sehr lange Zeit abgespeichert, ob die Daten während dieser Zeit jedoch immer korrekt bleiben, ist zu bezweifeln. Oftmals werden Daten einmalig erhoben, jedoch später nicht mehr aktualisiert. Dies kann für den Einzelnen schwerwiegende Folgen haben:
  - Durch sog. Scoring-Verfahren (siehe Abschnitt 1.7) kann einem Einzelnen eine schlechte Kreditwürdigkeit unterstellt werden. Basiert der Scoring-Wert auf falschen Informationen, kann ein an und für sich kreditwürdiger Bürger Mühe haben, einen Kredit zu bekommen, einen Handy-Vertrag abzuschliessen oder Waren gegen Rechnung zu bestellen. Da Daten „haften" bleiben, kann dies für den Betroffenen einen Nachteil auf Lebzeiten darstellen.
  - Wer sich heutzutage für eine Stelle bewirbt, der muss damit rechnen, „*gegoogelt*"[20] zu werden. Nun können so Informationen zu Tage kommen, die vom vermeintlich zukünftigen Arbeitgeber als negativ bewertet werden. Ob es sich bei den gefundenen Informationen wirklich um die entsprechende Person handelt, hängt oftmals vom Namen ab (zu einem gewissen „Hans Meier" wird man bestimmt mehr Informationen finden als zu einem „Hans-Joachim Samsa"). Auch können dabei Äusserungen von Personen (z.B. aus Internetforen) auftauchen, zu denen sie heutzutage gar nicht mehr stehen. Dies kann gerade für die Generationen zu einem Nachteil werden, die bereits während der Kindheit und der Pubertät Gebrauch vom Internet macht. Daten aus dem Internet zu verbannen ist praktisch unmöglich, somit kann man sich im Internet seinen Ruf auf Lebzeiten ruinieren. Noch schlimmer ist jedoch, dass Drittpersonen unter falscher Namensangabe den Ruf anderer Personen ruinieren können, selbst die Löschung von Falschinformationen ist allein technisch praktisch nicht durchführbar.
- **Verkauf von vertraulichen Informationen:** Gelegenheit macht bekanntlich Diebe. Wer vertrauliche Daten hortet, kann daraus ohne grossen Aufwand Kapital schlagen. Dieser illegale Handel von vertraulichen Daten ist zudem strafrechtlich kaum verfolgbar, zumal die Auswirkungen auf den Informationshandel für die „Opfer" kaum nachvollziehbar sind.

20 http://de.wikipedia.org/wiki/Googeln#Das_Verb_.E2.80.9Egoogeln.E2.80.9C

  - In einigen grösseren Supermarktketten gibt es heutzutage Kundenkärtchen, womit sich die Händler scheinbar bei ihren Kunden für die Treue bedanken möchten. Aus diesen Daten lässt sich einiges über den Lebensstil des Konsumenten aussagen (Alkohol- und Tabakkonsum, ungesunde Ernährung, familiäre Verhältnisse). Bestimmte Versicherungsangebote lohnen sich für die Versicherungsgesellschaft vor allem dann, wenn sich der Versicherte einer guten Gesundheit erfreut und so ein geringes finanzielles Risiko darstellt. Versicherungen könnten so durch den (illegalen) Erwerb der gesammelten Konsuminformationen ihre Rentabilität steigern, indem sie Leute mit einem ungesunden Lebenswandel ausschliessen bzw. gar nicht erst aufnehmen. In der Schweiz darf zwar niemand für die Grundversicherung abgelehnt werden (siehe *volle Freizügigkeit*[21]), dennoch könnte man hierzulande für eine Zusatz- oder eine Risikolebensversicherung aufgrund seines Konsumverhaltens abgelehnt werden.

- **Potentiell sensible Daten:** Informationen, die wir über uns Preis geben, scheinen uns oftmals im jeweiligen Kontext als nicht besonders schützenswert. Für ein Preisausschreiben muss man seine Adresse angeben, ansonsten kann einem ja schliesslich der Gewinn nicht zugestellt werden (man muss jedoch damit rechnen, dass die Adresse für Werbezwecke weiterverkauft wird). Heikler wird es bei Angaben über politische und sexuelle Gesinnung, Herkunft und Religion.
  - So erscheint es einem heute wohl kaum als gefährlich, sich irgendwo als homosexuellen, sozialdemokratischen Juden polnischer Herkunft abspeichern zu lassen. In Rechtsstaaten gibt es ja schliesslich Mehrparteien-Systeme, es herrscht Religionsfreiheit und Homosexualität gilt weitgehend als akzeptiert. Blickt man jedoch nur ein halbes Jahrhundert in der Geschichte zurück, so erkennt man, dass unsere demokratische Rechtsordnung nicht zwingend als endgültig gilt. Sollte eines Tages wieder eine totalitäre Regierung herrschen, könnten einige Informationen schnell lebensgefährlich werden. Wer sich dann (fälschlicher- oder korrekterweise) in einem „Schwulen-Register“, einer „Juden-Datenbank“ oder einem Verzeichnis „linksgerichteter Personen“ befindet, könnte dann um Leib und Leben bedroht sein.

4.3.2 Genormtes und konformes Verhalten

Moderne Überwachungssysteme funktionieren heutzutage häufig ohne jeglichen menschlichen Aufwand, dies wurde ausführlich in Kapitel 1 belegt. Überwachungskameras können im Zusammenspiel mit der entsprechenden Software Gesichter erkennen oder „auffälliges“ Verhalten feststellen.

Nun stellt sich die Frage; was ist „auffälliges“ Verhalten? Mithilfe von Überwachungskameras können beispielsweise nur Bewegungsabläufe ausgewertet werden, welche dann mit einer bestimmten Norm verglichen werden müssten. So müsste man auch eine bestimmte Norm finden, was denn „normale“ und „abnormale“ Bewegung ist. Vielleicht wird so eines Tages das Monty Python'sche *Ministry of Silly Walks*[22] doch noch zur Realität! Doch Spass beiseite; wer aufgrund einer Behinderung nicht „normal“ gehen kann, der könnte schnell den Fokus auf sich ziehen und so Ziel einer genaueren Überprüfung werden. Hier kann man eindeutig von einer Diskriminierung behinderter Personen sprechen.

Gibt es eine Norm, wie man sich auf der Strasse zu bewegen hat, damit man nicht registriert wird, so werden sich die Menschen an einen bestimmten Gang gewöhnen müssen. Man stelle sich eine „Armee“ von Menschen vor, die sich auf der Strasse alle gleich bewegen (als Zyniker könnte man nun behaupten, dass dieser Gang wohl dem Stechschritt entsprechen müsse). Dies kann man definitiv als Einschnitt in die Freiheit bezeichnen.

21 http://www.comparis.com/krankenkassen/info/glossar.aspx?id=KK_Info_freizuegigkeit

22 http://en.wikipedia.org/wiki/Silly_Walks

Dieses Szenario ist glücklicherweise noch weit von der Realität entfernt. Eine wichtige Erkenntnis daraus ist jedoch, dass sich Menschen, die sich beobachtet fühlen, anders verhalten, als sie es eigentlich tun möchten[23]. Die Menschen verhalten sich unter Überwachung nicht mehr natürlich, da sie ansonsten „aus dem Raster fallen" könnten. Fühlt sich der Bürger nun in immer mehr Lebenssituationen überwacht, so wird er sich auch an immer mehr Normen anpassen müssen. Die Folgen daraus wären fatal. Es entstünde so ein *Einheitsbürger*, dessen Verhaltensweisen genau voraussehbar und der somit auch sehr einfach zu beeinflussen wäre. So ein Einheitsbürger wäre weder zu innovativen Erfindungen, noch zu kreativer Arbeit fähig. Dies würde einerseits negative Folgen für die Wirtschaft, andererseits auch eine grosse Einbusse für die Kultur bedeuten.

Auch hier lohnt sich ein Blick auf Orwell's 1984. So verhält sich der Protagonist Winston überall wo er Kameras vermutet möglichst unauffällig. Fühlt er sich dann jedoch in seiner geheimen „Schreibecke" unbeobachtet, ist er zur Kritik an der Regierung und an der Gesellschaft fähig. Auch mietet er sich mit seiner Affäre Julia ein vermeintlich unüberwachtes Zimmer an, wo die beiden verbotenerweise einer sexuellen Beziehung nachgehen. Sämtliche kritischen und intellektuellen Überlegungen, wie auch emotionalen Szenen sind jeweils an Plätzen angesiedelt, wo keine Überwachung zu vermuten ist (die Szenen nach der Verhaftung ausgenommen).

Der Mensch kann sein Potential nur an den Orten entfalten, an denen er sich frei, d.h. unüberwacht fühlt.

4.3.3 Zur-Schau-Stellung der Privatsphäre

Wie man aus den vergangenen drei Kapiteln schliessen kann, werden für die Überwachung scheinbar gigantische Aufwände getätigt. In Tat und Wahrheit hat sich um die Überwachung ein ganzer Wirtschaftszweig gebildet, von dem tausende von Arbeitsplätzen abhängig sind. Doch nicht immer muss viel Aufwand betrieben werden, um etwas über Personen erfahren zu können. Vielmehr scheinen einzelne Individuen ihre Privatangelegenheiten der Öffentlichkeit geradezu aufdrängen zu wollen. Dies mag einerseits aus narzisstischen Gründen geschehen (man bedenke die sog. „Klatschzeitungen"), andererseits aus Unvorsicht bzw. schlicht und einfach aus Ignoranz.

Ein wichtiges Stichwort dazu ist das sog. *Social Networking*. Internetgemeinschaften wie z.B. Facebook, StudiVZ (das Studentenverzeichnis) oder MySpace verzeichnen monatlich einen Mitgleiderzuwachs im zweistelligen Prozentbereich. In diesem *Communities* offenbaren die Mitglieder der Aussenwelt nicht nur Geburtsdaten, Adressen oder Telefonnummern, auch kulturelle Vorlieben (z.B. der Musikgeschmack) als auch die politische Gesinnung werden für die ganze Welt zugänglich gemacht. Auch veröffentlichen Benutzer dieser Plattformen Foto- und Videomaterial. Hier reicht die Spannweite von ganz harmlosen Portraits bis zu Videoaufzeichnungen von Parties, auf denen Rauschgift konsumiert wird. Auch besteht die Möglichkeit, sich virtuelle Freunde zu machen. Hier entsteht eine Freundschaft jedoch durch Mausklick, nicht etwa aufgrund eines jahrelangen Vertrauensverhältnisses. Anhand sog. „Freundes-Listen" können ganze soziale Netzwerke reproduziert werden. Dies kann für die anderen Mitglieder des virtuellen Freundeskreises ganz reale Folgen haben; wird beispielsweise eine Person eines Netzwerks des Handels von Kinderpornografie verdächtigt, so könnten die anderen Mitglieder des Freundeskreises ebenfalls – so schnell wie unschuldig – verdächtigt werden.

Ein anderes Beispiel für die „Veröffentlichung" der Privatsphäre stellen Mobiltelefone dar. Hat man früher in einem stillen Kämmerlein, abseits seiner Mitmenschen telefoniert, so werden heute Restaurants, öffentliche Plätze oder ganze Eisenbahnwaggons zu riesigen Telefonzellen umfunktioniert. Mir persönlich fällt immer wieder auf, wie viele und welche Informationen Personen über sich preisgeben, die im Zug telefonieren – teilweise mit „übertriebener" Lautstärke. So wäre ich am Ende einer Zugfahrt oftmals bestens über intime Details und die neusten Erlebnisse von Mobiltelefon-Nutzern informiert, würde ich nur aufmerksam genug zuhören.

23 McGrath, John E.: Loving Big Brother. Performance, Privacy and Surveillance Space. London/New York 2004

Wer seine Privatsphäre so leichtfertig vor sich hin trägt, scheint Datenschutz für unnötig zu halten.

4.3.4 Gefahren eines öffentlichen Prangers

In den USA werden „aus Sicherheitsgründen" immer wieder Informationen über Straftäter im Internet veröffentlicht[24]. Man will den Bürgern so eine Möglichkeit bieten, diesen Kriminellen fern zu bleiben. Diese Entwicklung ist jedoch äusserst problematisch:

1. Straftäter werden an einen öffentlichen Internet-Pranger gestellt, sie sind dann der ganzen Welt als Verbrecher ersichtlich und werden dementsprechend abgestempelt. Dies erschwert die Resozialisierung von ehemaligen Straftätern, bedenke man nur, dass ein zukünftiger Arbeitgeber seine Bewerber mit hoher Wahrscheinlichkeit „googeln" wird. Wer einmal auf einer Verbrecher-Liste gelandet ist, wird so kaum mehr die Chance erhalten, einer beruflichen Tätigkeit nachzugehen.
2. Betroffene von Gewalt- oder Sexualdelikten könnten Rachegelüste gegen die jeweiligen Täter hegen. Hat ein Verbrecher nun aber seine Haftstrafe abgesessen, sollte er eigentlich seine Schuld beglichen haben, er steht mit dem Gesetz wieder im Reinen. Es besteht jedoch die Gefahr, dass sich Opfer nachträglich an ihren Peinigern rächen wollen. Dazu stellt eine Internetdatenbank mit der Adresse der ehemaligen Verbrecher einen komfortablen Ausgangspunkt für Selbstjustiz zur Verfügung. Auch könnten die Opfer von späteren Verbrechen diejenigen Personen verdächtigen, die sich schon ähnlicher Verbrechen strafbar gemacht haben. Diese Personen könnten nun zur idealen Zielscheibe der Öffentlichkeit werden.

Will man Schwerverbrecher wieder an unserer Gesellschaft teilnehmen lassen können, müssen wir deren Privatsphäre anerkennen und respektieren!

4.3.5 Hat der Bürger nichts dazu gelernt?

Immer wieder wurde in dieser Arbeit auf unseren nördlichen Nachbarn Deutschland verwiesen. Deutschland hat einerseits eine sehr umfangreiche Vergangenheit zum Thema Überwachung, denkt man etwa an die Gestapo im dritten Reich oder an die Stasi in der DDR. Leider zeigen sich in Deutschland wieder einige solcher Tendenzen:

Abbildung 8: Wolfgang Schäuble

1. Nach dem zweiten Weltkrieg wurden polizeiliche und geheimdienstliche Befugnisse stark getrennt. Dies wurde im sog. *Trennungsgrundsatz*[25] in der Verfassung festgehalten. Auf diese Weise wollte man eine neue Behörde analog der Gestapo verhindern. Seit den Terroranschlägen vom 11. September 2001 gerät dieser Trennungsgrundsatz jedoch immer weiter unter Beschuss, polizeiliche und geheimdienstliche Behörden arbeiten immer stärker zusammen, auch sollen sie Zugriff auf gemeinsame Datenbestände erhalten.
2. Wie bereits mehrmals erwähnt, hat Deutschland die sog. Vorratsdatenspeicherung beschlossen (siehe Abschnitt 1.4).
3. Die sog. Online-Durchsuchung ist zwar in Deutschland noch nicht beschlossene Sache, wird aber von geheimdienstlichen Behörden durchaus schon praktiziert (siehe Abschnitt 1.3). Diese Praxis mag uns vielleicht an die Stasi erinnern, in Deutschland befürworten jedoch knapp zwei Drittel der Wähler die Online-Durchsuchung[26].

24 http://www.heise.de/tp/r4/artikel/4/4585/1.html

25 http://de.wikipedia.org/wiki/Trennungsgrundsatz

26 http://politbarometer.zdf.de/ZDFde/inhalt/0/0,1872,7004800,00.html?dr=1

4. Der deutsche Innenminister Wolfgang Schäuble zeigte sich fasziniert vom *Government Communications Headquarter* (GCHQ) in Grossbritannien. Hierbei handelt es sich um eine 1.8 Milliarden € teure Überwachungsanlage, die rund 4'000 Mitarbeiter beschäftigt. Schäuble plant nun eine eigene Abhörzentrale zur Telekommunikationsüberwachung in Köln.[27] In diesem Zuge sollen auch polizeiliche und geheimdienstliche Befugnisse näher aneinander rücken, was im Konflikt mit dem Trennungsgrundsatz steht.

Es bleibt somit nur zu hoffen, dass die Bürger endlich erwachen und sich gegen solche Vorhaben zur Wehr setzen. Man darf also auf die anstehenden Bundestagswahlen in Deutschland (Herbst 2009) und die kommenden Präsidentschaftswahlen in den USA (Herbst 2008) gespannt sein.

4.3.6 Kann man sich schützen?

Nun drängt sich natürlich die Frage auf, ob man sich denn vor diesen Bedrohungen schützen kann. Die Beantwortung dieser Frage würde zumindest ein weiteres, fünftes Kapitel erfordern. Somit sollen hiermit nur einige wichtige Merkregeln wiedergegeben werden, die man sich auch für den Alltag merken kann.

- Wer sich vor diesen Gefahren schützen will, der muss verantwortungsvoll mit Informationen über sich selbst umgehen.
- Dazu kann es auch gehören, dass man auf bestimmte angenehme Sachen, wie z.B. auf Preisausschreiben oder Prämien für Kundentreue verzichtet.
- Man sollte immer nur die Informationen über sich und Angehörige preisgeben, die unbedingt notwendig sind.
- Auch sollte man stets darauf achten, welche Informationen man im Internet über sich preisgibt – das Netz vergisst nichts!
- Die Wahrung der Privatsphäre ist eines der wichtigsten Verdienste der Demokratie. Die Privatsphäre ist zu verteidigen, sei es im Alltag oder an der Abstimmungsurne.

27 DER SPIEGEL, Ausgabe 21/2008 – „Der ganz grosse Lauschangriff“, S. 20

Schlussteil

In diesem Teil sollen nun die eigentlichen Fragen beantwortet werden, die in den vorhergehenden vier Kapiteln bearbeitet wurden.

Technische Mittel zur Überwachung (Dominic Kurmann)

- Frage: *Mit welchen technischen Mitteln überwacht der Staat seine Bürger, die Wirtschaft die Konsumenten?*
- Antwort: Es sollte klar sein, dass die einzelnen Themen, über die wir in diesem Kapitel berichtet haben, nur einen Teil davon darstellen, was noch alles möglich wäre. Die unserer Meinung nach wichtigsten Punkte, die uns auch direkt betreffen könnten, wurden behandelt. Jede technische Neuerung, sei es das Telefon, das Internet oder das Handy, hat immer wieder die Diskussion um die Wahrung der individuellen Autonomie aufgeworfen. Die Anzahl der entzündeten Debatten um die Gefährdung der Privatsphäre belegt: Das Private ist keine Angelegenheit privaten, sondern öffentlichen Interesses.

Für die Recherchen in diesem Kapitel wurde hauptsächlich das Internet verwendet. Dort ist es möglich immer über die neusten Entwicklungen und Gesetzesentscheide auf dem laufenden gehalten zu werden. Ein Buch, das sich mit dem Thema Überwachung befasst, hat mir geholfen eine grobe Struktur über die wichtigsten Punkte zu erhalten. Dann wurden die wichtigen Informationen gesammelt, wobei sich das Problem stellte, diese zu verarbeiten. Zu diesem Thema fanden wir eine Vielzahl an Berichten, die es nach Verwendungsmöglichkeit zu sortieren galt. In einem letzten Schritt wurden dann die einzelnen Beiträge zusammengestellt.

Durch persönliches Interesse an moderner Technik war mir das Thema nicht ganz fremd. Ich war über vielerlei schon unterrichtet und konnte so auch eigene Erfahrungen einfach einbringen. Ein wenig schockierend ist es schon, wenn man sieht, was heutzutage alles möglich ist. Aber auch die Neugier über das Kommende lässt mich gespannt in die Zukunft blicken.

Sinn und Zweck der Überwachung (Ruedi Hauri)

- Frage: *Wozu dient eigentlich Überwachung, was will man damit erreichen?*
- Antwort: Wenn man das entsprechende Kapitel liest merkt man schnell, dass die Motive für Überwachung grundverschieden sind und folglich auch ihre Ziele. Um die gestellte Frage genau beantworten zu können, müsste man also jeden Fall für sich beurteilen. Generell kann jedoch gesagt werden, dass wer überwacht, Wissen benötigt, um dieses dann, vorzugsweise zu seinem eigenen Vorteil, einzusetzen. Es sollen Ziele erreicht werden, die man sich selbst gesteckt hat. Überwachung ist also nichts anderes als ein Mittel um eigene Vorstellungen und Vorgaben verwirklichen zu können.

Ich muss gestehen, dass mir das Verfassen dieser Arbeit nicht leicht gefallen ist. Die Hauptgründe dafür sind persönlicher Natur, ich möchte deshalb nicht weiter darauf eingehen. Dazu kommt, dass ich mir zum Thema Überwachung noch gar nie wirklich Gedanken gemacht hatte. Ich musste also bei Null anfangen um überhaupt eine grobe Übersicht über diesen Stoff zu bekommen. Etliche Mühe bereitete mir auch das Auffinden geeigneter, zu meinem Kapitel passender, Literatur. Durch das Internet kam ich trotzdem zu meinen Informationen und konnte auch ein weniges an passenden Büchern auftreiben.

Abschliessend möchte ich sagen, dass ich dem Thema Überwachung nicht mehr so teilnahms- und sorglos gegenüberstehen werde wie bis anhin. Die Auseinandersetzung mit diesem Thema war sehr interessant und erschreckend. Erschreckend deshalb, weil ich mir nun ein Bild über die Gefahren, die von der Überwachung ausgehen, machen kann.

Konkrete Fälle von Überwachung (Philipp Rölli)

- Frage: *In welchen konkreten Fällen führt(e) Überwachung zu mehr Sicherheit?*
- Antwort: In Einzelfällen ist die Videoüberwachung massgeblich daran beteiligt, Verbrechen im Nachhinein aufzuklären. Vor allem in England wurden mehrere solcher Fälle in den Medien gross inszeniert. In der Schweiz werden solche Fälle als Beweis der Wirksamkeit und als Rechtfertigung der Videoüberwachung herangezogen. Wie sich die Videoüberwachung jedoch auf die Gesamtkriminalität und somit auf eine Erhöhung der Sicherheit auswirkt, ist noch wenig erforscht. Laut einer britischen Studie ist die Auswirkung aber eher gering.

Aus aktuellem politischen Anlass war die Untersuchung der Wirksamkeit der Videoüberwachung sehr interessant. Die Schwierigkeit lag darin, dass die Argumente für eine Videoüberwachung häufig völlig aus der Luft gegriffen sind. Tatsächlich sind aber kaum aussagekräftige Untersuchungen vorhanden. Dank dem sehr guten Buch „Das Ende der Privatsphäre“ von Peter Schaar bin ich auf weiterführende Informationen gestossen. Die eigentlich einfache Frage, wie wirksam Videoüberwachung ist, liess sich nicht ohne weiteres beantworten. Schlussendlich stützte ich einen grossen Teil des dritten Kapitels auf einer britischen Studie ab. Persönlich habe ich dadurch profitiert, dass ich heute die Videoüberwachung viel differenzierter betrachte und auch bewusster als eine mögliche Einschränkung der Freiheit auffasse.

Bedrohung durch Überwachung (Patrick Bucher)

- Frage: *Worin besteht eine Bedrohung durch Überwachung, was soll sich der Bürger daran stören?*
- Antwort: Überwachung verträgt sich ab einer gewissen Grössenordnung überhaupt nicht mehr mit unserer demokratischen Rechtsordnung. So hat Überwachung einen negativen Einfluss auf die freie Meinungsbildung, gefährdet die Pressefreiheit und scheint an manchen Stellen sogar unser Rechtssystem zu untergraben. Da der Bürger nicht weiss, welche Daten über ihn erhoben und wie diese anschliessend ausgewertet werden, fühlt er sich verunsichert, was sich negativ auf das Vertrauensverhältnis zwischen Bürger und Staat auswirken kann; *Kontrolle ist gut, Vertrauen ist besser.*

Mir ist die Verfassung des vierten Kapitels relativ leicht gefallen. Dies mag dadurch begründet sein, dass ich einerseits das Thema der Maturaarbeit in diese Richtung gelenkt habe und dass ich mich andererseits bereits privat mit dieser Problematik beschäftigt habe. Vor gut einem Jahr bin ich der Überwachung noch recht unkritisch gegenüber gestanden. Dies hat sich jedoch schlagartig geändert, als ich den Roman 1984 im vergangenen Sommer gelesen hatte. Nun blickte ich immer kritischer auf die Überwachung an meinem Arbeitsplatz, wo eine regelrechte „Kontrollwut“ vorherrschte (was unter anderem für mich ein Grund war die Arbeitsstelle zu wechseln).

Mein Vorwissen erarbeitete ich mir durch die Lektüre verschiedener Bücher. Auch Zeitschriften haben mir als Quelle gedient, gerade im SPIEGEL ist beinahe wöchentlich über einen Skandal zum Thema Überwachung zu lesen. Auch erhielt ich von Mitgliedern des Chaos Computer Club Ulm einige hilfreiche Hinweise für die Arbeit. Folglich konnte ich mein Kapitel recht frei verfassen, ohne dass ich mich ständig an Bücher hätte „klammern“ müssen.

Sicherheit durch Überwachung?

- Frage: *Sicherheit durch Überwachung?*
- Antwort: Generell kann man sagen, dass eine starke Überwachung zu mehr Sicherheit führen kann. Eine vollständige Sicherheit könnte jedoch höchstens durch eine vollständige Überwachung (also durch ein Orwell-Szenario) erreicht werden. So etwas können wir nicht

wollen! Der Gegenpol zum Polizeistaat stellt die Anarchie dar. Findet gar keine Überwachung mehr statt, so können wir nicht mehr damit rechnen, dass unsere Gesetze auch angewendet werden. Dorthin sollte die Reise ebenfalls nicht gehen. Es gilt also abzuwägen, in welchen Fällen die Überwachung sinnvoll ist und in welchen Fällen wir besser darauf verzichten. Wer die ganze Problematik mit einfachen Parolen (*„Überwachung: Ja – ich habe schliesslich gar nichts zu verbergen“* oder: *„Datenschutz ist Täterschutz“*) herunterzuspielen versucht, dem mangelt es an politischem Feingefühl. Ohne Sicherheit ist keine Freiheit möglich, ohne Freiheit ist unser Leben jedoch nicht mehr lebenswert. Es geht also darum, die Balance zu halten. Die Diskussion um die Überwachung ist ungefähr so alt wie unsere Zivilisation und wird uns wohl noch bis ans Ende unserer Tage beschäftigen.

Wir möchten diese Arbeit gerne mit einem Zitat beschliessen:

„Wer die Freiheit aufgibt um Sicherheit zu gewinnen, der wird am Ende beides verlieren.“

Benjamin Franklin (1706-1790), einer der Gründerväter der Vereinigten Staaten von Amerika

Literatur- und Quellenangaben

Sachbücher

- Ström, Pär: *Die Überwachungsmafia*. Hanser Verlag 2005, 1. Auflage, ISBN 3-446-22980-9
- Schaar, Peter: *Das Ende der Privatsphäre*. C. Bertelsmann Verlag 2007, 1. Auflage, ISBN 978-3-570-00993-2
- Gaycken, Sandro und Kurz, Constanze: *1984.exe: Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien*. transcript Verlag 2008, 1. Auflage, ISBN 3-89942-766-1

Romane

- Orwell, George: *1984*. Ullstein Verlag 2003, 30. Auflage, ISBN 978-3-548-23410-6
- Huxley, Aldous: *Brave New World*. Vintage Verlag 2004, ISBN 978-0-099-47746-4
- Bradbury, Ray: *Fahrenheit 451*. Diogenes Verlag 2008, ISBN 978-3-257-20862-7
- Samjatin, Jewgenij: *Wir*. Kiepenheuer & Witsch Verlag 1984, ISBN 3-462-01607-5

Internet

- Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB
  - http://www.edoeb.admin.ch/
  - http://www.admin.ch
- DER SPIEGEL Online
  - http://www.spiegel.de/
- Chaos Computer Club Deutschland
  - http://www.ccc.de/
- Chaos Computer Club Ulm
  - http://ulm.ccc.de/
- Neue Zürcher Zeitung Online
  - http://www.nzz.ch/
- Wikipedia
  - http://wikipedia.de/
- Heise
  - http://heise.de/
- Dokumentation „Alltag Überwachung“
  - http://video.google.com/videoplay?docid=-3124200616466196 27&hl=en

Bildnachweis

- Das Titelbild zeigt zwei Überwachungskameras, das Symbol für Überwachung schlechtin. Gefunden wurde es auf dem Online-Shop eines Elektronik-Versandhauses. Somit ist nicht nur das Bild an sich, sondern auch dessen Quelle symbolisch zu betrachten. Das Versandhaus ELV vertreibt unter anderem Überwachungskameras ab einem Preis von rund 90 €. Geworben wird mit Bezeichnungen wie z.B. „Professionelle Überwachungstechnik zum Einsteigerpreis“. Somit haben nun auch Privatpersonen die Gelegenheit, ihr Eigenheim und die angrenzende Umgebung zu überwachen.
  - Quelle: http://www.elv.de/
- Die anderen Abbildungen wurden zumeist der freien Internet-Enzyklopädie *Wikipedia* (bzw. der freien Mediensammlung *Wikimedia Commons*[28]) entnommen. Diese Abbildungen sind jeweils so lizenziert, dass sie für die Verwendung in einer solchen Arbeit unproblematisch sind.

Abbildungsverzeichnis

28 http://commons.wikimedia.org/wiki/Main_Page